Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ（Cisco IOS XE Gibraltar 16.10.x）ソフトウェア コンフィギュレーション ガイド

初版：2018 年 11 月 20 日

最終更新：2019 年 3 月 14 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

はじめに

表記法

このマニュアルでは、以下の表記法を使用しています。

表記法	説明
^ または Ctrl	^ 記号と Ctrl は両方ともキーボードの Control（Ctrl）キーを表します。たとえば、^D または Ctrl+D というキーの組み合わせは、Ctrl キーを押しながら D キーを押すことを意味します（ここではキーを大文字で表記していますが、小文字で入力してもかまいません）。
太字	コマンド、キーワード、およびユーザーが入力するテキストは**太字**で記載されます。
イタリック フォント	文書のタイトル、新規用語、強調する用語、およびユーザが値を指定する引数は、イタリック体で示しています。
`Courier` フォント	システムが表示する端末セッションおよび情報は、`courier` フォントで示しています。
`太字の courier` フォント	**`太字の Courier`** フォントは、ユーザが入力しなければならないテキストを示します。
[x]	角カッコの中の要素は、省略可能です。
...	構文要素の後の省略記号（3 つの連続する太字ではないピリオドでスペースを含まない）は、その要素を繰り返すことができることを示します。
|	パイプと呼ばれる縦棒は、一連のキーワードまたは引数の選択肢であることを示します。

表記法	説明
[x | y]	どれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
{x | y}	どれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システムプロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

読者への警告の表記法

このマニュアルでは、読者への警告に次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

ヒント 「問題解決に役立つ情報」です。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイント アドバイス 時間を節約する方法です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 安全上の重要な注意事項

この警告マークは「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。ステートメント 1071

これらの注意事項を保存しておいてください

関連資料

（注） deviceをインストールまたはアップグレードする前に、deviceのリリースノートを参照してください。

- 次の URL にある Cisco Catalyst 9800-40 ワイヤレス コントローラのマニュアル：

  http://www.cisco.com/go/c9800
- 次の URL にある Cisco Catalyst 9800-80 ワイヤレス コントローラのマニュアル：

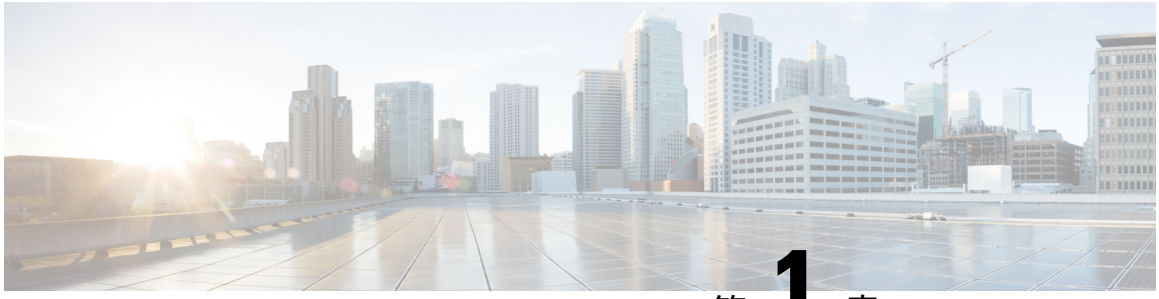
  http://www.cisco.com/go/c9800

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカルサポート、その他の有用な情報について、毎月更新される『What's New in Cisco Product Documentation』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/c/en/us/td/docs/general/whatsnew/whatsnew.html

『What's New in Cisco Product Documentation』はRSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。



第 1 章

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの概要

Cisco Catalyst® 9800 シリーズ ワイヤレス コントローラは、インテントベースのネットワーキング向けに設計された次世代ワイヤレス コントローラです。Catalyst 9800 シリーズ コントローラは IOS XE ベースであり、Aironet の優れた RF 性能と IOS XE のインテントベースのネットワーキング機能を統合して、進化と成長を続ける組織にクラス最高水準のワイヤレス エクスペリエンスを生み出します。

コントローラは、物理および仮想（プライベートおよびパブリック クラウド）フォーム ファクタで展開可能であり、Cisco DNA Center、Netconf/YANG、Cisco Prime Infrastructure、Web ベース GUI、または CLI を使用して管理できます。

Catalyst 9800 シリーズ ワイヤレス コントローラは、次のように、さまざまなフォーム ファクタに対応しており、展開オプションに合わせて選択できます。

- Catalyst 9800 シリーズ ワイヤレス コントローラ アプライアンス
- クラウド向け Catalyst 9800 シリーズ ワイヤレス コントローラ
- スイッチ向け Cisco Catalyst 9800 組み込み型ワイヤレス

設定データ モデルは、再利用可能性、簡略化されたプロビジョニング、柔軟性とモジュール化の向上を基盤とし、拡張に応じたネットワークの管理を支援し、動的に変化し続けるビジネスと IT の要件の管理を簡略にします。このモデルは、マップ アクセス ポイント（AP）のモデルを 3 種類のタグに提供します。クライアントと AP では、タグ内に含まれているプロファイルから設定が導出されます。

新しい設定モデルの要素

タグ

タグのプロパティは、タグに関連付けられているポリシーのプロパティによって定義されます。プロパティはさらに、関連付けられているクライアントまたは AP によって継承されます。タグにはさまざまなタイプがあり、それぞれが異なるプロファイルに関連付けられています。タグにはすべて、システムのブートアップ時に作成されたデフォルトが備わっています。

プロファイル

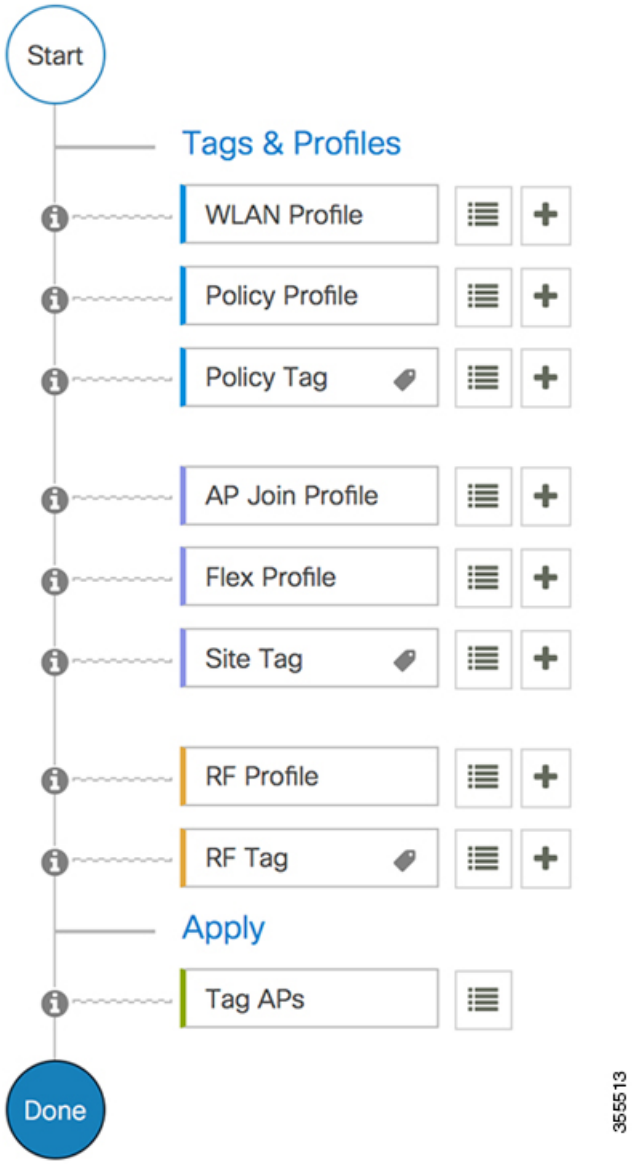
プロファイルは、AP に関連付けられているクライアントまたは AP 自身に適用される属性のセットを表します。プロファイルは、タグ全体で使用できる再利用可能なエンティティです。

設定ワークフロー

次の一連のステップで、設定の論理的順序を定義します。WLANプロファイル以外のすべてのプロファイルとタグにはデフォルトのオブジェクトが割り当てられています。

1. 次のプロファイルを作成します。
   - WLAN
   - ポリシー
   - サイト
   - RF
2. 次のタグを作成します。
   - ポリシー
   - サイト
   - RF
3. タグを AP に関連付けます。

図 *1* : 設定ワークフロー



初期設定

コントローラの設定

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの初期設定ウィザードは簡素化されていて、コントローラ用のインストールおよび設定インターフェイスとしてすぐに利用できます。ここでは、コントローラを小規模から大規模までのあらゆるネットワーク ワイヤレス環境で動作するようにセットアップする手順について説明します。このような環境では、アクセス ポイ

ントをシンプルなソリューションとしてまとめることにより、社員ワイヤレス アクセスやゲスト ワイヤレス アクセスなどのさまざまなサービスをネットワーク上で提供できます。

GUI を使用したコントローラの設定

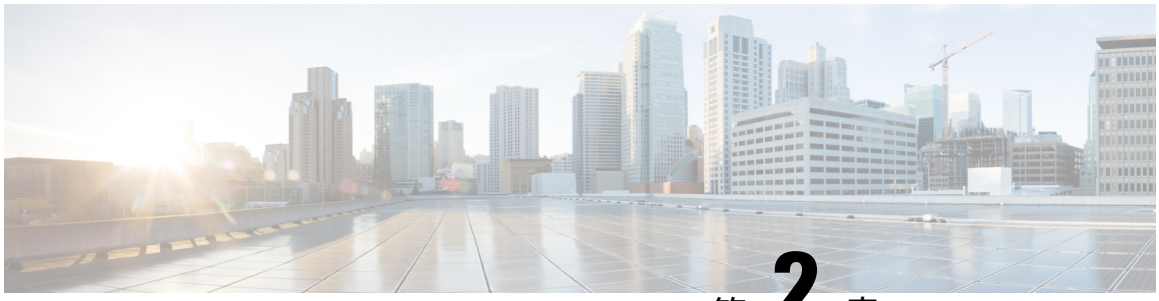
GUI を使用してコントローラを設定するには、『Cisco Catalyst 9800 Wireless Controller for Cloud Install Guide』の「プライベート/パブリック クラウド用デイゼロ WebUI ウィザード」の項を参照してください。

CLI を使用したコントローラの設定

CLI を使用してコントローラを設定するには、『Cisco Catalyst 9800 Wireless Controller for Cloud Install Guide』の「設定ダイアログ」の項を参照してください。

第 I 部

システム設定



第 2 章

システム設定

新しい設定モデルについて

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ は、さまざまなタグ（rf タグ、ポリシー タグ、サイトタグ）を使用して、ワイヤレス コントローラの設定を簡素化します。アクセス ポイントでは、タグ内に含まれているプロファイルから設定が導出されます。

プロファイルは、特定のターゲットに適用される機能固有の属性とパラメータの集まりです。設定のターゲットとなるのは、AP、無線、および WLAN です。Rf タグには無線プロファイルが、ポリシータグには flex-profile と ap-join-profile が、ワイヤレスタグには WLAN プロファイルとポリシー プロファイルが、それぞれ含まれています。

新しい設定モデル（flexconnectモード）は、たとえば小売店舗やキャンパスなど、WLANが同じである地理的に分散したサイトを中央のコントローラで管理するのに役に立ちます。ローカルの展開またはトポロジに基づいてネットワークと無線のプロファイルに多少の変更が生じるだけです。

ポリシー タグ

ポリシー タグは、WLANプロファイルからポリシー プロファイルへのマッピングを構成します。WLANプロファイルは、WLANの無線特性を定義します。ポリシー プロファイルは、クライアントのネットワーク ポリシーとスイッチング ポリシーを定義します（APポリシーも構成する Quality of Service（QoS）は除きます）。

ポリシー タグにはWLANポリシー プロファイルのマップが含まれています。そのようなエントリはポリシー タグごとに16個あります。マップ エントリの変更は、WLANプロファイルとポリシー プロファイルのステータスに基づいて影響を受けます。たとえば、マップ（WLAN1およびPolicy1）がポリシー タグに追加された場合、WLANプロファイルとポリシー プロファイルの両方が有効になっていると、その定義がポリシー タグを使用してAPにプッシュされます。ただし、これらのいずれかが無効状態になっている場合には、定義はAPにプッシュされません。同様に、WLANプロファイルがすでにAPによってブロードキャストされている場合は、ポリシー タグでコマンドの no 形式を使用して削除できます。

サイト タグ

サイト タグはサイトのプロパティを定義するもので、flex プロファイルと AP join プロファイルが含まれています。対応する flex またはリモート サイトに固有の属性は、flex プロファイルの一部となります。flexプロファイルとは別に、サイト タグは物理サイトに固有の属性も構成します（そのため、再利用可能なエンティティであるプロファイルの一部にすることはできません）。たとえば、効率的なアップグレードのためのマスター AP のリストは、flex プロファイルの一部ではなくサイト タグの一部になります。

flexプロファイル名またはAPプロファイル名がサイト タグで変更された場合、APは、Datagram Transport Layer Security（DTLS）セッションを切断することによってコントローラへの再参加を強制されます。サイト タグが作成されると、AP プロファイルと flex プロファイルはデフォルト値（default-ap-profile と default-flex-profile）に設定されます。

RF タグ

RF タグには IEEE 802.11a および IEEE 802.11b の RF プロファイルが含まれています。デフォルトの RF タグにはグローバル設定が含まれています。どちらのプロファイルにも、それぞれの無線についてグローバル RF プロファイルの同じデフォルト値が含まれています。

プロファイル

プロファイルは、特定のターゲットに適用される機能固有の属性とパラメータの集まりです。設定のターゲットとなるのは、AP、無線、およびWLANです。プロファイルは、タグ全体で使用できる再利用可能なエンティティです。プロファイル（タグで使用されます）は、APまたはそれに関連付けられているクライアントのプロパティを定義します。

WLAN プロファイル

WLAN プロファイルは、同じまたは異なるサービスセット識別子（SSID）で設定されます。SSIDは、コントローラがアクセスするための特定の無線ネットワークを識別します。同じSSIDで WLAN を作成すると、同じ無線 LAN 内で異なるレイヤ 2 セキュリティ ポリシーを割り当てることができます。

同じ SSID を持つ WLAN を区別するには、各 WLAN に対して一意のプロファイル名を作成します。同じSSIDを持つWLANには、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントがWLANを選択できるように、一意のレイヤ2セキュリティポリシーが設定されている必要があります。スイッチング ポリシーとネットワーク ポリシーは WLAN 定義の一部ではありません。

ポリシー プロファイル

ポリシー プロファイルは、広義にはネットワーク ポリシーとスイッチング ポリシーで構成されます。ポリシー プロファイルはタグ全体にわたって再利用可能なエンティティです。AP またはコントローラに適用されるクライアントのポリシーとなっているものはすべて、ポリシープロファイルに移動されます。たとえば、VLAN、ACL、QoS、セッション タイムアウト、アイドル タイムアウト、AVC プロファイル、bonjour プロファイル、ローカル プロファイリング、デバイス分類、BSSIDQoSなどが該当します。ただし、WLANのワイヤレス関連のセキュリティ属性と機能はすべて、WLAN プロファイルの配下にグループ化されます。

flex プロファイル

flex プロファイルには、flex グループの一部となっている属性が含まれています。ただし、ポリシー属性はポリシープロファイルとともにグループ化されます。flex プロファイルにはリモート サイト固有のパラメータも含まれています。たとえば、EAP プロファイル（APがローカルRADIUSサーバ情報の認証サーバとして機能する場合に使用可能）、VLANとACLのマッピング、VLAN 名と ID のマッピングなどです。

AP join プロファイル

デフォルトの AP join プロファイルの値には、グローバル AP パラメータと AP グループ パラメータが設定されます。AP join プロファイルには、CAPWAP、IPv4 および IPv6、UDP Lite、ハイ アベイラビリティ、再送信設定パラメータ、グローバル AP フェールオーバー、HyperLocation 設定パラメータ、Telnet および SSH、11u パラメータなどのパラメータが含まれています。

（注） Telnet は次の Cisco AP モデルではサポートされていません。1542D、1542I、1562D、1562E、1562I、1562PS、1800S、1800T、1810T、1810W、1815M、1815STAR、1815TSN、1815T、1815T、1815W、1832I、1840I、1852E、1852I、2802E、2802I、2802H、3700C、3800、3802E、3802I、3802P、4800、9115AXI、9115AXE、9117I、APVIRTUAL、9120AXE、および9120AXI。

RF プロファイル

RF プロファイルには、AP の共通の無線設定が含まれています。RF プロファイルは、AP グループに属するすべての AP に適用され、そのグループ内のすべての AP に同じプロファイルが設定されます。

AP の静的な関連付け

AP を静的に設定できるのは、ポリシータグ、サイト タグ、および RF タグを使用した場合のみです。AP はイーサネット MAC アドレスによって識別され、AP およびタグへの関連付けは設定としてコントローラに保存されます。

AP タグの変更

AP タグを変更すると、DTLS 接続がリセットされ、AP が強制的にコントローラに再参加します。設定でタグが 1 つだけ指定されている場合は、他のタイプにデフォルト タグが使用されます。たとえば、ポリシー タグのみが指定されている場合は、サイト タグと RF タグに対して default-site-tag と default-rf-tag が使用されます。

ワイヤレス プロファイル ポリシーの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞を選択します。

ステップ 2 [Policy Profile] ページで、[Add] をクリックします。

ステップ 3 [Add Policy Profile] ウィンドウの [General] タブで、ポリシー プロファイルの名前と説明を入力します。

ステップ 4 ポリシー プロファイルを有効にするには、[Status] を [Enabled] に設定します。

ステップ 5 スライダを使用して、[Passive Client] と [Encrypted Traffic Analytics] を有効または無効にします。

ステップ 6 [CTS Policy] セクションで、次について適切なステータスを選択します。

- [Inline Tagging]：コントローラまたはアクセス ポイントが送信元 SGT を認識するために使用するトランスポート メカニズム。
- [SGACL Enforcement]

ステップ 7 デフォルトの **SGT** を指定します。有効な範囲は 2 ～ 65519 です。

ステップ 8 [WLAN Switching Policy] セクションで、必要に応じて次を選択します。

- [Central Switching]
- [Central Authentication]
- [Central DHCP]

- [Central Association Enable]
- [Flex NAT/PAT]

ステップ 9 [Save & Apply to Device] をクリックします。

ワイヤレス プロファイル ポリシーの設定（CLI）

ワイヤレス プロファイル ポリシーを設定するには、次の手順に従います。

（注） クライアントが古いコントローラから新しいコントローラ（Prime Infrastructure により管理されている）に移動すると、IP アドレスが ARP またはデータ グリーニングによって学習されている場合は、クライアントの古いIPアドレスが保持されます。このシナリオを回避するには、ポリシー プロファイルで **ipv4 dhcp required** コマンドを有効にします。そうしない場合は、24 時間後にならないと IP アドレスが更新されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy rr-xyz-policy-1`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**idle-timeout** *timeout* 例： `Device(config-wireless-policy)# idle-timeout 1000`	（任意）アイドル タイムアウト時間を秒単位で設定します。
ステップ 4	**vlan** *vlan-id* 例： `Device(config-wireless-policy)# vlan 24`	VLAN 名または VLAN ID を設定します。
ステップ 5	**accounting-list** *list-name* 例： `Device(config-wireless-policy)# accounting-list user1-list`	IEEE 802.1x のアカウンティング リストを設定します。

	コマンドまたはアクション	目的
ステップ 6	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**show wireless profile policy summary** 例： `Device# show wireless profile policy summary`	設定されたポリシー プロファイルを表示します。 （注） （任意）ポリシー プロファイルに関する詳細情報を表示するには、**show wireless profile policy detailed** *policy-profile-name* コマンドを使用します。

flex プロファイルの設定

Flex プロファイルを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex rr-xyz-flex-profile`	RF プロファイルを設定し、RF プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**description** 例： `Device(config-wireless-flex-profile)# description xyz-default-flex-profile`	（任意）RF プロファイルのデフォルト パラメータを有効にします。
ステップ 4	**arp-caching** 例： `Device(config-wireless-flex-profile)# arp-caching`	（任意）ARP キャッシングを有効にします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-wireless-flex-profile)# end`	設定を保存し、コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**show wireless profile flex summary** 例： `Device# show wireless profile flex summary`	（任意）flex プロファイルパラメータを表示します。 （注） flex プロファイルに関する詳細なパラメータを表示するには、**show wireless profile flex detailed** *flex-profile-name* コマンドを使用します。

AP プロファイルの設定（GUI）

始める前に

デフォルトの AP join プロファイルの値には、グローバル AP パラメータと AP グループ パラメータが設定されます。AP join プロファイルには、CAPWAP IPv4/IPv6、UDP Lite、ハイ アベイラビリティ、再送信設定パラメータ、グローバル AP フェールオーバー、HyperLocation 設定パラメータ、Telnet/SSH、11u パラメータなどのパラメータが含まれています。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。

ステップ 2 [AP Join Profile] ページで、[Add] をクリックします。

[Add AP Join Profile] ページが表示されます。

ステップ 3 [General] タブで、AP join プロファイルの名前と説明を入力します。

ステップ 4 AP を簡単に探せるように、デバイスに接続されているすべての AP の LED 状態を点滅に設定するには、[LED State] チェックボックスをオンにします。

ステップ 5 [Client] タブの [Statistics Timer] セクションに、AP が自身の 802.11 統計情報をコントローラに送信する時間を秒単位で入力します。

ステップ 6 [TCP MSS Configuration] セクションで、[Adjust MSS Enable] チェックボックスをオンにして、[Adjust MSS] の値を入力します。ルータを通過する一時的なパケットの最大セグメント サイズ（MSS）を入力または更新できます。TCP MSS の調整により、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の最大セグメント サイズ（MSS）を設定できます。

CAPWAP 環境では、Lightweight アクセス ポイントは CAPWAP ディスカバリ メカニズムを使用してデバイスを検知してから、デバイスに CAPWAP join 要求を送信します。デバイスは、アクセス ポイントがデバイスに join することを許可する CAPWAP join 応答をアクセス ポイントに送信します。

アクセス ポイントがデバイスに参加すると、デバイスによってアクセス ポイントの設定、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。

ステップ 7 [CAPWAP] タブでは次の設定が行えます。

- ハイ アベイラビリティ

  すべてのアクセスポイントのプライマリおよびセカンダリ バックアップ コントローラを、プライマリ、セカンダリ、第3、プライマリ バックアップ、セカンダリ バックアップの順序で設定できます（プライマリ、セカンダリ、または第3のコントローラが応答しない場合に使用されます）。また、ハートビート タイマーやディスカバリ要求タイマーなどのさまざまなタイマーを設定できます。コントローラの障害検出時間を短縮するには、高速ハートビート間隔（コントローラとアクセスポイントの間）に設定するタイムアウト値をより小さくします。高速ハートビート タイマーの期限（ハートビート間隔ごとの）を過ぎると、アクセス ポイントは最後のインターバルでコントローラからデータ パケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセスポイントは高速エコー要求をコントローラへ送信します。

a) [High Availability] タブで、[Fast Heartbeat Timeout] フィールドに時間（秒単位）を入力して、すべてのアクセス ポイントのハートビート タイマーを設定します。ハートビート間隔の値を小さく指定すると、デバイスの障害検出にかかる時間が短縮されます。
b) [Heartbeat Timeout] フィールドに時間（秒単位）を入力して、すべてのアクセス ポイントのハートビート タイマーを設定します。ハートビート間隔の値を小さく指定すると、デバイスの障害検出にかかる時間が短縮されます。
c) [Discovery Timeout] フィールドに 1 ～ 10 秒の範囲（両端を含む）の値を入力して、AP ディスカバリ要求タイマーを設定します。
d) [Primary Discovery Timeout] フィールドに 30 ～ 3000 秒の範囲（両端を含む）の値を入力して、アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。
e) [Primed Join Timeout] フィールドに 120 ～ 43200 秒の範囲（両端を含む）の値を入力して、アクセス ポイントのプライマリ join タイムアウトを設定します。
f) [Retransmit Timers Count] フィールドに、AP からデバイスに（またはその逆に）要求を再送信する回数を入力します。有効な範囲は、3 ～ 8 です。
g) [Retransmit Timers Interval] フィールドに、要求の再送信から次の再送信までの時間を入力します。有効な範囲は、2 ～ 5 です。
h) フォールバックを有効にするには、[Enable Fallback] チェックボックスをオンにします。
i) [Primary Controller] の名前と IP アドレスを入力します。
j) [Secondary Controller] の名前と IP アドレスを入力します。
k) [Save & Apply to Device] をクリックします。

- 高度

a) [Advanced] タブで、[Enable VLAN Tagging] チェックボックスをオンにして、VLAN のタグ付けを有効にします。
b) [Enable Data Encryption] チェックボックスをオンにして、データグラム トランスポート層セキュリティ（DTLS）データ暗号化を有効にします。
c) [Enable Jumbo MTU] をオンにして、大きい最大伝送ユニット（MTU）を有効にします。MTU とは、ネットワークが送信できる最大の物理パケット サイズのことで、バイト単位で測定されます。MTU よりも大きなメッセージは送信前に小さなパケットに分割されます。ジャンボ フレームとは、標準のイーサネット フレーム サイズである 1518 バイト（レイヤ 2（L2）ヘッダーと FCS を含む）より大きいフレームのことです。フレーム サイズの定義は IEEE 標準の一部ではないため、ベンダーによって異なります。
d) [Link Latency] ドロップダウン リストを使用して、リンク遅延を選択します。リンク遅延は、AP からコントローラ、およびコントローラから AP における CAPWAP ハートビート パケット（エコー要求および応答）のラウンドトリップ時間をモニタします。
e) [Preferred Mode] ドロップダウン リストからモードを選択します。
f) [Save & Apply to Device] をクリックします。

ステップ 8 [AP] タブでは次の設定が行えます。

- 一般

a) [General] タブで、[Switch Flag] チェックボックスをオンにしてスイッチを有効にします。
b) パワー インジェクタが使用されている場合は、[Power Injector State] チェックボックスをオンにします。パワーインジェクタにより、ローカル電源、インラインパワー対応のマルチポート スイッチ、およびマルチポート電源パッチパネルに代替電源のオプションが提供され、AP の無線 LAN 配置の柔軟性が向上します。
c) [Power Injector Type] ドロップダウン リストで、次のオプションからパワー インジェクタ タイプを選択します。

   - [Installed]：現在接続されているスイッチ ポートの MAC アドレスを AP に調べさせ記憶させる場合に使用します（この選択は、パワーインジェクタが接続されていることを前提としています）。
   - [Override]：最初に MAC アドレスの一致を検証せずに、AP が高電力モードで稼働できるようにします。

d) [Injector Switch MAC] フィールドに、スイッチの MAC アドレスを入力します。
e) 関連する国コードを入力します。特定の運用国を国コードで指定できます（フランスは FR、スペインは ES など）。
f) [EAP Type] ドロップダウン リストから、EAP タイプとして [EAP-FAST]、[EAP-TLS]、または [EAP-PEAP] を選択します。
g) [AP Authorization Type] ドロップダウン リストから、タイプとして [CAPWAP DTLS +] または [CAPWAP DTLS] のいずれかを選択します。
h) [Client Statistics Reporting Interval] セクションに、5 GHz および 2.4 GHz の無線の間隔を秒単位で入力します。
i) 拡張モジュールを有効にするには [Enable] チェックボックスをオンにします。
j) [Profile Name] ドロップダウン リストから、メッシュのプロファイル名を選択します。

k) [Save & Apply to Device] をクリックします。

- HyperLocation：Cisco Hyperlocation は、ワイヤレス クライアントの場所を 1 メートルの精度で追跡できるロケーション ソリューションです。このオプションを選択すると、NTP サーバを除く画面内の他のすべてのフィールドが無効になります。

a) [Hyperlocation] タブで、[Enable Hyperlocation] チェックボックスをオンにします。
b) 低い RSSI を持つパケットを除外するには、[Detection Threshold] の値を入力します。有効な範囲は -100 ～ -50 dBmです。
c) BAR をクライアントに送信する前のスキャン サイクルの数を設定するには、[Trigger Threshold] の値を入力します。有効な範囲は 0 ～ 99 です。
d) トリガー後にスキャン サイクルの値をリセットするには、[Reset Threshold] の値を入力します。有効な範囲は 0 ～ 99 です。
e) [NTP Server] の IP アドレスを入力します。
f) [Save & Apply to Device] をクリックします。

- BLE：AP が Bluetooth Low Energy（BLE）対応の場合はビーコン メッセージを送信できます。ビーコン メッセージは、低電力リンクを介して送信されるデータまたは属性のパケットです。これらの BLE ビーコンは、ヘルス モニタリング、プロキシミティ検出、アセット トラッキング、およびストア内ナビゲーションに頻繁に使用されます。AP ごとに、すべての AP に対してグローバルに設定される BLE ビーコン設定をカスタマイズできます。

a) [BLE] タブで、[Beacon Interval] フィールドに値を入力して、AP が近くにあるデバイスにビーコン アドバタイズメントを送出する頻度を指定します。範囲は 1 ～ 10 です。デフォルトは 1 です。
b) [Advertised Attenuation Level] フィールドに、減衰レベルを入力します。範囲は 40 ～ 100 で、デフォルトは 59 です。
c) [Save & Apply to Device] をクリックします。

- パケット キャプチャ：パケット キャプチャ機能では、ワイヤレス クライアントのトラブルシューティングを行うために AP 上のパケットをキャプチャできます。パケット キャプチャ操作は、指定されたパケット キャプチャ フィルタに基づいて、AP が動作している現在のチャネルの無線ドライバによって、AP 上で実行されます。

a) [Packet Capture] タブで、ドロップダウン リストから [AP Packet Capture Profile] を選択します。
b) または、[+] 記号をクリックして新しいプロファイルを作成することもできます。
c) AP パケット キャプチャ プロファイルの名前および説明を入力します。
d) [Buffer Size] を入力します。
e) [Duration] を入力します。
f) [Truncate Length] の情報を入力します。
g) [Server IP] フィールドに、TFTP サーバの IP アドレスを入力します。
h) [File Path] フィールドに、ディレクトリ パスを入力します。
i) ユーザ名とパスワードの詳細を入力します。
j) [Password Type] ドロップダウン リストから、タイプを選択します。

k) [Packet Classifiers] セクションで、オプションを使用して、キャプチャするパケットを選択または入力します。
l) [Save] をクリックします。
m) [Save & Apply to Device] をクリックします。

ステップ 9 [Management] タブでは次の設定が行えます。

- デバイス

a) [Device] タブで、TFTP サーバの [TFTP Downgrade] セクションの [IPv4/IPv6 Address] を入力します。
b) [Image File Name] フィールドに、ソフトウェア イメージ ファイルの名前を入力します。
c) [Facility Value] ドロップダウン リストから、適切な機能を選択します。
d) ホストの IPv4 または IPv6 アドレスを入力します。
e) 適切な [Log Trap Value] を選択します。
f) 必要に応じて、Telnet か SSH またはその両方の設定を有効にします。
g) 必要に応じて、コア ダンプを有効にします。
h) [Save & Apply to Device] をクリックします。

- ユーザ

a) [User] タブで、ユーザ名とパスワードの詳細を入力します。
b) 適切なパスワード タイプを選択します。
c) [Secret] フィールドに、カスタムのシークレット コードを入力します。
d) 適切なシークレット タイプを選択します。
e) 適切な暗号化タイプを選択します。
f) [Save & Apply to Device] をクリックします。

- クレデンシャル

a) [Credentials] タブで、ローカルのユーザ名とパスワードの詳細を入力します。
b) 適切なローカル パスワード タイプを選択します。
c) 802.1x ユーザ名とパスワードの詳細を入力します。
d) 適切な 802.1x パスワード タイプを選択します。
e) セッションが期限切れになるまでの時間を秒単位で入力します。
f) 必要に応じて、ローカル クレデンシャルや 802.1 x クレデンシャルを有効にします。
g) [Save & Apply to Device] をクリックします。

- CDP インターフェイス

a) [CDP Interface] タブで、必要に応じて CDP の状態を有効にします。
b) グループ NAS ID を入力します。RADIUS サーバがカスタマイズされた認証応答を送信できるように、異なるグループにユーザを分類する認証要求を介して、コントローラによって RADIUS サーバに Network Access Server identifier（NAS-ID）が送信されます。
c) [Save & Apply to Device] をクリックします。

ステップ 10 不正検出を有効にするには、[Rogue AP] タブで [Rogue Detection] チェックボックスをオンにします。

ステップ 11 [Rogue Detection Minimum RSSI] フィールドに、RSSI 値を入力します。

ステップ 12 [Rogue Detection Transient Interval] フィールドに、一時的な間隔の値を入力します。

ステップ 13 [Rogue Detection Report Interval] フィールドに、レポート間隔の値を入力します。

ステップ 14 不正な封じ込めの自動レート選択を有効にするには、[Rogue Containment Automatic Rate Selection] チェックボックスをオンにします。

ステップ 15 [Auto Containment on FlexConnect Standalone] チェックボックスをオンにして、この機能を有効にします。

ステップ 16 [Save & Apply to Device] をクリックします。

AP プロファイルの設定（CLI）

AP プロファイルを設定するには、次の手順に従います。

始める前に

（注） コントローラの AP join プロファイルを変更した場合、NTP サーバの IP は AP にプッシュされません。これは、HyperLocation 機能の時間感度に対応するために AP プロファイル固有の NTP サーバ IP が導入され、HyperLocation の動作ステータスが Up の場合にのみ AP にプッシュされるためです。この動作は、すべての HyperLocation 関連の TLV（トリガーしきい値、リセットしきい値、および検出しきい値）に適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *ap-profile* 例： `Device(config)# ap profile xyz-ap-profile`	AP プロファイルを設定し、AP プロファイル コンフィギュレーション モードを開始します。 （注） 名前付きプロファイルを削除した場合、そのプロファイルに関連付けられていた AP はデフォルト プロファイルに戻らなくなります。

	コマンドまたはアクション	目的
ステップ 3	**description** *ap-profile-name* 例： `Device(config-ap-profile)# description "xyz ap profile"`	AP プロファイルの説明を追加します。
ステップ 4	**cdp** 例： `Device(config-ap-profile)# cdp`	すべての Cisco AP について CDP を有効にします。
ステップ 5	**end** 例： `Device(config-ap-profile)# end`	設定を保存し、コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**show ap profile** *profile-name***summary** 例： `Device# show ap profile xyz-ap-profile summary`	（任意）AP join プロファイルの数を表示します。 （注） AP join プロファイルに関する詳細情報を表示するには、**show ap profile** *profile-name***detailed** コマンドを使用します。

RF プロファイルの設定（GUI）

始める前に

プライマリ コントローラとバックアップ コントローラを設定する前に、AP 参加プロファイルがすでに設定済みであることを確認します。

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[RF]** を選択します。
ステップ 2 [RF Profile] ページで、[Add] をクリックします。
ステップ 3 [General] タブで、RF プロファイルの名前を入力します。
ステップ 4 適切な [Radio Band] を選択します。
ステップ 5 プロファイルを有効にするには、ステータスを [Enable] に設定します。
ステップ 6 RF プロファイルの [Description] を入力します。
ステップ 7 [Save & Apply to Device] をクリックします。

RF プロファイルの設定（CLI）

RF プロファイルを設定するには、次の手順に従います。

始める前に

ワイヤレス RF タグを同時に設定する場合は、ここで作成したものと同じ RF プロファイル名を使用してください。RF プロファイル名に不一致がある場合（たとえば、RF タグに存在しない RF プロファイルが含まれている場合など）、対応する無線は起動しません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz rf-profile** *rf-profile* 例： `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	RF プロファイルを設定し、RF プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**default** 例： `Device(config-rf-profile)# default`	（任意）RF プロファイルのデフォルト パラメータを有効にします。
ステップ 4	**no shutdown** 例： `Device(config-rf-profile)# no shutdown`	デバイスで RF プロファイルを有効にします。
ステップ 5	**end** 例： `Device(config-rf-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ap rf-profile summary** 例： `Device# show ap rf-profile summary`	（任意）使用可能な RF プロファイルのサマリーを表示します。
ステップ 7	**show ap rf-profile name** *rf-profile* **detail** 例： `Device# show ap rf-profile name rfprof24_1 detail`	（任意）特定の RF プロファイルに関する詳細情報を表示します。

サイト タグの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] ＞ > を選択します。
ステップ 2 [Manage Tags] ページで、[Site] タブをクリックします。
ステップ 3 [Add] をクリックして、[Add Site Tag] ウィンドウを表示します。
ステップ 4 サイト タグの名前と説明を入力します。
ステップ 5 サイト タグに付加する必要がある [AP Join Profile] を選択します。
ステップ 6 必要に応じて、必要な [Control Plane Name] を選択します。
ステップ 7 必要に応じて、[Local Site] を有効にします。
ステップ 8 [Save & Apply to Device] をクリックします。

サイト タグの設定（CLI）

サイト タグを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site rr-xyz-site`	サイト タグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**flex-profile** *flex-profile-name* 例： `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	flex プロファイルを設定します。 （注） サイト タグでローカル サイトが設定されている場合、flex プロファイル設定をサイト タグから削除することはできません。

	コマンドまたはアクション	目的
		（注） サイトタグをFlexconnectとして設定するには、**no local-site** コマンドを使用する必要があります。そうしないとflexプロファイル設定が有効になりません。
ステップ4	**description** *site-tag-name* 例： `Device(config-site-tag)# description "default site tag"`	サイトタグの説明を追加します。
ステップ5	**end** 例： `Device(config-site-tag)# end`	設定を保存し、コンフィギュレーションモードを終了して、特権EXECモードに戻ります。
ステップ6	**show wireless tag site summary** 例： `Device# show wireless tag site summary`	（任意）サイトタグの数を表示します。 （注） タグに関する詳細情報を表示するには、**show wireless tag site detailed** *site-tag-name* コマンドを使用します。 （注） サイトタグとポリシータグの両方が設定されていない場合、**show wireless loadbalance tag affinity wncd** *wncd-instance-number* コマンドの出力にはデフォルトタグ（サイトタグ）タイプが表示されます。

ポリシー タグの設定（GUI）

手順

ステップ1 **[Configuration]** > **[Tags & Profiles]** > **[Tags]** > **[Policy]** を選択します。
ステップ2 [Add] をクリックして、[Add Policy Tag] ウィンドウを表示します。
ステップ3 ポリシー タグの名前と説明を入力します。
ステップ4 [Add] をクリックして、WLANとポリシーをマッピングします。

ステップ 5 適切なポリシープロファイルを使用してマッピングするWLANプロファイルを選択し、チェック アイコンをクリックします。

ステップ 6 [Save & Apply to Device] をクリックします。

ポリシー タグの設定（CLI）

ポリシー タグを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag policy** *policy-tag-name* 例： `Device(config-policy-tag)# wireless tag policy rr-xyz-policy-tag`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1`	ポリシー プロファイルを WLAN プロファイルにマッピングします。
ステップ 4	**end** 例： `Device(config-policy-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 5	**show wireless tag policy summary** 例： `Device# show wireless tag policy summary`	（任意）設定済みのポリシー タグを表示します。 （注） ポリシー タグに関する詳細情報を表示するには、**show wireless tag policy detailed** *policy-tag-name* コマンドを使用します。

ワイヤレス RF タグの設定（GUI）

手順

ステップ 1 a) [Configuration] > [Tags & Profiles] > [RF] > > > を選択します。

ステップ 2 [Add] をクリックして、[Add RF Tag] ウィンドウを表示します。

ステップ 3 RF タグの名前と説明を入力します。

ステップ 4 RF タグに関連付けるために必要な [Dot 11a RF Profile] と [Dot 11b RF Profile] を選択します。

ステップ 5 [Save & Apply to Device] をクリックします。

ワイヤレス RF タグの設定（CLI）

ワイヤレス RF タグを設定するには、次の手順に従います。

始める前に

- RF タグでは 2つのプロファイル（IEEE 802.11a および IEEE 802.11b）のみを使用できます。
- AP タグ タスクを設定するときに作成したものと同じ AP タグ名を使用してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag rf** *rf-tag* 例： `Device(config)# wireless tag rf rftag1`	RF タグを作成し、ワイヤレス RF タグ コンフィギュレーション モードを開始します。
ステップ 3	**24ghz-rf-policy** *rf-policy* 例： `Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1`	RF タグに IEEE 802.11b RF ポリシーを付加します。 dot11a ポリシーを設定するには、**5ghz-rf-policy** コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	**description** *policy-description* 例： `Device(config-wireless-rf-tag)# description Test`	RF タグの説明を追加します。
ステップ 5	**end** 例： `Device(config-wireless-rf-tag)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show wireless tag rf summary** 例： `Device# show wireless tag rf summary`	使用可能な RF タグを表示します。
ステップ 7	**show wireless tag rf detailed** *rf-tag* 例： `Device# show wireless tag rf detailed rftag1`	特定の RF タグの詳細情報を表示します。

AP へのポリシー タグとサイト タグの付加（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

[All Access Points] セクションに、ネットワーク上にあるすべての AP の詳細が表示されます。

ステップ 2 AP の設定の詳細を編集するには、その AP の行を選択します。

[Edit AP] ウィンドウが表示されます。

ステップ 3 [General] タブの [Tags] セクションで、[Configuration] > [Tags & Profiles] > [Tags] ページで作成した、該当するポリシー タグ、サイト タグ、および RF タグを指定します。 > >

ステップ 4 [Update & Apply to Device] をクリックします。

AP へのポリシー タグとサイト タグの付加（CLI）

ポリシー タグとサイト タグを AP に付加するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap** *mac-address* 例： `Device(config)# ap F866.F267.7DFB`	Cisco AP を設定し、AP プロファイル コンフィギュレーション モードを開始します。 （注） *mac-address* 有線 mac アドレスである必要があります。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	ポリシー タグを AP にマッピングします。
ステップ 4	**site-tag** *site-tag-name* 例： `Device(config-ap-tag)# site-tag rr-xyz-site`	サイト タグを AP にマッピングします。
ステップ 5	**rf-tag** *rf-tag-name* 例： `Device(config-ap-tag)# rf-tag rf-tag1`	RF タグを関連付けます。
ステップ 6	**end** 例： `Device(config-ap-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**show ap tag summary** 例： `Device# show ap tag summary`	（任意）AP の詳細と AP に関連付けられているタグを表示します。
ステップ 8	**show ap name** <*ap-name*> **tag info** 例： `Device# show ap name ap-name tag info`	（任意）AP 名とタグ情報を表示します。
ステップ 9	**show ap name** <*ap-name*> **tag detail** 例： `Device# show ap name ap-name tag detail`	（任意）AP 名とタグの詳細を表示します。

AP フィルタ

AP フィルタの概要

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの新しい設定モデルでタグが導入され、タグをアクセス ポイント（AP）に関連付けるための複数のソースが作成されました。タグ ソースは、スタティック設定、AP フィルタ エンジン、AP 単位の PNP、またはデフォルトのタグ ソースにすることができます。これに加えて、タグの優先順位も重要な役割を果たします。AP フィルタ機能は、シームレスで直感的な方法でこれらの課題に対処します。

AP フィルタ機能では、設定に基づいて、タグ ソースが正しい優先順位で整理されます。

AP フィルタ機能を無効にすることはできません。ただし、**ap filter-priority** *priority filter-name* コマンドを使用してタグ ソースの相対的な優先順位を設定できます。

タグの優先順位の設定

複数のタグ ソースがあるとネットワーク管理者にとってあいまいになる可能性があります。これに対処するため、タグの優先順位を定義できます。AP がコントローラに参加すると、優先順位に基づいてタグが選択されます。優先順位が設定されていない場合は、デフォルトが使用されます。

タグの優先順位を設定するには、次の手順を使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# 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	**ap tag-source-priority** *source-priority* **source {filter | pnp}** **例：** `Device(config)# ap tag-source-priority 2 source pnp`	AP タグ ソースの優先順位を設定します。 （注） AP フィルタの設定は必須ではありません。静的、フィルタ、および PnP については、デフォルトの優先順位があります。
ステップ 3	**end** **例：** `Device(config)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**ap tag-sources revalidate** 例： `Device# ap tag-sources revalidate`	Revalidates AP タグ ソースを再検証します。優先順位は、このコマンドの実行後にのみアクティブになります。 （注） フィルタと PnP の優先順位を変更した場合、それらを評価するには **revalidate** コマンドを実行します。

AP フィルタの作成

AP フィルタは、コントローラで使用されるアクセス コントロール リスト（ACL）に似ており、グローバル レベルで適用されます。AP 名はフィルタとして追加できます。また、必要に応じて他の属性を追加することもできます。フィルタ条件はディスカバリ要求の一部として追加します。

（注） PnP サーバでタグ名を設定できます（flex グループや AP グループと同様）。また、AP はタグ名を、ディスカバリ要求と join 要求の一部として保存し送信します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap filter name** *filter_name* 例： `Device(config)# ap filter filter-1`	AP フィルタを設定します。
ステップ 3	**ap name-regex** *regular-expression* 例： `Device(config-ap-filter)# ap name-regex testany`	正規表現に基づいて AP フィルタを設定します。
ステップ 4	**tag policy** *policy-tag* 例： `Device(config-ap-filter)# tag policy pol-tag1`	このフィルタのポリシー タグを設定します。

	コマンドまたはアクション	目的
ステップ 5	**tag rf** *rf-tag* 例： `Device(config-ap-filter)# tag rf rf-tag1`	このフィルタの RF タグを設定します。
ステップ 6	**tag site** *site-tag* 例： `Device(config-ap-filter)# tag site site1`	このフィルタのサイト タグを設定します。
ステップ 7	**end** 例： `Device(config-ap-filter)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

フィルタの優先順位の設定と更新

フィルタの優先順位を設定および更新するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap filter priority** *priority* **filter-name** *filter-name* 例： `Device(config)# ap filter priority 10 filter-name test1`	AP フィルタの優先順位を設定します。 （注） 優先順位のないフィルタはアクティブではありません。同様に、フィルタを使用せずにフィルタの優先順位を設定することはできません。
ステップ 3	**end** 例： `Device(config-ap)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

AP フィルタの設定の確認

タグ ソースとフィルタ、およびそれらの優先順位を表示するには、次の **show** コマンドを使用します。

タグ ソースの優先順位を表示するには、次のコマンドを使用します。

```
Device# show ap tag sources

Priority Tag source
--------------------------------
0 Static
1 Filter
2 AP
3 Default
```

使用可能なフィルタを表示するには、次のコマンドを使用します。

```
Device# show ap filter all

Filter Name                      regex                                Policy Tag
                RF Tag                           Site Tag
-------------------------------------------------------------------------------------------------
first                            abcd                                 pol-tag1
                rf-tag1                          site-tag1
test1                            testany
                                                 site1
filter1                          testany
```

アクティブなフィルタのリストを表示するには、次のコマンドを使用します。

```
Device# show ap filters active

Priority   Filter Name                      regex                                Policy
 Tag                        RF Tag                           Site Tag

-------------------------------------------------------------------------------------------------
10         test1                            testany
                                                 site1
```

AP タグのソースを表示するには、次のコマンドを使用します。

```
Device# show ap tag summary

Number of APs: 4

AP Name AP Mac Site Tag Name Policy Tag Name RF Tag Name Misconfigured Tag Source
-------------------------------------------------------------------------------------------------
AP002A.1034.CA78 002a.1034.ca78 named-site-tag named-policy-tag named-rf-tag No Filter
AP00A2.891C.2480 00a2.891c.2480 named-site-tag named-policy-tag named-rf-tag No Filter
AP58AC.78DE.9946 58ac.78de.9946 default-site-tag default-policy-tag default-rf-tag No
AP
AP0081.C4F4.1F34 0081.c4f4.1f34 default-site-tag default-policy-tag default-rf-tag No
Default
```

ロケーション設定でのアクセスポイントの設定

ロケーションの設定について

ロケーションの設定時には次の操作を実行できます。

- AP のサイトまたはロケーションを設定する。
- このロケーションのタグ セットを設定する。
- このロケーションに AP を追加する。

どのロケーションも、次のコンポーネントで構成されます。

- 一意のタグのセット。各タイプ（ポリシー、RF、サイト）に 1 つずつ。
- タグに適用されるイーサネット MAC アドレスのセット。

この機能は、既存のタグ解決スキームと連携して機能します。ロケーションは、既存のシステムに対する新しいタグ ソースと見なされます。静的なタグ ソースに対しても同様です。

ロケーションの設定の前提条件

アクセス ポイントを 1 つのロケーションで設定する場合、同じアクセス ポイントを別の場所に設定することはできません。

アクセス ポイントのロケーションの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless Setup]** > **[Basic]** を選択します。
ステップ 2 [Basic Wireless Setup] ページで、[Add] をクリックします。
ステップ 3 [General] タブで、ロケーションの名前と説明を入力します。
ステップ 4 [Location Type] を [Local] または [Flex] のいずれかに設定します。
ステップ 5 スライダを使用して、[Client Density] を [Low]、[Typical]、または [High] に設定します。このプラグインにより、AP の RF 特性が設定されます。
ステップ 6 [Apply] をクリックします。

アクセス ポイントのロケーションの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**ap location name** *location_name* 例： `Device(config)# ap location name location1`	アクセス ポイントのロケーションを設定します。 アクセス ポイントのロケーションを削除するには、このコマンドの **no** 形式を実行します。
ステップ 3	**tag** { **policy** *policy_name*| **rf** *rf_name* | **site** **site_name**} 例： `Device(config-ap-location)# tag policy policy_tag` `Device(config-ap-location)# tag rf rf_tag` `Device(config-ap-location)# tag site site_tag`	ロケーションのタグを設定します。
ステップ 4	**location** *description* 例： `Device(config-ap-location)# location description`	ロケーションに説明を追加します。
ステップ 5	**end** 例： `Device(config-ap-location)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ロケーションへのアクセス ポイントの追加（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless Setup]** > **[Basic]** を選択します。

ステップ 2 [Basic Wireless Setup] ページで、[Add] をクリックし、次を設定します。

- 一般
- 無線ネットワーク
- AP プロビジョニング

ステップ 3 [AP Provisioning] タブの [Add/Select APs] セクションで、AP の MAC アドレスを入力し、右矢印をクリックして、関連付けられているリストに AP を追加します。

ステップ 4 [Available AP List] の検索オプションを使用して、選択した AP リストから AP を選択し、右矢印をクリックして、関連付けられているリストに AP を追加します。

ステップ 5 [Apply] をクリックします。

ロケーションへのアクセス ポイントの追加（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap location name** *location_name* 例： `Device(config)# ap location name location1`	アクセス ポイントのロケーションを設定します。
ステップ 3	**ap-eth-mac** *ap_ethernet_mac* 例： `Device(config-ap-location)# ap-eth-mac 188b.9dbe.6eac`	アクセス ポイントをロケーションに追加します。
ステップ 4	**end** 例： `Device(config-ap-location)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。 （注） AP をロケーションに追加した後、AP が自動的にリセットされて新しい設定が取得される場合があります。

ロケーション設定での SNMP の設定

ロケーションの設定における SNMP の前提条件

- 管理ポートが稼働している必要があります。
- SNMP コマンドをクエリする場合、管理ポートには 10x のネットワーク IP アドレスが必要です。これは、SNMP の **getmany** を発行する IP アドレスが **10.x.x.x** ネットワークにあるためです。

SNMP MIB

SNMP MIB は、論理エンティティと物理エンティティを表す一連の管理対象オブジェクトと、それらの間の関係に関する情報を提供します。

表 *1 : MIB* オブジェクトと注記

MIB オブジェクト	注
cLApLocationName	AP ロケーションの名前を提供します。
cLApLocationPolicyTag	ロケーションに設定されているポリシータグを提供します。
cLApLocationSitetag	ロケーションに設定されているサイト タグを提供します。
cLApLocationRfTag	ロケーションに設定されている RF タグを提供します。
cLAssociatedApsApMac	ロケーションに設定されている AP を提供します。

ロケーション設定の確認

AP ロケーション設定のサマリーを表示するには、次のコマンドを使用します。

```
Device# show ap location summary

Location Name           Description         Policy Tag           RF Tag
Site Tag
-------------------------------------------------------------------------------------------------
first                   first floor         default-policy-tag   default-rf-tag
default-site-tag
second                  second floor        default-policy-tag   default-rf-tag
default-site-tag
```

特定のロケーションについて AP ロケーション設定の詳細を表示するには、次のコマンドを使用します。

```
Device# show ap location details first
Location Name.....................: first
Location description..............: first floor
Policy tag........................: default-policy-tag
Site tag..........................: default-site-tag
RF tag............................: default-rf-tag

Configured list of APs
005b.3400.0af0
005b.3400.0bf0
```

AP タグのサマリーを表示するには、次のコマンドを使用します。

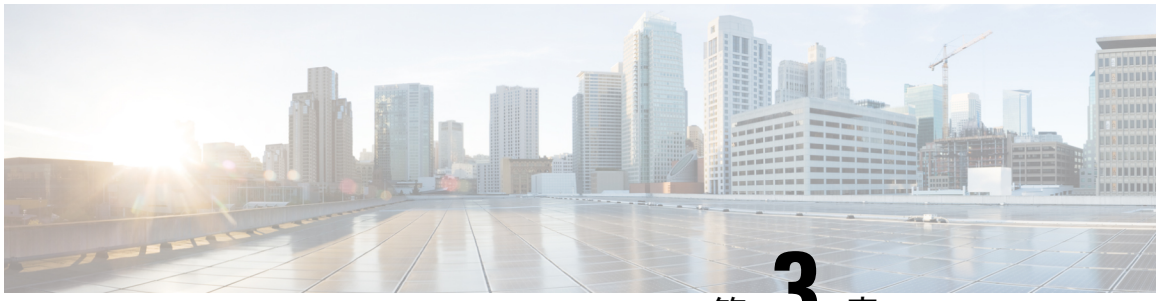
```
Device# show ap tag summary
Number of APs: 4
AP Name       AP Mac           Site Tag Name       Policy Tag Name       RF Tag Name
    Misconfigured   Tag Source
-------------------------------------------------------------------------------------------------
Asim_5-1      005b.3400.02f0   default-site-tag    default-policy-tag    default-rf-tag
     Yes             Filter
Asim_5-2      005b.3400.03f0   default-site-tag    default-policy-tag    default-rf-tag
     No              Default
```

```
Asim_5-9      005b.3400.0af0   default-site-tag    default-policy-tag    default-rf-tag
     No              Location
Asim_5-10     005b.3400.0bf0   default-site-tag    default-policy-tag    default-rf-tag
     No              Location
```

ロケーションの統計情報の確認

AP ロケーションの統計情報を表示するには、次のコマンドを使用します。

```
Device# show ap location stats

Location name    APs joined     Clients joined     Clients on 11a     Clients on 11b

-------------------------------------------------------------------------------------------------
first             2             0                   3                  4

second            0             0                   0                  0
```



第 3 章

RF プロファイル

RF タグ プロファイル

RF プロファイルを使用すると、共通のカバレッジ ゾーンを共有する AP のセットをグループ化し、そのカバレッジ ゾーン内の AP に対する RRM の動作を選択的に変更できます。たとえば、多くのユーザが集まる、または会合するエリアに、大学が高密度の AP を展開する場合があります。この場合は、同一チャネル干渉を管理しながら、セル密度に対処するために、データ レートと電力の両方を操作する必要があります。隣接エリアでは、通常のカバレッジが提供されますが、そのような操作によって高密度エリアのカバレッジが失われることがあります。

RF プロファイルと RF タグを使用すると、異なる環境やカバレッジ ゾーンで動作する AP のセットに対する RF 設定を最適化できます。RF プロファイルは IEEE 802.11 無線用に作成され、RF タグにマッピングされているすべての AP に適用されます。つまり、その RF タグを持つ AP はすべて同じプロファイル設定になります。

AP タグの設定（GUI）

始める前に

プライマリ コントローラとバックアップ コントローラを設定する前に、AP 参加プロファイルがすでに設定済みであることを確認します。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。
ステップ 2 [Manage Tags] ページで、[AP] タブをクリックします。
ステップ 3 [Tag Source] タブで、タグ ソースをドラッグ アンドドロップして優先順位を変更します。
ステップ 4 必要に応じて、[Revalidate Tag Sources on APs] チェックボックスをオンにします。
ステップ 5 [Apply] をクリックします。
ステップ 6 [Static] タブで、[Add] をクリックします。
ステップ 7 [Associate Tags to AP] ウィンドウで、MAC アドレスを入力します。
ステップ 8 適切な [Policy Tag Name]、[Site Tag Name]、[RF Tag Name] を選択します。
ステップ 9 [Save & Apply to Device] をクリックします。
ステップ 10 [Filter] タブで、[Add] をクリックします。
ステップ 11 [Associate Tags to AP] ウィンドウで、ルールと AP 名の正規表現を入力します。
ステップ 12 スライダを使用して、[Active] を有効にします。
ステップ 13 [Priority] を入力します。有効な範囲は 0 ～ 127 です。
ステップ 14 適切な [Policy Tag Name]、[Site Tag Name]、[RF Tag Name] を選択します。
ステップ 15 [Save & Apply to Device] をクリックします。

AP タグの設定（CLI）

AP タグを作成するには、次の手順に従います。

始める前に

ワイヤレス RF タグで作成したものと同じ AP タグを使用していることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap** *mac-address* 例： `Device(config)# ap 188b.9dbe.6eac`	AP タグ コンフィギュレーション モードを開始します。 **重要** AP MAC アドレスのみを使用してください。イーサネット MACアドレスは使用しないでください。

	コマンドまたはアクション	目的
ステップ 3	**rf-tag** *rf-tag* 例： `Device(config-ap-tag)# rf-tag rftag1`	名前付き RF タグを設定し、AP MAC アドレスをタグに追加します。
ステップ 4	**end** 例： `Device(config-ap-tag)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show ap tag summary** 例： `Device# show ap tag summary`	使用可能な AP のタグのサマリーを表示します。

次のタスク

ワイヤレス RF タグを設定します。

RF プロファイルの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [RF] を選択します。 > >

ステップ 2 [RF Profile] ページで、[Add] をクリックし、次を設定します。

- 一般
- 802.11
- RRM
- 高度

ステップ 3 [General] タブで、次の手順を実行します。

a) RF プロファイルの名前および説明を入力します。
b) 適切な無線帯域を選択します。
c) プロファイルを有効にするには、ステータスを [Enable] に設定します。
d) [Save & Apply to Device] をクリックします。

ステップ 4 [802.11] タブで、次の手順を実行します。

a) 必要な動作レートを選択します。
b) 対応するチェックボックスをオンにして、必要な [802.11n MCS Rates] を選択します。
c) [Save & Apply to Device] をクリックします。

ステップ 5 [RRM] > [General] タブで、次の手順を実行します。

a) [Interference] フィールドに、外部干渉しきい値を 0 ～ 100 パーセントの範囲で入力します。デフォルトは 10 です。

b) [Clients] フィールドに、クライアントのしきい値を 1 ～ 75 のクライアント数の範囲で入力します。デフォルト値は 12 です。

c) [Noise] フィールドに、外部ノイズしきい値を -127 ～ 0 dBm の範囲で入力します。デフォルト値は -70 です。

d) [Utilization] フィールドに、RF 使用率のしきい値を 0 ～ 100% の範囲で入力します。デフォルトは 80 です。

ステップ 6 [RRM] > [Coverage] タブで、次の手順を実行します。

a) [Minimum Client Level] フィールドに、クライアントレベルを入力します。

b) [Data RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ～ -90 dBm で、デフォルト値は -80 dBm です。

c) [Voice RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ～ -90 dBm で、デフォルト値は -75 dBm です。

d) [Exception Level] フィールドに、目的のカバレッジしきい値未満で動作している AP の無線上におけるクライアントの最大必要割合を入力します。値の範囲は 0 ～ 100% で、デフォルト値は 25% です。

ステップ 7 [RRM] > [TPC] タブで、次の手順を実行します。

a) [Maximum Power level] フィールドに、この無線での電力レベルの割り当てを入力します。最大送信電力を設定すると、RRM では、デバイスに接続されているすべてのアクセス ポイントはこの送信電力レベルを上回ることはできません（電力が RRM TPC で設定されているかカバレッジ ホールの検出で設定されているかは関係ありません）。

b) [Minimum Power level] フィールドに、この無線での最小電力レベルの割り当てを入力します。

c) [Power Threshold V1] フィールドに、アクセス ポイントのパワーを減らすかどうか判断する際に RRM で使用する切断信号レベルを入力します。

ステップ 8 [RRM] > [DCA] タブで、次の手順を実行します。

a) [Avoid Foreign AP Interference] チェックボックスをオンにすると、コントローラの RRM アルゴリズムで、Lightweight アクセス ポイントにチャネルを割り当てるときに、外部アクセス ポイント（無線ネットワークに含まれないもの）からの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、オフにします。たとえば RRM では、外部アクセス ポイントに近いチャネルをアクセス ポイントが回避するようにチャネル割り当てを調整できます。デフォルト値はオンです。

b) 適切なチャネル幅を選択します。

c) [DCA Channels] セクションの [DCA Channel] フィールドに、現在選択されているチャネルが表示されます。チャネルを選択するには、該当するチェックボックスをオンにします。802.11a/n/ac 帯域の拡張 UNII-2 チャネル（100、104、108、112、116、132、136、および 140）は、チャネル リストには表示されません。チャネル リストにこれらのチャネルを含めるには、[Extended UNII-2 Channels] チェックボックスをオンにします。

d) [Save & Apply to Device] をクリックします。

ステップ 9 [Advanced] タブで、[High Density Parameters] セクションに次の情報を入力します。

a) [Max Clients] フィールドで、グローバルに許可されるクライアントの最大数を設定します。

b) [Multicast Data Rate] ドロップダウンを使用して、マルチキャスト トラフィックのデータ レートを選択します。

無線のデフォルト データ レートを使用するようにデバイスを設定するには、[auto] を選択します。

c) [Rx SOP Threshold] ドロップダウンを使用して [Receiver Start of Packet Detection Threshold (Rx SOP)] を設定し、AP 無線機がパケットを復調してデコードする Wi-Fi 信号レベルを dBm 単位で決定します。RXSOP のレベルが高いほど、無線機の感度が低くなり、レシーバ セルのサイズが小さくなります。セル サイズを小さくすることで、クライアントは、可能な限り最高のデータ レートを使用して最も近いアクセス ポイントに接続します。無線のデフォルトのしきい値を使用するようにデバイスを設定するには、[auto] を選択します。

ステップ 10 [Client Distribution] セクションで、次を入力します。

- [Load Balancing Window]：1 ～ 20 の値を入力して、ロード バランシング ウィンドウと、最も負荷の低い AP のクライアント アソシエーションの数を指定します。
- [Load Balancing Denial Count]：0 ～ 10 の値を入力して、特定の AP のクライアント アソシエーションが拒否される回数を指定します。

ステップ 11 [High Speed Roam] セクションで、[Mode Enable] チェックボックスをオンにして、モードを有効にします。

ステップ 12 [Neighbor Timeout] フィールドに、ネイバー タイムアウト値を入力します。

ステップ 13 [Client Network Preference] ドロップダウン リストから、クライアント ネットワーク設定を選択します。

ステップ 14 [ATF Configuration] セクションで、スライダを使用して [Status] と [Bridge Client Access] を有効または無効にします。

ステップ 15 [Save & Apply to Device] をクリックします。

RF プロファイルの設定（CLI）

RF プロファイルを設定するには、次の手順に従います。

始める前に

ワイヤレス RF タグを同時に設定する場合は、ここで作成したものと同じ RF プロファイル名を使用してください。RF プロファイル名に不一致がある場合（たとえば、RF タグに存在しない RF プロファイルが含まれている場合など）、対応する無線は起動しません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz rf-profile** *rf-profile* 例： `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	RF プロファイルを設定し、RF プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**default** 例： `Device(config-rf-profile)# default`	（任意）RF プロファイルのデフォルト パラメータを有効にします。
ステップ 4	**no shutdown** 例： `Device(config-rf-profile)# no shutdown`	デバイスで RF プロファイルを有効にします。
ステップ 5	**end** 例： `Device(config-rf-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ap rf-profile summary** 例： `Device# show ap rf-profile summary`	（任意）使用可能な RF プロファイルのサマリーを表示します。
ステップ 7	**show ap rf-profile name** *rf-profile* **detail** 例： `Device# show ap rf-profile name rfprof24_1 detail`	（任意）特定の RF プロファイルに関する詳細情報を表示します。

ワイヤレス RF タグの設定（GUI）

手順

ステップ 1 a) [Configuration] > [Tags & Profiles] > [RF] > > > を選択します。

ステップ 2 [Add] をクリックして、[Add RF Tag] ウィンドウを表示します。

ステップ 3 RF タグの名前と説明を入力します。

ステップ 4 RF タグに関連付けるために必要な [Dot 11a RF Profile] と [Dot 11b RF Profile] を選択します。

ステップ 5 [Save & Apply to Device] をクリックします。

ワイヤレス RF タグの設定（CLI）

ワイヤレス RF タグを設定するには、次の手順に従います。

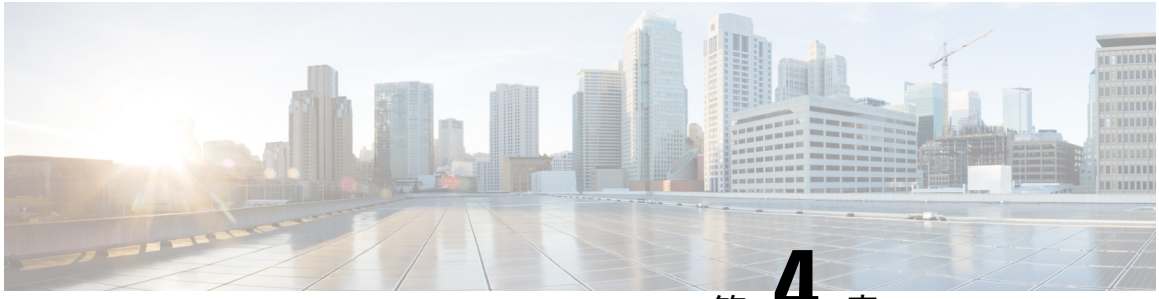
始める前に

- RF タグでは 2つのプロファイル（IEEE 802.11a および IEEE 802.11b）のみを使用できます。
- AP タグ タスクを設定するときに作成したものと同じ AP タグ名を使用してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag rf** *rf-tag* 例： `Device(config)# wireless tag rf rftag1`	RF タグを作成し、ワイヤレス RF タグ コンフィギュレーション モードを開始します。
ステップ 3	**24ghz-rf-policy** *rf-policy* 例： `Device(config-wireless-rf-tag)# 24ghz-rf-policy rfprof24_1`	RF タグに IEEE 802.11b RF ポリシーを付加します。 dot11a ポリシーを設定するには、**5ghz-rf-policy** コマンドを使用します。
ステップ 4	**description** *policy-description* 例： `Device(config-wireless-rf-tag)# description Test`	RF タグの説明を追加します。
ステップ 5	**end** 例： `Device(config-wireless-rf-tag)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show wireless tag rf summary** 例： `Device# show wireless tag rf summary`	使用可能な RF タグを表示します。

	コマンドまたはアクション	目的
ステップ 7	**show wireless tag rf detailed** *rf-tag* 例： `Device# show wireless tag rf detailed rftag1`	特定の RF タグの詳細情報を表示します。



第 4 章

BIOS 保護

コントローラでの BIOS 保護

BIOS 保護を使用すると、Intel ベースのプラットフォームの BIOS フラッシュを保護し、安全に更新することができます。BIOS 保護が使用されていない場合、Intel プラットフォームの BIOS を保存するフラッシュ ユーティリティは書き込み保護されません。そのため、BIOS の更新が適用されると、悪意のあるコードも適用されてしまいます。

デフォルトでは、BIOSイメージが含まれているフラッシュをバンドルし、BIOSフラッシュでの書き込みを可能にする BIOS カプセルを介してのみアップデートを受け入れることによって、BIOS 保護が機能します。

BIOS 保護を使用した BIOS または ROMMON のアップグレード

BIOSまたはROMMONをアップグレードするには、次のようにBIOS保護機能を使用します。

1. ROMMON バイナリと一緒にバンドルされている新しい BIOS イメージ カプセルが、ROMMON アップグレード スクリプトによってシスコ デバイスのメディアに挿入されます。
2. その後、シスコ デバイスは、新しい BIOS/ROMMON のアップグレードが行えるようにリセットされます。
3. リセット時に、元の BIOS によって更新されたカプセルが検出され、更新された BIOS が使用可能かどうかが判定されます。
4. その後、元の BIOS によって BIOS カプセルのデジタル署名が検証されます。署名が有効な場合は、元の BIOS によってフラッシュ ユーティリティから書き込み保護が削除され、

SPI フラッシュが新しい BIOS イメージに更新されます。BIOS カプセルが無効な場合は、SPI フラッシュは更新されません。

5. 新しい BIOS/ROMMON イメージが SPI フラッシュに書き込まれた後、SPI フラッシュの必要な領域が再び書き込み保護されます。
6. カードがリセットされると、更新された BIOS がリブートされます。
7. カプセルが BIOS によって削除されます。

BIOS のアップグレード

手順

BIOS カプセルを更新するには、**upgrade rom-monitor filename** コマンドを使用します。

例：

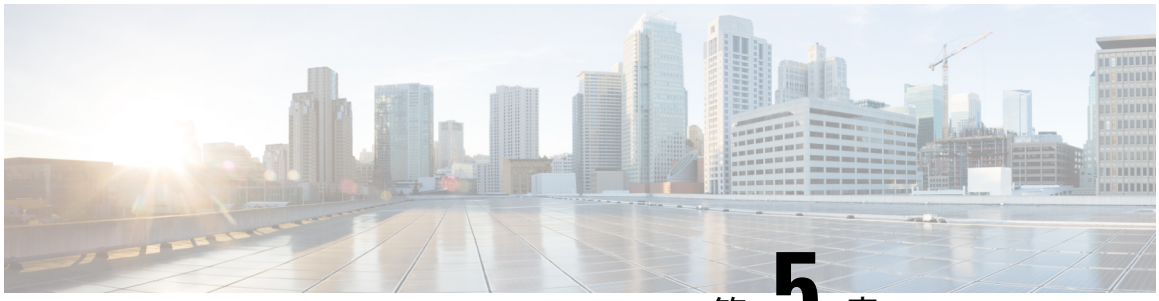
```
upgrade rom-monitor filename bootflash:capsule.pkg <slot>
```

例

次に、BIOS 保護のアップグレードを確認する例を示します。

```
Device# upgrade rom-monitor filename bootflash:qwlc-rommon-capsule-p106.pkg all
Verifying the code signature of the ROMMON package...
Chassis model AIR-CT5540-K9 has a single rom-monitor.

Upgrade rom-monitor

Target copying rom-monitor image file

Secure update of the ROMMON image will occur after a reload.

8388608+0 records in
8388608+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 11.9671 s, 701 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 0.414327 s, 316 kB/s
Copying ROMMON environment
8388608+0 records in
8388608+0 records out
8388608 bytes (8.4 MB, 8.0 MiB) copied, 31.1199 s, 270 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 2.44015 s, 53.7 kB/s
131072+0 records in
131072+0 records out
131072 bytes (131 kB, 128 KiB) copied, 2.43394 s, 53.9 kB/s
ROMMON upgrade complete.
```

```
To make the new ROMMON permanent, you must restart the RP.
Device#reload
```



第 5 章

スマート ライセンシング

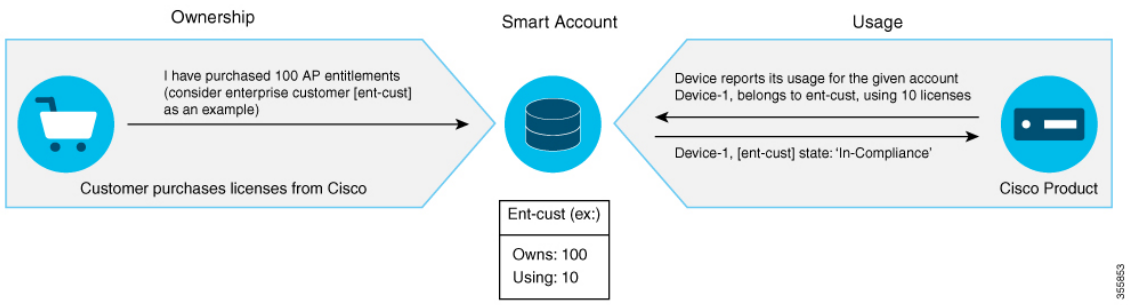
シスコ スマート ライセンシングの情報

このドキュメントでは、シスコ スマート ライセンシング ソフトウェアの設定と動作について説明します。

シスコ スマートライセンシングは、ユーザアカウントにフローティングライセンスを提供するソフトウェアインベントリ管理システムです。

スマートライセンシングには Cisco Smart Software Manager が付属しています。これは、ご使用のすべてのシスコ ソフトウェアライセンスを 1 つの Web サイトで一元管理できる中央のポータルです。

図 *2:* 所有権、スマートアカウント、および使用状況の関係



（注） 前提条件として、Smart Call Home HTTPS サーバを使用して、ご使用のコントローラをサテライト SSM（お客様の敷地内の VM）または CSSM（Cisco Cloud）に登録してください。

製品が CSSM に登録されると、8 時間ごとにスマートアカウントまたはバーチャルアカウントを使用してライセンスの使用状況を表示できるようになります。

アクセスポイントは、次の AIR ライセンスレベルをサポートしています。

- AIR Network Essential（AIR-NE）
- AIR Network Advantage（AIR-NA）
- AIR DNA Essential（AIR-DNA-E）
- AIR DNA Advantage（AIR-DNA-A）

（注） デフォルトモードは AIR-DNA-A です。

（注） コントローラで使用可能なライセンスレベルは AIR-DNA-A と *AIR-DNA-E* です。DNA ライセンスを更新しない場合は、AIR-DNA-A または AIR-DNA-E ライセンスレベルとして設定し、期限切れになった時点で Network Advantage または Network Essentials のライセンスレベルに移行することができます。

スマートライセンシングの予約タイプ

ライセンスの予約とは、ノードロックされたライセンスを予約してコントローラにインストールするためのメカニズムのことです。

ライセンスの予約タイプは次のとおりです。

- Permanent License Reservation（PLR）：すべてのライセンスが予約されます。

- Specified License Reservation（SLR）：特定のライセンスのみが予約されます。期限ライセンスをサポートしています。

コントローラは、スマートライセンシングまたはサービス予約について4つの異なる権限付与の登録またはレポートをサポートしています。接続しているすべての AP において、コントローラの一意の値プロパティを利用するために、Cisco DNA Center ライセンスが必要です。

（注） コントローラは、デフォルトとして AIR DNA-A で起動します。ライセンスレベルを変更した場合は、再起動が必要です。

権限付与レポート

権限付与レポートは、コントローラ上のアクセスポイントの数を Cisco Smart Software Manager（CSSM）に報告するだけのものです。

権限付与レポートは、コントローラ上で設定されている AIR ライセンスレベルに基づきます。

（注） AIR-DNA-E および AIR-DNA-A レベルの場合は、2 種類の権限付与レポートが実行されます。たとえば、コントローラが AP 数として 100 をレポートした場合、権限付与レポートには 100 AIR-NE および 100 AIR-DNA-E が表示されます。同様に、100 AIR-NA および 100 AIR-DNA-A も CSSM に表示されます。

スマートアカウントの作成

手順

	コマンドまたはアクション	目的
ステップ 1	Cisco Software Central の Web ページに移動します。	https://software.cisco.com/# [Cisco Software Central] ページが表示されます。
ステップ 2	[Important News] ポップアップウィンドウで、[Get a Smart Account] をクリックします。	（または） [Administration] 領域の [Request a Smart Account] をクリックします。 手順に従ってスマートアカウントを作成します。 （注） スマートライセンシングを使用するにはスマートアカウントが必要です。

スマートライセンシングの使用

始める前に

スマートライセンシングの使用方法に関する大まかな手順については、次の手順に従ってください。

手順

	コマンドまたはアクション	目的
ステップ 1	デバイスをスマートライセンシング用に設定します。	
ステップ 2	**CSSM** のお客様の **[Smart Account]** > **[Virtual Account]** にログインして、トークンを生成します。	
ステップ 3	デバイスで次のコマンドを実行します。	`Device# license smart register idtoken <token_ID>` （注） *token_ID* は CSSM Web ポータルから取得できます。 CSSM の詳細については、次を参照してください。 https://www.cisco.com/c/en/us/buy/smart-accounts/software-manager-satellite.html

Specified License Reservation（SLR）の使用

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**license smart reservation** 例： `Device(config)# license smart reservation`	コントローラで Specified License Reservation モードを有効にします。
ステップ 3	**license smart reservation request local** 例：	要求コードを生成します。

	コマンドまたはアクション	目的
	`Device(config)# license smart reservation request local`	（注） この要求コードを Cisco Smart Software M ポータルに入力します。 `CB-ZL-AIR-9500C-K9:9J4FVHMBXCO-BjSeU`
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

CSSM での Specified License Reservation の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	CSSM にログインします。	
ステップ 2	CSSM に要求コードを入力します（「Specified License Reservation（SLR）の使用」を参照）。Specified License Reservation（SLR）の使用 （52 ページ）	
ステップ 3	コントローラでアクティブになっているライセンスに従って、必要なライセンスを選択します。	
ステップ 4	次のコマンドを使用して、コントローラで *auth-code* ファイルを生成します。	`Device# conf t` `Device(config)# license smart reservation install file <>` `Device(config)# end`
ステップ 5	次のコマンドを使用して、コントローラの認証ステータスを確認します。	`Device# enable` `Device# show license reservation`

スマート ソフトウェア ライセンシングのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	次のリンクを使用して、Cisco Software Central の Web ページに移動します。	https://software.cisco.com/#

	コマンドまたはアクション	目的
		[Cisco Software Central] ページが表示されます。
ステップ 2	[License] タブで、[Smart Software Licensing] をクリックします。	[Smart Software Licensing] ページが表示されます。
ステップ 3	[Inventory] タブをクリックして、[Virtual Account: Accounting] ページの詳細を表示します。	
ステップ 4	[New Token] をクリックして、製品インスタンスをこのバーチャルアカウントに登録します。	[Create Registration Token] ページが表示されます。
ステップ 5	[Description]フィールドに、ID トークンの説明を入力します。	
ステップ 6	エクスポート制御機能を許可するには、[Allow export-controlled functionality on the products registered with this token] チェックボックスをオンにします。	
ステップ 7	[Create Token] をクリックします。	（注） ワイヤレスコントローラを使用してライセンスを購入することはできません。すべてのライセンスは、アクセスポイントを使用して購入できます。

Smart Call Home レポートの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**call-home reporting contact-email-addr** *email-address* **http-proxy** *proxy-server port-number* 例：	Call Home レポートを有効にします。 • *port-number*：有効な範囲は 1 ～ 65535 です。

	コマンドまたはアクション	目的
	`Device(config)# call-home reporting contact-email-addr sample@cisco.com http-proxy 120.20.2.2 5`	
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。 （注） Smart Call Home の詳細については、次 https://www.cisco.com/c/en/us/td/docs/switc

AIR ライセンスレベルの設定 (GUI)

手順

ステップ 1 [Administration] > [Licensing] の順に選択します。

ステップ 2 [Change Wireless License Level] をクリックします。[Change Wireless License Level] ダイアログボックスが表示されます。

ステップ 3 ドロップダウンを使用してライセンスレベルを選択します。

ステップ 4 [New Level] の値を変更した後、[Save & Reload] または [Save without Reload] をクリックします。[Reload] をクリックしてデバイスをリロードすることもできます。リロードの間、デバイスへのネットワーク接続は失われます。続行する場合は、[Yes] をクリックします。

ステップ 5 更新アイコンをクリックしてデバイスを更新します。

AIR ライセンスレベルの設定 (GUI)

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**license air level {air-network-advantage | air-network-essentials}** 例：	AIR ライセンスレベルを設定します。 • air-network-advantage：AIR Network Advantage ライセンスレベルです。

	コマンドまたはアクション	目的
	Device(config)# **license air level air-network-advantage** Device(config)# **license air level air-network-essentials**	• air-network-essentials：AIR Network Essential ライセンスレベルです。
ステップ 3	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AIR Network Essentials ライセンスレベルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： Device# 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	**license air level network-essentials addon air-dna-essentials** 例： Device(config)# **license air level network-essentials addon air-dna-essentials**	AIR Network Essentials ライセンスレベルを設定します。
ステップ 3	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AIR Network Advantage ライセンスレベルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**license air level air-network-advantage addon air-dna-advantage** 例： `Device(config)# license air level air-network-advantage addon air-dna-advantage`	AIR Network Advantage ライセンスレベルを設定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

スマートライセンシングの設定の確認

スマートライセンシングのステータスとライセンスの使用状況を確認するには、次のコマンドを使用します。

```
Device# show license all
Smart Licensing Status
======================
Smart Licensing is ENABLED

Registration:
  Status: UNREGISTERED
  Export-Controlled Functionality: Not Allowed

License Authorization:
  Status: EVAL MODE
  Evaluation Period Remaining: 73 days, 1 hours, 33 minutes, 8 seconds

Utility:
Status: DISABLED

Data Privacy:
  Sending Hostname: yes
    Callhome hostname privacy: DISABLED
    Smart Licensing hostname privacy: DISABLED
  Version privacy: DISABLED

Transport:
  Type: Callhome

License Usage
==============
(AIR_network_essential):
  Description:
  Count: 1
  Version: 1.0
  Status: EVAL MODE

Product Information
===================
UDI: PID:L-AIR-9500C-K9,SN:9J4FVHMBXCO
```

```
Agent Version
=============
Smart Agent for Licensing: 4.5.3_rel/43
Component Versions: SA:(1_3_dev)1.0.15, SI:(dev22)1.2.1, CH:(rel5)1.0.3, PK:(dev18)1.0.3

Reservation Info
================
License reservation: DISABLED
```

スマートライセンシングのステータスを確認するには、次のコマンドを使用します。

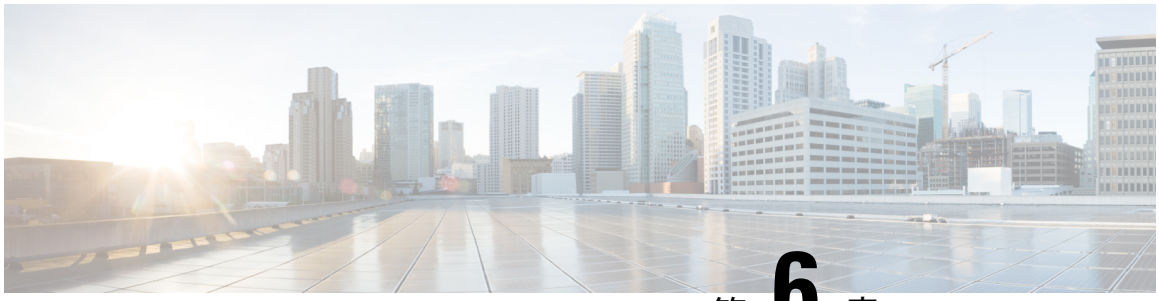
```
Device# show license status
Tue Oct 02 07:34:36.023 IST
Smart Licensing is ENABLED
  Initial Registration: SUCCEEDED on Mon Oct 01 2018 21:55:46 IST
  Last Renewal Attempt: None
  Registration Expires: Sun Dec 29 2018 11:49:40 IST
License Authorization:
  Status: AUTHORIZED on Mon Oct 01 2018 21:55:46 IST
  Last Communication Attempt: SUCCEEDED on Mon Oct 01 2018 21:55:46 IST
  Next Communication Attempt: Thu Nov 02 2018 21:56:10 IST
    Communication Deadline: Sun Dec 29 2018 11:49:16 IST
```

AIR ライセンスレベルとスマートライセンシングのステータスを確認するには、次のコマンドを使用します。

```
Device# show version
AIR License Level: AIR DNA Advantage
Next reload AIR license Level: AIR DNA Advantage

Smart Licensing Status: UNREGISTERED/No Licenses in Use
```

第 II 部

Lightweight アクセスポイント



第 6 章

国コード

国番号について

コントローラおよびアクセスポイントは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。アクセスポイント内の無線は、製造時に特定の規制区域に割り当てられています（ヨーロッパの場合にはEなど）。しかし、国番号を使用すると、稼働する特定の国を指定できます（フランスの場合にはFR、スペインの場合にはESなど）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

日本の国番号について

国番号は、各国で合法的に使用できるチャネルを定義します。日本で使用できる国番号は、次のとおりです。

- JP：コントローラに join できるのは、-J 無線のみです。
- J2：コントローラに join できるのは、-P 無線のみです。
- J3：WLC に join できるのは、-U、-P、および -Q（1550/1600/2600/3600 以外）無線ですが、-U の周波数を使用します。
- J4：コントローラに join できるのは、2.4G JPQU および 5G PQU です。

（注） 1550、1600、2600、および 3600 AP には J4 が必要です。

日本の規制区域のアクセスポイントでサポートされているチャネルと電力レベルの一覧については、『Channels and Maximum Power Settings for Cisco Aironet Lightweight Access Points』を参照してください。

国番号の設定の前提条件

- 通常、deviceごとに1つの国番号を設定します。deviceの物理的な場所とそのアクセスポイントが一致しているコードを1つ設定します。deviceごとに最大20個の国番号を設定できます。これによって複数の国がサポートされ、1台のdeviceからさまざまな国にあるアクセスポイントを管理できます。
- multiple-country 機能を使用している場合、同じ RF グループに join する予定のすべてのdeviceは、同じ国のセットを同じ順序で設定する必要があります。
- アクセスポイントは、使用可能なすべての法定周波数を使用できます。ただし、アクセスポイントは関連するドメインでサポートされる周波数に割り当てられます。
- RF グループリーダーに設定されている国リストによって、メンバーが動作するチャネルが決定します。このリストは、RF グループメンバーに設定されている国とは無関係です。
- 日本の規制ドメインにあるdeviceの場合は、最後にdeviceをブートしたときにdeviceで設定した 1 つ以上の日本の国番号（JP、J2、または J3）を持っている必要があります。
- 日本の規制ドメインにあるdeviceの場合は、deviceに join された - J 規制ドメインのアクセスポイントを少なくとも 1 つ持っている必要があります。

Country Code の設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > [Country] の順に選択します。 > > >

ステップ 2 [Country] ページで、アクセスポイントがインストールされている各国のチェックボックスをオンにします。複数のチェックボックスをオンにした場合、RRM チャネルと電力レベルが共通のチャネルと電力レベルに制限されることを記載したメッセージが表示されます。

ステップ 3 [Apply] をクリックします。

国番号の設定方法

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**show wireless country supported** 例： `Device# show wireless country supported`	使用可能なすべての国番号のリストを表示します。
ステップ 3	**configure terminal** 例： `Device# 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 4	**ap dot11 24ghz shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	802.11b/g ネットワークをディセーブルにします。
ステップ 5	**ap dot11 5ghz shutdown** 例： `Device(config)# ap dot11 24ghz shutdown`	802.11a ネットワークをディセーブルにします。
ステップ 6	**ap country** *country_code* 例： `Device(config)# ap country IN`	コントローラに参加しているアクセスポイントが、その AP の国番号と対応する規制ドメインコードと一致するように、コントローラの国番号を設定します。
ステップ 7	**show wireless country configured** 例： `Device# show wireless country configured`	設定されている国を表示します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

	コマンドまたはアクション	目的
ステップ 9	**show wireless country channels** 例： `Device# show wireless country channels`	deviceに設定された国番号の使用可能なチャネルのリストを表示します。 （注） ステップ 6 で複数の国番号を設定した場合にのみ、ステップ 9 ～ 17 を実行します。
ステップ 10	**configure terminal** 例： `Device# 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 11	**no ap dot11 5ghz shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	802.11a ネットワークをイネーブルにします。
ステップ 12	**no ap dot11 24ghz shutdown** 例： `Device(config)# no ap dot11 24ghz shutdown`	802.11b/g ネットワークをイネーブルにします。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 14	**ap name** *cisco-ap* **shutdown** 例： `Device# ap name AP02 shutdown`	アクセスポイントをディセーブルにします。 （注） 国番号を設定しているアクセスポイントのみをディセーブルにすることを確認します。
ステップ 15	**ap name** *cisco-ap* **country** *country_code* 例：	コントローラの国番号リストから、国番号を持つ各アクセスポイントを割り当てます。

	コマンドまたはアクション	目的
	`Device# ap name AP02 country US`	（注） • 選択した国番号が、アクセスポイントの無線のうち少なくとも1つの無線の規制ドメインに適合していることを確認します。 • 国番号を変更する前に、アクセスポイントを無効にします。
ステップ 16	**ap name** *cisco-ap* **no shutdown** 例： `Device# ap name AP02 no shutdown`	アクセスポイントを有効にします。

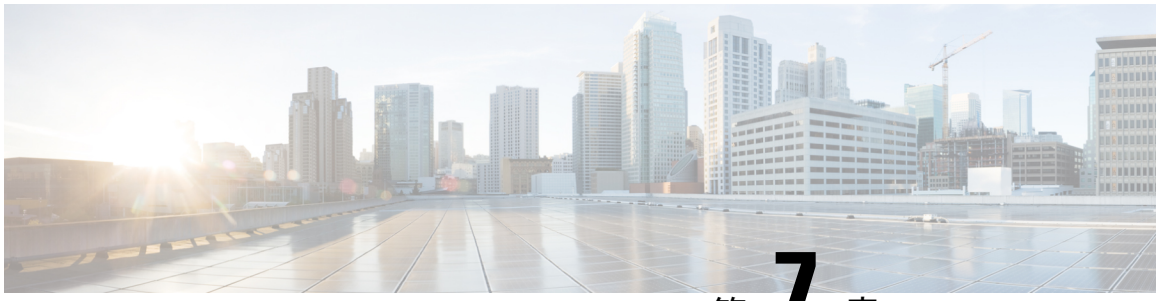
国番号の設定例

国番号のチャネル リストの表示：例

次に、deviceに設定されている国番号に使用可能なチャネルの一覧を表示する例を示します。

```
Device# show wireless country channels

Configured Country.......................: US - United States
KEY: * = Channel is legal in this country and may be configured manually.
     A = Channel is the Auto-RF default in this country.
     . = Channel is not legal in this country.
     C = Channel has been configured for use by Auto-RF.
     x = Channel is available to be configured for use by Auto-RF.
  (-,-) = (indoor, outdoor) regulatory domain allowed by this country.
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11bg         :
Channels         :                  1 1 1 1 1
                  1 2 3 4 5 6 7 8 9 0 1 2 3 4
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US    : A * * * * A * * * * A . . .
Auto-RF          : . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
802.11a          :                        1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
Channels         :3 3 3 4 4 4 4 4 5 5 6 6 0 0 0 1 1 2 2 2 3 3 4 4 5 5 6 6
                  4 6 8 0 2 4 6 8 2 6 0 4 0 4 8 2 6 0 4 8 2 6 0 9 3 7 1 5
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
(-A ,-AB ) US    : . A . A . A . A A A A A * * * * * . . . * * * A A A A*
Auto-RF          : . . . . . . . . . . . . . . . . . . . . . . . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
4.9GHz 802.11a   :
Channels         :                  1 1 1 1 1 1 1 1 1 1 2 2 2 2 2 2 2
                  1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
US (-A ,-AB )    : * * * * * * * * * * * * * * * * * * * A * * * * * A
```

```
Auto-RF          : . . . . . .
-----------------:+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```



第 7 章

モニタモード

モニタモードの概要

RFID タグの監視とロケーション計算を最適化するには、802.11b/g アクセスポイント無線用の 2.4GHz 帯域内で最高 4 つのチャネルでトラッキングの最適化を有効化できます。この機能を使用して、通常、タグが動作するようにプログラムされているチャネル（チャネル 1、6、11 など）のみをスキャンすることができます。

（注） 対応するモードのサイトタグを使用して、AP を特定のモード（センサーモードからローカルモードまたは flex モード）に移動できます。AP がどのモードにもタグ付けされていない場合は、デフォルトのサイトタグで指定されたモードにフォールバックします。

モニタモードの有効化（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [Access Points] ページで、[All Access Points] セクションを展開し、編集する AP の名前をクリックします。

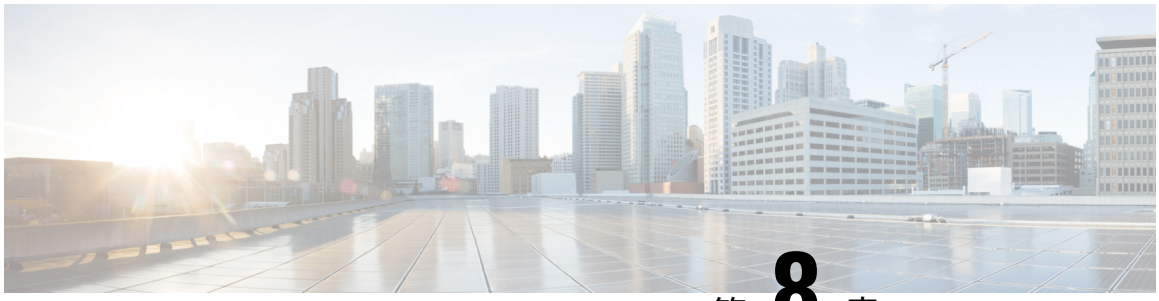
ステップ 3 [Edit AP] ページで、[General] タブをクリックし、[AP Mode] ドロップダウンリストから [Monitor] を選択します。

ステップ 4 [Update & Apply to Device] をクリックします。

モニタモードの有効化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name* **mode monitor** 例： `Device# ap name 3602a mode monitor`	アクセスポイントのモニタモードを有効にします。
ステップ 2	**ap name** *ap-name***monitor tracking-opt** 例： `Device# ap name 3602a monitor tracking-opt`	使用する国でサポートされる動的チャネル割り当て（DCA）チャネルのみをスキャンするようにアクセスポイントを設定します。
ステップ 3	**ap name** *ap-name* **monitor dot11b** [*first-channel second-channel third-channel fourth-channel*] 例： `Device# ap name 3602a monitor dot11b 1 2 3 4`	アクセス ポイントによりスキャンされる特定の 802.11b チャネルを最大 4 つ選択します。 米国では、チャネル変数に 1 ～ 11 の値（両端の値を含む）を割り当てることができます。その他の国ではさらに多くのチャネルがサポートされています。少なくともチャネルを 1 つ割り当てる必要があります。 （注） 使用可能なチャネルを表示するには、**show ap dot11 {24ghz | 5ghz} channel** コマンドを使用します。
ステップ 4	**show ap dot11 {24ghz | 5ghz} monitor-mode summary** 例： `Device# show ap dot11 5ghz monitor-mode summary`	モニタモードですべてのアクセスポイントを表示します。
ステップ 5	**show ap dot11 {24ghz | 5ghz} channel** 例： `Device# show ap dot11 5ghz channel`	次に、802.11a チャネル割り当ての設定と統計情報の例を示します。



第 8 章

センサーモード

センサーモードの概要

このようなワイヤレスネットワークは、IT専門家がいつでも常駐できるとは限らない遠隔地の施設で特に発展していますが、そのような状況の中で、潜在的な接続性の問題について、ユーザが接続性の低下を訴えたり気付いたりする前に迅速に特定して解決できる能力がますます重要になってきています。

こうした問題に対処するため、シスコはワイヤレス サービス アシュアランスと、「センサーモード」と呼ばれる新しいAPモードを導入しました。詳細については、『Cisco Aironet Sensor Deployment Guide』を参照してください。

センサー モードの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name***mode sensor** 例：	アクセス ポイントのセンサー モードを有効にします。

	コマンドまたはアクション	目的
	`Device# ap name AP4001.7A39.2E12 mode sensor`	（注）

	コマンドまたはアクション	目的
		センサーモードの AP は、次の AP 単位の設定をサポートしていません。 • ap name <ap-name> [no] shutdown • ap name <ap-name> dot11 24ghz SI • ap name <ap-name> dot11 24ghz antenna ext-ant-gain <ext-ant-gain-number> • ap name <ap-name> dot11 24ghz antenna selection [external | internal] • ap name <ap-name> dot11 24ghz beamforming • ap name <ap-name> dot11 24ghz channel [<channel-number> | auto] • ap name <ap-name> dot11 24ghz cleanair • ap name <ap-name> dot11 24ghz dot11n antenna [A | B | C | D] • ap name <ap-name> dot11 24ghz shutdown • ap name <ap-name> dot11 24ghz txpower [<transmit-power-level> | auto] • ap name <ap-name> dot11 24ghz slot <slot-number> SI • ap name <ap-name> dot11 24ghz slot <slot-number> antenna ext-ant-gain <ext-ant-gain-number> • ap name <ap-name> dot11 24ghz slot <slot-number> antenna selection [external | internal] • ap name <ap-name> dot11 24ghz slot <slot-number>

	コマンドまたはアクション	目的
		beamforming • ap name < ap name > dot11 24ghz slot < slot-number > channel [< channel-number > | auto] • ap name <ap-name> dot11 24ghz slot <slot-number> cleanair • ap name <ap-name> dot11 24ghz slot <slot-number> dot11n antenna [A | B | C | D] • ap name <ap-name> dot11 24ghz slot <slot-number> shutdown • ap name <ap-name> dot11 24ghz slot <slot-number> txpower [<trasnmit-power-level> | auto] • ap name <ap-name> dot11 5ghz txpower [<transmit-power-level> | auto] • ap name <ap-name> dot11 5ghz SI • ap name <ap-name> dot11 5ghz antenna ext-ant-gain <ext-ant-gain> • ap name <ap-name> dot11 5ghz antenna mode [omni | sectorA | sectorB] • ap name <ap-name> dot11 5ghz antenna selection [external | internal] • ap name <ap-name> dot11 5ghz beamforming • ap 名 <ap-name> dot11 5ghz channel <channel-number> • ap name <ap-name> dot11 5ghz channel auto

	コマンドまたはアクション	目的
		• ap name <ap-name> dot11 5ghz channel width [160 MHz | 20 MHz | 40 MHz | 80 MHz | 80+80 MHz] • ap name <ap-name> dot11 5ghz cleanair • ap name <ap-name> dot11 5ghz dot11n antenna [A | B | C | D | E | F | G | H] • ap name <ap-name> dot11 5ghz rrm channel <channel-number> • ap name <ap-name> dot11 5ghz secondary-80 <channel-number> • ap name <ap-name> dot11 5ghz shutdown • ap name <ap-name> dot11 5ghz slot <slot-number> SI • ap name <ap-name> dot11 5ghz slot <slot-number> antenna ext-ant-gain <ext-ant-gain-number> • ap name <ap-name> dot11 5ghz slot <slot-number> antenna mode [omni | sectorA | sectorB] • ap name <ap-name> dot11 5ghz slot <slot-number> antenna selection [external | internal] • ap name <ap-name> dot11 5ghz slot <slot-number> beamforming • ap name <ap-name> dot11 5ghz slot <slot-number> channel <channel-number> • ap name <ap-name> dot11 5ghz slot <slot-number> channel auto

	コマンドまたはアクション	目的
		• ap name <ap-name> dot11 5ghz slot <slot-number> channel width [160 MHz | 20 MHz | 40 MHz | 80 MHz] • ap name <ap-name> dot11 5ghz slot <slot-number> cleanair • ap name <ap-name> dot11 5ghz slot <slot-number> dot11n antenna [A | B | C | D | E | F | G | H] • ap name <ap-name> dot11 5ghz slot <slot-number> rrm channel <channel-number> • ap name <ap-name> dot11 5ghz slot <slot-number> shutdown • ap name <ap-name> dot11 5ghz slot <slot-number> txpower [<transmit-power-level> | auto] • ap name <ap-name> dot11 dual-band channel <channel-number> • ap name <ap-name> dot11 dual-band channel auto • ap name <ap-name> dot11 dual-band channel width [160W | 20W | 40W | 80W] • ap name <ap-name> dot11 dual-band txpower [<transmit-power-level> | auto] • ap name <ap-name> dot11 dual-band antenna ext-ant-gain <ext-ant-gain-number> • ap name <ap-name> dot11 dual-band band [24ghz | 5ghz]

	コマンドまたはアクション	目的
		• ap name <ap-name> dot11 dual-band role {auto | manual [client-serving | monitor]} • ap name <ap-name> dot11 dual-band cleanair • ap name <ap-name> dot11 dual-band cleanair band [24Ghz | 5Ghz] • ap name <ap-name> dot11 dual-band dot11n antenna [A | B | C | D] • ap name <ap-name> dot11 dual-band shutdown • ap name <ap-name> dot11 dual-band slot <slot-number> antenna ext-ant-gain <ext-ant-gain-number> • ap name <ap-name> dot11 dual-band slot <slot-number> band [24ghz | 5ghz] • ap name <ap-name> dot11 dual-band slot <slot-number> channel <channel-number> • ap name <ap-name> dot11 dual-band slot <slot-number> channel auto • ap name <ap-name> dot11 dual-band slot <slot-number> channel width [160 MHz | 20 MHz | 40 MHz | 80 MHz] • ap name <ap-name> dot11 dual-band slot <slot-number> cleanair • ap name <ap-name> dot11 dual-band slot <slot-number> cleanair band [24Ghz | 5Ghz]

	コマンドまたはアクション	目的
		• ap name <ap-name> dot11 dual-band slot <slot-number> dot11n antenna [A | B | C | D] • ap name <ap-name> dot11 dual-band slot <slot-number> role {auto | manual [client-serving | monitor]} • ap name <ap-name> dot11 dual-band slot <slot-number> shutdown • ap name <ap-name> dot11 dual-band slot <slot-number> txpower [<transmit-power-level> | auto]

センサーモードの設定の確認

AP のモードを確認するには、次の **show** コマンドを使用します。

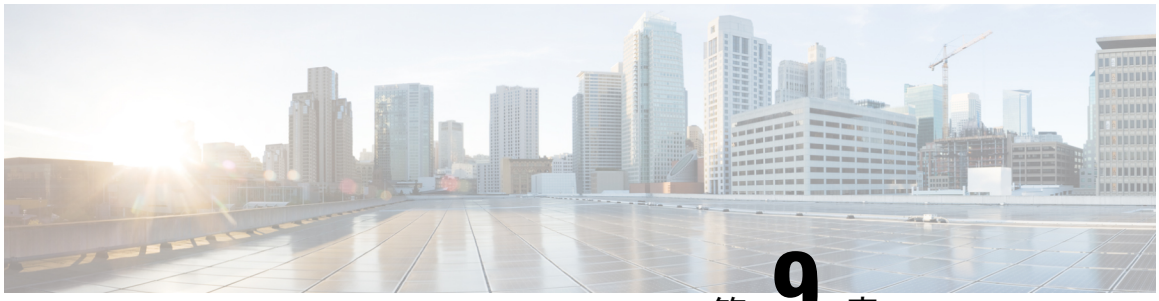
```
Device# show ap dot11 dual-band summary
AP Name          Mac Address    Slot Admin   State Oper State Width Txpwr Mode Subband
channel
-------------------------------------------------------------------------------------
AP4001.7A39.2E12 7070.8b24.1ba0  0   Enabled  N/A   NA   N/A   Sensor All (Sensor)
```

センサーモードでの AP のチャネルで Txpower、Channel width、Oper state、および「（Sensor）」を確認するには、次の **show** コマンドを使用します。

```
Device# show ap dot11 24ghz summary
AP Name          Mac Address    Slot  Admin   State  Oper  State Width Txpwr Channel
-------------------------------------------------------------------------------------
AP4001.7A39.2E12 7070.8b24.1ba0 0    Enabled   N/A   N/A    N/A (Sensor)
AP-SIDD-3702I    80e0.1d6a.3520 0    Enabled   Down   20   *1/8 (22 dBm)(11)
```

センサーモードでの AP のチャネルで Txpower、Channel width、Oper state、および「（Sensor）」を確認するには、次の **show** コマンドを使用します。

```
Device# show ap dot11 5ghz summary
AP Name          Mac Address    Slot  Admin   State  Oper  State Width Txpwr Channel
-------------------------------------------------------------------------------------
AP4001.7A39.2E12 7070.8b24.1ba0  1   Enabled   N/A   N/A   N/A   (Sensor)
AP-SIDD-3702I    80e0.1d6a.3520  1   Enabled   Down  40    1/6   (17 dBm) (100,104)*
```



第 9 章

AP 優先度

アクセスポイントに対するフェールオーバープライオリティの設定について

各コントローラには、定義された数のアクセスポイント用通信ポートが装備されています。未使用のアクセスポイントポートがある複数のコントローラが同じネットワーク上に展開されている場合、1 つのコントローラが故障すると、ドロップしたアクセスポイントは、自動的に未使用のコントローラポートをポーリングして、そのポートにアソシエートします。

次に、アクセスポイントのフェールオーバープライオリティを設定する際の注意事項を示します。

- バックアップコントローラがプライオリティレベルの高いアクセスポイントからの join 要求を認識できるよう、また、プライオリティレベルの低いアクセスポイントを必要に応じて関連付け解除してポートを使用可能にできるようにワイヤレスネットワークを設定できます。
- フェールオーバーのプライオリティレベルは、通常の無線ネットワークの運用中は無効です。コントローラ障害後に使用できるバックアップ コントローラ ポートよりも多くのアソシエーション要求が発生する場合のみ有効となります。
- コントローラがフルスケールになっている、またはプライマリコントローラで障害が発生し、APがセカンダリコントローラにフォールバックする場合、APのプライオリティはコントローラへの接続中にチェックされます。
- ネットワークのフェールオーバープライオリティを有効にして、個別のアクセスポイントにプライオリティを割り当てることができます。
- デフォルトでは、すべてのアクセスポイントはプライオリティレベル 1 に設定されています。これは、最も低いプライオリティレベルです。このため、これよりも高いプライオリ

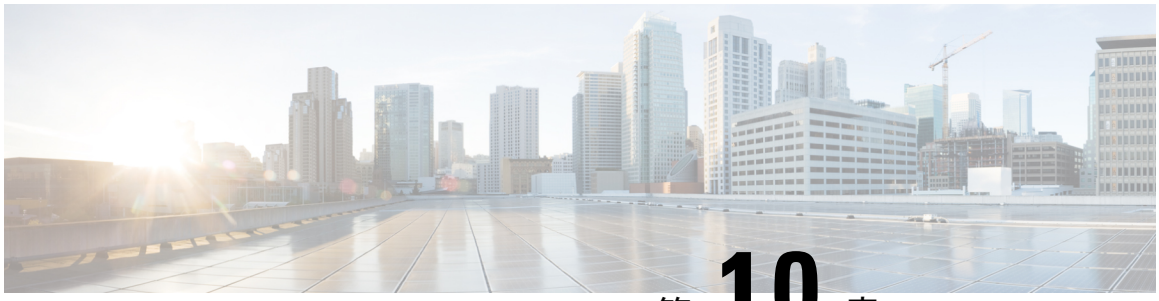
ティレベルを必要とするアクセスポイントにのみ、プライオリティレベルを割り当てる必要があります。

AP プライオリティの設定

（注） アクセスポイントのプライオリティの範囲は 1 ～ 4 で、4 が最高です。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name* **priority** *priority* 例： `Device# ap name AP44d3.ca52.48b5 priority 1`	アクセス ポイントのプライオリティを指定します。
ステップ 2	**show ap config general** 例： `Device# show ap config general`	すべてのアクセスポイントに共通の情報を表示します。
ステップ 3	**show ap name** *ap-name* **config general** 例： `Device# show ap name AP44d3.ca52.48b5 config general`	特定のアクセスポイントの設定を表示します。



第 10 章

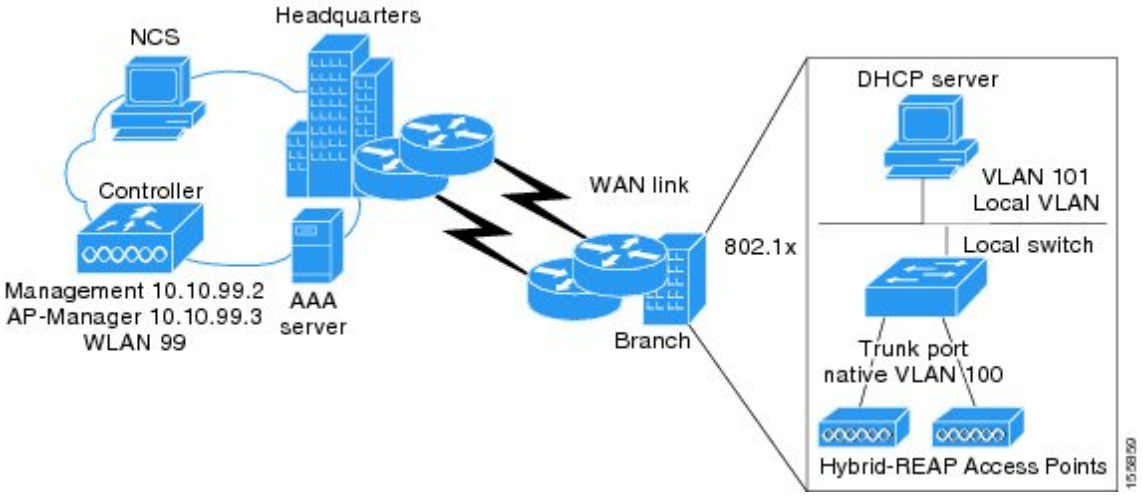
FlexConnect

FlexConnect について

FlexConnect（以前は、ハイブリッド リモート エッジ アクセス ポイントまたは H-REAP と呼ばれていました）は、ブランチオフィスとリモートオフィスに導入されるワイヤレスソリューションです。これにより顧客は、各オフィスでコントローラを展開することなく、本社オフィスからワイドエリアネットワーク（WAN）経由で、支社またはリモートオフィスのアクセスポイント（AP）を設定および制御できるようになります。FlexConnect アクセスポイントは、コントローラへの接続を失ったとき、クライアント データ トラフィックをローカルにスイッチングし、クライアント認証をローカルで実行できます。コントローラに接続されているときには、トラフィックをコントローラに送り返すこともできます。接続モードで、FlexConnect アクセスポイントは、ローカル認証も実行できます。

図 *3 : FlexConnect* の導入

次の図に、FlexConnect の一般的な導入を示します。



コントローラソフトウェアでは、FlexConnect アクセスポイントに対する耐障害性をより強化した方法が提供されています。以前のリリースでは、コントローラから解除されるたびに、FlexConnect アクセスポイントはスタンドアロンモードに移行します。中央でスイッチされるクライアントのアソシエーションは解除されます。ただし、FlexConnect アクセス ポイントはローカルにスイッチされたクライアントに引き続き対応します。FlexConnect アクセスポイントがコントローラ（またはスタンバイコントローラ）に再joinすると、すべてのクライアントが接続解除され、再度認証されます。この機能は強化されており、クライアントと FlexConnect アクセスポイント間の接続はそのまま保持され、クライアントによるシームレスな接続が実現します。アクセスポイントとコントローラの両方の設定が同じ場合は、クライアントと AP 間の接続が維持されます。

クライアント接続が確立された後に、コントローラはクライアントの元の属性を復元しません。クライアントのユーザ名、現在のレートとサポートされているレート、およびリッスン間隔値は、セッションタイマーが切れた後でのみデフォルト値にリセットされます。

FlexConnect アクセスポイントは、1 ロケーションにつき何台でも展開できます。複数の FlexConnect グループを 1 つのロケーションで定義できます。

コントローラは、ユニキャストパケットまたはマルチキャストパケットの形式でアクセスポイントにマルチキャストパケットを送信できます。FlexConnect モードでは、アクセスポイントはユニキャスト形式でのみマルチキャストパケットを受信できます。

FlexConnect アクセスポイントは、1 対 1 のネットワークアドレス変換（NAT）設定をサポートします。また、真のマルチキャストを除くすべての機能に対して、ポートアドレス変換（PAT）をサポートします。NAT 境界を越えるマルチキャストもサポートされます（ユニキャストオプションを使用して設定されている場合）。FlexConnect アクセスポイントは、中央でスイッチされるすべての WLAN に対して真のマルチキャストが動作するときを除き、多対 1 の NAT または PAT境界もサポートします。

（注） NAT と PAT は FlexConnect アクセスポイントではサポートされていますが、対応するコントローラではサポートされていません。シスコは、NAT/PAT 境界の背後にコントローラを置く構成はサポートしません。

アクセスポイントで、これらのセキュリティタイプがローカルにアクセス可能である場合、VPN および Point-to-Point Tunnel Protocol（PPTP）は、ローカルにスイッチされるトラフィックに対してサポートされます。

FlexConnect アクセスポイントは複数の SSID をサポートします。

ワークグループブリッジおよびユニバーサル ワークグループ ブリッジは、ローカルにスイッチされるクライアントの FlexConnect アクセスポイントでサポートされます。

FlexConnect は、IPv4 の動作と同様にトラフィックをローカル VLAN にブリッジすることによって、IPv6 クライアントをサポートしています。FlexConnect は、最大 100 のアクセスポイントのグループに対するクライアントモビリティをサポートしています。

ローカルモードから FlexConnect モードに移行しても、アクセスポイントをリブートする必要はありません。

FlexConnect 認証プロセス

アクセスポイントは、ブート時にコントローラを検索します。コントローラが見つかると、そのコントローラに join し、最新のソフトウェアイメージと設定をコントローラからダウンロードして、無線を初期化します。ダウンロードした設定は不揮発性メモリに保存されて、スタンドアロンモードで使用されます。

（注） 最新のコントローラソフトウェアのダウンロード後に、アクセスポイントをリブートしたら、アクセスポイントを FlexConnect モードへ変換する必要があります。

（注） 802.1X は、Cisco 2700 シリーズの AP の AUX ポートではサポートされていません。

FlexConnect アクセスポイントは、次のいずれかの方法でコントローラの IP アドレスを認識できます。

- アクセスポイントの IP アドレスが DHCP サーバから割り当て済みの場合は、通常の CAPWAP または LWAPP ディスカバリプロセスを介してコントローラを検出します。

  （注） OTAP はサポートされていません。

- アクセスポイントに固定 IP アドレスが割り当てられている場合は、DHCP オプション 43 以外の方法のディスカバリプロセスを使用してコントローラを検出します。アクセスポイントがレイヤ3ブロードキャストでコントローラを検出できない場合は、DNS 解決を使用することをお勧めします。DNS を使用すれば、固定 IP アドレスを持ち DNS サーバを認識しているアクセスポイントは、最低 1 つのコントローラを見つけることができます。
- CAPWAP と LWAPP のどちらのディスカバリメカニズムも使用できないリモートネットワークにあるコントローラを検出できるようにするには、プライミングを使用してください。この方法を使用すると、アクセスポイントの接続先のコントローラを（アクセスポイントの CLI により）指定できます。

FlexConnectアクセスポイントがコントローラに到達できるとき（接続モードと呼ばれます）、コントローラはクライアント認証を支援します。FlexConnect アクセスポイントがコントローラにアクセスできないとき、アクセスポイントはスタンドアロンモードに入り、独自にクライアントを認証します。

（注） アクセスポイント上の LED は、デバイスが異なる FlexConnect モードに入るときに変化します。LED パターンの情報については、アクセスポイントのハードウェア インストール ガイドを参照してください。

クライアントが FlexConnect アクセスポイントにアソシエートするとき、アクセスポイントではすべての認証メッセージをコントローラに送信し、WLAN設定に応じて、クライアントデータパケットをローカルにスイッチする（ローカルスイッチング）か、コントローラに送信（中央スイッチング）します。クライアント認証（オープン、共有、EAP、Web 認証、および NAC）とデータパケットに関して、WLAN は、コントローラ接続の設定と状態に応じて、次のいずれかの状態になります。

- 中央認証、中央スイッチング：コントローラがクライアント認証を処理し、すべてのクライアントデータはコントローラにトンネルを通じて戻されます。この状態は、接続済みモードの場合にだけ有効です。
- 中央認証、ローカルスイッチング：コントローラがクライアント認証を処理し、FlexConnect アクセスポイントがデータパケットをローカルにスイッチします。クライアントが認証に成功した後、コントローラは新しいペイロードと共にコンフィギュレーションコマンドを送信し、FlexConnect アクセスポイントに対して、ローカルにデータパケットのスイッチを始めるように指示します。このメッセージはクライアントごとに送信されます。この状態は接続モードにのみ適用されます。

（注） FlexConnect ローカルスイッチング、中央認証導入では、静的 IP アドレスを持つパッシブクライアントが存在する場合は、[WLAN] > [Advanced] タブで [Learn Client IP Address] 機能を無効にすることをお勧めします。

- ローカル認証、ローカルスイッチング：FlexConnect アクセスポイントがクライアント認証を処理し、クライアントデータパケットをローカルにスイッチします。この状態はスタンドアロンモードおよび接続済みモードの場合に有効です。

  接続済みモードでは、アクセスポイントは、ローカルで認証されたクライアントに関する最小限の情報をコントローラに提供します。次の情報はコントローラでは使用できません。

  - ポリシータイプ
  - アクセス VLAN
  - VLAN 名
  - サポートされるレート
  - 暗号化の暗号

    ローカル認証は、ラウンドトリップ遅延が 100 ms を超えず、最大伝送単位（MTU）が 576 バイトを下回らない、最小帯域幅が 128 kbps のリモートオフィス設定を維持できない場合に役立ちます。ローカル認証で、認証機能はアクセスポイント自体に存在します。ローカル認証は、ブランチ オフィスの遅延要件を短縮できます。

    （注） ローカル認証は、ローカルスイッチングモードの FlexConnect アクセスポイントの WLAN 上のみで有効にできます。

    ローカル認証に関する注意事項は、次のとおりです。

  - ゲスト認証は、FlexConnect ローカル認証を有効にした WLAN で実行できません。
  - コントローラ上でのローカル RADIUS はサポートされていません。
  - クライアントが認証されたら、ローミングはグループ内のコントローラおよび他の FlexConnect アクセスポイントがクライアント情報に更新された後でのみサポートされます。
  - 接続モードのローカル認証には、WLAN 設定が必要です。

    （注） FlexConnectアクセスポイントに接続している、ローカルにスイッチされたクライアントがIPアドレスを更新し、またjoinする場合に、クライアントは実行状態のまま残ります。これらのクライアントはコントローラによって再認証されません。

- 認証ダウン、スイッチダウン：この状態になると、WLAN は既存クライアントのアソシエーションを解除し、ビーコン要求とプローブ要求の送信を停止します。この状態はスタンドアロンモードおよび接続済みモードの両方の場合に有効です。

- 認証ダウン、ローカルスイッチング：WLANは新しいクライアントからの認証の試行をすべて拒否しますが、既存クライアントを保持するために、ビーコン応答とプローブ応答の送信は続けます。この状態はスタンドアロンモードでのみ有効です。

FlexConnectアクセスポイントがスタンドアロンモードになると、オープン、共通、WPA-PSK、または WPA2-PSK の認証用に設定された WLAN は、「ローカル認証、ローカルスイッチング」状態になり、新しいクライアント認証を続行します。コントローラ ソフトウェア リリース 4.2 以降のリリースでは、これは 802.1X、WPA-802.1X、WPA2-802.1X、または CCKM 用に設定されたWLANでも正しい設定です。ただし、これらの認証タイプでは外部のRADIUSサーバが設定されている必要があります。FlexConnect アクセスポイントでローカル RADIUS サーバを設定して、スタンドアロンモードで、またはローカル認証との組み合わせで 802.1X をサポートすることもできます。

その他の WLAN は、「認証停止、スイッチング停止」状態（WLAN が中央スイッチング用に設定されている場合）または「認証停止、ローカルスイッチング」状態（WLAN がローカルスイッチング用に設定されている場合）のいずれかになります。

FlexConnect アクセスポイントがスタンドアロンモードではなく、コントローラに接続されている場合、コントローラはプライマリ RADIUS サーバを使用します。コントローラがプライマリ RADIUS サーバにアクセスする順序は、[RADIUS Authentication Servers] ページまたは **config radius auth add** CLI コマンドで指定された順序になります（特定の WLAN のサーバ順序がオーバーライドされている場合を除く）。ただし、802.1X EAP 認証を使用する場合は、クライアントを認証するために、スタンドアロンモードのFlexConnectアクセスポイント用のバックアップ RADIUS サーバが必要となります。

（注） コントローラはバックアップ RADIUS サーバを使用しません。コントローラはローカル認証モードでバックアップ RADIUS サーバを使用します。

バックアップ RADIUS サーバは、個々のスタンドアロンモード FlexConnect アクセスポイントに対して設定することも（コントローラの CLI を使用）、スタンドアロンモード FlexConnect アクセスポイントのグループに対して設定することも（GUI または CLI を使用）できます。個々のアクセスポイントに対して設定されたバックアップサーバは、FlexConnectに対するバックアップ RADIUS サーバ設定よりも優先されます。

Web 認証がリモートサイトで FlexConnect のアクセスポイントに使用されると、クライアントはリモートローカルサブネットから IP アドレスを取得します。最初の URL 要求を解決するため、DNSがサブネットのデフォルトゲートウェイを介してアクセスできます。コントローラが DNS クエリーの応答パケットを代行受信およびリダイレクトするには、これらのパケットは CAPWAP 接続を介してデータセンターでコントローラにアクセスする必要があります。Web 認証プロセス中、FlexConnect のアクセスポイントは DNS と DHCP メッセージのみを許可します。つまり、アクセスポイントは、クライアントの Web 認証が完了するまで DNS 応答メッセージをコントローラに転送します。クライアントの Web 認証が完了すると、すべてのトラフィックがローカルでスイッチされます。

（注） コントローラが NAC に対して設定されている場合、クライアントはアクセスポイントが接続モードにある場合にのみアソシエートできます。NACが有効の場合、WLANがローカルスイッチングに設定されている場合でも、有害な（または検疫された）VLANを作成して、このVLANに割り当てられているクライアントのデータトラフィックがコントローラを通過できるようにする必要があります。クライアントが検疫 VLAN に割り当てられると、そのクライアントのデータパケットはすべて中央でスイッチングされます。隔離VLANの作成の詳細については、「動的インターフェイスの設定」の項を参照してください。NAC アウトオブバンドサポートの設定の詳細については、「NAC アウトオブバンド統合の設定」の項を参照してください。

FlexConnect アクセスポイントがスタンドアロンモードになると、次のようになります。

- アクセスポイントは、ARP経由でデフォルトゲートウェイに到達できるかどうかを確認します。その場合、アクセスポイントはコントローラへの到達を試行し続けます。

アクセスポイントが ARP を確立できない場合は、次のことが起こります。

- アクセスポイントは5回の検出を試行し、それでもコントローラを検出できない場合は、新しい DHCP IP を取得するために、イーサネットインターフェイス上で DHCP を更新しようとします。
- アクセスポイントが、5回再試行して失敗した場合、インターフェイスのIPアドレスを再度更新します。これは 3 回試行されます。
- 3回の試行が失敗した場合、アクセスポイントは固定IPに戻ってリブートします（アクセス ポイントが固定 IP を使用して設定されている場合のみ）。
- リブートの実行により、アクセス ポイントの不明なエラーの可能性が排除されます。

アクセスポイントがコントローラとの接続を再確立すると、すべてのクライアントをアソシエート解除して、コントローラからの新しい設定情報を適用し、クライアントの接続を再度許可します。

FlexConnect の制約事項

- 固定 IP アドレスまたはDHCPアドレスを持つFlexConnectアクセスポイントを展開することができます。DHCP の状況では、DHCP サーバはローカルに使用可能であり、ブート時にアクセスポイントの IP アドレスを提供できる必要があります。
- FlexConnect は最大で 4 つの断片化されたパケット、または最低 576 バイトの最大伝送単位（MTU）WAN リンクをサポートします。
- アクセスポイントとコントローラの間のラウンドトリップ遅延が300ミリ秒（ms）を超えてはなりません。また、CAPWAP コントロールパケットは他のすべてのトラフィックよりも優先される必要があります。300 ミリ秒のラウンドトリップ遅延を実現できないシナリオでは、ローカル認証を実行するようにアクセスポイントを設定します。

- クライアント接続は、アクセスポイントがスタンドアロンモードから接続モードに移行するときに RUN 状態になっている、ローカルにスイッチされたクライアントに対してのみ復元されます。アクセスポイントのモードが移行すると、アクセスポイントの無線もリセットされます。
- コントローラの設定は、アクセスポイントがスタンドアロンモードになった時点と、アクセスポイントが接続済みモードに戻った時点の間で同じである必要があります。同様に、アクセスポイントがセカンダリコントローラまたはバックアップコントローラにフォールバックする場合、プライマリコントローラとセカンダリコントローラまたはバックアップコントローラの設定は同じである必要があります。
- 新規に接続したアクセスポイントは、FlexConnect モードでブートできません。
- 802.11r Fast Transition ローミングは、ローカル認証で運用中は Cisco Aironet 1830 シリーズおよび 1850 シリーズ AP ではサポートされません。
- NAC アウトオブバンド統合がサポートされるのは、WLAN が FlexConnect の中央スイッチングを行うように設定されている場合だけです。FlexConnect のローカルスイッチングを行うように設定されている WLAN での使用はサポートされていません。
- FlexConnect アクセスポイントのプライマリコントローラとセカンダリコントローラの設定が同一であることが必要です。設定が異なると、アクセスポイントはその設定を失い、特定の機能（WLAN の無効化、VLAN、静的チャネル番号など）が正しく動作しないことがあります。さらに、FlexConnect アクセスポイントの SSID とそのインデックス番号を両方のコントローラで同じにしてください。
- アクセスポイントで設定された syslog サーバと組み合わせて、FlexConnect アクセス ポイントを設定する場合、アクセスポイントがリロードされ、1 以外のネイティブ VLAN になった後、初期化時に、アクセスポイントからの syslog パケットで VLAN ID 1 のタグが付けられているものはほとんどありません。
- MAC フィルタリングは、スタンドアロンモードの FlexConnect アクセスポイントではサポートされていません。ただし、MAC フィルタリングは、接続モードの FlexConnect アクセスポイントでのローカルスイッチングと中央認証はサポートされています。また、FlexConnect アクセスポイントを持つローカルにスイッチされる WLAN の Open SSID、MAC フィルタリングおよび RADIUS NAC は、MAC が Cisco ISE でチェックされる有効な設定です。
- FlexConnect で、IPv6 ACL、ネイバー ディスカバリ キャッシュ、および IPv6 NDP パケットの DHCPv6 スヌーピングはサポートされていません。
- FlexConnect では、[Client Detail] ウィンドウに IPv6 クライアントのアドレスは表示されません。
- ローカルにスイッチされた WLAN を使用した FlexConnect アクセスポイントでは、IP ソースガードを実行したり、ARP スプーフィングを防止したりすることができません。中央でスイッチングされる WLAN では、ワイヤレスコントローラが IP ソースガードおよび ARP スプーフィングを実行します。

- ローカルスイッチングを使用する FlexConnect AP における ARP スプーフィング攻撃を防ぐために、ARP インスペクションを使用することを推奨します。
- FlexConnect AP の WLAN でローカルスイッチングを有効にすると、AP はローカルスイッチングを実行します。ただし、ローカルモードの AP に対しては、中央スイッチングが実行されます。

  FlexConnect モードの AP とローカルモードの AP 間におけるクライアントのローミングがサポートされていないシナリオでは、移動後の VLAN の違いが原因で、クライアントが正しい IP アドレスを取得できない場合があります。また、FlexConnect モード AP とローカルモード AP 間の L2 および L3 のローミングはサポートされていません。
- FlexConnect スタンドアロンモードの Wi-Fi Protected Access バージョン 2（WPA2）、接続モードのローカル認証、または接続モードの CCKM 高速ローミングの場合、Advanced Encryption Standard（AES）のみがサポートされます。
- FlexConnect スタンドアロンモードの Wi-Fi Protected Access（WPA）、接続モードのローカル認証、または接続モードの CCKM 高速ローミングの場合、Temporal Key Integrity Protocol（TKIP）のみがサポートされます。
- TKIP による WPA2 および AES による WPA は、スタンドアロンモード、接続モードのローカル認証、および接続モードの CCKM 高速ローミングではサポートされません。
- Cisco Aironet 1830 シリーズおよび 1850 シリーズの AP では、オープンな WPA（PSK および 802.1x）認証のみサポートされています。
- Cisco Aironet 1830 シリーズおよび 1850 シリーズ AP では、802.11r Fast Transition ローミングのみサポートされています。
- ローカルにスイッチングされた WLAN の AVC は、第 2 世代の AP でサポートされています。
- 外部 RADIUS サーバでユーザが利用できない場合は、ローカル認証のフォールバックはサポートされません。
- ローカルスイッチングおよびローカル認証で FlexConnect AP 用に設定された WLAN については、dot11 クライアント情報の同期がサポートされます。
- Cisco Aironet 1830 シリーズおよび 1850 シリーズ AP では、DNS Override はサポートされていません。
- Cisco Aironet 1830 シリーズおよび 1850 シリーズ AP は、IIPv6 をサポートしていません。ただし、ワイヤレス クライアントはこれらの AP 全体に IPv6 トラフィックを渡すことができます。
- flex プロファイルでは、Flex モードで VLAN グループはサポートされていません。
- 個々のクライアントまたは無線で許可されるメディアストリームの最大数の設定は、FlexConnect モードではサポートされていません。

- APがFlexConnectモード（接続されているかスタンドアロン）であり、ローカルスイッチングとローカル認証を実行している場合、WLANクライアントアソシエーションの制限は機能しません。
- FlexConnect モードのローカル スイッチング クライアントは、Cisco Aironet 1810 シリーズ AP の RLAN プロファイルの IP アドレスを取得しません。
- IPv6 RADIUS サーバは FlexConnect AP 用に設定できません。IPv4 設定のみがサポートされます。

サイトタグの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site rr-xyz-site`	サイトタグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**flex-profile** *flex-profile-name* 例： `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	flexプロファイルをサイトタグにマッピングします。
ステップ 4	**ap-profile** *ap-profile* 例： `Device(config-site-tag)# ap-profile xyz-ap-profile`	AP プロファイルをワイヤレスサイトに割り当てます。
ステップ 5	**description** *site-tag-name* 例： `Device(config-site-tag)# description "default site tag"`	サイトタグの説明を追加します。
ステップ 6	**no local-site** 例： `Device(config-site-tag)# no local-site`	アクセスポイントを FlexConnect モードに移行します。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-site-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 8	**show wireless tag site summary** 例： `Device# show wireless tag site summary`	（任意）サイトタグのサマリーを表示します。

ポリシー タグの設定（CLI）

ポリシー タグを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag policy** *policy-tag-name* 例： `Device(config-policy-tag)# wireless tag policy rr-xyz-policy-tag`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device(config-policy-tag)# wlan rr-xyz-wlan-aa policy rr-xyz-policy-1`	ポリシー プロファイルを WLAN プロファイルにマッピングします。
ステップ 4	**end** 例： `Device(config-policy-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 5	**show wireless tag policy summary** 例： `Device# show wireless tag policy summary`	（任意）設定済みのポリシー タグを表示します。 （注） ポリシー タグに関する詳細情報を表示するには、**show wireless tag policy detailed** *policy-tag-name* コマンドを使用します。

AP へのポリシータグとサイトタグの付加（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] の順に選択します。

[All Access Points] セクションに、ネットワーク内のすべての AP の詳細が表示されます。

ステップ 2 AP の設定の詳細を編集するには、その AP の行を選択します。

[Edit AP] ウィンドウが表示されます。

ステップ 3 [General] タブの [Tags] セクションで、[Configuration] > [Tags & Profiles] > [Tags] ページで作成した、該当するポリシータグ、サイトタグ、および RF タグを指定します。

ステップ 4 [Update & Apply to Device] をクリックします。

AP へのポリシー タグとサイト タグの付加（CLI）

ポリシー タグとサイト タグを AP に付加するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap** *mac-address* 例： `Device(config)# ap F866.F267.7DFB`	Cisco AP を設定し、AP プロファイル コンフィギュレーション モードを開始します。 （注） *mac-address* 有線 mac アドレスである必要があります。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	ポリシー タグを AP にマッピングします。
ステップ 4	**site-tag** *site-tag-name* 例：	サイトタグを AP にマッピングします。

	コマンドまたはアクション	目的
	`Device(config-ap-tag)# site-tag rr-xyz-site`	
ステップ 5	**rf-tag** *rf-tag-name* 例： `Device(config-ap-tag)# rf-tag rf-tag1`	RF タグを関連付けます。
ステップ 6	**end** 例： `Device(config-ap-tag)# end`	設定を保存し、コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**show ap tag summary** 例： `Device# show ap tag summary`	（任意）AP の詳細と AP に関連付けられているタグを表示します。
ステップ 8	**show ap name** <*ap-name*> **tag info** 例： `Device# show ap name ap-name tag info`	（任意）AP 名とタグ情報を表示します。
ステップ 9	**show ap name** <*ap-name*> **tag detail** 例： `Device# show ap name ap-name tag detail`	（任意）AP 名とタグの詳細を表示します。

FlexConnect の設定

（注） 設定作業は、ここにリストされている順序で実行する必要があります。

リモートサイトでのスイッチの設定

手順

ステップ 1 FlexConnect を有効にするアクセスポイントを、スイッチ上のトランクまたはアクセスポートに接続します。

（注） この手順に示す設定例では、FlexConnect アクセスポイントはスイッチ上のトランクポートに接続されます。

ステップ 2 次の設定例は、FlexConnect アクセスポイントをサポートするようにスイッチを設定する方法を示しています。

この設定例では、FlexConnect アクセスポイントは、トランクインターフェイス FastEthernet 1/0/2 に接続され、ネイティブ VLAN 100 を使用します。このアクセスポイントは、このネイティブ VLAN 上での IP 接続を必要とします。リモートサイトのローカルサーバとリソースは、VLAN 101 上にあります。DHCP プールがスイッチの両方の VLAN のローカルスイッチ内に作成されます。最初の DHCP プール（ネイティブ）は FlexConnect アクセスポイントにより使用され、2 つ目の DHCP プール（ローカルスイッチング）は、クライアントがローカルでスイッチングされる WLAN にアソシエートする場合、クライアントにより使用されます。

```
.
.
.
ip dhcp pool NATIVE
   network 209.165.200.224 255.255.255.224
   default-router 209.165.200.225
   dns-server 192.168.100.167
!
ip dhcp pool LOCAL-SWITCH
   network 209.165.201.224 255.255.255.224
   default-router 209.165.201.225
   dns-server 192.168.100.167
!
interface FastEthernet1/0/1
 description Uplink port
 no switchport
 ip address 209.165.202.225 255.255.255.224
!
interface FastEthernet1/0/2
 description the Access Point port
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 100
 switchport trunk allowed vlan 101
 switchport mode trunk
!
interface Vlan100
 ip address 209.165.200.225 255.255.255.224
!
interface Vlan101
 ip address 209.165.201.225 255.255.255.224
end
!
.
.
.
```

FlexConnect に対するコントローラの設定

次の 2 つの環境で FlexConnect のコントローラを設定できます。

- 中央でスイッチされる WLAN
- ローカルでスイッチされる WLAN

FlexConnect のコントローラの設定には、中央でスイッチされる WLAN とローカルにスイッチされる WLAN を作成する操作が含まれます。次の表に、3 つの WLAN の例を示します。

表 *2 : WLAN* のシナリオ

WLAN	セキュリティ	認証	スイッチング	インターフェイスマッピング（VLAN）
Employee	WPA1+WPA2	中央	中央	Management（中央でスイッチされる VLAN）
Employee-local	WPA1+WPA2（PSK）	ローカル	ローカル	101（ローカルにスイッチされる VLAN）
Guest-central	Web 認証	中央	中央	Management（中央でスイッチされる VLAN）
Employee-local-auth	WPA1+WPA2	ローカル	ローカル	101（ローカルにスイッチされる VLAN）

FlexConnect モードでのローカルスイッチングの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞を選択します。

ステップ 2 [Policy profile] ページで、ポリシープロファイルの名前をクリックして編集するか、[Add] をクリックして新しいポリシープロファイルを作成します。

ステップ 3 表示される [Add/Edit Policy Profile] ウィンドウで、[Central Switching] チェックボックスをオフにします。

ステップ 4 [Update & Apply to Device] をクリックします。

FlexConnect モードでのローカルスイッチングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy rr-xyz-policy-1`	WLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**no central switching** 例： `Device(config-wireless-policy)# no central switching`	WLAN をローカルスイッチング用に設定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

FlexConnect モードでの中央スイッチングの設定（GUI）

始める前に

ポリシープロファイルが設定されていることを確認します。ポリシープロファイルが設定されていない場合は、「ポリシープロファイルの設定（GUI）」の項を参照してください。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞を選択します。

ステップ 2 [Policy Profile] ページで、ポリシーを選択します。

ステップ 3 [Edit Policy Profile] ウィンドウの [General] タブで、スライダを使用して [Central Switching] を有効または無効にします。

ステップ 4 [Update & Apply to Device] をクリックします。

FlexConnect モードでの中央スイッチングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy rr-xyz-policy-1`	WLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**central switching** 例： `Device(config-wireless-policy)# central switching`	WLAN を中央スイッチング用に設定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

FlexConnect のアクセスポイントの設定

詳細については、サイト タグの設定（CLI） （21 ページ）を参照してください。

WLAN 上のローカル認証用のアクセスポイントの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞を選択します。

ステップ 2 [Policy Profile] ページで、ポリシープロファイル名を選択します。[Edit Policy Profile] ウィンドウが表示されます。

ステップ 3 [General] タブで、[Central Authentication] チェックボックスをオフにします。

ステップ 4 [Update & Apply to Device] をクリックします。

WLAN 上のローカル認証用のアクセスポイントの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy rr-xyz-policy-1`	WLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**no central authentication** 例： `Device(config-wireless-policy)# no central authentication`	WLAN を ローカル認証用に設定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クライアントデバイスの WLAN への接続

FlexConnect に対するコントローラの設定 （92 ページ）で作成した WLAN にクライアントデバイスを接続するためのプロファイルを作成するには、次の手順に従ってください。

シナリオ例（FlexConnect に対するコントローラの設定 （92 ページ）を参照）では、クライアントに 3 つのプロファイルがあります。

1. 「employee」WLAN に接続するには、WPA または WPA2 と PEAP-MSCHAPV2 認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、コントローラの管理 VLAN によってクライアントに IP アドレスが割り当てられます。
2. 「local-employee」WLAN に接続するには、WPA または WPA2 認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、ローカルスイッチのVLAN 101 によってクライアントに IP アドレスが割り当てられます。
3. 「guest-central」WLAN に接続するには、オープンの認証を使用するクライアントプロファイルを作成します。クライアントが認証されると、アクセスポイントへのネットワークローカルの VLAN 101 によってクライアントに IP アドレスが割り当てられます。クライアントが接続すると、ローカルユーザは Web ブラウザに任意の HTTP アドレスを入力できます。ユーザは、Web 認証プロセスを完了するために、自動的にコントローラに誘導されます。Web ログインウィンドウが表示されたら、ユーザはユーザ名とパスワードを入力します。

FlexConnect イーサネットフォールバックの設定

FlexConnect イーサネットフォールバックについて

イーサネットリンクが機能しないときに無線をシャットダウンするように AP を設定できます。イーサネットリンクが使用可能状態に戻った場合、無線を使用可能状態に戻すように AP を設定できます。この機能は、接続されている AP に依存しない、またはスタンドアロンモードです。無線がシャットダウンすると、AP は WLAN をブロードキャストしないため、クライアントは最初のアソシエーションおよびローミングで AP に接続することができません。

FlexConnect イーサネットフォールバックの制約事項

- FlexConnectイーサネットフォールバックの設定はグローバルレベルで、すべてFlexConnect AP に適用できます。ただし、この機能は Cisco AP1130、AP1240、および AP1150 には適用されません。
- FlexConnect イーサネットフォールバック機能は、Cisco AP1520 や AP1550 などの複数のポートが使用されている AP には適用されません。
- イーサネットインターフェイスで設定するキャリア遅延は、ヒステリシスに基づいてインターフェイスをシャットダウンおよびリロードします。したがって、設定する遅延が、イーサネットおよび802.11インターフェイスがシャットダウンおよびリロードされる前の実際の遅延とは異なる場合があります。

FlexConnect イーサネットフォールバックの設定

始める前に

この機能は、複数のポートを持つ AP には適用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *flex-profile-name* 例： `Device(config)# wireless profile flex test`	ワイヤレス flex プロファイルを設定し、ワイヤレス flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**fallback-radio-shut** 例： `Device(config-wireless-flex-profile)# fallback-radio-shut`	無線インターフェイスのシャットダウンを有効にします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show wireless profile flex detailed** *flex-profile-name* 例： `Device# show wireless profile flex detailed test`	（任意）選択したプロファイルに関する詳細情報を表示します。

AP での flex AP ローカル認証（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Flex] > > を選択します。

ステップ 2 [Flex] ページで、 flex プロファイルの名前をクリックするか、[Add] をクリックして新規に作成します。

ステップ 3 表示される [Add/Edit Flex Profle] ウィンドウで、[Local Authentication] タブをクリックします。

ステップ 4 [RADIUS Server Group] ドロップダウンリストからサーバグループを選択します。

ステップ 5 [AP Fast Profile] ドロップダウンリストからプロファイルを選択します。

ステップ 6 次を有効にするか無効にするかを選択します。

- [LEAP]：Lightweight Extensible Authentication Protocol（LEAP）は、ワイヤレス LAN 向けの 802.1X 認証タイプであり、クライアントと RADIUS サーバ間で、共有秘密としてログオンパスワードを使用した強力な相互認証をサポートします。LEAP では、ユーザ単位、セッション単位の動的な暗号化キーが提供されます。
- [PEAP]：Protected Extensible Authentication Protocol（PEAP）は、暗号化および認証された Transport Layer Security（TLS）トンネル内でExtensible Authentication Protocol（EAP）をカプセル化するプロトコルです。
- [TLS]：Transport Layer Security（TLS）は、コンピュータネットワーク経由での通信のセキュリティを提供する暗号化プロトコルです。
- [RADIUS]：Remote Authentication Dial-In User Service（RADIUS）は、ネットワークサービスに接続して使用するユーザに対して、一元化された認証、許可、およびアカウンティング（AAA またはトリプル A）の管理を提供するネットワーキングプロトコルです。

ステップ 7 [Users] セクションで、[Add] をクリックします。

ステップ 8 ユーザ名とパスワードの詳細を入力し、[Save] をクリックします。

ステップ 9 [Save & Apply to Device] をクリックします。

AP での flex AP ローカル認証（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 2	**aaa session-id common** 例： `Device(config)# aaa session-id common`	RADIUS グループから、特定のコールに対して送信されるすべてのセッション ID 情報が同じであることを確認します。
ステップ 3	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	RADIUS グループのシステム認証制御を有効にします。
ステップ 4	**eap profile** *name* 例： `Device(config)# eap profile aplocal-test`	EAP プロファイルを作成します。
ステップ 5	**method fast** 例： `Device(config-eap-profile)# method fast`	プロファイルで FAST 方式を設定します。
ステップ 6	**exit** 例： `Device(config-radius-server)# exit`	コンフィギュレーション モードに戻ります。
ステップ 7	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex default-flex-profile`	flex ポリシーを設定します。
ステップ 8	**local-auth ap eap-fast** *name* 例：	EAP-FAST プロファイルの詳細を設定します。

	コマンドまたはアクション	目的
	`Device(config-wireless-flex-profile)# local-auth ap eap-fast aplocal-test`	
ステップ 9	**local-auth ap leap** 例： `Device(config-wireless-flex-profile)# local-auth ap leap`	LEAP 方式を設定します。
ステップ 10	**local-auth ap peap** 例： `Device(config-wireless-flex-profile)# local-auth ap peap`	PEAP 方式を設定します。
ステップ 11	**local-auth ap username** *username* 例： `Device(config-wireless-flex-profile)# local-auth ap username test1 test1`	ユーザ名とパスワードを設定します。
ステップ 12	**local-auth ap username** *username password* 例： `Device(config-wireless-flex-profile)# local-auth ap username test2 test2`	別のユーザ名とパスワードを設定します。
ステップ 13	**exit** 例： `Device(config-wireless-flex-profile)# exit`	コンフィギュレーションモードに戻ります。
ステップ 14	**wireless profile policy** *policy-profile* 例： `Device(config)# wireless profile policy default-policy-profile`	プロファイルポリシーを設定します。
ステップ 15	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	ポリシープロファイルを無効にします。
ステップ 16	**no central authentication** 例： `Device(config)# no central authentication`	中央（コントローラ）認証を無効にします。
ステップ 17	**vlan-id** *vlan-id* 例： `Device(config)# vlan-id 54`	VLAN 名または VLAN ID を設定します。

	コマンドまたはアクション	目的
ステップ 18	**no shutdown** 例： `Device(config)# no shutdown`	設定をイネーブルにします。

外部 Radius サーバを使用した Flex AP ローカル認証

このモードでは、アクセスポイントがクライアント認証を処理し、クライアントデータパケットをローカルにスイッチングします。この状態はスタンドアロンモードおよび接続済みモードの場合に有効です。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 2	**aaa session-id common** 例： `Device(config)# aaa session-id common`	RADIUS グループから、特定のコールに対して送信されるすべてのセッション ID 情報が同じであることを確認します。
ステップ 3	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	RADIUS グループのシステム認証制御を有効にします。
ステップ 4	**radius server** *server-name* 例： `Device(config)# radius server Test-SERVER1`	RADIUS サーバ名を指定します。 （注） FreeRADIUS over RADSEC でクライアントを認証するには、1024 ビットよりも長い RSA キーを生成する必要があります。これを行うには、**crypto key generate rsa general-keys exportable label** *name* コマンドを使用します。
ステップ 5	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* } 例：	RADIUS サーバのプライマリパラメータを指定します。

	コマンドまたはアクション	目的
	`Device(config-radius-server)# address ipv4 124.3.50.62 auth-port 1112 acct-port 1113`	
ステップ 6	**key** *string* 例： `Device(config-radius-server)# key test123`	deviceと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。
ステップ 7	**radius server** *server-name* 例： `Device(config)# radius server Test-SERVER2`	RADIUS サーバ名を指定します。
ステップ 8	**address {ipv4 | ipv6}** *ip address* {**auth-port** *port-number* | **acct-port** *port-number* } 例： `Device(config-radius-server)# address ipv4 124.3.52.62 auth-port 1112 acct-port 1113`	RADIUS サーバのセカンダリパラメータを指定します。
ステップ 9	**key** *string* 例： `Device(config-radius-server)# key test113`	deviceと RADIUS サーバ上で動作する RADIUS デーモンとの間で使用される認証および暗号キーを指定します。
ステップ 10	**exit** 例： `Device(config-radius-server)# exit`	コンフィギュレーションモードに戻ります。
ステップ 11	**aaa group server radius** *server-group* 例： `Device(config)# aaa group server radius aaa_group_name`	RADIUS サーバグループの識別を作成します。
ステップ 12	**exit** 例： `Device(config-sg-radius)# exit`	RADIUS サーバグループ コンフィギュレーション モードを終了します。
ステップ 13	**radius server** *server-name* 例： `Device(config)# radius server Test-SERVER1`	RADIUS サーバ名を指定します。
ステップ 14	**radius server** *server-name* 例：	RADIUS サーバ名を指定します。

	コマンドまたはアクション	目的
	`Device(config-radius-server)# radius server Test-SERVER2`	
ステップ 15	**exit** 例： `Device(config-radius-server)# exit`	RADIUS サーバ コンフィギュレーション モードを終了します。
ステップ 16	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex default-flex-profile`	新しい flex ポリシーを作成します。
ステップ 17	**local-auth radius-server-group** *server-group* 例： `Device(config-wireless-flex-profile)# local-auth radius-server-group aaa_group_name`	認証サーバグループ名を設定します。
ステップ 18	**exit** 例： `Device(config-wireless-flex-profile)# exit`	コンフィギュレーションモードに戻ります。
ステップ 19	**wireless profile policy** *policy-profile* 例： `Device(config)# wireless profile policy default-policy-profile`	WLANポリシープロファイルを設定します。
ステップ 20	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	ポリシープロファイルを無効にします。
ステップ 21	**no central authentication** 例： `Device(config-wireless-policy)# no central authentication`	中央（コントローラ）認証を無効にします。
ステップ 22	**vlan-id** *vlan-id* 例： `Device(config-wireless-policy)# vlan-id 54`	VLAN 名または VLAN ID を設定します。
ステップ 23	**no shutdown** 例：	設定をイネーブルにします。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# no shutdown`	

FlexConnect のための NAT-PAT

中央の DHCP サーバを使用してリモートサイト間でクライアントにサービスを提供する場合は、NAT-PAT を有効にする必要があります。

AP は、クライアントから着信するトラフィックを変換し、クライアントの IP アドレスを自身の IP アドレスに置き換えます。

（注） NAT と PAT を有効にするには、（**ipv4 dhcp required**）コマンドを使用して、ローカルスイッチング、中央の DHCP、および DHCP Required を有効にする必要があります。

WLAN またはリモート LAN 用の NAT-PAT の設定

WLAN の作成

WLAN を作成するには、ここに記載されている手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan wlan-demo 1 ssid-demo`	WLAN コンフィギュレーション サブモードを開始します。 • *wlan-name*：プロファイル名を入力します。入力できる範囲は英数字で 1 ～ 32 文字です。 • *wlan-id*：WLAN ID を入力します。範囲は 1 ～ 512 です。 • *SSID-name*：この WLAN に対する Service Set Identifier（SSID）を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。

	コマンドまたはアクション	目的
		（注） すでにWLANを設定している場合は、*wlan wlan-name* コマンドを入力します。
ステップ 3	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をシャットダウンします。
ステップ 4	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ワイヤレス プロファイル ポリシーと NAT-PAT の設定

ワイヤレス プロファイル ポリシーと NAT-PAT を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy nat-enabled-policy`	NAT のポリシープロファイルを設定します。
ステップ 3	**no central switching** 例： `Device(config-wireless-policy)# no central switching`	WLAN をローカルスイッチング用に設定します。
ステップ 4	**ipv4 dhcp required** 例： `Device(config-wireless-policy)# ipv4 dhcp required`	WLAN の DHCP パラメータを設定します。
ステップ 5	**central dhcp** 例： `Device(config-wireless-policy)# central dhcp`	ローカルにスイッチされるクライアントの中央 DHCP を設定します。

	コマンドまたはアクション	目的
ステップ 6	**flex nat-pat** 例： `Device(config-wireless-policy)# flex nat-pat`	NAT-PAT を有効にします。
ステップ 7	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ポリシープロファイルを有効にします。
ステップ 8	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシープロファイルへの WLAN のマッピング

WLAN をポリシープロファイルにマッピングするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy demo-tag`	ポリシータグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device(config-policy-tag)# wlan wlan-demo policy nat-enabled-policy`	ポリシープロファイルを WLAN プロファイルにマッピングします。
ステップ 4	**end** 例： `Device(config-policy-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

サイトタグの設定

サイトタグを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site flex-site`	サイトタグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**no local-site** 例： `Device(config-site-tag)# no local-site`	アクセスポイントを FlexConnect モードに移行します。
ステップ 4	**end** 例： `Device(config-site-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

アクセスポイントへのポリシータグとサイトタグの付加

ポリシータグとサイトタグをアクセスポイントに付加するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap** *mac-address* 例： `Device(config)# ap F866.F267.7DFB`	Cisco AP を設定し、ap-tag コンフィギュレーション モードを開始します。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag demo-tag`	ポリシータグを AP にマッピングします。
ステップ 4	**site-tag** *site-tag-name* 例： `Device(config-ap-tag)# site-tag flex-site`	サイトタグを AP にマッピングします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-ap-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

FlexConnect のスプリットトンネリング

中央でスイッチされる WLAN に関連付けられた WAN リンクに接続するクライアントが、ローカルサイトに存在するデバイスにトラフィックを送信する必要がある場合は、そのトラフィックを CAPWAP 経由でコントローラに送信する必要があります。すると、同じトラフィックが CAPWAP 経由で、または何らかの帯域外の接続を利用してローカルサイトに送り返されます。

このプロセスでは WAN リンクの帯域幅が無駄に消費されます。この問題を回避するため、スプリットトンネリング機能を使用できます。これは、クライアントから送信されるトラフィックをパケットの内容に基づいて分類できるようにする機能です。一致するパケットはローカルでスイッチされ、残りのトラフィックは中央でスイッチされます。ローカルサイトに存在するデバイスの IP アドレスと一致するクライアントによって送信されるトラフィックを、ローカルでスイッチされるトラフィックとして分類し、残りのトラフィックを中央でスイッチされるトラフィックとして分類できます。

AP でローカルのスプリットトンネリングを設定するには、（**ipv4 dhcp required**）コマンドを使用して、WLAN で DCHP Required が有効になっていることを確認します。これにより、スプリット WLAN に関連付けられているクライアントが DHCP を使用できるようになります。

WLAN またはリモート LAN 用のスプリットトンネリングの設定

スプリットトンネリング用のアクセス コントロール リストの定義

スプリットトンネリング用のアクセス コントロール リスト（ACL）を定義するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ip access-list extended** *name* 例： `Device(config)# ip access-list extended split_mac_acl`	名前を使用して拡張 IPv4 アクセスリストを定義し、アクセス リスト コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**deny ip any host** *hostname* 例： `Device(config-ext-nacl)# deny ip any host 9.9.2.21`	トラフィックを中央でスイッチングできるようにします。
ステップ 4	**permit ip any any** 例： `Device(config-ext-nacl)# permit ip any any`	トラフィックをローカルでスイッチングできるようにします。
ステップ 5	**end** 例： `Device(config-ext-nacl)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

定義済み ACL への ACL ポリシーのリンク

定義した ACL に ACL ポリシーをリンクするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex flex-profile`	flex プロファイルを設定し、flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**acl-policy** *acl policy name* 例： `Device(config-wireless-flex-profile)# acl-policy split_mac_acl`	ACL ポリシーを、定義した ACL 用に設定します。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

WLAN の作成

WLAN を作成するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan wlan-demo 1 ssid-demo`	WLAN の名前と ID を指定します。 • *wlan-name*：プロファイル名を入力します。入力できる範囲は英数字で 1 ～ 32 文字です。 • *wlan-id*：WLAN ID を入力します。範囲は 1 ～ 512 です。 • *SSID-name*：この WLAN に対する Service Set Identifier（SSID）を入力します。SSID を指定しない場合、WLAN プロファイル名は SSID として設定されます。
ステップ 3	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 4	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ワイヤレス プロファイル ポリシーとスプリット MAC ACL 名の設定

ワイヤレス プロファイル ポリシーとスプリット MAC ACL 名を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy split-tunnel-enabled-policy`	WLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**flex split-mac-acl** *split-mac-acl-name* 例： `Device(config-wireless-policy)# flex split-mac-acl split_mac_acl`	スプリットMAC ACL名を設定します。 （注） flex とポリシープロファイルのリンクには、同じACL名を使用する必要があります。
ステップ 4	**central switching** 例： `Device(config-wireless-policy)# central switching`	WLAN を中央スイッチング用に設定します。
ステップ 5	**central dhcp** 例： `Device(config-wireless-policy)# central dhcp`	中央でスイッチされるクライアント用に中央の DHCP を有効にします。
ステップ 6	**ipv4 dhcp required** 例： `Device(config-wireless-policy)# ipv4 dhcp required`	WLAN の DHCP パラメータを設定します。
ステップ 7	**ipv4 dhcp server** *ip_address* 例： `Device(config-wireless-policy)# ipv4 dhcp server 9.1.0.100`	DHCP サーバのオーバーライド IP アドレスを設定します。
ステップ 8	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ポリシープロファイルを有効にします。

ポリシープロファイルへの WLAN のマッピング

WLAN をポリシープロファイルにマッピングするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy split-tunnel-enabled-tag`	ポリシータグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device(config-policy-tag)# wlan wlan-demo policy split-tunnel-enabled-policy`	ポリシープロファイルを WLAN プロファイルにマッピングします。
ステップ 4	**end** 例： `Device(config-policy-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

サイト タグの設定

サイトタグを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site flex-site`	サイトタグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**no local-site** 例： `Device(config-site-tag)# no local-site`	**Local site** はサイトタグでは設定しません。
ステップ 4	**flex-profile** *flex-profile-name* 例： `Device(config-site-tag)# flex-profile flex-profile`	flex プロファイルを設定します。
ステップ 5	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config-site-tag)# end`	ンフィギュレーション モードを終了できます。

アクセスポイントへのポリシータグとサイトタグの付加

ポリシータグとサイトタグをアクセスポイントに付加するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap** *ethernet-mac-address* 例： `Device(config)# ap 188b.9dbe.6eac`	APを設定し、APタグ コンフィギュレーション モードを開始します。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag split-tunnel-enabled-tag`	ポリシータグを AP にマッピングします。
ステップ 4	**site-tag** *site-tag-name* 例： `Device(config-ap-tag)# site-tag flex-site`	サイトタグをAPにマッピングします。
ステップ 5	**end** 例： `Device(config-ap-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

VLAN ベースの FlexConnect 用中央スイッチング

FlexConnectローカルスイッチングでは、VLAN定義がアクセスポイントで使用できない場合、対応するクライアントはトラフィックを通過させません。このシナリオは、AAA サーバがクライアント認証の一部として VLAN を返す場合に適用されます。

WLAN が flex でローカルにスイッチングされ、AP 側で VLAN が設定されている場合、トラフィックはローカルにスイッチングされます。AP で VLAN が定義されていない場合、VLAN はパケットをドロップします。

VLAN0 ベースの中央スイッチングが有効になっている場合、対応する AP はトンネリングを通じてトラフィックをコントローラに送り返します。その後、コントローラはトラフィックを対応する VLAN に転送します。

VLAN ベースの中央スイッチングの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞を選択します。

ステップ 2 ポリシープロファイルの名前をクリックします。

ステップ 3 [Edit Policy Profile] ウィンドウで、次のタスクを実行します。

a) [Central Switching] を [Disabled] 状態に設定します。

b) [Central DHCP] を [Disabled] 状態に設定します。

c) [Central Authentication] を [Enabled] 状態に設定します。

ステップ 4 [Advanced] タブをクリックします。

ステップ 5 [AAA Policy] で、[Allow AAA Override] チェックボックスをオンにして、AAA オーバーライドを有効にします。

ステップ 6 [WLAN Flex Policy] で、[VLAN Central Switching] チェックボックスをオンにして、ポリシープロファイルで VLAN ベースの中央スイッチングを有効にします。

ステップ 7 [Update & Apply to Device] をクリックします。

VLAN ベースの中央スイッチングの設定（CLI）

VLAN ベースの中央スイッチングを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	ワイヤレス ポリシー プロファイルを設定します。
ステップ 3	**no central switching** 例：	WLAN をローカルスイッチング用に設定します。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# no central switching`	
ステップ 4	**no central dhcp** 例： `Device(config-wireless-policy)# no central dhcp`	ローカル DHCP モードを設定します。このモードでは、DHCP が AP で実行されます。
ステップ 5	**central authentication** 例： `Device(config-wireless-policy)# central authentication`	WLAN を中央認証用に設定します。
ステップ 6	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA ポリシーのオーバーライドを設定します。
ステップ 7	**flex vlan-central-switching** 例： `Device(config-wireless-policy)# flex vlan-central-switching`	VLANベースの中央スイッチングを設定します。
ステップ 8	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。
ステップ 9	**show wireless profile policy detailed** *default-policy-profile* 例： `Device# show wireless profile policy detailed default-policy-profile`	（任意）ポリシープロファイルの詳細情報を表示します。

FlexConnect の OfficeExtend アクセスポイント

Cisco OfficeExtend アクセス ポイント（OEAP）は、コントローラからリモートロケーションの Cisco AP へのセキュア通信を提供して、インターネットを通じて会社の WLAN を従業員の自宅にシームレスに拡張します。ホームオフィスにおけるユーザの使用感は、会社のオフィスとまったく同じです。アクセスポイントとコントローラの間の Datagram Transport Layer Security（DTLS）による暗号化は、すべての通信のセキュリティを最高レベルにします。

（注） コントローラ IP を、OEAP を使用したゼロタッチ展開用に事前に構成してください。他のすべてのホームユーザは、AP からローカル SSID を設定することで、同じアクセスポイントを使用して自宅用に接続できます。

OfficeExtend アクセスポイントの設定

OfficeExtend アクセスポイントを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *flex-profile-name* 例： `Device(config)# wireless profile flex test`	ワイヤレス flex プロファイルを設定し、ワイヤレス flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**office-extend** 例： `Device(config-wireless-flex-profile)# office-extend`	Flexconnect AP の OfficeExtend AP モードを有効にします。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 （注） flex プロファイルを作成した後、OEAP が flex connect モードであり、対応するサイトタグにマッピングされていることを確認します。 OfficeExtend は、デフォルトでは無効になっています。アクセスポイントの設定をクリアして工場出荷時のデフォルト設定に戻す場合は、コマンド Device# **clear ap config** *cisco-ap* を入力します。

OfficeExtend アクセスポイントの無効化

OfficeExtend アクセスポイントを無効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *flex-profile-name* 例： `Device(config)# wireless profile flex test`	ワイヤレス flex プロファイルを設定し、ワイヤレス flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**no office-extend** 例： `Device(config-wireless-flex-profile)# no office-extend`	Flexconnect AP の OfficeExtend AP モードを無効にします。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

OfficeExtend アクセスポイントからの個人用 SSID のクリア

アクセスポイントから個人用 SSID をクリアするには、次のコマンドを実行します。

ap name *Cisco_AP* **clear-personal-ssid**

例：OfficeExtend 設定の表示

次に、OfficeExtend 設定を表示する例を示します。

```
Device# show ap config general

Cisco AP Name   : ap_name
================================================

Cisco AP Identifier                              : 70db.986d.a860
Country Code                                     : Multiple Countries : US,IN
Regulatory Domain Allowed by Country             : 802.11bg:-A   802.11a:-ABDN
AP Country Code                                  : US  - United States
AP Regulatory Domain
  Slot 0                                         : -A
  Slot 1                                         : -D
MAC Address                                      : 002c.c899.7b84
```

```
IP Address Configuration                        : DHCP
IP Address                                      : 9.9.48.51
IP Netmask                                      : 255.255.255.0
Gateway IP Address                              : 9.9.48.1
CAPWAP Path MTU                                 : 1485
Telnet State                                    : Disabled
SSH State                                       : Disabled
Jumbo MTU Status                                : Disabled
Cisco AP Location                               : default location
Site Tag Name                                   : flex-site
RF Tag Name                                     : default-rf-tag
Policy Tag Name                                 : split-tunnel-enabled-tag
AP join Profile                                 : default-ap-profile
Primary Cisco Controller Name                   : uname-controller
Primary Cisco Controller IP Address             : 9.9.48.34
Secondary Cisco Controller Name                 : uname-controller1
Secondary Cisco Controller IP Address           : 0.0.0.0
Tertiary Cisco Controller Name                  : uname-ewlc2
Tertiary Cisco Controller IP Address            : 0.0.0.0
Administrative State                            : Enabled
Operation State                                 : Registered
AP Mode                                         : FlexConnect
AP Submode                                      : Not Configured
Office Extend Mode                              : Enabled
Remote AP Debug                                 : Disabled
Logging Trap Severity Level                     : information
Software Version                                : 16.8.1.1
Boot Version                                    : 1.1.2.4
Mini IOS Version                                : 0.0.0.0
Stats Reporting Period                          : 0
LED State                                       : Enabled
PoE Pre-Standard Switch                         : Disabled
PoE Power Injector MAC Address                  : Disabled
Power Type/Mode                                 : PoE/Full Power (normal mode)
```

プロシキ ARP

プロキシ ARP は、他のルートを学習する場合の最も一般的な方法です。プロキシ ARP を使用すると、ルーティング情報を持たないイーサネットホストと、他のネットワークまたはサブネット上のホストとの通信が可能になります。このホストでは、すべてのホストが同じローカルイーサネット上にあり、ARP を使用して MAC アドレスを学習すると想定されています。Deviceが送信元と異なるネットワーク上にあるホストに宛てたARP要求を受信した場合、Deviceはそのホストへの最適なルートがあるかどうかを調べます。最適なルートがある場合、デバイスは自身のイーサネットMACアドレスが格納されたARP応答パケットを送信します。要求の送信元ホストはパケットをDeviceに送信し、スイッチは目的のホストにパケットを転送します。プロキシ ARP は、すべてのネットワークをローカルな場合と同様に処理し、IP アドレスごとに ARP 要求を実行します。

AP は ARP プロキシとして動作し、ワイヤレスクライアントの代わりに ARP 要求に応答します。

FlexConnect AP 用のプロキシ ARP の有効化

FlexConnect AP 用にプロキシ ARP を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *flex-policy* 例： `Device(config)# wireless profile flex flex-test`	WLANポリシープロファイルを設定し、ワイヤレス flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**arp-caching** 例： `Device(config-wireless-flex-profile)# arp-caching`	ARP キャッシングを有効にします。 （注） ARP キャッシングを無効にするには、**no arp-caching** コマンドを使用します。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config | section wireless profile flex** 例： `Device# show running-config | section wireless profile flex`	ARP 設定情報を表示します。
ステップ 6	**show wireless profile flex detailed** *flex-profile-name* 例： `Device# show wireless profile flex detailed flex-test`	（任意）flexプロファイルの詳細情報を表示します。
ステップ 7	**show arp summary** 例： `Device# show arp summary`	（任意）ARPのサマリーを表示します。

合法的傍受

トラフィックの合法的傍受

シスコのワイヤレス ソリューションを使用すると、モニタリングを目的としてトラフィックの流れを合法的に傍受することが可能です。

シスコの AP がトラフィックに関する syslog レコードを作成し、そのレコードをコントローラに送信します。IPv4プロトコルと IPv6プロトコルの両方からのトラフィックが記録されます。AP は、設定された間隔で syslog レコードをコントローラに送信し、コントローラはそれらのレコードを AP から受信するとすぐに syslog サーバに転送します。

トラフィックの合法的傍受の制限

- IPv6 プロトコルをサポートするには、コントローラで IPv6 を有効にします。
- この機能は、Flex + Bridge モードで動作している Cisco Wave 2 AP と、Flex モードで動作している Cisco Wave 2 AP でサポートされます。
- Cisco Wave 2 AP をサポートします。

合法的傍受の設定

デフォルトでは、**lawful-interception** コマンドは無効になっています。コマンドを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**Configure Terminal** 例： `Device# 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	**wireless lawful-interception host** {*ipv4 addr* | *ipv6 addr*} 例： `Device(config)# wireless lawful-interception host X:X:X:X::X`	コントローラで lawful-interception を有効にし、LI サーバの IP アドレスを設定します（IPv4 および IPv6 ホスト）。
ステップ 3	**ap profile** <*ap-profile-name*> 例： `Device(config)# ap profile ap-profile-name`	AP プロファイルを設定します。

	コマンドまたはアクション	目的
ステップ 4	**[no] lawful-interception** 例： `Device(config-ap-profile)# [no] lawful-interception`	合法的傍受機能を有効にします。この機能を無効にするには、このコマンドの**no**形式を使用します。デフォルトでは、合法的傍受機能は無効になっています。
ステップ 5	**lawful-interception timer** *timer-value* 例： `Device(config-ap-profile)#lawful-interception timer 70`	合法的傍受のレポート間隔を秒単位で設定します。デフォルトでは、タイマーは 60 秒です。

合法的傍受のステータスの確認

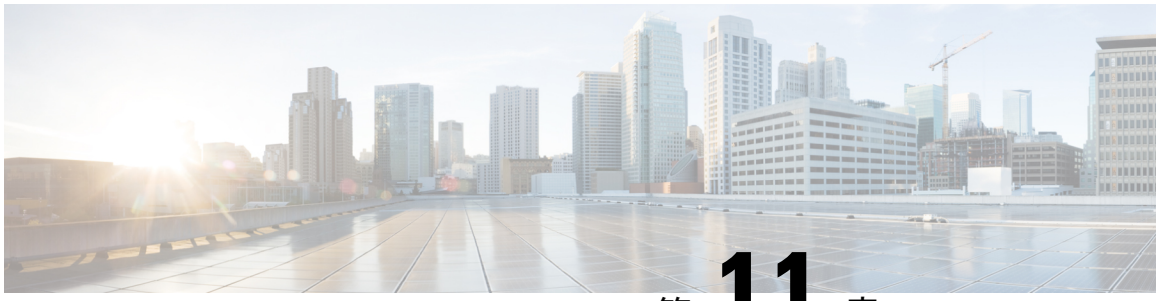
合法的傍受のステータスを確認するには、次の **show** コマンドを使用します。

```
Device#show wireless lawful-interception status
-------------------------------------------
Number AP profiles with LI enabled:     1
-------------------------------------------
Last Nexthop MAC address resolution state: Resolved
SRC IP address:             9.9.71.51
LI host IP address:         9.9.71.98
Ingress SRC MAC address:    0000.0002.0001
Egress SRC MAC address:     001e.7a9a.e9ff
Nexthop MAC address:        0050.56a0.80f4

--------------------------
LI Internal Data
--------------------------
Egress Vlan:     9
Plumb Ifid:      4026531841
Recent LI history (most recent on top):
Timestamp                          Event                          Context
-------------------------   -------------------------
---------------------------------06/21/2018 12:47:05.594163     NH_MAC_ADDR_RESULT
    next_hop mac:0050.56a0.80f4
06/21/2018 12:47:05.594081     CPP_PLUMB                  egress src
mac:001e.7a9a.e9ff,vlan:9
06/21/2018 12:47:05.593739     NH_MAC_ADDR_RESULT         next_hop mac:0050.56a0.80f4
06/21/2018 12:47:05.590337     CPP_UNPLUMB                egress src
mac:001e.7a9a.e9ff,vlan:9
06/21/2018 12:47:01.561553     NH_MAC_ADDR_RESULT         next_hop mac:0050.56a0.80f4
06/21/2018 12:47:01.555291     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
9.9.71.98
06/21/2018 12:47:01.555060     MGMT_IF_CHANGE

06/21/2018 12:47:00.618530     CPP_PLUMB                  egress src
mac:001e.7a9a.e9ff,vlan:9
06/21/2018 12:47:00.607985     MAGIC_MAC_RESOLVED         0000.0002.0001
06/21/2018 12:47:00.607290     MAGIC_MAC_REQ

06/21/2018 12:47:00.606344     NH_MAC_ADDR_RESULT         next_hop mac:0050.56a0.80f4
06/21/2018 12:47:00.601806     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
9.9.71.98
06/21/2018 12:47:00.600603     MGMT_IF_CHANGE

06/21/2018 12:46:55.847387     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
```

```
9.9.71.98
06/21/2018 12:46:55.847094     MGMT_IF_CHANGE

06/21/2018 12:46:54.937173     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
9.9.71.98
06/21/2018 12:46:54.936310     MGMT_IF_CHANGE

06/21/2018 12:46:53.186883     NH_MAC_ADDR_SUBSCRIBE      src IP: 9.9.71.51,dst IP:
9.9.71.98
06/21/2018 12:46:53.134721     MGMT_IF_CHANGE

06/21/2018 12:46:52.965403     MGMT_IF_CHANGE
```

特定の AP で合法的傍受が有効になっているかどうかを確認するには、次の **show** コマンドを使用します。

```
show ap name <ap_name> config general | include Lawful-Interception
Lawful-Interception Admin status               : Enabled
Lawful-Interception Oper status                : Enabled
```



第 11 章

データ DTLS

データ Datagram Transport Layer Security について

Datagram Transport Layer Security（DTLS）により、DTLS を使用してアクセスポイントとコントローラ間で送信される CAPWAP データパケットを暗号化できます。これは、TLS に基づいて制御パケットとデータパケットの両方を暗号化できる標準トラック IETF プロトコルです。CAPWAP 制御パケットは、コントローラとアクセスポイント間で交換される管理パケットです。一方、CAPWAPデータパケットは、転送された無線フレームをカプセル化するものです。CAPWAP コントロールおよびデータパケットはそれぞれ異なる UDP ポートである 5246（コントロール）および 5247（データ）で送信されます。

アクセスポイントが DTLS データ暗号化をサポートしない場合、DTLS はコントロールプレーンにのみ有効となり、データプレーンの DTLS セッションは確立されません。

アクセスポイントがデータ DTLS をサポートしている場合は、コントローラから新しい設定を受信した後にデータ DTLS を有効にします。アクセスポイントは、ポート5247でDTLS ハンドシェイクを実行し、ハンドシェイクが成功すると DTLS セッションを確立します。すべてのデータトラフィック（アクセスポイントからコントローラへの、およびコントローラからアクセスポイントへの）が暗号化されます。

データ DTLS の設定（GUI）

コントローラ上のアクセスポイントのDTLSデータ暗号化を有効にするには、次の手順に従います。

手順

ステップ 1 [Configuration] > [Tags and Profile] > [AP Join] > > をクリックします。

ステップ 2 [Add] をクリックして新しい [AP Join Profile] を作成するか、既存のプロファイルをクリックして編集します。

ステップ 3 [CAPWAP] > [Advanced] > をクリックします。

ステップ 4 Datagram Transport Layer Security（DTLS）データ暗号化を有効にするには、[Enable Data Encryption] チェックボックスをオンにします。

ステップ 5 [Update & Apply to Device] をクリックします。

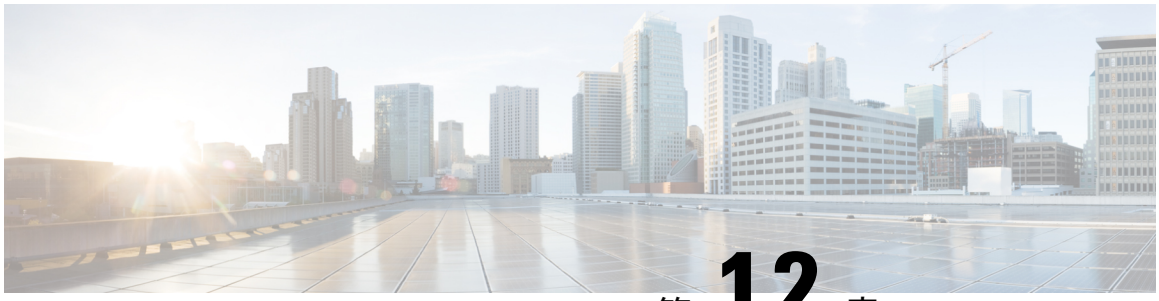
データ DTLS の設定（CLI）

コントローラ上のアクセスポイントのDTLSデータ暗号化を有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *ap-profile* 例： `Device(config)# ap profile test-ap-profile`	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。 （注） 例に示すように、デフォルトの AP プロファイル（default-ap-profile）を使用するか、または名前付き AP プロファイルを作成できます。
ステップ 3	**link-encryption** 例： `Device(config-ap-profile)# link-encryption`	プロファイルに基づいてリンク暗号化を有効にします。システムから次のメッセージが表示されたら、[Yes] で応答します。 `Enabling link-encryption will reboot the APs with link-encryption.` `Are you sure you want to continue? (y/n)[y]:`
ステップ 4	**end** 例： `Device(config-ap-profile)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show wireless dtls connections** 例： `Device# show wireless dtls connections`	（任意）このコントローラに join した AP に対して確立された DTLS セッションを表示します。
ステップ 6	**show ap link-encryption** 例： `Device# show ap link-encryption`	（任意）AP から受信したリンク暗号化関連の統計情報（リンク暗号化が有効か無効か）のカウンタを表示します。



第 12 章

自律アクセスポイントの Lightweight モードへの変換

自律アクセスポイントの Lightweight モードへの変換に関するガイドライン

- Lightweight モードに変換したアクセスポイントは、無線ドメインサービス（WDS）をサポートしません。変換したアクセスポイントは、Cisco ワイヤレス LAN device とのみ通信し、WDS デバイスとは通信できません。ただし、アクセスポイントがコントローラにアソシエートする際、device が WDS に相当する機能を提供します。
- すべての Cisco Lightweight アクセスポイントでは、無線ごとに 16 の Basic Service Set Identifier（BSSID）およびアクセスポイントごとに合計 16 のワイヤレス LAN をサポートします。変換されたアクセスポイントがdeviceにアソシエートすると、アクセスポイントがアクセスポイントグループのメンバーでない限り、ID 1 ～ 16 のワイヤレス LAN のみがアクセスポイントにプッシュされます。

- Lightweightモードに変換したアクセスポイントは、DHCP、DNS、またはIPサブネットブロードキャストを使用してIPアドレスを取得し、deviceを検出する必要があります。

Lightweight モードに変換される Autonomous アクセスポイントについて

Autonomous Cisco Aironet アクセスポイントを Lightweight モードに変換できます。Lightweight モードにアクセスポイントをアップグレードすると、アクセスポイントはdeviceと通信し、deviceから設定とソフトウェアイメージを受信します。

Lightweight モードから Autonomous モードへの復帰

Autonomous アクセスポイントを Lightweight モードに変換してから、Autonomous モードをサポートするCisco IOSリリース（Cisco IOSリリース12.3(7)JA以前のリリース）をロードして、そのアクセスポイントをLightweight装置からAutonomous装置に戻すことができます。アクセスポイントがdeviceにアソシエートされている場合、deviceを使用して Cisco IOS リリースをロードできます。アクセスポイントがdeviceにアソシエートされていない場合、TFTPを使用して Cisco IOS リリースをロードできます。いずれの方法でも、ロードする Cisco IOS Release を含む TFTP サーバにアクセスポイントがアクセスできる必要があります。

DHCP オプション 43 および DHCP オプション 60 の使用

Cisco Aironet アクセスポイントは、DHCP オプション 43 に Type-Length-Value（TLV）形式を使用します。DHCP サーバは、アクセスポイントの DHCP ベンダー クラス ID（VCI）文字列に基づいてオプションを返すよう、プログラムする必要があります（DHCPオプション60）。

DHCPオプション43の設定方法については、ご使用のDHCPサーバの製品ドキュメンテーションを参照してください。『Converting Autonomous Access Points to Lightweight Mode』には、には、DHCP サーバのオプション 43 の設定手順の例が記載されています。

アクセスポイントが、サービス プロバイダー オプション AIR-OPT60-DHCP を選択して注文された場合、そのアクセスポイントの VCI 文字列は、前の表にある VCI 文字列と異なります。VCI 文字列のサフィックスはServiceProviderです。たとえば、このオプションを指定した1260は、VCI 文字列 Cisco AP c1260-ServiceProvider を返します。

（注） DHCP サーバから取得するdeviceの IP アドレスがユニキャスト IP アドレスであることを確認してください。DHCPオプション43を設定する場合は、マルチキャストアドレスとしてdeviceの IP アドレスを設定しないでください。

DHCP オプション 60 の制約事項

- Cisco Wave2 AP は、長さが最大 256 文字の文字列のみをサポートします。

（注） 文字列の長さが制限を超えると、DHCP 検出プロセス中にデフォルト値が送信されます。

変換したアクセスポイントがクラッシュ情報をDeviceに送信する方法

変換したアクセスポイントが予期せずリブートした場合、アクセスポイントではクラッシュ発生時にローカルフラッシュメモリ上にクラッシュファイルが保存されます。装置のリブート後、アクセスポイントはリブートの理由をdeviceに送信します。クラッシュにより装置がリブートした場合、deviceは既存の CAPWAP メッセージを使用してクラッシュファイルを取得し、deviceのフラッシュメモリにそれを保存します。クラッシュ情報コピーは、deviceがアクセスポイントからこれを取得した時点でアクセスポイントのフラッシュメモリから削除されます。

変換したアクセスポイントからのメモリコアダンプのアップロード

デフォルトでは、Lightweight モードに変換したアクセスポイントは、deviceにメモリコアダンプを送信しません。この項では、device GUI または CLI を使用してアクセスポイントコアダンプをアップロードする手順について説明します。

変換されたアクセスポイントの MAC アドレスの表示

コントローラが変換されたアクセス ポイントの MAC アドレスをコントローラ GUI の情報ページに表示する方法には、いくつか異なる点があります。

- [AP Summary] ウィンドウには、変換されたアクセス ポイントのイーサネット MAC アドレスのリストが、コントローラにより表示されます。
- [AP Detail] ウィンドウには、変換されたアクセス ポイントの BSS MAC アドレスとイーサネット MAC アドレスのリストが、コントローラにより表示されます。
- [Radio Summary] ページには、変換されたアクセスポイントのリストがdeviceにより無線 MAC アドレス順に表示されます。

Lightweight アクセスポイントの静的 IP アドレスの設定

DHCP サーバに IP アドレスを自動的に割り当てさせるのではなく、アクセス ポイントに IP アドレスを指定する場合は、コントローラ GUI または CLI を使用してアクセス ポイントに固定 IP アドレスを設定できます。静的 IP アドレスは、通常、AP 数の限られた導入でのみ使用されます。

固定 IP アドレスがアクセスポイントに設定されている場合は、DNS サーバとアクセスポイントが属するドメインを指定しない限り、アクセスポイントはドメインネームシステム（DNS）

解決を使用してdeviceを検出できません。device CLI または GUI のいずれかを使用して、これらのパラメータを設定できます。

（注） アクセス ポイントを設定して、アクセス ポイントの以前の DHCP アドレスが存在したサブネット上にない固定 IP アドレスを使用すると、そのアクセス ポイントはリブート後に DHCP アドレスにフォール バックします。アクセス ポイントが DHCP アドレスにフォール バックした場合は、**show ap config general** *Cisco_AP* CLI コマンドを入力すると、アクセス ポイントがフォールバック IP アドレスを使用していることが表示されます。ただし、GUI は固定 IP アドレスと DHCP アドレスの両方を表示しますが、DHCP アドレスをフォールバック アドレスであるとは識別しません。

Lightweight アクセスポイントの Autonomous アクセスポイントへの再変換方法

Lightweight アクセスポイントを Autonomous モードに戻す方法（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *Cisco_AP* **tftp-downgrade** *tftp_server_ip_address tftp_server_image_filename* 例： `Device# ap name AP02 tftp-downgrade 10.0.0.1 tsrvname`	Lightweight アクセスポイントを Autonomous モードに戻します。 （注） このコマンドを入力したら、アクセスポイントが再起動するまで待機し、CLI または GUI を使用してアクセスポイントを再設定します。

モードボタンと TFTP サーバを使用して Lightweight アクセスポイントを Autonomous モードに戻す方法

手順

ステップ 1 TFTP サーバ ソフトウェアを実行している PC に、10.0.0.2 ～ 10.0.0.30 の範囲に含まれる固定 IP アドレスを設定します。

ステップ 2 コンピュータの TFTP サーバ フォルダにアクセスポイントのイメージファイル（たとえば、1140 シリーズ アクセスポイントの場合は *c1140-k9w7-tar.123-7.JA.tar* ）が存在すること、およびその TFTP サーバがアクティブであることを確認します。

ステップ 3 TFTP サーバフォルダ内の 1140 シリーズ アクセスポイントのイメージファイルの名前を c1140-k9w7-tar.default に変更します。

ステップ 4 カテゴリ 5（CAT5）のイーサネット ケーブルを使用して、PC をアクセス ポイントに接続します。

ステップ 5 アクセス ポイントの電源を切ります。

ステップ 6 MODE ボタンを押しながら、アクセスポイントに電源を再接続します。

（注） アクセスポイントの MODE ボタンを有効にしておく必要があります。

ステップ 7 [MODE] ボタンを押し続けて、ステータス LED が赤色に変わったら（約 20 ～ 30 秒かかります）、[MODE] ボタンを放します。

ステップ 8 アクセス ポイントがリブートしてすべての LED が緑色に変わり、ステータス LED が緑色に点滅するまで待ちます。

ステップ 9 アクセス ポイントがリブートしたら、GUI または CLI を使用してアクセス ポイントを再設定します。

アクセスポイントの認可

以降の項では、アクセスポイントを許可するさまざまな方法について説明します。

ローカルデータベースを使用したアクセスポイントの許可（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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 3	**ap auth-list ap-policy authorize-ap** 例： `Device(config)# ap auth-list ap-policy authorize-ap`	アクセスポイントの許可ポリシーを設定します。
ステップ 4	**username** *user_name* **mac** ［**aaa attribute list** *list_name*］ 例： `Device(config)# username aaa.bbb.ccc mac aaa attribute list attrlist`	（任意）アクセスポイントの MAC アドレスをローカルで設定します。
ステップ 5	**aaa new-model** 例： `Device(config)# aaa new-model`	新しいアクセス コントロール コマンドと機能をイネーブルにします
ステップ 6	**aaa authorization credential-download** {*auth_list* | **default**} **local** 例： `Device(config)# aaa authorization credential-download auth_download local`	ローカルサーバから EAP 資格情報をダウンロードします。
ステップ 7	**aaa attribute list** リスト 例： `Device(config)# aaa attribute list alist`	（任意）AAA 属性リストの定義を設定します。
ステップ 8	**aaa session-id common** 例： `Device(config)# aaa session-id common`	AAA の共通セッション ID を設定します。
ステップ 9	**aaa local authentication default authorization default** 例： `Device(config)# aaa local authentication default authorization default`	（任意）ローカル認証方式リストを設定します。
ステップ 10	**end**	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 11	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP01 config general`	特定のアクセスポイントに対応する設定情報を表示します。

RADIUS サーバを使用したアクセスポイントの許可（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *server-name* 例： `Device(config)# radius server ise`	RADIUS サーバ コンフィギュレーション モードを開始します。
ステップ 4	**address** {**ipv4** | **ipv6**} *radius-server-ipv4-address-or-name* **auth-port** *udp-port-auth-server* **acct-port** *udp-port-acct-server* 例： `Device(config-radius-server)# address ipv4 224.0.0.1 auth-port 1645 acct-port 1646`	RADIUS サーバや他のサーバのパラメータを設定します。
ステップ 5	**key** *0 cisco* 例： `Device(config-radius-server)# key 0 cisco`	RADIUS 認証サーバのクリア テキストの暗号キーを設定します。
ステップ 6	**exit** 例： `Device(config-radius-server)# exit`	特権 EXEC モードに戻ります。
ステップ 7	**aaa group server radius** *server-group* 例：	RADIUS サーバ グループの定義を設定します。

	コマンドまたはアクション	目的
	`Device(config)# aaa group server radius ise-group`	（注） *server-group* はサーバグループ名です。有効な範囲は1～32文字の英数字です。
ステップ 8	**server name** *ise* 例： `Device(config-sg-radius)# server name ise`	RADIUS サーバ名を設定します。
ステップ 9	**ip radius source-interface** *vlan* 例： `Device(config-sg-radius)# ip radius source-interface vlan`	RADIUS パケットでの送信元アドレスのインターフェイスを指定します。
ステップ 10	**exit** 例： `Device(cconfig-sg-radius)# exit`	特権 EXEC モードに戻ります。
ステップ 11	**aaa authorization network default group** *default-server-group* **local** 例： `Device(config)# aaa authorization network default group ise-group local`	許可の方法をローカルに設定します。
ステップ 12	**aaa authorization credential-download default group** *default-server-group* **local** 例： `Device(config)# aaa authorization credential-download default group ise-group local`	ローカルサーバ、RADIUS サーバ、または LDAP サーバから EAP クレデンシャルをダウンロードするようにローカルデータベースを設定します。

変換したアクセスポイントでの Reset ボタンのディセーブル化（CLI）

Lightweight モードに変換したアクセスポイントの [Reset] ボタンを有効または無効にすることができます。[Reset] ボタンには、アクセスポイントの外面に「MODE」と書かれたラベルが付けられています。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**no ap reset-button** 例： `Device(config)# no ap reset-button`	deviceに関連付けられ、変換したすべてのアクセスポイントの [Reset] ボタンを無効にします。 （注） deviceに関連付けられ、変換したすべてのアクセスポイントの [Reset] ボタンを有効にするには、**ap reset-button** コマンドを入力します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**ap name** *cisco_ap* **reset-button** 例： `Device# ap name AP02 reset-button`	指定した変換済みアクセスポイントの [Reset] ボタンを有効にします。

AP クラッシュ ログ情報のモニタリング

（注） device GUI を使用してこのタスクを実行する手順は現在利用できません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**show ap crash-file** 例： `Device# show ap crash-file`	クラッシュファイルがdeviceにダウンロードされているかどうかを確認します。

アクセスポイントでの固定 IP アドレスの設定方法

アクセスポイントでの固定 IP アドレスの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *Cisco_AP* **static-ip ip-address** *static_ap_address* **netmask** *static_ip_netmask* **gateway** *static_ip_gateway* 例： `Device# ap name AP03 static-ip ip-address 9.9.9.16 netmask 255.255.0.0 gateway 9.9.9.2`	アクセスポイントの固定 IP アドレスを設定します。このコマンドには、次のキーワードと引数が含まれます。 • **ip-address**：Ciscoアクセスポイントの固定 IP アドレスを指定します。 • *ip-address*：Ciscoアクセスポイントの固定 IP アドレス。 • **netmask**：Cisco アクセスポイントの固定 IP ネットマスクを指定します。 • *netmask*：Ciscoアクセス ポイントの固定 IP ネットマスク。 • **gateway**：Cisco アクセス ポイントゲートウェイを指定します。 • *gateway*：Cisco アクセス ポイントゲートウェイの IP アドレス。 アクセスポイントがリブートしてdeviceに再 join し、指定した固定 IP アドレスがアクセスポイントにプッシュされます。固定 IP アドレスがアクセスポイントに送信された後、DNS サーバの IP ア

	コマンドまたはアクション	目的
		ドレスおよびドメイン名を設定できます。アクセスポイントのリブート後にステップ 3 とステップ 4 を実行します。
ステップ 3	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 4	**configure terminal** 例： `Device# 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 5	**ap static-ip name-server** *nameserver_ip_address* 例： `Device(config)# ap static-ip name-server 10.10.10.205`	特定のアクセスポイントまたはすべてのアクセスポイントが DNS 解決を使用してdeviceを検出できるよう DNS サーバを設定します。 （注） DNS サーバ設定を元に戻すには、**no ap static-ip name-server** *nameserver_ip_address* コマンドを入力します。
ステップ 6	**ap static-ip domain** *static_ip_domain* 例： `Device(config)# ap static-ip domain domain1`	特定のアクセスポイントまたはすべてのアクセスポイントが属するドメインを設定します。 （注） ドメイン名の設定を元に戻すには、**no ap static-ip domain** *static_ip_domain* コマンドを入力します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show ap name** *Cisco_AP* **config general** 例： `Device# show ap name AP03 config general`	アクセスポイントの IP アドレス設定を表示します。

アクセスポイントでの固定 IP アドレスの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [All Access Points] セクションで、 [AP Name] をクリックします。

ステップ 3 表示される [Edit AP] ウィンドウで、[IP Config] セクションに移動します。

ステップ 4 [Static IP (IPv4/IPv6)] チェックボックスをオンにします。これでスタティック IP の詳細ペインがアクティブになります。

ステップ 5 [Static IP]、[Netmask]、[Gateway]、[DNS IP Address] を入力します。

ステップ 6 [Update & Apply to Device] をクリックします。

TFTPリカバリ手順を使用したアクセスポイントのリカバリ

手順

ステップ 1 必要なリカバリイメージを Cisco.com（ap3g2-k9w8-tar.152-2.JA.tar）からダウンロードし、ご利用の TFTP サーバのルートディレクトリにインストールします。

ステップ 2 TFTP サーバをターゲットのアクセスポイントと同じサブネットに接続して、アクセス ポイントをパワーサイクリングします。アクセスポイントは TFTP イメージから起動し、次にdeviceにジョインしてサイズの大きなアクセスポイントのイメージをダウンロードし、アップグレード手順を完了します。

ステップ 3 アクセスポイントが回復したら、TFTP サーバを削除できます。

Autonomous アクセスポイントを Lightweight モードに変換する場合の設定例

例：アクセスポイントの IP アドレス設定の表示

次に、アクセスポイントの IP アドレス設定を表示する例を示します。

```
Device# show ap name AP03 dot11 24ghz config general
Cisco AP Identifier.............. 4
Cisco AP Name.................... AP6
IP Address Configuration..................... Static IP assigned
IP Address.................................... 10.10.10.118
IP NetMask.................................... 255.255.255.0
Gateway IP Addr............................... 10.10.10.1
Domain........................................ Domain1
Name Server................................... 10.10.10.205
...
```

例：アクセスポイントのクラッシュファイル情報の表示

次の例は、アクセスポイントのクラッシュファイル情報を表示する方法を示しています。このコマンドを使用して、ファイルがdeviceにダウンロードされたかどうかを確認できます。

```
Device# show ap crash-file
Local Core Files:
lrad_AP1130.rdump0 (156)

The number in parentheses indicates the size of the file. The size should
be greater than zero if a core dump file is available.
```

AP MAC 許可

AP 許可ポリシー機能により、許可された AP のみがコントローラにとの関連付けを行えるようになります。AP を許可するには、AP のイーサネット MAC アドレスを登録する必要があります。登録は、コントローラまたは外部 RADIUS サーバでローカルに行うことができます。

AP MAC 許可の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**[no] ap auth-list ap-policy authorize-ap** *profile-name* 例： `Device(config)# ap auth-list ap-policy authorize-ap`	AP 許可ポリシーを設定します。
ステップ 3	**end** 例：	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config)# end`	
ステップ 4	**show ap auth-list** *value-in-dBm* 例： `Device# show ap auth-list`	AP MAC 許可のステータスを表示します。

設定例

1. ローカルデータベース設定：

```
Device(config)# aaa authorization network default local
Device(config)# aaa authorization credential-download default local
```

2. ユーザ名設定：

```
Device(config)# username e4c72281151a mac
```

ユーザ名は AP のイーサネット MAC アドレスであり、AP がコントローラに関連付けられる前に許可されます。AP のイーサネット MAC アドレスには英数字を使用できます。文字は小文字で指定する必要があります。スペースまたは特殊文字は使用できません。AP のイーサネット MAC アドレスを取得するには、**show ap summary** コマンドを使用します。

アクセスポイントでのイーサネット VLAN タギング

アクセスポイントでのイーサネット VLAN タギングについて

AP コンソールのまたはコントローラから直接イーサネット インターフェイスで VLAN タギングを設定できます。設定はフラッシュメモリに保存され、ローカルにスイッチングされるすべてのトラフィックとともに、すべての CAPWAP フレームは設定されるように VLAN タグを使用し、VLAN にはマッピングされていません。

アクセス ポイントでのイーサネット VLAN タギングの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。

ステップ 2 AP join プロファイルの名前をクリックするか、[Add] をクリックして新しい AP join プロファイルを作成します。

ステップ 3 表示される [Add/Edit AP Join Profile] ウィンドウで、[CAPWAP] タブをクリックし、[Advanced] タブをクリックします。

ステップ 4 [Enable VLAN Tagging] チェックボックスをオンにして、AP join プロファイルの VLAN タギングを有効にします。

ステップ 5 [Update & Apply to Device] をクリックします。

アクセスポイントでのイーサネット VLAN タギングの設定（CLI）

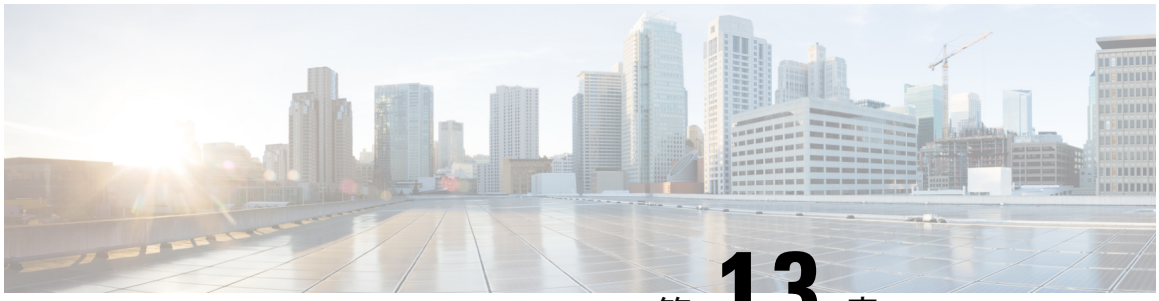
AP でイーサネット VLAN タギングを設定するには、次の手順に従います。

始める前に

- ブリッジモードの MAP では、VLAN タギングはサポートされていません。AP がブリッジモードに設定されている場合、この機能は自動的に無効になります。
- VLAN タグ付けが有効になっている場合、flex ネイティブ VLAN ID を AP 用に設定することはできません。
- AP がフェールオーバー中にワイヤレスコントローラの検出に失敗した場合、FlexConnect スタンドアロンモードの AP（VLAN タグが有効になっている）が 10 分ごとにリロードされることがあります。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name* **vlan-tag** *vlan-id* **例**： `Device# ap name AP1 vlan-tag 12` `Device# ap name AP1 no vlan-tag`	非ブリッジ AP の VLAN タギングを設定します。設定をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 2	**ap vlan-tag** *vlan-id* **例**： `Device# ap vlan-tag 1000` `Device# ap no vlan-tag`	すべての非ブリッジ AP の VLAN タギングを設定します。設定をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**show ap config general** **例**： `Device# show ap config general`	（任意）すべての AP に共通の情報を表示します。



第 13 章

AP クラッシュ ファイルのアップロード

AP クラッシュ ファイルのアップロード

変換したアクセス ポイントが予期せずリブートした場合、アクセス ポイントではクラッシュ発生時にローカル フラッシュ メモリ上にクラッシュ ファイルが保存されます。装置のリブート後、リブートの理由がアクセス ポイントからデバイスに送信されます。クラッシュにより装置がリブートした場合、デバイスは既存の CAPWAP メッセージを使用してクラッシュ ファイルを取得し、デバイスのフラッシュ メモリに保存します。クラッシュ情報のコピーは、デバイスがアクセス ポイントから取得した時点でアクセス ポイントのフラッシュ メモリから削除されます。

- デバイス障害の場合：システム レポートは障害が発生したメンバーで生成されます。スタック内の他のメンバーではレポートは生成されません。
- スイッチオーバーの場合：システム レポートはハイ アベイラビリティ（HA）のメンバー スイッチでのみ生成されます。非 HA メンバーについてはレポートは生成されません。

（注） リロード時はレポートは生成されません。

プロセスのクラッシュ時には、次の情報がデバイスからローカルに収集されます。

- 完全なプロセスコア
- トレースログ
- Cisco IOS の syslog（非アクティブなクラッシュの場合には保証されません）
- システムプロセス情報
- ブートアップログ
- リロードログ

- 特定のタイプの /proc 情報

これらの情報はすべて、個別のファイルに格納された後、アーカイブされて1つのバンドルに圧縮されます。これにより、クラッシュのスナップショットを1つの場所で取得して、分析のためにボックス外に移動できるようになります。このレポートは、スイッチがROMMON/ブートローダにダウンする前に生成されます。

（注） 完全なコアおよびトレースログ以外はテキストファイルです。

crashinfo ファイル

デフォルトでは、システムレポートファイルが生成されて /crashinfo ディレクトリに保存されます。容量不足のためにcrashinfoファイルのパーティションに保存できない場合は、/flashディレクトリに保存されます。

ファイルを表示するには、**dir crashinfo:** コマンドを入力します。次に、crashinfoディレクトリの出力例を示します。

```
Switch#dir crashinfo:
Directory of crashinfo:/
46553 drwx 1024 Jun 29 2015 14:52:09 +00:00 ap_crash
12 -rw- 0 Jan 1 1970 00:00:11 +00:00 koops.dat
11 -rw- 0 Mar 22 2013 07:50:30 +00:00 deleted_crash_files
13 -rwx 594269 Mar 22 2013 07:50:30 +00:00 crashinfo_platform_mgr_20130322-075017-UTC
14 -rw- 44 Sep 9 2015 09:28:47 +00:00 last_crashinfo
15 -rw- 355 Sep 9 2015 09:29:31 +00:00 last_systemreport_log
16 -rw- 105753 Mar 22 2013 07:50:47 +00:00 system-report_1_20130322-075017-UTC.gz
17 -rw- 39 Sep 9 2015 09:29:31 +00:00 last_systemreport
18 -rwx 585996 Mar 22 2013 08:01:58 +00:00 crashinfo_platform_mgr_20130322-080144-UTC
19 -rw- 105065 Mar 22 2013 08:02:15 +00:00 system-report_1_20130322-080144-UTC.gz
20 -rwx 3426209 Sep 9 2015 06:49:12 +00:00 crashinfo_iosd_20150909-064754-UTC
21 -rwx 9540376 Sep 9 2015 06:49:13 +00:00 fullcore_iosd_20150909-064754-UTC
22 -rw- 469476 Sep 9 2015 06:49:56 +00:00 system-report_1_20150909-064754-UTC.gz
23 -rwx 3425350 Sep 9 2015 09:28:47 +00:00 crashinfo_iosd_20150909-092728-UTC
24 -rwx 9535535 Sep 9 2015 09:28:47 +00:00 fullcore_iosd_20150909-092728-UTC
25 -rw- 459709 Sep 9 2015 09:29:28 +00:00 system-report_1_20150909-092728-UTC.gz
26 -rw- 0 Sep 22 2015 11:11:33 +00:00 tracelogs.J8C

50601 drwx 10240 Oct 28 2015 22:42:50 +00:00 tracelogs

248354816 bytes total (204800000 bytes free)
```

システムレポートは、次の形式で crashinfo ディレクトリにあります。

```
system-report_[switch number]_[date]-[timestamp]-UTC.gz
```

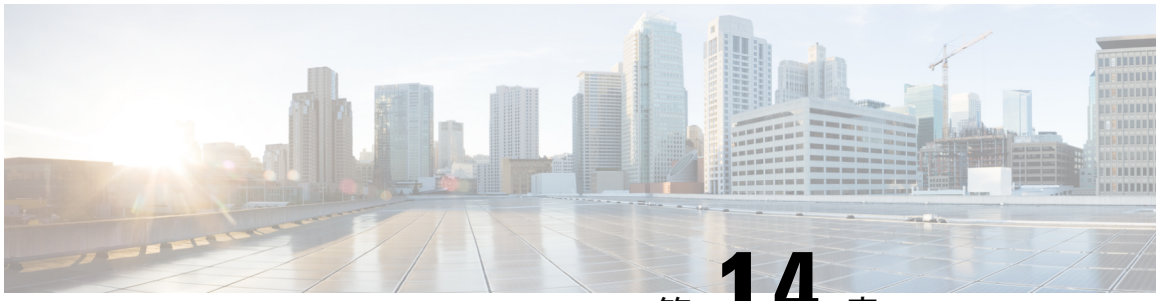
スイッチがクラッシュしたら、システムレポートファイルを確認します。最後に生成されたシステムレポートファイルは crashinfo ディレクトリの下に last_systemreport というファイル名で保存されます。システム レポートおよび crashinfo ファイルは、Technical Assistance Center が問題のトラブルシューティングを行う際に役立ちます。

（注） トレースログやその他の目的に使用できる領域を確保するため、システム レポートやトレースアーカイブはコピー後に flash ディレクトリや crashinfo ディレクトリから消去することが重要です。

AP クラッシュ ファイルのアップロードの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **crash-file get-crash-data**	AP クラッシュ情報を収集します。クラッシュ ファイルは、APがレディ状態までリロードした後に自動的にアップロードされます。したがって、このコマンドは手動で実行する必要はありません。
ステップ 3	**ap name** *ap-name* **crash-file get-radio-core-dump slot** {**0** | **1**}	スロット 0 またはスロット 1 の AP コアダンプ ファイルを収集します。
ステップ 4	**ap name** *ap-name* **core-dump** *tftp-ip crash-file* **uncompress**	指定した TFTP の場所に AP クラッシュ コアダンプ ファイルをアップロードします。
ステップ 5	**show ap crash-file** 例： `Device(config)# show ap crash-file` `Local Core Files:` `lrad_AP1130.rdump0 (156)` `The number in parentheses indicates the size of the file. The size should be greater than zero if a core dump file is available.`	クラッシュ ファイルがデバイスにダウンロードされているかどうかを確認します。



第 14 章

AP 単位の不正

AP 単位の不正

不正検出は、AP 単位で、または AP のグループに対して設定されます。不正 AP 検出は AP プロファイルの下で設定されます。デフォルトで有効になっている不正 AP 検出設定は、デフォルトの AP プロファイルの一部です。

このリリースでは、次のコマンドが廃止されました。

- **wireless wps rogue detection enable**
- **wireless wps rogue detection report-interval** *interval*
- **wireless wps rogue detection min-rssi** *rssi*
- **wireless wps rogue detection min-transient-time** *transtime*
- **wireless wps rogue detection containment flex-connect**
- **wireless wps rogue detection containment auto-rate**

不正検出の有効化

不正検出を有効にするための大まかな手順は次のとおりです。

- AP プロファイルの設定
- ワイヤレス サイト タグの定義と AP プロファイルの割り当て
- AP へのワイヤレス サイト タグの関連付け

不正検出の有効化

AP プロファイルの設定（GUI）

始める前に

デフォルトの AP join プロファイルの値には、グローバル AP パラメータと AP グループ パラメータが設定されます。AP join プロファイルには、CAPWAP IPv4/IPv6、UDP Lite、ハイ アベイラビリティ、再送信設定パラメータ、グローバル AP フェールオーバー、HyperLocation 設定パラメータ、Telnet/SSH、11u パラメータなどのパラメータが含まれています。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] を選択します。

ステップ 2 [Add] ボタンをクリックします[Add AP Join Profile] 画面が表示されます。

ステップ 3 [General] タブをクリックします。

ステップ 4 [Name] フィールドに AP join プロファイルの名前を入力し、[Description] フィールドに説明を入力します。

ステップ 5 AP を簡単に探せるように、デバイスに接続されているすべての AP の LED 状態を点滅に設定するには、[LED State] チェックボックスをオンにします。

ステップ 6 [Client] タブの [Statistics Timer] セクションに、AP が自身の 802.11 統計情報をコントローラに送信する時間を秒単位で入力します。

ステップ 7 [TCP MSS Configuration] セクションで、[Adjust MSS Enable] チェックボックスをオンにして、[Adjust MSS] の値を入力します。ルータを通過する一時的なパケットの最大セグメント サイズ（MSS）を入力または更新できます。TCP MSS の調整により、ルータを通過する一時的なパケット（特に SYN ビットが設定された TCP セグメント）の最大セグメント サイズ（MSS）を設定できます。CAPWAP 環境では、Lightweight アクセス ポイントは CAPWAP ディスカバリ メカニズムを使用してデバイスを検知してから、デバイスに CAPWAP join 要求を送信します。デバイスは、アクセス ポイントがデバイスに join することを許可する CAPWAP join 応答をアクセス ポイントに送信します。アクセス ポイントがデバイスに参加すると、デバイスによってアクセス ポイントの設定、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。アクセス ポイントがデバイスに参加すると、デバイスによってアクセス ポイントの設定、ファームウェア、制御トランザクション、およびデータ トランザクションが管理されます。

ステップ 8 [CAPWAP] タブでは次の設定が行えます。

- ハイ アベイラビリティ：すべてのアクセス ポイントのプライマリおよびセカンダリ バックアップ コントローラを、プライマリ、セカンダリ、第3、プライマリ バックアップ、セカンダリ バックアップの順序で設定できます（プライマリ、セカンダリ、または第3のコントローラが応答しない場合に使用されます）。また、ハートビート タイマーやディスカバリ要求タイマーなどのさまざまなタイマーを設定できます。コントローラの障害検出時

間を短縮するには、高速ハートビート間隔（コントローラとアクセス ポイントの間）に設定するタイムアウト値をより小さくします。高速ハートビート タイマーの期限（ハートビート間隔ごとの）を過ぎると、アクセス ポイントは最後のインターバルでコントローラからデータ パケットを受信したかどうかを判断します。パケットが何も受信されていない場合、アクセス ポイントは高速エコー要求をコントローラへ送信します。

1. [High Availability] タブで、[Fast Heartbeat Timeout] フィールドに時間（秒単位）を入力して、すべてのアクセス ポイントのハートビート タイマーを設定します。ハートビート間隔の値を小さく指定すると、デバイスの障害検出にかかる時間が短縮されます。
2. [Heartbeat Timeout] フィールドに時間（秒単位）を入力して、すべてのアクセス ポイントのハートビート タイマーを設定します。ハートビート間隔の値を小さく指定すると、デバイスの障害検出にかかる時間が短縮されます。
3. [Discovery Timeout] フィールドに 1 ～ 10 秒の範囲（両端を含む）の値を入力して、AP ディスカバリ要求タイマーを設定します。
4. [Primary Discovery Timeout] フィールドに 30 ～ 3000 秒の範囲（両端を含む）の値を入力して、アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。
5. [Primed Join Timeout] フィールドに 120 ～ 43200 秒の範囲（両端を含む）の値を入力して、アクセス ポイントのプライマリ join タイムアウトを設定します。
6. [Retransmit Timers Count] フィールドに、AP からデバイスに（またはその逆に）要求を再送信する回数を入力します。有効な範囲は、3 ～ 8 です。
7. [Retransmit Timers Interval] フィールドに、要求の再送信から次の再送信までの時間を入力します。有効な範囲は、2 ～ 5 です。
8. フォールバックを有効にするには、[Enable Fallback] チェックボックスをオンにします。
9. [Primary Controller] の名前と IP アドレスを入力します。
10. [Secondary Controller] の名前と IP アドレスを入力します。
11. [Save & Apply to Device] をクリックします。

- 高度

1. [Advanced] タブで、[Enable VLAN Tagging] チェックボックスをオンにして、VLAN のタグ付けを有効にします。
2. [Enable Data Encryption] チェックボックスをオンにして、データグラム トランスポート層セキュリティ（DTLS）データ暗号化を有効にします。
3. [Enable Jumbo MTU] をオンにして、大きい最大伝送ユニット（MTU）を有効にします。MTU とは、ネットワークが送信できる最大の物理パケット サイズのことで、バイト単位で測定されます。MTU よりも大きなメッセージは送信前に小さなパケットに分割されます。ジャンボ フレームとは、標準のイーサネット フレーム サイズである

1518 バイト（レイヤ 2（L2）ヘッダーと FCS を含む）より大きいフレームのことです。フレーム サイズの定義は IEEE 標準の一部ではないため、ベンダーによって異なります。

4. [Link Latency] ドロップダウン リストを使用して、リンク遅延を選択します。リンク遅延は、AP からコントローラ、およびコントローラから AP における CAPWAP ハートビート パケット（エコー要求および応答）のラウンドトリップ時間をモニタします。
5. [Preferred Mode] ドロップダウン リストからモードを選択します。
6. [Save & Apply to Device] をクリックします。

ステップ 9 [AP] タブでは次の設定が行えます。

- 一般

1. [General] タブで、[Switch Flag] チェックボックスをオンにしてスイッチを有効にします。
2. パワー インジェクタが使用されている場合は、[Power Injector State] チェックボックスをオンにします。パワーインジェクタにより、ローカル電源、インライン パワー対応のマルチポート スイッチ、およびマルチポート電源パッチ パネルに代替電源のオプションが提供され、AP の無線 LAN 配置の柔軟性が向上します。
3. [Power Injector Type] ドロップダウン リストで、次のオプションからパワー インジェクタ タイプを選択します。
   - [Installed]：現在接続されているスイッチ ポートの MAC アドレスを AP に調べさせ記憶させる場合に使用します（この選択は、パワーインジェクタが接続されていることを前提としています）。
   - [Override]：最初に MAC アドレスの一致を検証せずに、AP が高電力モードで稼働できるようにします。
4. [Injector Switch MAC] フィールドに、スイッチの MAC アドレスを入力します。
5. 関連する国コードを入力します。特定の運用国を国コードで指定できます（フランスは FR、スペインは ES など）。
6. [EAP Type] ドロップダウン リストから、EAP タイプとして [EAP-FAST]、[EAP-TLS]、または [EAP-PEAP] を選択します。
7. [AP Authorization Type] ドロップダウン リストから、タイプとして [CAPWAP DTLS +] または [CAPWAP DTLS] のいずれかを選択します。
8. [Client Statistics Reporting Interval] セクションに、5 GHz および 2.4 GHz の無線の間隔を秒単位で入力します。
9. 拡張モジュールを有効にするには [Enable] チェックボックスをオンにします。

10. [Profile Name] ドロップダウン リストから、メッシュのプロファイル名を選択します。
11. [Save & Apply to Device] をクリックします。

- HyperLocation：Cisco Hyperlocation は、ワイヤレス クライアントの場所を 1 メートルの精度で追跡できるロケーション ソリューションです。このオプションを選択すると、NTP サーバを除く画面内の他のすべてのフィールドが無効になります。
  1. [Hyperlocation] タブで、[Enable Hyperlocation] チェックボックスをオンにします。
  2. 低い RSSI を持つパケットを除外するには、[Detection Threshold] の値を入力します。有効な範囲は -100 ～ -50 dBmです。
  3. BAR をクライアントに送信する前のスキャン サイクルの数を設定するには、[Trigger Threshold] の値を入力します。有効な範囲は 0 ～ 99 です。
  4. トリガー後にスキャン サイクルの値をリセットするには、[Reset Threshold] の値を入力します。有効な範囲は 0 ～ 99 です。
  5. [NTP Server] の IP アドレスを入力します。
  6. [Save & Apply to Device] をクリックします。

- BLE：AP が Bluetooth Low Energy（BLE）対応の場合はビーコン メッセージを送信できます。ビーコンメッセージは、低電力リンクを介して送信されるデータまたは属性のパケットです。これらの BLE ビーコンは、ヘルス モニタリング、プロキシミティ検出、アセット トラッキング、およびストア内ナビゲーションに頻繁に使用されます。AP ごとに、すべての AP に対してグローバルに設定される BLE ビーコン設定をカスタマイズできます。
  1. [BLE] タブで、[Beacon Interval] フィールドに値を入力して、AP が近くにあるデバイスにビーコン アドバタイズメントを送出する頻度を指定します。範囲は 1 ～ 10 です。デフォルトは 1 です。
  2. [Advertised Attenuation Level] フィールドに、減衰レベルを入力します。範囲は 40 ～ 100 で、デフォルトは 59 です。
  3. [Save & Apply to Device] をクリックします。

- パケット キャプチャ：パケット キャプチャ機能では、ワイヤレス クライアントのトラブルシューティングを行うために AP 上のパケットをキャプチャできます。パケット キャプチャ操作は、指定されたパケット キャプチャ フィルタに基づいて、AP が動作している現在のチャネルの無線ドライバによって、AP 上で実行されます。
  1. [Packet Capture] タブで、ドロップダウン リストから [AP Packet Capture Profile] を選択します。
  2. または、[+] 記号をクリックして新しいプロファイルを作成することもできます。
  3. AP パケット キャプチャ プロファイルの名前および説明を入力します。
  4. [Buffer Size] を入力します。

5. [Duration] を入力します。
6. [Truncate Length] の情報を入力します。
7. [Server IP] フィールドに、TFTP サーバの IP アドレスを入力します。
8. [File Path] フィールドに、ディレクトリ パスを入力します。
9. ユーザ名とパスワードの詳細を入力します。
10. [Password Type] ドロップダウン リストから、タイプを選択します。
11. [Packet Classifiers] セクションで、オプションを使用して、キャプチャするパケットを選択または入力します。
12. [Save] をクリックします。
13. [Save & Apply to Device] をクリックします。

ステップ 10 [Management] タブでは次の設定が行えます。

- デバイス

1. [Device] タブで、TFTP サーバの [TFTP Downgrade] セクションの [IPv4/IPv6 Address] を入力します。
2. [Image File Name] フィールドに、ソフトウェア イメージ ファイルの名前を入力します。
3. [Facility Value] ドロップダウン リストから、適切な機能を選択します。
4. ホストの IPv4 または IPv6 アドレスを入力します。
5. 適切な [Log Trap Value] を選択します。
6. 必要に応じて、Telnet か SSH またはその両方の設定を有効にします。
7. 必要に応じて、コア ダンプを有効にします。
8. [Save & Apply to Device] をクリックします。

- ユーザ

1. [User] タブで、ユーザ名とパスワードの詳細を入力します。
2. 適切なパスワード タイプを選択します。
3. [Secret] フィールドに、カスタムのシークレット コードを入力します。
4. 適切なシークレット タイプを選択します。
5. 適切な暗号化タイプを選択します。
6. [Save & Apply to Device] をクリックします。

- クレデンシャル

  1. [Credentials] タブで、ローカルのユーザ名とパスワードの詳細を入力します。
  2. 適切なローカル パスワード タイプを選択します。
  3. 802.1x ユーザ名とパスワードの詳細を入力します。
  4. 適切な 802.1x パスワード タイプを選択します。
  5. セッションが期限切れになるまでの時間を秒単位で入力します。
  6. 必要に応じて、ローカル クレデンシャルや 802.1 x クレデンシャルを有効にします。
  7. [Save & Apply to Device] をクリックします。

- CDP インターフェイス

  1. [CDP Interface] タブで、必要に応じて CDP の状態を有効にします。
  2. グループ NAS ID を入力します。RADIUS サーバがカスタマイズされた認証応答を送信できるように、異なるグループにユーザを分類する認証要求を介して、コントローラによって RADIUS サーバに Network Access Server identifier（NAS-ID）が送信されます。
  3. [Save & Apply to Device] をクリックします。

ステップ 11 不正検出を有効にするには、[Rogue AP] タブで [Rogue Detection] チェックボックスをオンにします。

ステップ 12 [Rogue Detection Minimum RSSI] フィールドに、RSSI 値を入力します。

ステップ 13 [Rogue Detection Transient Interval] フィールドに、一時的な間隔の値を入力します。

ステップ 14 [Rogue Detection Report Interval] フィールドに、レポート間隔の値を入力します。

ステップ 15 不正な封じ込めの自動レート選択を有効にするには、[Rogue Containment Automatic Rate Selection] チェックボックスをオンにします。

ステップ 16 [Auto Containment on FlexConnect Standalone] チェックボックスをオンにして、この機能を有効にします。

ステップ 17 [Save & Apply to Device] をクリックします。

AP プロファイルの設定

AP プロファイルを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *ap-profile* 例： `Device(config)# ap profile xyz-ap-profile`	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。
ステップ 3	**description** *ap-profile-name* 例： `Device(config-ap-profile)# description "xyz ap profile"`	AP プロファイルの説明を追加します。
ステップ 4	**rogue detection enable** 例： `Device(config-ap-profile)# rogue detection enable`	個々のアクセス ポイントの不正検出を有効にします。 不正検出はデフォルトで有効になっています。不正検出が無効になっている場合は、このコマンドを使用します。
ステップ 5	**rogue detection report-interval** *interval* 例： `Device(config-ap-profile)# rogue detection report-interval 12`	AP からコントローラに不正検出レポートを送信する間隔を秒単位で指定します。 interval のデフォルト値は 10 です。
ステップ 6	**rogue detection min-rssi** *rssi* 例： `Device(config-ap-profile)# rogue detection min-rssi -128`	AP が不正を検出するための不正の最小 RSSI 値を指定します。 最小 RSSI 値は -128 です。
ステップ 7	**rogue detection min-transient-time** *transtime* 例： `Device(config-ap-profile)# rogue detection min-transient-time 120`	不正が初めてスキャンされた後、AP で不正を連続的にスキャンする間隔を指定します。 最小一時時間の最小値は 0 です。
ステップ 8	**rogue detection containment flex-connect** 例： `Device(config-ap-profile)# rogue detection containment flex-connect`	スタンドアロンの FlexConnect アクセスポイントに対して自動封じ込めオプションを設定します。 デフォルトでは、このオプションは無効になっています。

	コマンドまたはアクション	目的
ステップ 9	**rogue detection containment auto-rate** 例： `Device(config-ap-profile)# rogue detection containment auto-rate`	不正の封じ込めの自動レートを設定します。 デフォルトでは、自動レートは無効になっています。

ワイヤレス サイト タグの定義と AP プロファイルの割り当て（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。
ステップ 2 [Tags] ページで、[Site] タブをクリックし、[Add] をクリックします。
ステップ 3 [Add Site Tag] ウィンドウで、[name] フィールドに名前を入力します。
ステップ 4 [AP Join Profile] ドロップダウン リストから AP プロファイルを選択します。
ステップ 5 [Save & Apply to Device] をクリックします。

ワイヤレス サイト タグの定義と AP プロファイルの割り当て（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag site***site-tag* 例： `Device(config)# wireless tag site sitetag1`	RF タグを作成し、ワイヤレス サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**ap-profile** *ap-profile* 例： `Device(config-site-tag)# ap-profile xyz-ap-profile`	AP プロファイルをワイヤレス サイトに割り当てます。
ステップ 4	**exit** 例： `Device(config-site-tag)# exit`	グローバル コンフィギュレーション モードに戻ります。

AP へのワイヤレス タグの関連付け（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] ＞ ＞を選択します。

ステップ 2 [AP] タブをクリックして、次を設定します。

- タグ ソース
- スタティック
- フィルタ

ステップ 3 [Static] タブで、[Add] をクリックして次の操作を実行します。

a) MAC アドレスを入力します。
b) 適切な [Policy Tag Name]、[Site Tag Name]、[RF Tag Name] を選択します。
c) [Save & Apply to Device] をクリックします。

ステップ 4 [Filter] タブで、[Add] をクリックして次の操作を実行します。

a) ルールと AP 名を入力します。
b) スライダを使用して、[Active] を有効にします。
c) プライオリティを入力します。有効な範囲は 0 ～ 127 です。
d) 適切な [Policy Tag Name]、[Site Tag Name]、[RF Tag Name] を選択します。
e) [Save & Apply to Device] をクリックします。

AP へのワイヤレス タグの関連付け（GUI）

Ap プロファイルで定義した不正設定を AP に適用するには、次の手順に従います。

（注） AP がデフォルト以外のサイト タグに明示的に関連付けられていない場合、AP は default-site-tag に関連付けられ、その結果 default-ap-profile の不正設定が使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**ap** *mac-address* 例： `Device(config)# ap F866.F267.7DFB`	Cisco AP を設定し、AP コンフィギュレーション モードを開始します。
ステップ 3	**site-tag** *site-tag-name* 例： `Device(config-ap-tag)# site-tag sitetag1`	ワイヤレス サイト タグを AP にマッピングします。

不正検出セキュリティ レベル

不正検出セキュリティ レベルの設定を使用して、不正検出パラメータを設定できます。

使用可能なセキュリティ レベルは次のとおりです。

- Critical：機密性の高い展開向けの基本不正検出。
- High：中規模な展開向けの基本不正検出。
- Low：小規模な展開向けの基本不正検出。
- Custom：デフォルトのセキュリティレベル（すべての検出パラメータが設定可能）。

（注） Critical、High、または Low の場合、一部の不正パラメータは固定されており、設定できません。

次の表に、事前に定義された 3 つのレベルについてパラメータの詳細を示します。

表 *3:* 不正検出：事前に定義されたレベル

パラメータ	Critical	High	Low
クリーンアップ タイマー	3600	1200	240
AAA 検証クライアント	ディセーブル	ディセーブル	ディセーブル
アドホック レポート	イネーブル	イネーブル	イネーブル
モニタモード レポート間隔	10 秒	30 秒	60 秒
最小 RSSI	-128 dBm	-80 dBm	-80 dBm

パラメータ	Critical	High	Low
一時間隔	600 秒	300 秒	120 秒
自動封じ込め モニタ モードの AP でのみ動作します。	ディセーブル	ディセーブル	ディセーブル
自動封じ込めレベル	1	1	1
同じ SSID の自動封じ込め	ディセーブル	ディセーブル	ディセーブル
不正 AP 上の有効なクライアントの自動封じ込め	ディセーブル	ディセーブル	ディセーブル
アドホックの自動封じ込め	ディセーブル	ディセーブル	ディセーブル
封じ込め自動レート	イネーブル	イネーブル	イネーブル
CMX によるクライアントの検証	イネーブル	イネーブル	イネーブル
封じ込め FlexConnect	イネーブル	イネーブル	イネーブル
RLDP	RLDP スケジューリングが無効になっている場合は、モニタ AP。	RLDP スケジューリングが無効になっている場合は、モニタ AP。	ディセーブル
RLDP の自動封じ込め	ディセーブル	ディセーブル	ディセーブル

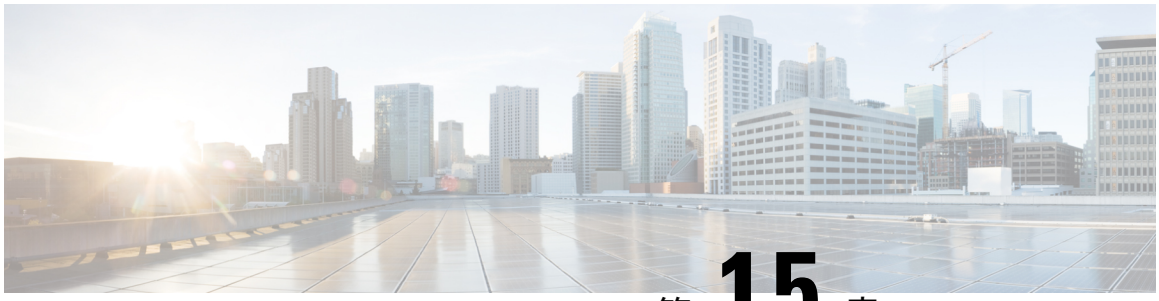
不正検出セキュリティレベルの設定

不正検出セキュリティレベルを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps rogue security-level custom** 例：	不正検出セキュリティ レベルを「カスタム」に設定します。

	コマンドまたはアクション	目的
	`Device(config)# wireless wps rogue security-level custom`	
ステップ 3	**wireless wps rogue security-level low** 例： `Device(config)# wireless wps rogue security-level low`	小規模展開向けの基本不正検出を設定するための不正検出セキュリティ レベルを設定します。
ステップ 4	**wireless wps rogue security-level high** 例： `Device(config)# wireless wps rogue security-level high`	中規模展開向けの不正検出を設定するための不正検出セキュリティ レベルを設定します。
ステップ 5	**wireless wps rogue security-level critical** 例： `Device(config)# wireless wps rogue security-level critical`	機密性の高い展開向けの不正検出を設定するための不正検出セキュリティ レベルを設定します。



第 15 章

アクセス ポイント プラグアンドプレイ

アクセス ポイント プラグアンドプレイの概要

プラグアンドプレイ（PnP）サーバは、コントローラにjoinする前のアクセス ポイント（AP）にステージング パラメータを提供します。AP はこのステージング設定を使用して、コントローラに join するときにランタイム設定を受け取ります。

AP PnP 機能を使用すると、PnP サーバからすべてのタグ関連情報を、事前設定された情報の一部として AP に、さらにコントローラに提供することができます。

設定はPNP サーバに「TXT」または「JSON」形式でアップロードでき、AP の詳細を追加することもできます。追加された AP の詳細は、「TXT」または「JSON」のコンフィギュレーション ファイルの詳細と一緒にマッピングされます。PnP サーバからプロビジョニングされている間、APはこの設定の詳細を取得します。取得した設定の詳細に基づいて、APはタグの詳細と一緒に、対応するコントローラに参加します。

PnP サーバからの AP のプロビジョニング

次のいずれかの方法で PnP サーバから AP をプロビジョニングできます。

- 「オプション 43」を使用して DHCP サーバまたはスイッチを設定します。たとえば、次のコード例を参照できます。

```
ip dhcp pool vlan10
 network 9.10.10.0 255.255.255.0
 default-router 9.10.10.1
  option 43 ascii 5A1D;B2;K4;|9.10.60.5;J80
```

- DNS を使用して DHCP サーバを設定します。たとえば、次のコード例を参照できます。

```
ip dhcp pool vlan10
```

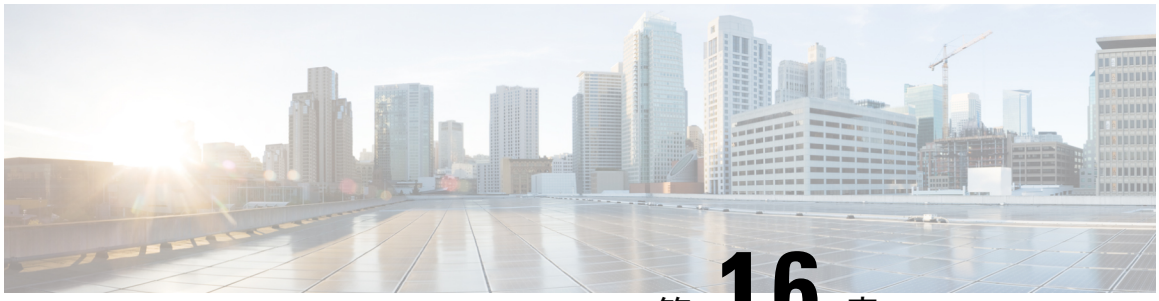
```
network 9.10.10.0 255.255.255.0
default-router 9.10.10.1
dns-server 9.8.65.5
domain-name dns.com
```

AP タグの設定の確認

次の例は、AP タグの設定を確認する方法を示しています。

```
Device# show ap tag summary
Number of APs: 5


AP Name                 AP Mac           Site Tag Name           Policy Tag Name
  RF Tag Name             Misconfigured    Tag Source

-------------------------------------------------------------------------------------

APd42c.4482.6102        d42c.4482.6102   default-site-tag        default-policy-tag
  default-rf-tag          No               Default

AP00c1.64d8.6af0        00c1.64d8.6af0   named-site-tag          named-policy-tag
  named-rf-tag            No               AP
```

（注） 2 行目の詳細には、PNP サーバから受け取るタグ ソースが反映されます。



第 16 章

シスコ アクセス ポイントの 802.11 パラメータ

2.4 GHz 無線サポート

指定したスロット番号に対する 2.4 GHz 無線サポートの設定

始める前に

（注） ここでは用語「802.11b 無線」または「2.4 GHz 無線」を同じ意味で使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ap name** *ap-name* **dot11 24ghz slot 0 SI** 例： `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 SI`	特定のアクセス ポイントのスロット 0 でホストされている専用の 2.4 GHz 無線のスペクトル インテリジェンス（SI）を有効にします。 ここで、**0** はスロット ID を示しています。
ステップ 3	**ap name** *ap-name* **dot11 24ghz slot 0 antenna** { **ext-ant-gain** *antenna_gain_value* | **selection** [**internal** | **external**]} 例： `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 antenna selection internal`	特定のアクセス ポイントのスロット 0 でホストされている 802.11b アンテナを設定します。 • **ext-ant-gain**：802.11b 外部アンテナゲインを設定します。*antenna_gain_value*：外部アンテナゲイン値を .5 dBi の倍数単位で参照します。有効な範囲は 0 ～ 4294967295 です。 • **selection**：802.11b アンテナの選択を設定します（内部または外部）。
ステップ 4	**ap name** *ap-name* **dot11 24ghz slot 0 beamforming** 例： `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 beamforming`	特定のアクセス ポイントのスロット 0 でホストされている 2.4 GHz 無線のビームフォーミングを設定します。
ステップ 5	**ap name** *ap-name* **dot11 24ghz slot 0 channel** {*channel_number* | **auto**} 例： `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 channel auto`	特定のアクセス ポイントのスロット 0 でホストされている 2.4 GHz 無線の高度な 802.11 チャネル割り当てパラメータを設定します。
ステップ 6	**ap name** *ap-name* **dot11 24ghz slot 0 cleanair** 例： `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 cleanair`	特定のアクセス ポイントのスロット 0 でホストされている 802.11b 無線の CleanAir を有効にします。
ステップ 7	**ap name** *ap-name* **dot11 24ghz slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} 例： `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 dot11n antenna A`	特定のアクセス ポイントのスロット 0 でホストされている 2.4 GHz 無線の 802.11n アンテナを設定します。 ここで、各変数は次のように定義されます。

	コマンドまたはアクション	目的
		A：アンテナ ポート A。 **B**：アンテナ ポート B。 **C**：アンテナ ポート C。 **D**：アンテナ ポート D。
ステップ 8	**ap name** *ap-name* **dot11 24ghz slot 0 shutdown** 例： `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 shutdown`	特定のアクセス ポイントのスロット 0 でホストされている 802.11b 無線を無効にします。
ステップ 9	**ap name** *ap-name* **dot11 24ghz slot 0 txpower** {*tx_power_level* | **auto**} 例： `Device# ap name AP-SIDD-A06 dot11 24ghz slot 0 txpower auto`	特定のアクセス ポイントのスロット 0 でホストされている 802.11b 無線の送信電力レベルを無効にします。 • *tx_power_level*：送信電力レベルを dBm 単位で示します。有効な範囲は 1 ～ 8 です。 • **auto**：自動 RF を有効にします。

5 GHz 無線サポート

指定したスロット番号に対する 5 GHz 無線サポートの設定

始める前に

（注） このドキュメントでは用語「802.11a 無線」または「5 GHz 無線」を同じ意味で使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 5ghz slot 1 SI** 例：	特定のアクセス ポイントのスロット 1 でホストされている専用の 5 GHz 無線

	コマンドまたはアクション	目的
	`Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 SI`	のスペクトル インテリジェンス（SI）を有効にします。 ここで、**1** はスロット ID を示しています。
ステップ 3	**ap name** *ap-name* **dot11 5ghz slot 1 antenna ext-ant-gain** *antenna_gain_value* 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna ext-ant-gain`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線の外部アンテナ ゲインを設定します。 *antenna_gain_value*：外部アンテナ ゲイン値を .5 dBi の倍数単位で参照します。有効な範囲は 0 ～ 4294967295 です。
ステップ 4	**ap name** *ap-name* **dot11 5ghz slot 1 antenna mode** [**omni** | **sectorA** | **sectorB**] 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna mode sectorA`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線のアンテナ モードを設定します。
ステップ 5	**ap name** *ap-name* **dot11 5ghz slot 1 antenna selection** [**internal** | **external**] 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 antenna selection internal`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線のアンテナ選択を設定します。
ステップ 6	**ap name** *ap-name* **dot11 5ghz slot 1 beamforming** 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 beamforming`	特定のアクセス ポイントのスロット 1 でホストされている 5 GHz 無線のビームフォーミングを設定します。
ステップ 7	**ap name** *ap-name* **dot11 5ghz slot 1 channel** {*channel_number* | **auto** | **width** [**20** | **40** | **80** | **160**]} 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 channel auto`	特定のアクセス ポイントのスロット 1 でホストされている 5 GHz 無線の高度な 802.11 チャネル割り当てパラメータを設定します。 ここで、各変数は次のように定義されます。 *channel_number*：チャネル番号を指します。有効な範囲は 1 ～ 173 です。
ステップ 8	**ap name** *ap-name* **dot11 5ghz slot 1 cleanair** 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 cleanair`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線の CleanAir を有効にします。

	コマンドまたはアクション	目的
ステップ 9	**ap name** *ap-name* **dot11 5ghz slot 1 dot11n antenna** {**A** | **B** | **C** | **D**} 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 dot11n antenna A`	特定のアクセス ポイントのスロット 1 でホストされている 5 GHz 無線の 802.11n アンテナを設定します。 ここで、各変数は次のように定義されます。 **A**：アンテナ ポート A。 **B**：アンテナ ポート B。 **C**：アンテナ ポート C。 **D**：アンテナ ポート D。
ステップ 10	**ap name** *ap-name* **dot11 5ghz slot 1 rrm channel** *channel* 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 rrm channel 2`	特定のアクセス ポイントのスロット 1 でホストされているチャネルを変更するもう 1 つの方法です。 ここで、各変数は次のように定義されます。 *channel*：802.11h チャネル アナウンスを使用して作成された新しいチャネルを指します。有効な範囲は 1 ～ 173 で、173 は、アクセス ポイントを展開している国の有効なチャネルです。
ステップ 11	**ap name** *ap-name* **dot11 5ghz slot 1 shutdown** 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 shutdown`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線を無効にします。
ステップ 12	**ap name** *ap-name* **dot11 5ghz slot 1 txpower** {*tx_power_level* | **auto**} 例： `Device# ap name AP-SIDD-A06 dot11 5ghz slot 1 txpower auto`	特定のアクセス ポイントのスロット 1 でホストされている 802.11a 無線を設定します。 • *tx_power_level*：送信電力レベルを dBm 単位で示します。有効な範囲は 1 ～ 8 です。 • **auto**：自動 RF を有効にします。

デュアルバンド（XOR）無線のサポートについて

Cisco 2800 および 3800 AP モデルのデュアルバンド（XOR）無線は、2.4 GHz 帯の利用、5 GHz 帯の利用、または同一 AP 上での両周波数帯の受動的な監視の機能を提供します。これらの AP は、クライアントに 2.4 GHz および 5 GHz 帯域でサービスを提供するように設定できます。または、メインの 5 GHz 無線がクライアントにサービスを提供しながら、フレキシブル無線で 2.4 GHz 帯と 5 GHz 帯の両方を順次スキャンします。

Cisco AP 2800 および 3800 モデルはデュアル 5 GHz 帯の動作に対応できるように設計されており、専用のマクロ/マイクロ アーキテクチャをサポートする「i」モデルと、マクロ/マクロをサポートする「e」および「p」モデルがあります。無線が帯域間を移動する場合（2.4 GHz から 5 GHz へ、またはその逆）、無線間で最適な分散を実現するには、クライアントをステアリングする必要があります。AP に 5 GHz 帯の無線が 2 つある場合、それらの無線はマクロ セルおよびマイクロ セルとして動作します。マクロマイクロ クライアント ステアリングを使用して、マクロとマイクロ間でクライアントをステアリングします。

XOR 無線のサポートのステアリングは、手動または自動で行うことができます。

- 無線での帯域の手動ステアリング：XOR 無線の帯域は手動でのみ変更できます。
- 無線での帯域の自動ステアリング：XOR 無線の帯域は、サイトの要件に従って帯域をモニタおよび変更するフレキシブル ラジオ アサインメント（FRA）機能によって変更されます。

デフォルトの XOR 無線サポートの設定

始める前に

（注） デフォルトの無線とは、スロット 0 でホストされている XOR 無線を指します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 dual-band antenna ext-ant-gain** *antenna_gain_value* 例：	特定のシスコ アクセス ポイントの 802.11 デュアルバンド アンテナを設定します。

	コマンドまたはアクション	目的
	`Device# ap name ap-name dot11 dual-band antenna ext-ant-gain 2`	*antenna_gain_value*：有効な範囲は 0 ～ 40 です。
ステップ 3	**ap name** *ap-name* **[no] dot11 dual-band shutdown** 例： `Device# ap name ap-name dot11 dual-band shutdown`	特定のシスコ アクセス ポイントでデフォルトのデュアルバンド無線をシャットダウンします。 無線を有効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**ap name** *ap-name* **dot11 dual-band txpower** {*transmit_power_level* | **auto**} 例： `Device# ap name ap-name dot11 dual-band txpower 2`	特定のシスコアクセス ポイントにおける無線の送信電力を設定します。
ステップ 5	**ap name** *ap-name* **dot11 dual-band role manual client-serving** 例： `Device# ap name ap-name dot11 dual-band role manual client-serving`	シスコアクセス ポイントでクライアントサービングモードに切り替えます。
ステップ 6	**ap name** *ap-name* **dot11 dual-band band 24ghz** 例： `Device# ap name ap-name dot11 dual-band band 24ghz`	2.4 GHz 無線帯域に切り替えます。
ステップ 7	**ap name** *ap-name* **dot11 dual-band channel** *channel-number* 例： `Device# ap name ap-name dot11 dual-band channel 2`	デュアルバンドのチャネルを入力します。 *channel-number*：有効な範囲は 1 ～ 173 です。
ステップ 8	**ap name** *ap-name* **dot11 dual-band channel auto** 例： `Device# ap name ap-name dot11 dual-band channel auto`	デュアルバンドの自動チャネル割り当てを有効にします。
ステップ 9	**ap name** *ap-name* **dot11 dual-band channel width**{**20 MHz** | **40 MHz** | **80 MHz** | **160 MHz**} 例： `Device# ap name ap-name dot11 dual-band channel width 20 MHz`	デュアルバンドのチャネル幅を選択します。

	コマンドまたはアクション	目的
ステップ 10	**ap name** *ap-name* **dot11 dual-band cleanair** 例： `Device# ap name ap-name dot11 dual-band cleanair`	デュアルバンド無線の Cisco CleanAir 機能を有効にします。
ステップ 11	**ap name** *ap-name* **dot11 dual-band cleanair band**{**24 GHz | 5 GMHz**} 例： `Device# ap name ap-name dot11 dual-band cleanair band 5 GHz` `Device# ap name ap-name [no] dot11 dual-band cleanair band 5 GHz`	Cisco CleanAir 機能の帯域を選択します。 Cisco CleanAir 機能を無効にするには、このコマンドの **no** 形式を使用します。
ステップ 12	**ap name** *ap-name* **dot11 dual-band dot11n antenna** {**A | B | C | D**} 例： `Device# ap name ap-name dot11 dual-band dot11n antenna A`	特定のアクセス ポイントの 802.11n デュアルバンドパラメータを設定します。
ステップ 13	**show ap name** *ap-name* **auto-rf dot11 dual-band** 例： `Device# show ap name ap-name auto-rf dot11 dual-band`	シスコ アクセス ポイントの自動 RF 情報を表示します。
ステップ 14	**show ap name** *ap-name* **wlan dot11 dual-band** 例： `Device# show ap name ap-name wlan dot11 dual-band`	シスコ アクセスポイントの BSSID のリストを表示します。

指定したスロット番号に対する XOR 無線サポートの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Access Points]** の順にクリックします。

ステップ 2 [Dual-Band Radios] セクションで、デュアルバンド無線を設定する AP を選択します。

AP の AP 名、MAC アドレス、CleanAir 機能、およびスロット情報が表示されます。HyperLocation 方式が HALO の場合は、アンテナの PID とアンテナの設計情報も表示されます。

ステップ 3 [Configure] をクリックします。
ステップ 4 [General] タブで、必要に応じて [Admin Status] を設定します。
ステップ 5 [CleanAir Admin Status] フィールドを [Enable] または [Disable] に設定します。
ステップ 6 [Update & Apply to Device] をクリックします。

指定したスロット番号に対する XOR 無線サポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 dual-band slot 0 antenna ext-ant-gain** *external_antenna_gain_value* 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンド アンテナを設定します。 *external_antenna_gain_value*：外部アンテナ ゲイン値（.5 dBi の倍数単位）。有効な範囲は 0 ～ 40 です。
ステップ 3	**ap name** *ap-name* **dot11 dual-band slot 0 band** {**24ghz** | **5ghz**} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線の現在の帯域を設定します。
ステップ 4	**ap name** *ap-name* **dot11 dual-band slot 0 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンド チャネルを設定します。 *channel_number*：有効な範囲は 1 ～ 165 です。
ステップ 5	**ap name** *ap-name* **dot11 dual-band slot 0 cleanair band** {**24Ghz** | **5Ghz**} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz`	特定のアクセス ポイントのスロット 0 でホストされているデュアルバンド無線の CleanAir 機能を有効にします。

	コマンドまたはアクション	目的
ステップ 6	**ap name** *ap-name* **dot11 dual-band slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A`	特定のアクセス ポイントのスロット 0 でホストされている 802.11n デュアルバンド パラメータを設定します。 ここで、各変数は次のように定義されます。 **A**：アンテナ ポート A を有効にします。 **B**：アンテナ ポート B を有効にします。 **C**：アンテナ ポート C を有効にします。 **D**：アンテナ ポート D を有効にします。
ステップ 7	**ap name** *ap-name* **dot11 dual-band slot 0 role** {**auto** | **manual** [**client-serving** | **monitor**]} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンドの役割を設定します。 デュアルバンドの役割は次のとおりです。 • **auto**：無線の役割を自動で選択することを指します。 • **manual**：無線の役割を手動で選択することを指します。
ステップ 8	**ap name** *ap-name* **dot11 dual-band slot 0 shutdown** 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown` `Device# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown`	特定のアクセス ポイントのスロット 0 でホストされているデュアルバンド無線を無効にします。 デュアルバンド無線を有効にするには、このコマンドの **no** 形式を使用します。
ステップ 9	**ap name** *ap-name* **dot11 dual-band slot 0 txpower** {*tx_power_level* | **auto**} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2`	特定のアクセスポイントのスロット 0 でホストされている XOR 無線のデュアルバンド送信電力を設定します。 • *tx_power_level*：送信電力レベルを dBm 単位で示します。有効な範囲は 1 ～ 8 です。 • **auto**：自動 RF を有効にします。

受信専用デュアルバンド無線サポート

受信専用デュアルバンド無線のサポートについて

この機能では、デュアルバンド無線を備えたアクセス ポイントのデュアルバンド受信専用無線機能を設定します。

このデュアルバンド受信専用無線は、分析、HyperLocation、ワイヤレス セキュリティ モニタリング、および BLE AoA* の専用となります。

この無線は常にモニタ モードでの機能を継続するため、3 番目の無線でチャネル設定や *tx-rx* 設定を行うことはできません。

アクセスポイントの受信専用デュアルバンドパラメータの設定

シスコ アクセス ポイントでの受信専用デュアルバンド無線による CleanAir の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 cleanair band** {**24Ghz** | **5Ghz**} 例： `Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 cleanair band 24Ghz` `Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 cleanair band 24Ghz`	特定のアクセスポイントで受信専用（Rx 専用）デュアルバンド無線による CleanAir を有効にします。 ここで、2 はスロット ID を示しています。 CleanAir を無効にするには、このコマンドの **no** 形式を使用します。

シスコ アクセス ポイントでの受信専用デュアルバンド無線の無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ap name** *ap-name* **dot11 rx-dual-band slot 2 shutdown** 例： `Device# ap name AP-SIDD-A06 dot11 rx-dual-band slot 2 shutdown` `Device# ap name AP-SIDD-A06 [no] dot11 rx-dual-band slot 2 shutdown`	特定のシスコ アクセス ポイントで受信専用デュアルバンド無線を無効にします。 ここで、2 はスロット ID を示しています。 受信専用デュアルバンド無線を有効にするには、このコマンドの **no** 形式を使用します。

クライアント ステアリングの設定（CLI）

始める前に

対応するデュアルバンド無線で Cisco CleanAir を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wireless macro-micro steering transition-threshold balancing-window** *number-of-clients(0-65535)* 例： `Device(config)# wireless macro-micro steering transition-threshold balancing-window 10`	設定した数のクライアントのマイクロ マクロ クライアント ロードバランシング ウィンドウを設定します。
ステップ 4	**wireless macro-micro steering transition-threshold client count** *number-of-clients(0-65535)* 例： `Device(config)# wireless macro-micro steering transition-threshold client count 10`	移行する最小クライアント数のマクロ マイクロ クライアント パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 5	**wireless macro-micro steering transition-threshold macro-to-micro** *RSSI-in-dBm(-128—0)* 例： `Device(config)# wireless macro-micro steering transition-threshold macro-to-micro -100`	マクロからマイクロへの移行の RSSI を設定します。
ステップ 6	**wireless macro-micro steering transition-threshold micro-to-macro** *RSSI-in-dBm(-128—0)* 例： `Device(config)# wireless macro-micro steering transition-threshold micro-to-macro -110`	マイクロからマクロへの移行の RSSI を設定します。
ステップ 7	**wireless macro-micro steering probe-suppression aggressiveness** *number-of-cycles(-128—0)* 例： `Device(config)# wireless macro-micro steering probe-suppression aggressiveness -110`	抑制するプローブ サイクル数を設定します。
ステップ 8	**wireless macro-micro steering probe-suppression hysteresis** *RSSI-in-dBm* 例： `Device(config)# wireless macro-micro steering probe-suppression hysteresis -5`	RSSI でのマクロからマイクロへのプローブを設定します。範囲は -6 ～ -3 です。
ステップ 9	**wireless macro-micro steering probe-suppression probe-only** 例： `Device(config)# wireless macro-micro steering probe-suppression probe-only`	プローブ抑制モードを有効にします。
ステップ 10	**wireless macro-micro steering probe-suppression probe-auth** 例： `Device(config)# wireless macro-micro steering probe-suppression probe-auth`	プローブおよびシングル認証抑制モードを有効にします。
ステップ 11	**show wireless client steering** 例： `Device# show wireless client steering`	ワイヤレス クライアント ステアリング情報を表示します。

デュアルバンド無線を備えたシスコアクセスポイントの確認

デュアルバンド無線によるアクセス ポイントを確認するには、次のコマンドを使用します。

```
Device# show ap dot11 dual-band summary

AP Name Subband Radio      Mac   Status Channel Power Level Slot ID Mode
-------------------------------------------------------------------------------
4800   All 3890.a5e6.f360 Enabled (40)* *1/8     (22 dBm)      0   Sensor
4800   All 3890.a5e6.f360 Enabled N/A    N/A       2               Monitor
```

第 17 章

802.1x サポート

802.1x 認証の概要

IEEE 802.1x ポートベースの認証は、不正なデバイスによるネットワーク アクセスを防止するためにデバイスに設定されます。デバイスでは、固定された構成に基づいて、ルータ、スイッチ、およびアクセス ポイントの機能を組み合わせることができます。802.1x 認証が有効になっているスイッチ ポートに接続しているデバイスはすべて、トラフィックの交換を開始する場合に、関連する EAP 認証モデルを実行する必要があります。

現在、Cisco Wave 2 AP は、EAP-FAST、EAP-TLS、EAP-PEAP の各方式のスイッチ ポートを使用した 802.1x 認証をサポートしています。そのため、設定を有効にしてコントローラから AP にクレデンシャルを提供できます。

EAP-FAST プロトコル

シスコが開発した EAP-FAST プロトコルでは、RADIUS を使用したセキュアな TLS トンネルを確立するために、AP では、インバンド プロビジョニング（セキュア チャネル内）またはアウトバンド プロビジョニング（手動）を介して提供される強力な共有キー（PAC）を必要とします。

（注） AP では MSCHAP バージョン 2 方式の EAP-FAST が使用されるため、EAP-FAST タイプの設定では AP に対して Dot1x クレデンシャルの設定が必要です。

EAP-TLS/EAP-PEAP プロトコル

EAP-TLS プロトコルまたは EAP-PEAP プロトコルは、証明書ベースの相互 EAP 認証を提供します。

EAP-TLS では、サーバ側証明書とクライアント側証明書の両方が必要であり、特定のセッションに対してデータを暗号化または復号化するために、セキュリティ保護された共有キーが導出されます。一方、EAP-PEAP ではサーバ側証明書のみ必要であり、クライアントはセキュリティ保護されたチャネルでパスワードベースのプロトコルを使用して認証を行います。

（注） EAP-PEAP タイプの設定では AP に対して Dot1x クレデンシャルの設定が必要です。また、AP では LSC のプロビジョニングを実行する必要もあります。AP では MSCHAP バージョン 2 方式の PEAP プロトコルが使用されます。

802.1x 認証の制限事項

- 802.1xはダイナミック ポートまたはイーサチャネル ポートではサポートされていません。
- 802.1x はメッシュ AP のシナリオではサポートされていません。
- クレデンシャルの不一致、または AP 上の証明書の期限切れ/無効が生じた場合、コントローラから回復することはありません。設定を修正するために再び AP に接続するには、スイッチ ポートで 802.1x 認証を無効にする必要があります。
- AP にインストールされた証明書では証明書失効チェックは実装されません。
- AP では ローカルで有効な証明書（LSC）を 1 つだけプロビジョニングでき、コントローラによる CAPWAP DTLS セッションの確立と、スイッチによる 802.1x 認証では、これと同じ証明書を使用する必要があります。コントローラのグローバルLSC設定が無効になった場合、AP では、すでにプロビジョニングされている LSC が削除されます。
- AP に設定のクリアが適用された場合、AP では 802.1x EAP タイプの設定と LSC 証明書が失われます。802.1x が必要な場合、AP では再度ステージング プロセスを実行する必要があります。

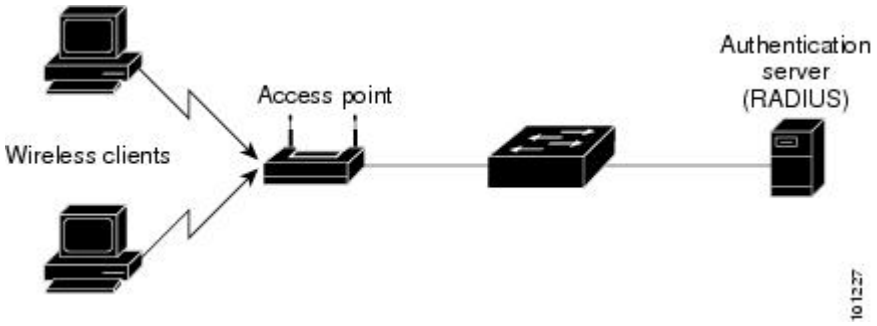
トポロジ - 概要

802.1x 認証のイベントは次のとおりです。

1. AP は 802.1x サプリカントとして機能し、RADIUS サーバに対してスイッチによって認証されます。RADIUS サーバは、EAP-FAST とともに EAP-TLS と EAP-PEAP も サポートします。dot1x 認証がスイッチ ポートで有効になっている場合、そのポートに接続しているデバイスは、802.1x トラフィック以外のデータを受信して転送するために自分自身を認証します。

2. 2. EAP-FAST 方式による認証を行うには、AP で RADIUS サーバのクレデンシャルが必要になります。クレデンシャルはコントローラで設定でき、そこから設定更新要求を介して AP に渡されます。EAP-TLS または EAP-PEAP の場合、AP では、ローカル CA サーバによって重要扱いにされた証明書（デバイス/ID および CA）が使用されます。

図 *4 :* 図 *1* : *802.1x* 認証のトポロジ



802.1x 認証タイプと LSC AP 認証タイプの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[AP Join]** を選択します。

ステップ 2 [AP Join Profile] ページで、[Add] をクリックします。

[Add AP Join Profile] ページが表示されます。

ステップ 3 **[AP]** > **[General]** タブで、[AP EAP Auth Configuration] セクションに移動します。

ステップ 4 [EAP Type] ドロップダウン リストから、EAP タイプとして [EAP-FAST]、[EAP-TLS]、または [EAP-PEAP] を選択して、dot1x 認証タイプを設定します。

ステップ 5 [AP Authorization Type] ドロップダウン リストから、タイプとして [CAPWAP DTLS +] または [CAPWAP DTLS] のいずれかを選択します。

ステップ 6 [Save & Apply to Device] をクリックします。

802.1x 認証タイプと LSC AP 認証タイプの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	特権 EXEC モードを有効にし、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 3	**ap profile** <profile-name> 例： `Device(config)# ap profile new-profile`	プロファイル名を指定します。
ステップ 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** 例： `Device(config-ap-profile)# dot1x eap-type`	dot1x 認証タイプを設定します。 **max-sessions**：AP ごとに開始される 802.1x セッションの最大数を設定します。 **username**：すべての AP の 802.1x ユーザ名を設定します。 **eap-type**：スイッチ ポートを使用した dot1x 認証タイプを設定します。 **lsc-ap-auth-state**：AP での LSC 認証状態を設定します。
ステップ 5	**dot1x eap-type {EAP-FAST | EAP-TLS | EAP-PEAP}** 例： `Device(config-ap-profile)# dot1x eap-type`	dot1x 認証タイプ（EAP-FAST、EAP-TLS、または EAP-PEAP）を設定します。
ステップ 6	**dot1x lsc-ap-auth-state {CAPWAP-DTLS | Dot1x-port-auth | Both}** 例： `Device(config-ap-profile)#dot1x lsc-ap-auth-state Dot1x-port-auth`	AP での LSC 認証状態を設定します。 **CAPWAP-DTLS**：CAPWAP DTLS にのみ LSC を使用します。 **Dot1x-port-auth**：ポートでの dot1x 認証にのみ LSC を使用します。

	コマンドまたはアクション	目的
		Both：CAPWAP-DTLS とポートでの Dot1x 認証の両方に LSC を使用します。
ステップ 7	**end** 例： `Device(config-ap-profile)# end`	AP プロファイル コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。

802.1x ユーザ名とパスワードの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[RF]** を選択します。
ステップ 2 [RF] ページで、プロファイルの名前をクリックするか、[Add] をクリックして新規に作成します。
ステップ 3 [Management] タブをクリックし、[Credentials] タブをクリックします。
ステップ 4 ローカルのユーザ名とパスワードの詳細を入力します。
ステップ 5 適切なローカル パスワード タイプを選択します。
ステップ 6 802.1x ユーザ名とパスワードの詳細を入力します。
ステップ 7 適切な 802.1x パスワード タイプを選択します。
ステップ 8 セッションが期限切れになるまでの時間を秒単位で入力します。
ステップ 9 必要に応じて、ローカル クレデンシャルや 802.1 x クレデンシャルを有効にします。
ステップ 10 [Update & Apply to Device] をクリックします。

802.1x ユーザ名とパスワードの設定（CLI）

次の手順では、すべての AP の 802.1x パスワードを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	特権 EXEC モードを有効にし、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 3	**ap profile** <profile-name> 例： `Device(config)# ap profile new-profile`	プロファイル名を指定します。
ステップ 4	**dot1x {max-sessions | username | eap-type | lsc-ap-auth-state}** 例： `Device(config-ap-profile)# dot1x eap-type`	dot1x 認証タイプを設定します。 **max-sessions**：AP ごとに開始される 802.1x セッションの最大数を設定します。 **username**：すべての AP の 802.1x ユーザ名を設定します。 **eap-type**：スイッチ ポートを使用した dot1x 認証タイプを設定します。 **lsc-ap-auth-state**：AP での LSC 認証状態を設定します。
ステップ 5	**dot1x username** <username> **password {0 | 8}** <password> 例： `Device(config-ap-profile)#dot1x username` *`username`* `password 0` *`password`*	すべての AP の dot1x パスワードを設定します。 0：暗号化されていないパスワードに従うことを指定します。 8：AES で暗号化されたパスワードに従うことを指定します。

スイッチ ポートでの 802.1x の有効化

次の手順では、スイッチ ポートで 802.1x を有効にします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	特権 EXEC モードを有効にし、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 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA を有効にします。
ステップ 4	**aaa authentication dot1x {default | listname} method1[method2...]** 例： `Device(config)# aaa authentication dot1x default group radius`	デバイスが AAA サーバと通信できるように、特権コマンド レベルにアクセスするユーザ権限の決定に使用される一連の認証方式を作成します。
ステップ 5	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 6	**interface type slot/port** 例： `Device(config)# interface fastethernet2/1`	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、802.1X 認証をイネーブルにするインターフェイスを指定します。
ステップ 7	**authentication port-control {auto | force-authorized | force-unauthorized}** 例： `Device(config-if)# authentication port-control auto`	インターフェイス上で 802.1x ポートベースの認証をイネーブルにします。 auto：IEEE 802.1x 認証をイネーブルにし、ポートを無許可ステートで開始します。ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンク ステートがダウンからアップに変更したとき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。デバイスはサプリカントの識別を要求し、サプリカントと認証サーバ間で認証メッセージのリレーを開始します。デバイスはサプリカントの MAC アドレスを使用して、ネットワーク アクセスを試みる各サプリカントを一意に識別します。 force-authorized：IEEE802.1x 認証をディセーブルにし、その結果、認証の交換を必要とせずにポートが許可済みステート

	コマンドまたはアクション	目的
		に変更されます。ポートは、クライアントの IEEE 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルト設定です。 force unauthorized：ポートが無許可ステートのままになり、サプリカントからの認証の試みをすべて無視します。デバイスは、このポートを介してサプリカントに認証サービスを提供することはできません。
ステップ 8	**dot1x pae [supplicant | authenticator | both]** 例： `Device(config-if)# dot1x pae authenticator`	
ステップ 9	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

スイッチ ポートでの 802.1x の確認

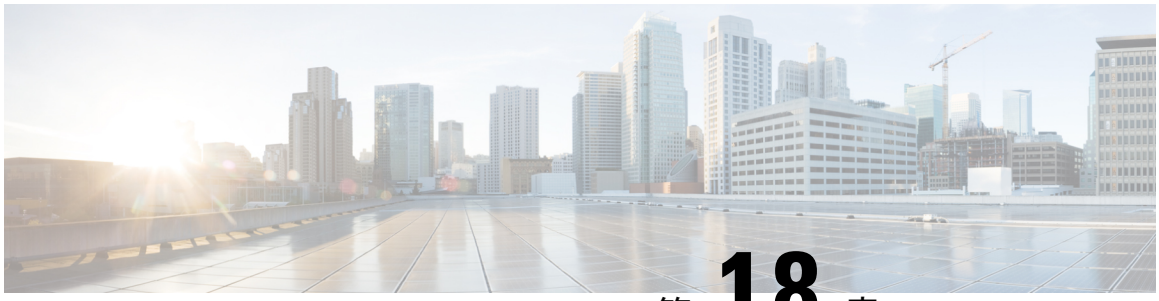
次の show コマンドは、スイッチ ポートでの 802.1x の認証状態を表示します。

```
Device# show dot1x all
Sysauthcontrol              Enabled
Dot1x Protocol Version      2
Dot1x Info for FastEthernet1
-----------------------------------
PAE                         = AUTHENTICATOR
PortControl                 = AUTO
ControlDirection            = Both
HostMode                    = MULTI_HOST
ReAuthentication            = Disabled
QuietPeriod                 = 60
ServerTimeout               = 30
SuppTimeout                 = 30
ReAuthPeriod                = 3600 (Locally configured)
ReAuthMax                   = 2
MaxReq                      = 2
TxPeriod                    = 30
RateLimitPeriod             = 0
Device#
```

認証タイプの確認

次の show コマンドは、AP プロファイルの認証状態を表示します。

```
Device#show ap profile <profile-name> detailed ?
  chassis  Chassis
  |        Output modifiers
  <cr>

Device#show ap profile <profile-name> detailed

  AP Profile Name        : default-ap-profile
  Description            : default ap profile
  …
  Dot1x EAP Method       : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
  LSC AP AUTH STATE      : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port
auth
```



第 18 章

CAPWAP リンク集約サポートの設定

リンク集約について

LAG を使用すると、インターフェイスごとにプライマリ ポートとセカンダリ ポートを設定する必要がなくなるため、コントローラの設定が簡素化されます。いずれかのコントローラ ポートに障害が発生した場合は、他のポートへトラフィックが自動的に移行します。少なくとも 1 つのコントローラ ポートが機能している限り、システムは継続して動作し、アクセス ポイントはネットワークに接続されたままとなります。また、ワイヤレス クライアントは引き続きデータを送受信します。

CAPWAP LAG サポートについて

CAPWAP LAG サポート機能は、CAPWAP 用に複数のイーサネット ポートをサポートしているアクセス ポイントに適用されます。

デュアル イーサネット ポートを搭載した 11AC AP では、データ チャネルで CAPWAP AP LAG サポートが必要です。

Cisco Aironet 1850、2800、および 3800 シリーズの AP では、2 番目のイーサネット ポートがデフォルトでリンク集約（LAG）ポートとして使用されます。この LAG ポートは LAG が無効になっている場合に RLAN ポートとして使用できます。

次の AP は、LAG ポートを RLAN ポートとして使用します。

- 1852E
- 1852I
- 2802E
- 2802I
- 3802E
- 3802I
- 3802P

CAPWAP LAG サポートの制約事項

- アクセス ポイントはCAPWAP AP LAG サポート向けに明確に有効にする必要があります。
- CAPWAP データは IPv6 をサポートしていません。
- LAG を有効にする場合はデータ DTLS を有効にしないでください。

コントローラでの CAPWAP LAG サポートの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap lag support** 例： `Device(config)# ap lag support`	コントローラでCAPWAP LAG サポートを有効にします。 （注） このコマンドを実行すると、次の警告文が表示されます。 *Changing the lag support will cause all the APs to disconnect.*（*LAG* のサポートを変更するとすべての *AP* が切断されます。） したがって、LAG 機能を持つすべての AP がリブートし、有効になっている CAPWAP LAG に join します。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

コントローラでの CAPWAP LAG のグローバルな有効化

CAPWAP LAG がコントローラでグローバルに有効になると、次のようになります。

- AP は、コントローラに join します。
- AP は、CAPWAP サポートを交換します。
- LAG が AP で有効になっている場合、LAG モードが開始されます。

コントローラでの CAPWAP LAG のグローバルな無効化

CAPWAP LAG がコントローラでグローバルに無効になると、次のようになります。

- AP は、コントローラに join します。
- AP は、CAPWAP サポートを交換します。
- LAG が AP ですでに有効になっている場合、AP LAG 設定が AP に送信されます。
- AP がリブートします。
- AP は、無効になった LAG を使用して再度 join します。

AP プロファイルの CAPWAP LAG の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**ap profile** *ap-profile* 例： `Device(config)# ap profile xyz-ap-profile`	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。 （注） 名前付きプロファイルを削除した場合、そのプロファイルに関連付けられていた AP はデフォルト プロファイルに戻らなくなります。
ステップ 3	**lag** 例： `Device(config-ap-profile)# lag`	AP プロファイルの CAPWAP LAG を有効にします。
ステップ 4	**end** 例： `Device(config-ap-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

AP プロファイルの CAPWAP LAG の無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *ap-profile* 例： `Device(config)# ap profile xyz-ap-profile`	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。 （注） 名前付きプロファイルを削除した場合、そのプロファイルに関連付けられていた AP はデフォルト プロファイルに戻らなくなります。
ステップ 3	**no lag** 例： `Device(config-ap-profile)# no lag`	AP プロファイルの CAPWAP LAG を無効にします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-ap-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

コントローラでの CAPWAP LAG サポートの無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**no ap lag support** 例： `Device(config)# no ap lag support`	コントローラで CAPWAP LAG サポートを無効にします。 （注） LAG 機能を持つすべての Ap がリブートし、無効になった CAPWAP LAG に join します。
ステップ 3	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

CAPWAP LAG サポートの設定の確認

すべてのシスコ AP のグローバル LAG ステータスを確認するには、次のコマンドを使用します。

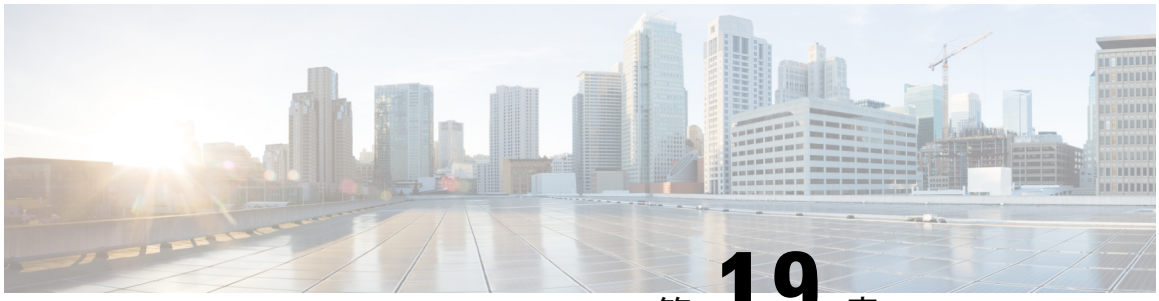
```
Device# show ap lag-mode
AP Lag-Mode Support Enabled
```

AP LAG 設定のステータスを確認するには、次のコマンドを使用します。

```
Device# show ap name <ap-name> config general
Cisco AP Identifier : 0008.3291.6360
Country Code : US
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-AB
AP Country Code : US - United States
::
AP Lag Configuration Status : Enabled/Disabled
Has AP negotiated lag based on AP capability and per AP config.
```

第 III 部

Radio Resource Management



第 19 章

Radio Resource Management

Radio Resource Management について

Radio Resource Management（RRM）ソフトウェアはdeviceに組み込まれており、ワイヤレスネットワークのリアルタイムでの無線周波数（RF）管理を一貫して行えるようにする組み込みのRFエンジニアとして機能します。RRMを使用すると、devicesは次の情報について、アソシエートされている Lightweight アクセス ポイントを継続的に監視できます。

- トラフィックの負荷：トラフィックの送受信に使用される帯域幅の合計量。これにより、無線 LAN 管理者は、ネットワークの拡大状況を追跡し、クライアントの需要を見越して計画を立てることができます。
- 干渉：他の 802.11 発信元から送られてくるトラフィック量。
- ノイズ：現在割り当てられているチャネルに干渉している 802.11 以外のトラフィック量。
- カバレッジ：接続されているすべてのクライアントの受信信号強度インジケータ（RSSI）と信号対雑音比（SNR）。
- その他：近くにあるアクセス ポイントの数。

RRM は次の機能を実行します。

- 無線リソースの監視
- 電力制御の送信
- チャネルの動的割り当て
- カバレッジ ホールの検出と修正

- RF グループ化

（注） AP が DCA チャネルのリストにないスタティック チャネルで動作している場合、RRM のグループ化は行われません。ネイバー探索プロトコル（NDP）は DCA チャネルでのみ送信されます。したがって、無線が DCA 以外のチャネルで動作している場合は、チャネルで NDP を受信しません。

無線リソースの監視

RRM は、ネットワークに追加された新しいdevicesや Lightweight アクセス ポイントを自動的に検出して設定します。その後、アソシエートされている近くの Lightweight アクセス ポイントを自動的に調整して、カバレッジとキャパシティを最適化します。

Lightweight アクセス ポイントでは、使用国で有効なすべての チャネルをスキャンできます。また、他の地域で使用可能なチャネルも同様です。ローカル モードのアクセス ポイントは、これらのチャネルのノイズと干渉を監視するために、最大で 60 ミリ秒の間「オフチャネル」になります。 不正アクセス ポイント、不正クライアント、アドホック クライアント、干渉しているアクセス ポイントを検出するために、この間に収集されたパケットが解析されます。

（注） 音声トラフィックやその他の重要なトラフィックがある場合（過去100ミリ秒内）、アクセス ポイントはオフチャネル測定を延期できます。また、アクセス ポイントは、WLAN スキャン プライオリティの設定に基づいてオフチャネルの測定を延期します。

各アクセス ポイントがオフチャネルになるのはすべての時間のわずか 0.2% です。この動作はすべてのアクセス ポイントに分散されるので、隣接するアクセス ポイントが同時にスキャンを実行して、無線 LAN のパフォーマンスに悪影響を及ぼすことはありません。

- モビリティ コントローラ（MC）：Cisco WLC 5700 シリーズ コントローラ、Cisco Catalyst 3850 スイッチ、Cisco Unified Wireless Network ソリューションのコントローラは MC として機能できます。MC には、その中で内部的に実行されている MC 機能および MA 機能があります。
- モビリティ エージェント（MA）：モビリティ エージェントは、モバイル クライアント用のクライアント モビリティ ステート マシンを維持するコンポーネントです。

RF グループについて

RF グループは、無線単位でネットワークの計算を実行するために、グローバルに最適化された方法で RRM の実行を調整するコントローラの論理的な集合です。802.11 ネットワーク タイプごとに RF グループが存在します。WLC を単一の RF グループにクラスタリングすることによって、RRM アルゴリズムは単一の WLC の機能を拡張できます。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラCisco Catalyst 9800 シリーズ ワイヤレス コントローラ

RF グループは、次のパラメータに基づいて作成されます。

- ユーザ設定の RF ネットワーク名。
- 無線レベルで実行されるネイバー探索。
- MC に設定されている国のリスト。

コントローラ間で実行する RF グループ化。

Lightweight アクセス ポイントは、定期的にネイバー メッセージを無線で送信します。同じ RF グループ名を使用しているアクセス ポイントは、相互に送信されたメッセージを検証します。

検証されたネイバー メッセージを、異なるコントローラ上のアクセス ポイントが -80dBm 以上の信号強度で受信すると、コントローラによって自動モードの RF 領域が動的に生成されます。静的モードで、リーダーは手動で選択され、メンバが RF グループに追加されます。。

（注） RF グループとモビリティ グループは、どちらもコントローラのクラスタを定義するという点では同じですが、用途に関しては異なります。RF グループはスケーラブルでシステム全体にわたる動的な RF 管理を実現するのに対して、モビリティ グループはスケーラブルでシステム全体にわたるモビリティとコントローラの冗長性を実現します。

RF グループ リーダー

RF グループ リーダーを次の 2 つの方法で設定することができます。

- 自動モード：このモードでは、RF グループのメンバーによって、グループのマスター電力およびチャネル スキームを管理する RF グループ リーダーが選ばれます。RF グループ アルゴリズムは、RF グループ リーダーを動的に選択し、RF グループ リーダーが常に存在していることを確認します。グループ リーダーの割り当ては変更されることがあります（たとえば、現在の RF グループ リーダーが動作しなくなった場合、または RF グループ メンバーが大幅に変更された場合）。
- 静的モード：このモードでは、ユーザは RF グループ リーダーとしてコントローラを手動で選択します。このモードでは、リーダーとメンバーは手動で設定されて固定されます。メンバが RF グループに join できない場合は、理由が表示されます。リーダーは、メンバーが前の試行で join しなかった場合、1 分ごとにメンバーとの接続を確立しようとします。

RF グループ リーダーは、システムによって収集されたリアルタイムの無線データを分析して、パワーおよびチャネルの割り当てを算出し、RF グループの各コントローラに送信します。RRM アルゴリズムによって、システム全体の安定性が保証され、チャネルおよびパワー スキームの変更を適切なローカル RF 領域に制限します。

（注） コントローラが特定の無線に対してリーダーとメンバを兼ねるようになると、グループ リーダーの一部として IPv4 および IPv6 アドレスが表示されます。

コントローラ A がメンバになり、コントローラ B がリーダーになると、コントローラ A は接続先のアドレスを使用して、コントローラ B の IPv4 アドレスまたは IPv6 アドレスのどちらかを表示します。

したがって、リーダーとメンバーの両方が同じでない場合は、メンバーのグループ リーダーとして IPv4 または IPv6 アドレスが 1 つだけ表示されます。

動的チャネル割り当て（DCA）が新しいチャネル計画を適用するための唯一の基準として最もパフォーマンスの低い無線を使用する必要がある場合、ピンニングまたはカスケードの問題が発生する可能性があります。

ピンニングが発生するのは、アルゴリズムによって RF グループの一部の無線に適したチャネル計画が検出されても、ネットワーク内の最も条件の悪い無線には適したチャネルオプションがないため、チャネル計画の変更が実施されない場合です。RF グループ内の最も条件の悪い無線によって、グループ内の他の無線がより適切なチャネル計画を探すことができなくなる場合があります。ネットワークの規模が大きければ大きいほど、よりピンニングになりやすいです。

1 つの無線のチャネルが変更された場合に、RF 領域の残りの無線を最適化するため、連続してチャネル変更が行われると、カスケードが発生します。このような無線を最適化すると、ネイバーおよびネイバーのチャネル計画が次善のものになり、チャネル最適化が起動されます。この影響は、すべてのアクセス ポイント無線が同じ RF グループに属している場合、複数のフロアまたは複数の建物に広がることがあります。この変更は、大きなクライアントの混乱を引き起こし、ネットワークを不安定にします。

ピンニングとカスケードの両方の主な原因は、潜在的なチャネル計画の変更が最もパフォーマンスの低い無線の RF 状態によって制御されることです。DCA アルゴリズムはこれを実行せず、代わりに次の処理を行います。

- 複数のローカル検索：DCA 検索アルゴリズムでは、単一の無線による単一のグローバル検索ではなく、同じ DCA の処理内で異なる無線によって開始される複数のローカル検索が実行されます。この変更によって、ピンニングとカスケードの両方に対応できるだけでなく、安定性を損なうことなく、DCA に必要な柔軟性と適合性が維持されます。
- 複数のチャネル計画変更イニシエータ（CPCI）：以前は、最も条件の悪い単一の無線が、チャネル計画変更の唯一のイニシエータでした。今では、RF グループ内の各無線が評価されて、イニシエータ候補として優先順位付けされるようになりました。生成されたリストはインテリジェントにランダム化されるので、最終的にすべての無線が評価され、ピンニングが発生する可能性はなくなります。
- チャネル計画変更の適用制限（ローカリゼーション）：各 CPCI 無線の場合、DCA アルゴリズムは適切なチャネル計画を求めてローカル検索を実行しますが、実際には CPCI 無線自身および 1 ホップ近隣のアクセス ポイントのみが現在の送信チャネルを変更できます。アクセス ポイントによるチャネル計画変更のトリガーの影響は、そのアクセス ポイント

の 2 RF ホップ内だけで認識され、実際のチャネル計画変更は 1 ホップ RF 領域内に制限されます。この制限はすべての CPCI 無線にわたって適用されるため、カスケードが発生する可能性はありません。

- 非 RSSI ベースの累積コスト メトリック：累積コスト メトリックによって、全範囲、領域、またはネットワークが指定のチャネル計画でどの程度のパフォーマンスを示すのかを測定します。チャネル計画の品質全体を把握する目的で、その領域内にあるすべてのアクセス ポイントに関する個々のコスト メトリックが考慮されます。これらのメトリックの使用で、すべてのチャネル計画変更に単一の各無線の品質の向上または低下が含まれるようになります。その目的は、単一の無線の品質は向上するが、他の複数の無線のパフォーマンスが大幅に低下するような、チャネル計画変更を避けることです。

RRM アルゴリズムは、指定された更新間隔（デフォルトでは 600 秒）で実行されます。更新間隔の合間に、RF グループ リーダーは各 RF グループ メンバにキープアライブ メッセージを送信し、リアルタイムの RF データを収集します。

（注） 複数の監視間隔を使用することもできます。詳細については、「RRM の設定」の項を参照してください。

RF グループ名

コントローラには RF グループ名が設定されます。この RF グループ名は、そのコントローラに参加しているすべてのアクセス ポイントに送信され、アクセス ポイントでは、この名前がハッシュ MIC をネイバー メッセージで生成するための共有秘密として使用されます。RF グループを作成するには、グループに含めるすべてのコントローラに同じ RF グループ名を設定します。

コントローラに参加しているアクセス ポイントが別のコントローラ上のアクセス ポイントから RF 伝送を受け取る可能性がある場合は、それらのコントローラに同じ RF グループ名を設定する必要があります。アクセス ポイント間の RF 伝送を受信する可能性がある場合、802.11 干渉およびコンテンションをできるだけ回避するには、システム全体にわたる RRM が推奨されます。

RF グループ内の不正アクセス ポイント検出

コントローラの RF グループを作成したら、コントローラに接続されているアクセス ポイントを、不正アクセスポイントを検出するように設定する必要があります。設定すると、アクセスポイントによって、隣接アクセス ポイントのメッセージ内のビーコンまたはプローブ応答フレームが選択され、RF グループの認証情報要素（IE）と一致するものが含まれているかどうかが確認されます。選択が正常に終了すると、フレームは認証されます。正常に終了しなかった場合は、認証されているアクセス ポイントによって、近隣のアクセス ポイントが不正アクセス ポイントとして報告され、その BSSID が不正テーブルに記録されます。さらに、このテーブルはコントローラに送信されます。

送信電力の制御

deviceは、リアルタイムの無線 LAN 状況に基づいて、アクセス ポイントの送信電力を動的に制御します。

伝送パワー コントロール（TPC）アルゴリズムによって、RF 環境での変化に応じて、アクセス ポイントの電力が増減します。多くの場合、TPC は干渉を低減させるため、アクセス ポイントの電力を下げようとします。しかし、アクセス ポイントで障害が発生したり、アクセス ポイントが無効になったりして、RF カバレッジに急激な変化が発生すると、TPC は周囲のアクセスポイントで電力を上げることもあります。この機能は、主にクライアントと関係があるカバレッジ ホールの検出とは異なります。TPC はアクセス ポイント間におけるチャネルの干渉を回避しながら、必要なカバレッジ レベルを達成するために、十分な RF 電力を提供します。

最小/最大送信電力の設定による TPC アルゴリズムの無効化

TPC アルゴリズムは、数多くのさまざまな RF 環境で RF 電力を分散させます。ただし、自動電力制御では、アーキテクチャの制限事項やサイトの制限事項のため、適切な RF 設計を実装できなかった一部のシナリオは解決できない可能性があります。たとえば、すべてのアクセス ポイントを互いに近づけて中央の廊下に設置する必要があるが、建物の端までカバレッジが必要とされる場合などです。

このようなケースでは、最大および最小の送信電力制限を設定し、TPC の推奨を無効化することができます。最大および最小の TPC 電力設定は、RF ネットワークの RF プロファイルを通じてすべてのアクセス ポイントに適用されます。

[Maximum Power Level Assignment] および [Minimum Power Level Assignment] を設定するには、[Tx Power Control] ウィンドウのフィールドに、RRM で使用される最大および最小の送信電力を入力します。これらのパラメータの範囲は -10 ～ 30 dBm です。最小値を最大値よりも大きくしたり、最大値を最小値よりも小さくしたりすることはできません。

最大送信電力を設定すると、RRM では、deviceに接続されているすべてのアクセス ポイントはこの送信電力レベルを上回ることはできません（電力が RRM TPC またはカバレッジ ホールの検出のどちらで設定されるかは関係ありません）。たとえば、最大送信電力を 11 dBm に設定すると、アクセス ポイントを手動で設定しない限り、アクセス ポイントが 11 dBm を上回って伝送を行うことはありません。

チャネルの動的割り当て

同じチャネル上の 2 つの隣接するアクセスポイントによって、信号のコンテンションや信号の衝突が発生することがあります。衝突の場合、アクセス ポイントではデータが受信されません。この機能は問題になることがあります。たとえば、誰かがカフェで電子メールを読むことで、近隣の会社のアクセスポイントのパフォーマンスに影響が及ぶような場合です。これらがまったく別のネットワークであっても、チャネル 1 を使用してカフェにトラフィックが送信されることによって、同じチャネルを使用している会社の通信が妨害される可能性があります。Devicesはアクセス ポイント チャネル割り当てを動的に割り当てて、衝突を回避し、キャパシ

ティとパフォーマンスを改善することができます。チャネルは、希少な RF リソースの浪費を防ぐために再利用されます。つまり、チャネル 1 はカフェから離れた別のアクセス ポイントに割り当てられます。これは、チャネル 1 をまったく使用しない場合に比べてより効率的です。

device の動的チャネル割り当て（DCA）機能は、アクセス ポイント間における隣接するチャネルの干渉を最小限に抑える上でも役立ちます。たとえば、チャネル 1 とチャネル 2 など、802.11b/g 帯域でオーバーラップする 2 つのチャネルは、同時に 11 または 54 Mbps を使用できません。device は、チャネルを効果的に再割り当てすることによって、隣接するチャネルを分離します。

（注） 非オーバーラップ チャネル（1、6、11 など）だけを使用することをお勧めします。

（注） チャネルの変更時に、無線をシャットダウンする必要はありません。

device は、さまざまなリアルタイムの RF 特性を検証して、次のようにチャネルの割り当てを効率的に処理します。

- アクセス ポイントの受信エネルギー：各アクセス ポイントとその近隣のアクセス ポイント間で測定された受信信号強度。チャネルを最適化して、ネットワーク キャパシティを最大にします。
- ノイズ：ノイズによって、クライアントおよびアクセスポイントの信号の品質が制限されます。ノイズが増加すると、有効なセル サイズが小さくなり、ユーザ エクスペリエンスが低下します。device では、ノイズ源を避けるようにチャネルを最適化することで、システム キャパシティを維持しながらカバレッジを最適化できます。過剰なノイズのためにチャネルが使用できない場合は、そのチャネルを回避できます。
- 802.11 干渉：干渉とは、不正アクセス ポイントや隣接するワイヤレス ネットワークなど、ワイヤレス LAN に含まれない 802.11 トラフィックのことです。Lightweight アクセス ポイントは、常にすべてのチャネルをスキャンして干渉の原因を調べます。802.11 干渉の量が定義済みの設定可能なしきい値（デフォルトは 10 %）を超えると、アクセス ポイントから device にアラートが送信されます。その場合、device では、RRM アルゴリズムを使用してチャネルの割り当てを動的に調整することで、干渉がある状況でシステム パフォーマンスを向上させることができます。このような調整によって、隣接する Lightweight アクセス ポイントが同じチャネルに割り当てられることがありますが、この設定は、干渉している外部アクセス ポイントが原因で使用できないチャネルにアクセス ポイントを割り当てたままにしておくよりも効果的です。

  また、他のワイヤレス ネットワークがある場合、device は、他のネットワークを補足するようにチャネルの使用を変更します。たとえば、チャネル 6 に 1 つのネットワークがある場合、隣接する無線 LAN はチャネル 1 または 11 に割り当てられます。この調整によって、周波数の共有が制限され、ネットワークのキャパシティが増加します。チャネルにキャパシティがほとんど残っていない場合、device はそのチャネルを回避できます。すべ

ての非オーバーラップ チャネルが使用される非常に大規模な展開では、deviceでも最適な処理が行われますが、期待値を設定する際に RF 密度を考慮する必要があります。

- 負荷および利用率：利用率の監視が有効な場合、たとえば、ロビーとエンジニアリング エリアを比較して、一部のアクセス ポイントが他のアクセス ポイントよりも多くのトラフィックを伝送するように展開されていることを、キャパシティの計算で考慮できます。deviceは、パフォーマンスが最も低いアクセス ポイントを改善するようにチャネルを割り当てることができます。チャネル構造を変更する際には、負荷を考慮して、現在ワイヤレス LAN に存在するクライアントへの影響を最小限に抑えるようにします。このメトリックによって、すべてのアクセス ポイントの送信パケットおよび受信パケットの数が追跡されて、アクセス ポイントのビジー状態が測定されます。新しいクライアントは過負荷のアクセス ポイントを回避し、別のアクセス ポイントにアソシエートします。*Load and utilization* パラメータはデフォルトでは無効になっています。

deviceは、この RF 特性情報を RRM アルゴリズムとともに使用して、システム全体にわたる判断を行います。相反する要求の解決にあたっては、軟判定メトリックを使用して、ネットワーク干渉を最小限に抑えるための最善の方法が選択されます。最終的には、3 次元空間における最適なチャネル設定が実現します。この場合、上下のフロアにあるアクセス ポイントが全体的な無線 LAN 設定において主要な役割を果たします。

（注） DCA は 2.4 GHz 帯域の 20 MHz チャネルのみサポートしています。

RRM スタートアップ モードは、次のような状況で起動されます

- シングルdevice環境では、deviceをアップグレードしてリブートすると、RRM スタートアップ モードが起動します。
- マルチdevice環境では、RRM スタートアップ モードは、RF グループ リーダーが選定されてから起動されます。

RRM スタートアップ モードは CLI からトリガーできます。

RRM スタートアップ モードは、100 分間（10 分間隔で 10 回繰り返し）実行されます。RRM スタートアップ モードの持続時間は、DCA 間隔、感度、およびネットワーク サイズとは関係ありません。スタートアップ モードは、定常状態のチャネル計画に収束するための高感度な（環境に対するチャネルを容易かつ敏感にする）10 回の DCA の実行で構成されます。スタートアップ モードが終了した後、DCA は指定した間隔と感度で実行を継続します。

（注） DCA アルゴリズム間隔は 1 時間に設定されますが、DCA アルゴリズムは常に 10 分間隔（デフォルト）で実行されます。最初の 10 サイクルでは 10 分ごとにチャネル割り当てが行われ、チャネルの変更は、DCA アルゴリズムに従って 10 分ごとに行われます。その後、DCA アルゴリズムは設定された時間間隔に戻ります。DCA アルゴリズム間隔は定常状態に従うため、DCA 間隔とアンカー時間の両方に共通です。

（注） RF グループ メンバーで動的チャネル割り当て（DCA）/伝送パワーコントロール（TPC）がオフになっていて、RF グループ リーダーが自動に設定されている場合、メンバーのチャネルまたは送信パワーは、RF グループ リーダーで実行されるアルゴリズムに従って変更されます。

動的帯域幅選択

11n から 11ac にアップグレードする際、動的帯域幅選択（DBS）アルゴリズムにより、さまざまな設定の移行がスムーズに行えます。

DBS の機能のポイントを以下に説明します。

- チャネル幅を動的に変更してネットワークのスループットを最大化する目的で、コア DCA に適用される階層に加えて、チャネル割り当てを行うバイアス層をさらに適用します。
- チャネルと Base Station Subsystem（BSS）の統計情報を常に監視することで、チャネル割り当てを調整します。
- 11n または 11ac クライアントの混在、負荷、トラフィック フロー タイプなどの一時パラメータを評価します。
- 高速に変化する統計情報に対しては、BSS チャネル幅を変化させるか、または 40 MHz ～ 80 MHz の帯域幅を選択できるように 11ac を介して一意の新しいチャネル方向に適応することで対応します。

カバレッジ ホールの検出と修正

RRM カバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線 LAN の無線カバレッジの領域を検出することができます。この機能によって、Lightweight アクセス ポイントを追加（または再配置）する必要があるというアラートが生成されます。

RRM 設定で指定されたレベルを下回るしきい値レベル（RSSI、失敗したクライアントの数、失敗したパケットの割合、および失敗したパケットの数）で Lightweight アクセス ポイント上のクライアントが検出されると、アクセス ポイントからdeviceに「カバレッジホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセスポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。device では、修正可能なカバレッジ ホールと不可能なカバレッジ ホールが識別されます。修正可能なカバレッジホールの場合、deviceでは、その特定のアクセス ポイントの送信電力レベルを上げることによってカバレッジホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジホールがdeviceによって解消されることはありません。ダウンストリームの送信電力を増加させても、ネットワーク内の干渉を増加させる可能性があるからです。

無線リソース管理の制約事項

RF グループの AP の数は 3000 に限定されています。

AP の最大数をすでに保持している RF グループに AP が join しようとすると、デバイスはアプリケーションを拒否し、エラーをスローします。

RRM の設定方法

ネイバー探索タイプの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。

ステップ 2 [Radio Resource Management] ページで、[5 GHz Band] または [2.4 GHz Band] のいずれかのタブをクリックします。

ステップ 3 [General] タブの [Noise/Interference/Rogue/CleanAir# Monitoring Channels] で、[RRM Neighbor Discover Type] ドロップダウン リストから [Transparent] または [Protected] のいずれかを選択します。

ステップ 4 設定を保存します。

ネイバー探索タイプの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz | 5ghz rrm ndp-type {protected | transparent}** 例： `Device(config)#ap dot11 24ghz rrm ndp-type protected` `Device(config)#ap dot11 24ghz rrm ndp-type transparent`	ネイバー探索タイプを設定します。デフォルトでは、モードは「transparent」に設定されます。 • [protected]：セキュアな通信にネイバー探索タイプを「protected」に設定します。 パケットが暗号化されます。

	コマンドまたはアクション	目的
		• [transparent]：ネイバー探索タイプを「transparent」に設定します。パケットはそのまま送信されます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RF グループの設定

この項では、GUI または CLI によって RF グループを設定する方法について説明します。

（注） 複数の Country Code 機能を使用している場合、同じ RF グループに join する予定のすべてのコントローラは、同じ国で構成された一連の国々を同じ順序で設定する必要があります。

（注） Auto モードでは、RF グループ リーダーは RF グループ安定化のためにグループ設定サイクルの最初の 3 回のランでは、TP と DCA をスキップします。

RF グループ選択モードの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。

ステップ 2 [RRM] ページで、関連する帯域のタブ（[5 GHz Band] または [2.4 GHz Band]）をクリックします。

ステップ 3 [RF Grouping] タブをクリックします。

ステップ 4 次のオプションから適切な [Group Mode] を選択します。

- Automatic：802.11 RF グループ選択を自動更新モードに設定します。
- Leader：802.11 RF グループ選択をリーダー モードに設定します。
- Off：802.11 RF グループ選択を無効にします。

ステップ 5 設定を保存します。

RF グループ選択モードの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz | 5ghz rrm group-mode{auto | leader | off}** 例： `Device(config)#ap dot11 24ghz rrm group-mode leader`	802.11 帯域の RF グループ選択モードを設定します。 • [auto]：802.11 RF グループ選択を自動更新モードに設定します。 • [leader]：リーダー モードで 802.11 RF グループ選択をリーダー モードに設定します。 • [off]：802.11 RF グループ選択をディセーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RF グループ名の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless rf-network** *name* 例： `Device (config)# wireless rf-network test1`	RF グループを作成します。グループ名は、最大 19 文字の ASCII 文字列で、大文字と小文字が区別されます。 （注） RF グループに含める各コントローラについて、この手順を繰り返します。
ステップ 3	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config)# end`	ンフィギュレーション モードを終了できます。

802.11 静的 RF グループのメンバの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。

ステップ 2 [RRM] ページで、[5 GHz Band] タブまたは [2.4 GHz Band] タブをクリックします。

ステップ 3 [RF Grouping] タブをクリックします。

ステップ 4 次のオプションから適切な [Group Mode] を選択します。

- [Automatic]（デフォルト）：RF グループのメンバによって、グループのマスター電力とチャネル スキームを管理する RF グループ リーダーが選ばれます。RF グループ アルゴリズムは、RF グループ リーダーを動的に選択し、RF グループ リーダーが常に存在していることを確認します。グループ リーダーの割り当ては変更されることがあります（たとえば、現在の RF グループ リーダーが動作しなくなった場合、または RF グループ メンバが大幅に変更された場合）。
- [Leader]：RF グループ リーダーとしてデバイスが手動で選ばれます。このモードでは、リーダーおよびメンバは手動で設定され、固定されます。メンバが RF グループに join できない場合は、理由が表示されます。メンバの管理IPアドレスとシステム名を使用して、リーダーに参加するようにメンバに要求します。メンバが前の試行で参加しなかった場合、リーダーは 1 分ごとにメンバとの接続の確立を試みます。
- [Off]：RF グループは設定されません。

ステップ 5 [Group Members] セクションで、[Add] をクリックします。

ステップ 6 表示される [Add Static Member] ウィンドウで、コントローラの名前と、コントローラの IPv4 または IPv6 アドレスを入力します。

ステップ 7 [Save & Apply to Device] をクリックします。

802.11 静的 RF グループのメンバの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**ap dot11 24ghz | 5ghz rrm group-member** *group_name ip_addr* 例： `Device(config)#ap dot11 24ghz rrm group-member Grpmem01 10.1.1.1`	802.11 静的 RF グループにメンバを設定します。グループ メンバをアクティブにするには、グループモードをリーダーに設定する必要があります。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力制御の設定

送信電力の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。

ステップ 2 [5 GHz Band] タブまたは [2.4 GHz Band] タブのいずれかで、[TPC] タブをクリックします。

ステップ 3 次の動的送信電力割り当てモードを選択します。

- [Automatic]（デフォルト）：送信電力は、この動作を許可するすべての AP で定期的に更新されます。
- [On Demand]：送信電力はオンデマンドで更新されます。このオプションを選択すると、[Invoke Power Update Once] が表示されます。RRM データを正常に適用するには、[Invoke Power Update Once] をクリックします。
- [Fixed]：動的な送信電力の割り当ては行われず、値はグローバルデフォルトに設定されます。

ステップ 4 この無線での最大および最小電力レベルの割り当てを入力します。最大送信電力を設定すると、RRM では、デバイスに接続されているすべてのアクセス ポイントはこの送信電力レベルを上回ることはできません（電力が RRM TPC で設定されているかカバレッジ ホールの検出で設定されているかは関係ありません）。たとえば、最大送信電力を 11 dBm に設定すると、アクセス ポイントを手動で設定しない限り、アクセス ポイントが 11 dBm を上回る伝送を行うことはありません。範囲は -10 ～ 30 dBmです。

ステップ 5 [Power Threshold] フィールドに、アクセス ポイントの電力を減らすかどうかを判断する際に RRM で使用する切断信号レベルを入力します。

このパラメータのデフォルト値は、選択した TPC バージョンによって異なります。TPCv1 の場合、デフォルト値は -70 dBm です。TPCv2 の場合、デフォルト値は -67 dBm です。アクセス

ポイントの送信電力レベルが必要以上に高い（または低い）場合は、デフォルト値を変更できます。このパラメータの範囲は –80 ～ –50 dBm です。

この値を –65 ～ –50 dBm の範囲で増やすと、アクセス ポイントは高い送信電力で動作するようになります。値を減らすと、逆の効果が得られます。多数のアクセス ポイントを設定している場合、ワイヤレス クライアントが認識する BSSID（アクセス ポイント）やビーコンの数を少なくするために、しきい値を –80 dBm または –75 dBm に下げるのが有用です。一部のワイヤレス クライアントは多数の BSSID や高速ビーコンを処理できない場合があり、デフォルトのしきい値では、問題のある動作を起こす可能性があります。

ステップ 6 [Apply] をクリックします。

送信電力制御のしきい値の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz | 5ghz rrm tpc-threshold** *threshold_value* 例： `Device(config)#ap dot11 24ghz rrm tpc-threshold -60`	自動電力割り当てのために RRM が使用する送信電力制御のしきい値を設定します。範囲は -80 ～ -50 です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

送信電力レベルの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**ap dot11 24ghz | 5ghz rrm txpower**{*trans_power_level* | **auto** | **max** | **min** | **once**} 例： `Device(config)#ap dot11 24ghz rrm txpower auto`	802.11 の送信電力レベルを設定します。 • [trans_power_level]：送信電力レベルを設定します。 • [auto]：自動 RF をイネーブルにします。 • [max]：最大自動 RF 送信電力を設定します。 • [min]：最小自動 RF 送信電力を設定します。 • [once]：自動 RF を一度だけイネーブルにします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 RRM パラメータの設定

高度な 802.11 チャネル割り当てパラメータの設定（GUI）

手順

ステップ 1　**[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。

ステップ 2　[DCA] タブで、[Channel Assignment Mode] を選択して、DCA モードを指定します。

- [Automatic]：デバイスによって、参加しているすべての AP についてチャネル割り当てが定期的に評価され、必要に応じて更新されます。
- [Freeze]：デバイスによって、参加しているすべての AP についてチャネル割り当てが評価され更新されます。このオプションを選択すると、[Invoke Channel Update Once] が表示されます。RRM データを正常に適用するには、[Invoke Channel Update Once] をクリックします。
- [Off]：DCA をオフにし、すべての AP の無線を帯域の最初のチャネル（デフォルト値）に設定します。このオプションを選択する場合は、すべての無線のチャネルを手動で割り当てる必要があります。

ステップ 3 [Interval] ドロップダウン リストで、DCA アルゴリズムの実行を許可する間隔を選択します。デフォルトの間隔は 10 分です。

ステップ 4 [AnchorTime] ドロップダウン リストで、DCA アルゴリズムの開始時刻を指定する数値を選択します。オプションは、0 ～ 23 の数値（両端の値を含む）で、午前 12 時～午後 11 時の時刻を表します。

ステップ 5 [Avoid Foreign AP Interference] チェックボックスをオンにすると、デバイスの RRM アルゴリズムで、Lightweight AP にチャネルを割り当てるときに、外部 AP（無線ネットワークに含まれないもの）からの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、チェックボックスをオフにします。たとえば RRM では、外部 AP に近いチャネルをアクセス ポイントに回避させるようにチャネル割り当てを調整できます。デフォルトでは、この機能は有効な状態です。

ステップ 6 [Avoid Cisco AP Load] チェックボックスをオンにすると、デバイスの RRM アルゴリズムで、チャネルを割り当てるときに、無線ネットワーク内の Cisco Lightweight AP からの 802.11 トラフィックが考慮されます。この機能を無効にする場合は、チェックボックスをオフにします。たとえば RRM では、トラフィックの負荷が高いアクセス ポイントに対して、より適切な再利用パターンを割り当てることができます。デフォルトでは、この機能は無効の状態です。

ステップ 7 [Avoid Non-802.11a Noise] チェックボックスをオンにすると、デバイスの RRM アルゴリズムで、Lightweight AP にチャネルを割り当てるときに、ノイズ（802.11 以外のトラフィック）が考慮されます。この機能を無効にする場合は、チェックボックスをオフにします。たとえば RRM では、電子レンジなど、AP 以外を原因とする重大な干渉があるチャネルを AP に回避させることができます。デフォルトでは、この機能は有効な状態です。

ステップ 8 [Avoid Persistent Non-WiFi Interference] チェックボックスをオンにすると、デバイスが WiFi 以外の持続的な干渉を無視できるようになります。

ステップ 9 [DCA Channel Sensitivity] ドロップダウン リストから、次のオプションのいずれかを選択して、チャネルを変更するかどうかを判断する際の、信号、負荷、ノイズ、干渉などの環境の変化に対する DCA アルゴリズムの感度を指定します。

- [Low]：環境の変化に対する DCA アルゴリズムの感度は特に高くありません。DCA しきい値は 5 dB です。
- [Medium]（デフォルト）：環境の変化に対する DCA アルゴリズムの感度は中程度です。DCA しきい値は 15 dB です。
- [High]：環境の変化に対する DCA アルゴリズムの感度が高くなります。DCA しきい値は 30 dB です。

ステップ 10 必要に応じて、[Channel Width] を設定します。RF のチャネル幅として、[20 MHz]、[40 MHz]、[80 MHz]、[160 MHz]、または [Best] を選択できます。これは 802.11a/n/ac（5 GHz）無線にのみ適用されます。

ステップ 11 [Auto-RF Channel List] セクションには、現在選択されているチャネルが表示されます。チャネルを選択するには、対応するチェックボックスをオンにします。

ステップ 12 [Event Driven RRM] セクションで、CleanAir 対応 AP が重大なレベルの干渉を検出したときに RRM を実行するには、[EDRRM] チェックボックスをオンにします。有効にした場合は、RRM が起動される感度しきい値レベルを設定し、カスタムしきい値を入力し、不正なデューティサイクルを開始する場合は [Rogue Contribution] チェックボックスをオンにします。

ステップ 13 [Apply] をクリックします。

高度な 802.11 チャネル割り当てパラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**high** | **low** | **medium**} 例： `Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high`	CleanAir のイベント駆動型 RRM パラメータを設定します。 • [High]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最高に指定します。 • [Low]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を最低に指定します。 • [Medium]：電波品質（AQ）値が示す非 Wi-Fi 干渉への感度を中間に指定します。
ステップ 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel dca** {**add** *channel-number* | **anchor-time** | **global** {**auto** | **once**} | **interval** | **min-metric** | **remove** *channel-number* | **sensitivity** {**high** | **low** | **medium**}} 例： `Device(config)#ap dot11 24ghz rrm channel dca interval 2`	802.11 帯域の動的チャネル割り当て（DCA）アルゴリズムパラメータを設定します。 • **add** *channel-number*：DCA リストに追加するチャネル番号を入力します。範囲は 1 ～ 14 です。 • [anchor-time]：DCA のアンカー時間を設定します。範囲は 0 ～ 23 時間です。 • [global]：すべての 802.11 Cisco AP の DCA モードを設定します。 • [auto]：自動 RF をイネーブルにします。 • [once]：自動 RF を一度だけイネーブルにします。

	コマンドまたはアクション	目的
		• [interval]：DCA のインターバル値を設定します。値は1、2、3、4、6、8、12、24時間です。デフォルト値 0 は 10 分を意味します。 • [min-metric]：DCA の最小 RSSI エネルギー メトリックを設定します。範囲は -100 ～ -60 です。 • **remove** *channel-number*：DCA リストから削除するチャネル番号を入力します。範囲は 1 ～ 14 です。 • [sensitivity]：環境の変化に対する DCA 感度レベルを設定します。 • [high]：最高の感度を指定します。 • [low]：最低の感度を指定します。 • [medium]：中間の感度を指定します。
ステップ 4	**ap dot11 5ghz rrm channel dca chan-width** {**20** | **40** | **80** | **best** | **160** | **best maximum** {**20** | **40** | **80** | **MAX**}} 例： `Device(config)#ap dot11 5ghz rrm channel dca chan-width best`	5 GHz 帯域のすべての 802.11 無線に対する DCA チャネル幅を設定します。チャネル幅を [20 MHz]、[40 MHz]、[80 MHz]、または [Best] に設定します。チャネル幅のデフォルト値は 20 MHz です。[Best] のデフォルト値は 80 MHz です。制約を設定する場合は、事前にチャネル帯域幅を [Best] に設定します。
ステップ 5	**ap dot11 5ghz rrm channel dca chan-width width-max** {**WIDTH_20MHz** | **WIDTH_40MHz** | **WIDTH_80MHz** | **WIDTH_MAX**} 例： `Device(config)#ap dot11 5ghz rrm channel dca chan-width width-max WIDTH_80MHz`	チャネルに割り当てることができる最大チャネル帯域幅を設定します。この例では、*WIDTH_80MHz* はチャネル帯域幅を 20 MHz、40 MHz、または 80 MHz に割り当てますが、それよりも大きい値は割り当てません。
ステップ 6	**ap dot11** {**24ghz** | **5ghz**} **rrm channel device** 例：	802.11 チャネル割り当てで、非 Wi-Fi デバイスの継続的な回避を設定します。

	コマンドまたはアクション	目的
	`Device(config)#ap dot11 24ghz rrm channel device`	
ステップ 7	**ap dot11** {**24ghz** | **5ghz**} **rrm channel foreign** 例： `Device(config)#ap dot11 24ghz rrm channel foreign`	チャネル割り当てで、外部 AP の 802.11 干渉の回避を設定します。
ステップ 8	**ap dot11** {**24ghz** | **5ghz**} **rrm channel load** 例： `Device(config)#ap dot11 24ghz rrm channel load`	チャネル割り当てで、Cisco AP の 802.11 負荷の回避を設定します。
ステップ 9	**ap dot11** {**24ghz** | **5ghz**} **rrm channel noise** 例： `Device(config)#ap dot11 24ghz rrm channel noise`	チャネル割り当てで、802.11 ノイズの回避を設定します。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 カバレッジ ホール検出の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択して、802.11a/n/ac（5 GHz）および 802.11b/g/n（2.4 GHz）無線の無線リソース管理パラメータを設定します。

ステップ 2 [Radio Resource Management] ページで、[Coverage] タブをクリックします。

ステップ 3 カバレッジ ホール検出を有効にするには、[Enable Coverage Hole Detection] チェックボックスをオンにします。

ステップ 4 [Data Packet Count] フィールドに、データ パケットの数を入力します。

ステップ 5 [Data Packet Percentage] フィールドに、データ パケットの割合を入力します。

ステップ 6 [Data RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ～ -90 dBm です。デフォルト値は -80 dBm です。

ステップ 7 [Voice Packet Count] フィールドに、音声データ パケットの数を入力します。

ステップ 8 [Voice Packet Percentage] フィールドに、音声データ パケットの割合を入力します。

ステップ 9 [Voice RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ～ -90 dBm です。デフォルト値は -80 dBm です。

ステップ 10 [Minimum Failed Client per AP] フィールドに、信号対雑音比（SNR）がカバレッジしきい値より低い AP 上の最小クライアント数を入力します。値の範囲は 1 ～ 75 で、デフォルト値は 3 です。

ステップ 11 [Percent Coverage Exception Level per AP] フィールドに、目的のカバレッジしきい値未満で動作しているアクセス ポイントの無線上におけるクライアントの最大必要割合を入力し、[Apply] をクリックします。値の範囲は 0 ～ 100% で、デフォルト値は 25% です。

802.11 カバレッジ ホール検出の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz | 5ghz rrm coverage data**{**fail-percentage | packet-count | rssi-threshold**} 例： `Device(config)#ap dot11 24ghz rrm coverage data fail-percentage 60`	データ パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンク データ パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100 % の範囲で設定します。 • [packet-count]：アップリンク データ パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：データ パケットの 802.11 最小受信カバレッジ レベルを、-90 ～ 60 dBm の範囲で設定します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm coverage exception global** 例外レベル 例： `Device(config)#ap dot11 24ghz rrm coverage exception global 50`	802.11 Cisco AP のカバレッジ例外レベルを、0 ～ 100 % の範囲で設定します。

	コマンドまたはアクション	目的
ステップ 4	**ap dot11 24ghz | 5ghz rrm coverage level global** *cli_min* 例外レベル 例： `Device(config)#ap dot11 24ghz rrm coverage level global 10`	802.11 Cisco AP クライアントの最小例外を、1 ～ 75 の範囲で指定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm coverage voice**{**fail-percentage | packet-count | rssi-threshold**} 例： `Device(config)#ap dot11 24ghz rrm coverage voice packet-count 10`	音声パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンク音声パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100 % の範囲で設定します。 • [packet-count]：アップリンク音声パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：音声パケットの 802.11 最小受信カバレッジ レベルを、-90 ～ -60 dBm の範囲で設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 イベント ロギングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz | 5ghz rrm logging**{**channel | coverage | foreign | load | noise | performance | txpower**} 例：	各種パラメータに対するイベント ロギングを設定します。 • [channel]：802.11 チャネル変更ロギング モードを設定します。

	コマンドまたはアクション	目的
	Device(config)#**ap dot11 24ghz rrm logging channel** Device(config)#**ap dot11 24ghz rrm logging coverage** Device(config)#**ap dot11 24ghz rrm logging foreign** Device(config)#**ap dot11 24ghz rrm logging load** Device(config)#**ap dot11 24ghz rrm logging noise** Device(config)#**ap dot11 24ghz rrm logging performance** Device(config)#**ap dot11 24ghz rrm logging txpower**	• [coverage]：802.11 のカバレッジ プロファイル ロギング モードを設定します。 • [foreign]：802.11 外部干渉プロファイル ロギング モードを設定します。 • [load]：802.11 負荷プロファイル ロギング モードを設定します。 • [noise]：802.11 ノイズプロファイル ロギング モードを設定します。 • [performance]：802.11 パフォーマンス プロファイル ロギング モードを設定します。 • [txpower]：802.11 送信電力変更ロギング モードを設定します。
ステップ 3	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 統計情報の監視の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択して、802.11a/n/ac（5 GHz）および 802.11b/g/n（2.4 GHz）無線の無線リソース管理パラメータを設定します。

ステップ 2 [Monitor Intervals(60 to 3600secs)] セクションで、次の手順を実行します。

a) 802.11 ノイズ測定間隔（チャネル スキャン間隔）を設定するには、[AP Noise Interval] を設定します。有効な範囲は 60 ～ 3600 秒です。

b) 802.11 信号測定間隔（ネイバー パケットの頻度）を設定するには、[AP Signal Strength Interval] を設定します。有効な範囲は 60 ～ 3600 秒です。

c) 802.11 カバレッジ測定間隔を設定するには、[AP Coverage Interval] を設定します。有効な範囲は 60 ～ 3600 秒です。

d) 802.11 負荷測定を設定するには、[AP Load Interval] を設定します。有効な範囲は 60 ～ 3600 秒です。

ステップ 3 [Apply] をクリックします。

802.11 統計情報の監視の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz | 5ghz rrm monitor channel-list**{**all | country | dca**} 例： `Device(config)#ap dot11 24ghz rrm monitor channel-list all`	noise/interference/rogue などのパラメータに 802.11 監視チャネル リストを設定します。 • [all]：すべてのチャネルを監視します。 • [country]：設定された国コードで使用するチャネルを監視します。 • [dca]：動的なチャネル割り当てで使用されるチャネルを監視します。
ステップ 3	**ap dot11 24ghz | 5ghz rrm monitor coverage** *interval* 例： `Device(config)#ap dot11 24ghz rrm monitor coverage 600`	802.11 のカバレッジ測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 4	**ap dot11 24ghz | 5ghz rrm monitor load** *interval* 例： `Device(config)#ap dot11 24ghz rrm monitor load 180`	802.11 負荷測定間隔を、60 ～ 3600 秒の範囲で設定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm monitor noise** *interval* 例： `Device(config)#ap dot11 24ghz rrm monitor noise 360`	802.11 のノイズ測定間隔（チャネル スキャン間隔）を、60 ～ 3600 秒の範囲で設定します。
ステップ 6	**ap dot11 24ghz | 5ghz rrm monitor signal** *interval* 例：	802.11 の信号測定間隔（ネイバーパケットの頻度）を、60 ～ 3600 秒の範囲で設定します。

	コマンドまたはアクション	目的
	`Device(config)#ap dot11 24ghz rrm monitor signal 480`	
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 パフォーマンス プロファイルの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。

ステップ 2 [AP Join] ページで、プロファイルの名前をクリックするか、[Add] をクリックして新規に作成します。

ステップ 3 [Add/Edit RF Profile] ウィンドウで、[RRM] タブをクリックします。

ステップ 4 表示される [General] タブで、次のパラメータを入力します。

a) [Interference (%)] フィールドに、802.11 f 外部干渉のしきい値を 0 ～ 100 パーセントの範囲で入力します。

b) [Clients] フィールドに、802.11 Cisco AP クライアント数のしきい値を 1 ～ 75 の範囲で設定します。

c) [Noise (dBm)] フィールドに、802.11 外部ノイズのしきい値を -127 ～ 0 dBm の範囲で入力します。

d) [Utilization(%)] フィールドに、802.11 RF 使用率のしきい値を 0 ～ 100% の範囲で入力します。

ステップ 5 [Update & Apply to Device] をクリックします。

802.11 パフォーマンス プロファイルの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz | 5ghz rrm profile clients** *cli_threshold_value* 例：	802.11 Cisco AP クライアント数のしきい値を、1 ～ 75 の範囲で設定します。

	コマンドまたはアクション	目的
	`Device(config)#ap dot11 24ghz rrm profile clients 20`	
ステップ 3	**ap dot11 24ghz | 5ghz rrm profile foreign** *int_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile foreign 50`	802.11 外部干渉のしきい値を、0 ～ 100 % の範囲で設定します。
ステップ 4	**ap dot11 24ghz | 5ghz rrm profile noise** *for_noise_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile noise -65`	802.11 外部ノイズのしきい値を、-127 ～ 0 dBm の範囲で設定します。
ステップ 5	**ap dot11 24ghz | 5ghz rrm profile throughput** *throughput_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile throughput 10000`	802.11 Cisco AP スループットのしきい値を、1000 ～ 10000000 バイト/秒の範囲で設定します。
ステップ 6	**ap dot11 24ghz | 5ghz rrm profile utilization** *rf_util_threshold_value* 例： `Device(config)#ap dot11 24ghz rrm profile utilization 75`	802.11 RF 使用率のしきい値を、0 ～ 100% の範囲で設定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

高度な 802.11 RRM の設定

チャネル割り当ての有効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。

ステップ 2 [RRM] ページで、関連する帯域のタブ（[5 GHz Band] または [2.4 GHz Band]）をクリックします。

ステップ 3 [DCA] タブをクリックします。

ステップ 4 [Dynamic Channel Assignment Algorithm] セクションで、次のオプションから適切な [Channel Assignment Mode] を選択します。

- [Automatic]：チャネル割り当てを自動に設定します。
- [Freeze]：チャネル割り当てをロックします。[Invoke Channel Update Once] をクリックして、割り当てられたチャネルを更新します。

ステップ 5 [Apply] をクリックします。

チャネル割り当ての有効化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm channel-update** 例： `Device# ap dot11 24ghz rrm channel-update`	シスコ アクセス ポイントごとに 802.11 チャネル選択の更新を有効にします。 （注） **ap dot11 {24ghz | 5ghz} rrm channel-update** を有効にすると、DCA アルゴリズムのチャネル割り当てに対してトークンが割り当てられます。

DCA 動作の再開

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm dca restart** 例：	802.11 無線の DCA サイクルを再開します。

	コマンドまたはアクション	目的
	`Device# ap dot11 24ghz rrm dca restart`	

電源割り当てパラメータの更新（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [Access Points] ページで、[5GHz] または [2.4 GHz] リストから AP 名をクリックします。

ステップ 3 **[Edit Radios]** > **[Configure]** > **[Tx Power Level Assignment]** セクションで、[Assignment Method] ドロップダウン リストから [Custom] を選択します。

ステップ 4 ドロップダウン リストから [Transmit Power] の値を選択します。

ステップ 5 [Update & Apply to Device] をクリックします。

電力割り当てパラメータの更新（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap dot11** {**24ghz** | **5ghz**} **rrm txpower update** 例： `Device# ap dot11 24ghz rrm txpower update`	各シスコ アクセス ポイントの 802.11 送信電力を更新します。

RF グループ内の不正アクセス ポイント検出の設定

RF グループ内の不正アクセス ポイント検出の設定（CLI）

始める前に

RF グループ内の各コントローラに同じ RF グループ名が設定されていることを確認します。

（注） この名前は、すべてのビーコン フレーム内の認証 IE を確認するために使用されます。コントローラに異なる名前が設定されている場合は、障害アラームが生成されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *Cisco_AP* **mode**{**monitor** | **clear** | **sensor** | **sniffer**} 例： `Device# ap name ap1 mode clear`	コントローラに接続されたすべてのアクセス ポイントについて、次の手順を実行します。 次の AP 動作モードを設定します。 • **monitor**：AP モードをモニタ モードに設定します。 • **clear**：AP モードをサイトに基づいてローカルまたはリモートにリセットします。 • **sensor**：AP モードをセンサー モードに設定します。 • **sniffer**：AP モードをワイヤレス スニファ モードに設定します。
ステップ 2	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 3	**configure terminal** 例： `Device# 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 4	**wireless wps ap-authentication** 例： `Device (config)# wireless wps ap-authentication`	不正なアクセスポイントの検出をイネーブルにします。
ステップ 5	**wireless wps ap-authentication threshold** *value* 例： `Device (config)# wireless wps ap-authentication threshold 50`	不正アクセス ポイント アラームが生成されるタイミングを指定します。検出期間内にしきい値（無効な認証 IE を含むアクセス ポイント フレームの数を示します）に達した場合またはしきい値を超えた場合に、アラームが生成されます。

	コマンドまたはアクション	目的
		しきい値の有効範囲は 1 ～ 255 で、デフォルトのしきい値は1です。アラームの誤判定を防止するには、しきい値を高い値に設定してください。 （注） RF グループ内のすべてのコントローラで、不正アクセス ポイントの検出としきい値をイネーブルにします。 （注） 不正アクセス ポイントの検出が有効になっていないコントローラがRF グループ内にある場合、この機能が無効になっているコントローラ上のアクセス ポイントは不正アクセス ポイントとして報告されます。

RRM パラメータと RF グループ ステータスの監視

RRM パラメータの監視

表 *4:* 無線リソース管理を監視するためのコマンド

コマンド	説明
show ap dot11 24ghz channel	802.11b チャネル割り当ての設定および統計情報を表示します。
show ap dot11 24ghz coverage	802.11b カバレッジの設定と統計情報を表示します。
show ap dot11 24ghz group	802.11b グループ化の設定と統計情報を表示します。
show ap dot11 24ghz logging	802.11b イベント ロギングの設定と統計情報を表示します。
show ap dot11 24ghz monitor	802.11b モニタリングの設定および統計情報を表示します。
show ap dot11 24ghz profile	すべての Cisco AP の 802.11b プロファイル情報を表示します。
show ap dot11 24ghz summary	802.11b Cisco AP の設定と統計情報を表示します。
show ap dot11 24ghz txpower	802.11b 送信電力制御の設定と統計情報を表示します。

コマンド	説明
show ap dot11 5ghz channel	802.11aチャネル割り当ての設定および統計情報を表示します。
show ap dot11 5ghz coverage	802.11a カバレッジの設定と統計情報を表示します。
show ap dot11 5ghz group	802.11a グループ化の設定と統計情報を表示します。
show ap dot11 5ghz logging	802.11a イベント ロギングの設定と統計情報を表示します。
show ap dot11 5ghz monitor	802.11a モニタリングの設定および統計情報を表示します。
show ap dot11 5ghz profile	すべての Cisco AP の 802.11a プロファイル情報を表示します。
show ap dot11 5ghz summary	802.11a Cisco AP の設定と統計情報を表示します。
show ap dot11 5ghz txpower	802.11a 送信電力制御の設定と統計情報を表示します。

RF グループ ステータスの確認（CLI）

ここでは、RF グループ ステータスの新しいコマンドについて説明します。

次のコマンドを使用して、 の RF グループ ステータスを確認できます。

表 *5:* アグレッシブ ロード バランシング コマンドの確認

コマンド	目的
show ap dot11 5ghz group	802.11a RF ネットワークの RF グループ リーダーであるコントローラの名前が表示されます。
show ap dot11 24ghz group	802.11b/g RF ネットワークの RF グループ リーダーであるコントローラの名前が表示されます。

例：RF グループの設定

次に、RF グループ名を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless rf-network test1
Device(config)# ap dot11 24ghz shutdown
Device(config)# end
Device # show network profile 5
```

次に、RF グループ内の不正アクセス ポイントの検出を設定する例を示します。

```
Device# ap name ap1 mode clear
Device# end
Device# configure terminal
```

```
Device(config)# wireless wps ap-authentication
Device(config)# wireless wps ap-authentication threshold 50
Device(config)# end
```

ED-RRM について

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAir のイベント駆動型 RRM 機能を使用すると、電波品質（AQ）に対してしきい値を設定できます。しきい値を超過した場合には、影響を受けたアクセス ポイントに対してチャネル変更がただちに行われます。イベント駆動型 RRM が原因でチャネルの変更が発生すると、選択を回避するためにチャネルが 3 時間ブラックリストに登録されます。ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir では AQ 測定値を使用してスペクトラムを連続的に評価するため、対応策を 30 秒以内に実行します。たとえば、アクセス ポイントがビデオ カメラからの干渉を受けた場合は、そのカメラが動作し始めてから 30 秒以内にチャネル変更によってアクセス ポイントを回復させることができます。

Cisco 仮想エラスティック ワイヤレス LAN コントローラ上での ED-RRM の設定（CLI）

手順

ステップ 1 次のコマンドを入力して、Cisco CleanAir 対応のアクセス ポイントで非常に高いレベルの干渉が検出された場合に、イベント駆動型無線リソース管理（RRM）の実行がトリガーされるよう設定します。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event** ：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM パラメータを設定します。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event sensitivity** {**low** | **medium** | **high** | **custom**}：802.11 の Cisco Lightweight アクセス ポイントの CleanAir による RRM 感度を設定します。デフォルトの選択は、Medium です。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event custom-threshold** *custom-threshold-value*：設定されたしきい値で ED-RRM イベントをトリガーします。カスタムしきい値の範囲は 1 ～ 99 です。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution**：不正な寄与を有効にします。

ap dot11 {**24ghz** | **5ghz**} **rrm channel cleanair-event rogue-contribution duty-cycle** *thresholdvalue*：不正な寄与のしきい値を設定します。値の範囲は 1 ～ 99 で、デフォルトの値は 80 です。

ステップ 2 次のコマンドを入力して、変更を保存します。

write memory

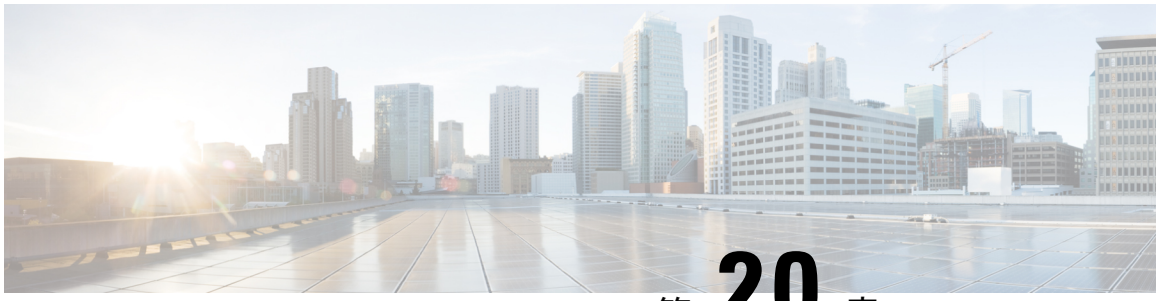
ステップ 3 次のコマンドを入力して、802.11a/n/ac または 802.11b/g/n ネットワークに対する CleanAir の設定を確認します。

show ap dot11 {24ghz | 5ghz} cleanair config

以下に類似した情報が表示されます。

```
CleanAir Solution................................ : Enabled
Air Quality Settings:
Air Quality Reporting........................ : Enabled
Air Quality Reporting Period (min)........... : 15
Air Quality Alarms........................... : Disabled
Air Quality Alarm Threshold.................. : 10
Unclassified Interference.................... : Disabled
Unclassified Severity Threshold.............. : 35
Interference Device Settings:
Interference Device Reporting................ : Enabled
BLE Beacon................................... : Enabled
Bluetooth Link............................... : Enabled
Microwave Oven............................... : Enabled
802.11 FH.................................... : Enabled
Bluetooth Discovery.......................... : Enabled
TDD Transmitter.............................. : Enabled
Jammer....................................... : Enabled
Continuous Transmitter....................... : Enabled
DECT-like Phone.............................. : Enabled
Video Camera................................. : Enabled
802.15.4..................................... : Enabled
WiFi Inverted................................ : Enabled
WiFi Invalid Channel......................... : Enabled
SuperAG...................................... : Enabled
Canopy....................................... : Enabled
Microsoft Device............................. : Enabled
WiMax Mobile................................. : Enabled
WiMax Fixed.................................. : Enabled
Interference Device Types Triggering Alarms:
BLE Beacon................................... : Disabled
Bluetooth Link............................... : Disabled
Microwave Oven............................... : Disabled
802.11 FH.................................... : Disabled
Bluetooth Discovery.......................... : Disabled
TDD Transmitter.............................. : Disabled
Jammer....................................... : Disabled
Continuous Transmitter....................... : Disabled
DECT-like Phone.............................. : Disabled
Video Camera................................. : Disabled
802.15.4..................................... : Disabled
WiFi Inverted................................ : Enabled
WiFi Invalid Channel......................... : Enabled
SuperAG...................................... : Disabled
Canopy....................................... : Disabled
Microsoft Device............................. : Disabled
WiMax Mobile................................. : Disabled
WiMax Fixed.................................. : Disabled
Interference Device Alarms................... : Disabled
AdditionalClean Air Settings:
CleanAir Event-driven RRM State.............. : Disabled
CleanAir Driven RRM Sensitivity.............. : LOW
CleanAir Driven RRM Sensitivity Level........ : 35
CleanAir Event-driven RRM Rogue Option....... : Disabled
CleanAir Event-driven RRM Rogue Duty Cycle... : 80
```

```
CleanAir Persistent Devices state..... : Disabled
CleanAir Persistent Device Propagation..... : Disabled
```



第 20 章

カバレッジ ホール検出

カバレッジ ホールの検出と修正

RRM カバレッジ ホール検出アルゴリズムは、堅牢な無線パフォーマンスに必要なレベルに達しない無線 LAN の無線カバレッジの領域を検出することができます。この機能によって、Lightweight アクセス ポイントを追加（または再配置）する必要があるというアラートが生成されます。

RRM 設定で指定されたレベルを下回るしきい値レベル（RSSI、失敗したクライアントの数、失敗したパケットの割合、および失敗したパケットの数）で Lightweight アクセス ポイント上のクライアントが検出されると、アクセス ポイントからdeviceに「カバレッジ ホール」アラートが送信されます。このアラートは、ローミング先の有効なアクセス ポイントがないまま、クライアントで劣悪な信号カバレッジが発生し続けるエリアが存在することを示します。device では、修正可能なカバレッジ ホールと不可能なカバレッジ ホールが識別されます。修正可能なカバレッジ ホールの場合、deviceでは、その特定のアクセス ポイントの送信電力レベルを上げることによってカバレッジ ホールが解消されます。送信電力を増加させることが不可能なクライアントや、電力レベルが静的に設定されているクライアントによって生じたカバレッジ ホールがdeviceによって解消されることはありません。ダウンストリームの送信電力を増加させても、ネットワーク内の干渉を増加させる可能性があるからです。

カバレッジ ホールの検出の設定（GUI）

クライアント アカウンティングを設定するには、次の手順に従います。

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** をクリックします。

このページでは、802.11 a/n/ac（5 GHz）および 802.11 b/g/n（2.4 GHz）無線の無線リソース管理パラメータと、フレキシブル ラジオ アサインメントのパラメータを設定できます。

ステップ 2 [Enable Coverage Hole Detection] チェックボックスをオンにします。

カバレッジ ホール検出を有効にします。

カバレッジ ホール検出の設定（CLI）

カバレッジホール検出（CHD）は、APによって監視されるアップストリームのRSSIメトリックに基づきます。

CHD を設定するには、次の手順に従います。

始める前に

設定を適用する前に、802.11 ネットワークを無効にしてください。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap dot11 {24ghz | 5ghz} rrm coverage** 例： `Device(config)# ap dot11 24ghz rrm coverage`	データ パケットの 802.11 カバレッジ レベルを設定します。 CHD を無効にするには、コマンドの **no** 形式を使用します。
ステップ 2	**ap dot11 {24ghz | 5ghz} rrm coverage data {fail-percentage | packet-count | rssi-threshold}** 例： `Device(config)# ap dot11 24ghz rrm coverage data fail-percentage 60`	データ パケットの 802.11 カバレッジ レベルを設定します。 • [fail-percentage]：アップリンク データ パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100 % の範囲で設定します。 • [packet-count]：アップリンク データ パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：データ パケットの 802.11 最小受信カバレッジ レベルを、-90 ～ 60 dBm の範囲で設定します。
ステップ 3	**ap dot11 {24ghz | 5ghz} rrm coverage exception global** 例外レベル 例：	802.11 Cisco AP のカバレッジ例外レベルを、0 ～ 100 % の範囲で設定します。

	コマンドまたはアクション	目的
	`Device(config)# ap dot11 24ghz rrm coverage exception global 50`	
ステップ 4	**ap dot11{24ghz | 5ghz}rrm coverage level global** *cli_min* 例外レベル 例： `Device(config)#ap dot11 24ghz rrm coverage level global 10`	802.11 Cisco AP クライアントの最小例外を、1 ～ 75 の範囲で指定します。
ステップ 5	**ap dot11 {24ghz | 5ghz} rrm coverage voice** {**fail-percentage | packet-count | rssi-threshold**} 例： `Device(config)# ap dot11 24ghz rrm coverage voice packet-count 10`	音声パケットの 802.11 カバレッジ ホール検出を設定します。 • [fail-percentage]：アップリンク音声パケットの 802.11 カバレッジ失敗率のしきい値を、1 ～ 100 % の範囲で設定します。 • [packet-count]：アップリンク音声パケットの 802.11 カバレッジ最小失敗数のしきい値を、1 ～ 255 の範囲で設定します。 • [rssi-threshold]：音声パケットの 802.11 最小受信カバレッジ レベルを、-90 ～ -60 dBm の範囲で設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 7	**show ap dot11 {24ghz | 5ghz} coverage** 例： `Device# show ap dot11 5ghz coverage`	CHD の詳細を表示します。

（注） 5 秒間で失敗したパケットの数と割合の両方が、**packet-count** および **fail-rate** コマンドに入力された値を超える場合、クライアントは事前アラーム状態にあると判断されます。コントローラでは、この情報を使用して、真のカバレッジ ホールと偽のカバレッジ ホールが区別されます。false positive は通常、大部分のクライアントに実装されているローミング ロジックが不適切であることが原因です。90 秒間で失敗したクライアントの数と割合の両方が、**coverage level global** および **coverage exception global** コマンドで入力された値を満たすか、これを超えている場合、カバレッジ ホールが検出されます。コントローラでは、カバレッジ ホールが修正可能かどうかが判断され、適切な場合は、その特定のアクセス ポイントの送信電力 レベルを上げることによってカバレッジ ホールが解消されます。

RF タグ プロファイルの CHD の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。

ステップ 2 [Coverage] タブで、[Enable Coverage Hole Detection] チェックボックスをオンにします。

ステップ 3 [Data Packet Count] フィールドに、データ パケットの数を入力します。

ステップ 4 [Data Packet Percentage] フィールドに、データ パケットの割合を入力します。

ステップ 5 [Data RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ～ -90 dBm です。デフォルト値は -80 dBm です。

ステップ 6 [Voice Packet Count] フィールドに、音声データ パケットの数を入力します。

ステップ 7 [Voice Packet Percentage] フィールドに、音声データ パケットの割合を入力します。

ステップ 8 [Voice RSSI Threshold] フィールドに、実際の値を dBm 単位で入力します。値の範囲は -60 ～ -90 dBm です。デフォルト値は -80 dBm です。

ステップ 9 [Minimum Failed Client per AP] フィールドに、信号対雑音比（SNR）がカバレッジしきい値より低い AP 上の最小クライアント数を入力します。値の範囲は 1 ～ 75 で、デフォルト値は 3 です。

ステップ 10 [Percent Coverage Exception Level per AP] フィールドに、目的のカバレッジしきい値未満で動作しているアクセス ポイントの無線上におけるクライアントの最大必要割合を入力し、[Apply] をクリックします。値の範囲は 0 ～ 100% で、デフォルト値は 25% です。

ステップ 11 [Apply] をクリックします。

RF タグ プロファイルの CHD の設定（CLI）

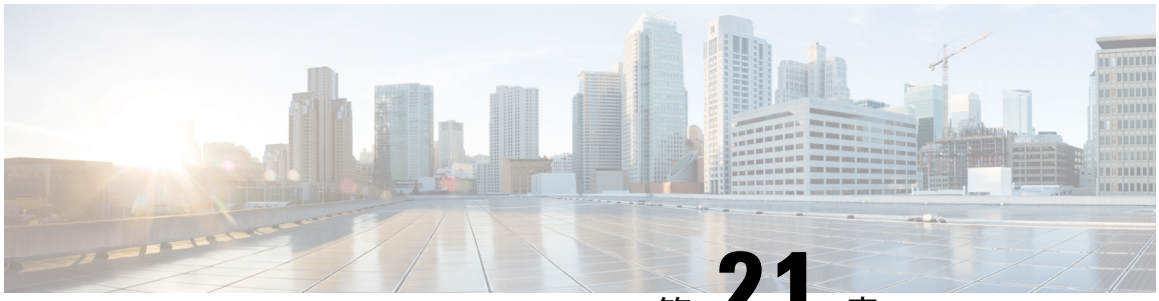
RF タグ プロファイルのカバレッジ ホール検出（CHD）を設定するには、次の手順に従います。

始める前に

RF タグ プロファイルがすでに作成されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 {24ghz | 5ghz} rf-profile** *rf-profile-tag* 例： `Device(config)# dot11 24ghz rf-profile alpha-rfprofile-24ghz`	データ パケットの 802.11 カバレッジ ホール検出を設定します。
ステップ 3	**coverage data rssi threshold** *threshold-value* 例： `Device(config-rf-profile)# coverage data rssi threshold -80`	アクセス ポイントが受信したデータ パケットの最小 RSSI 値を設定します。有効な値の範囲は -90 ～ -60 dBm です。
ステップ 4	**end** 例： `Device(config-rf-profile)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show ap dot11 24ghz rf-profile summary** 例： `Device# show ap dot11 24ghz rf-profile summary`	使用可能な RF プロファイルのサマリーを表示します。



第 21 章

ローミングの最適化

ローミングの最適化について

ローミングの最適化は、遠隔地のアクセス ポイントに長時間アソシエートし続けているクライアントや、接続が不安定な Wi-Fi ネットワークに接続を試みるアウトバウンド クライアントの問題を解決します。この機能は、クライアント データ パケットの RSSI とデータ レートに基づいてクライアントをアソシエート解除します。クライアントは、RSSI アラーム条件が満たされ、現在のデータ レートが最適化ローミング データ レートのしきい値を下回っている場合にアソシエート解除されます。データ レート オプションを無効にして、RSSI のみをクライアントのアソシエート解除に使用するようにできます。

ローミングの最適化は、クライアントの RSSI が低いときにもクライアント アソシエーションを阻止します。この機能は、RSSI しきい値に照らして受信クライアントの RSSI をチェックします。このチェックで、クライアントに有効な接続がない限り、クライアントの Wi-Fi ネットワークへの接続が阻止されます。クライアントはビーコンを受信して Wi-Fi ネットワークに接続できても、信号が弱いために安定した接続をサポートできない場合がよくあります。

ローミングの最適化を使用することによって、無線に対してクライアント カバレッジ レポート間隔を設定することもできます。クライアント カバレッジの統計情報には、データ パケット RSSI、カバレッジ ホールの検出および軽減（CHDM）の事前アラーム障害、再送信要求と現在のデータ レートが含まれます。

最適化されたローミングは、次のシナリオで役立ちます。

- クライアントを積極的に切断することによってスティッキー クライアントの問題に対処する。
- データ RSSI パケットをアクティブに監視する。
- RSSI が、設定されたしきい値よりも低くなるとクライアントのアソシエーションを解除する。

ローミングの最適化の制約事項

- 802.11a/b ネットワークを無効にするまで、ローミングの最適化の間隔を設定できません。
- 基本サービス セット（*BSS*）移行が 802.11v 対応クライアントに送信され、切断タイマーの期限が切れる前にそのクライアントが他の BSS に移行していない場合、対応するクライアントは強制的に切断されます。802.11v 対応クライアントの場合、BSS 移行はデフォルトで有効になります。

ローミングの最適化の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Advanced]** を選択します。

ステップ 2 [Advanced] ページで、関連する帯域のタブ（[5 GHz Band] または [2.4 GHz Band]）をクリックします。

ステップ 3 [Optimized Roaming Mode] チェックボックスをオンにして機能を有効にします。

ステップ 4 必要な [Optimized Roaming Date Rate Threshold] を選択します。しきい値のオプションは 802.11a ネットワークと 802.11b ネットワークで異なります。

ステップ 5 設定を保存します。

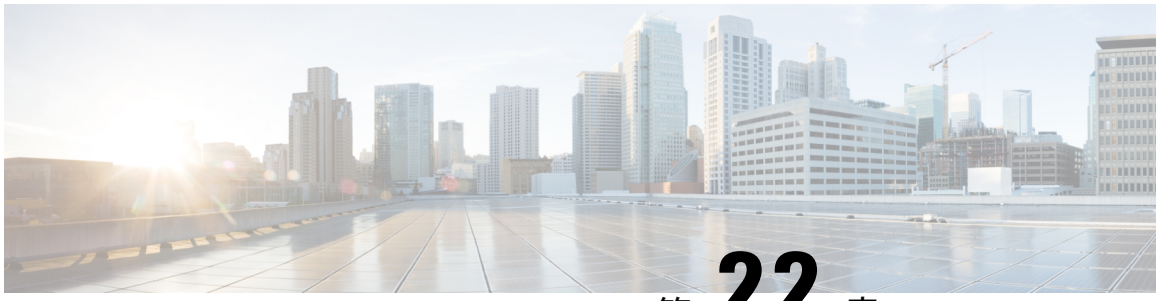
ローミングの最適化の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**ap dot11 5ghz rrm optimized-roam** 例： `Device(config)# ap dot11 5ghz rrm optimized-roam`	802.11a または 802.11b のローミングの最適化を設定します。 デフォルトでは、ローミングの最適化は無効になっています。
ステップ 2	**ap dot11 5ghz rrm optimized-roam reporting-interval** *interval-seconds* 例：	802.11a または 802.11b ネットワークのクライアント カバレッジのレポート間隔を設定します。

	コマンドまたはアクション	目的
ステップ 3	次のコマンドを入力して、802.11a ネットワークのクライアント カバレッジのレポート間隔を設定します。	**ap dot11 5ghz rrm optimized-roam reporting-interval** *interval-seconds* 範囲は 5 ～ 90 秒です。デフォルト値は 90 秒です。 （注） ローミングの最適化のレポート間隔を設定する前に、802.11a ネットワークを無効にする必要があります。 アクセス ポイントは、次の条件に基づいてクライアント統計情報をコントローラに送信します。 • **reporting-interval** *interval-seconds* がデフォルトで 90 秒に設定されている場合。 • カバレッジ ホール検出（CHD）の赤色アラームにより、ローミングの最適化時に障害が発生している間にのみ **reporting-interval** *interval-seconds* が設定されている場合（たとえば、10 秒）。
ステップ 4	次のコマンドを入力して、802.11a ネットワークのしきい値データ レートを設定します。	**ap dot11 5ghz rrm optimized-roam data-rate-threshold** *mbps* 802.11a の場合、設定可能なデータ レートは、1、2、5.5、6、9、11、12、18、24、36、48、および 54 です。データ レートを無効にするには DISABLED を設定します。
ステップ 5	このコマンドを入力して、各帯域のローミングの最適化の情報を表示します。	**show ap dot11 5ghz optimized-roaming** `(Cisco Controller) > show ap dot11 5ghz optimized-roaming` `802.11a OptimizedRoaming` `Mode : Disabled` `Reporting Interval : 90 seconds` `Rate Threshold : Disabled`

	コマンドまたはアクション	目的
		Hysteresis : 6 db
ステップ 6	次のコマンドを入力して、最適なローミング統計に関する情報を表示します。	**show ap dot11 5ghz optimized-roaming statistics** (Cisco Controller) > **show wireless statistics ap dot11 5ghz optimized-roaming statistics** 802.11a OptimizedRoaming statistics Disassociations : 0 Rejections : 0



第 22 章

シスコ フレキシブル ラジオ アサインメント

フレキシブル ラジオ アサインメントについて

フレキシブル ラジオ アサインメント（FRA）は、Cisco 3800 および 2800 AP でリリースされたハードウェアを活用するものです。FRA は、NDP の測定値を分析するために RRM に追加された新機能で、ネットワークにおける新しいフレキシブル ラジオ（2.4 GHz、5 GHz、またはモニター）の役割を決定するために使用されるハードウェアを管理します。

従来のレガシー デュアルバンド AP では、常に無線スロットが 2 つあり（帯域ごとに 1 スロットずつ）、サービスを提供している帯域別に整理されていました（スロット 0 = 802.11b/g/n、スロット 1 = 802.11a/n/ac）。

フレキシブル ラジオ（XOR）は、2.4 GHz または 5 GHz 帯域の利用、もしくは同一 AP 上での両帯域の受動的な監視機能を提供します。提供される AP モデルはデュアル 5 GHz 帯の動作に対応できるように設計されており、専用のマクロ/マイクロ アーキテクチャをサポートする Cisco AP「i」モデルと、マクロ/マクロ アーキテクチャをサポートする「e」および「p」モデルがあります。

内部アンテナ（「i」シリーズ モデル）で FRA を使用すると、2 つの 5 GHz 無線をマイクロ/マクロ セル モードで使用できます。外部アンテナ（「e」モデルと「p」モデル）で FRA を使用すると、2 つの完全に分離したマクロ セル（ワイド エリア セル）または 2 つのマイクロ セル（スモール セル）を作成できるようにアンテナを配置し、HDX または任意の組み合わせを実現できます。

FRA は、2.4 Ghz 無線の冗長性の測定値の計算や維持を行い、COF（Coverage Overlap Factor）と呼ばれる新しい測定メトリックとして示します。

この機能は既存の RRM に統合され、レガシー AP との混在環境で動作します。「AP モード」の選択では、AP 全体（スロット 0 およびスロット 1）が、以下を含む複数の動作モードのいずれかに設定されます。

- Local Mode
- Monitor Mode
- FlexConnect モード
- Sniffer Mode
- Spectrum Connect Mode

XOR が導入される前は、AP のモードを変更すると、 AP 全体、つまり両方の無線スロット 0 およびスロット 1 に変更が伝達されていました。スロット 0 の位置に XOR 無線を追加することで、1 つの無線インターフェイスを以前のモードの多くで動作させることができ、AP 全体を 1 つのモードに配置する必要がなくなりました。この概念を 1 つの無線レベルに適用する場合、「ロール」と呼ばれます。現在は次の 3 つのロールを割り当てることができます。

- Client Serving
- 2.4 GHz（1）または 5 GHz（2）
- Monitor-Monitor モード（3）

（注）
- 「モード」：AP 全体（スロット 0 とスロット 1）に割り当てられます。
- 「ロール」：単一の無線インターフェイス（スロット 0）に割り当てられます。

FRA 機能の利点

- 2.4 GHz 過剰カバレッジの問題を解決。
- 2 つの異なる 5-GHz セルを作成して使用可能な通信時間を倍増。
- 1 つのイーサネット ドロップを持つ 1 つの AP が 2 つの 5 GHz AP のように機能可能。
- 通信時間を効率化させるためのマクロ/マイクロ セルの概念の導入。
- より大きなカバレッジ セル内の 1 つのエリアにより多くの帯域幅を適用可能。
- 非線形トラフィックの処理に使用可能。
- 1 つの AP での High Density Experience（HDX）の向上。
- 対応するユーザが XOR 無線をバンド サービス クライアント モードまたはモニタ モードで選択可能。

FRA 無線の設定（CLI）

FRA 無線を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**[no] ap fra** 例： `Device(config)# [no] ap fra`	AP 上で FRA を有効または無効にします。
ステップ 4	**ap fra interval** 例： `Device(config)# ap fra interval 3`	FRA の間隔を時間単位で設定します。範囲は 1 ～ 24 時間です。 （注） FRA 間隔は、設定済みの RRM 間隔よりも長くする必要があります。
ステップ 5	**ap fra sensitivity** {**high** | **medium** | **low**} • **high**：FRA カバレッジのオーバーラップ感度を **high** に設定します。 • **medium**：FRA カバレッジのオーバーラップ感度を **medium** に設定します。 • **low**：FRA カバレッジのオーバーラップ感度を **low** に設定します。 例： `Device(config)# ap fra sensitivity high`	FRA 感度を設定します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

	コマンドまたはアクション	目的
ステップ 7	**ap fra revert** {**all** | **auto-only**}{**auto** | **static**} 例： `Device# ap fra revert all auto`	XOR 無線状態をロールバックします。 • **all**: すべての XOR 無線を元に戻します。 • **auto-only**：現在自動バンド選択になっている XOR 無線のみを元に戻します。 • **auto**：XOR 無線を自動バンド選択モードに設定します。 • **static**：XOR 無線を静的 2.4 GHz 帯域に設定します。
ステップ 8	**show ap dot11** {**24ghz** | **5ghz**} **summary** 例： `Device# show ap dot11 5ghz summary`	802.11 Cisco AP の設定と統計情報を表示します。
ステップ 9	Device# **show ap fra** 例： `Device# show ap fra` `FRA State` `: Disabled` `FRA Sensitivity` `: medium (95%)` `FRA Interval` `: 1 Hour(s)` `AP Name MAC Address` `Slot ID Current-Band COF %` `Suggested Mode` `AP00A6.CA36.295A 006b.f09c.8290` `0 2.4GHz None` `2.4GHz` `COF : Coverage Overlap Factor` `test_machine#`	現在の FRA 設定を表示します。
ステップ 10	**show ap name** *ap-name* **config dot11 dual-band** 例： `Device# show ap name config dot11 dual-band`	特定の AP における現在の 802.11 デュアルバンドパラメータを表示します。

FRA 無線の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** > **[FRA]** を選択します。

ステップ 2 [Flexible Radio Assignment] ページで、FRA ステータスを有効にし、各 AP の重複する 2.4 GHz または 5 GHz カバレッジを確認し、[FRA Status] フィールドで [Enabled] を選択します。デフォルトでは、FRA ステータスは無効になっています。

ステップ 3 [FRA Interval]ドロップダウン リストで、[FRA run interval] を選択します。間隔の値の範囲は 1 ～ 24 時間です。FRA ステータスを有効にした後でのみ、[FRA run interval] の値を選択できます。

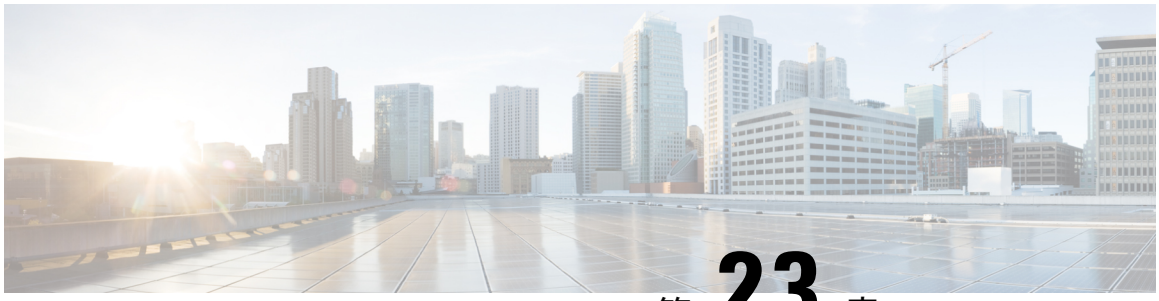
ステップ 4 [FRA Sensitivity]ドロップダウン リストで、無線を冗長と見なすために必要なカバレッジ オーバーラップ係数（COF）のパーセンテージを選択します。FRA ステータスを有効にした後にのみ、サポートされている値を選択できます。

次の値がサポートされています。

- [Low]：100%
- [Medium]（デフォルト）：95%
- [High]：90%

[Last Run] フィールドと [Last Run Time] フィールドには、FRA が最後に実行された時刻と、FRA が実行された時刻が表示されます。

ステップ 5 [Apply] をクリックします。



第 23 章

XOR 無線サポート

デュアルバンド（XOR）無線のサポートについて

Cisco 2800 および 3800 AP モデルのデュアルバンド（XOR）無線は、2.4 GHz 帯の利用、5 GHz 帯の利用、または同一 AP 上での両周波数帯の受動的な監視の機能を提供します。これらの AP は、クライアントに 2.4 GHz および 5 GHz 帯域でサービスを提供するように設定できます。または、メインの 5 GHz 無線がクライアントにサービスを提供しながら、フレキシブル無線で 2.4 GHz 帯と 5 GHz 帯の両方を順次スキャンします。

Cisco AP 2800 および 3800 モデルはデュアル 5 GHz 帯の動作に対応できるように設計されており、専用のマクロ/マイクロ アーキテクチャをサポートする「i」モデルと、マクロ/マクロをサポートする「e」および「p」モデルがあります。無線が帯域間を移動する場合（2.4 GHz から 5 GHz へ、またはその逆）、無線間で最適な分散を実現するには、クライアントをステアリングする必要があります。AP に 5 GHz 帯の無線が 2 つある場合、それらの無線はマクロ セルおよびマイクロ セルとして動作します。マクロマイクロ クライアント ステアリングを使用して、マクロとマイクロ間でクライアントをステアリングします。

XOR 無線のサポートのステアリングは、手動または自動で行うことができます。

- 無線での帯域の手動ステアリング：XOR 無線の帯域は手動でのみ変更できます。
- 無線での帯域の自動ステアリング：XOR 無線の帯域は、サイトの要件に従って帯域をモニタおよび変更するフレキシブル ラジオ アサインメント（FRA）機能によって変更されます。

デフォルトの XOR 無線サポートの設定

始める前に

（注） デフォルトの無線とは、スロット 0 でホストされている XOR 無線を指します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 dual-band antenna ext-ant-gain** *antenna_gain_value* 例： `Device# ap name ap-name dot11 dual-band antenna ext-ant-gain 2`	特定のシスコ アクセス ポイントの 802.11 デュアルバンド アンテナを設定します。 *antenna_gain_value*：有効な範囲は 0 ～ 40 です。
ステップ 3	**ap name** *ap-name* **[no] dot11 dual-band shutdown** 例： `Device# ap name ap-name dot11 dual-band shutdown`	特定のシスコ アクセス ポイントでデフォルトのデュアルバンド無線をシャットダウンします。 無線を有効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**ap name** *ap-name* **dot11 dual-band txpower** {*transmit_power_level* | **auto**} 例： `Device# ap name ap-name dot11 dual-band txpower 2`	特定のシスコ アクセス ポイントにおける無線の送信電力を設定します。
ステップ 5	**ap name** *ap-name* **dot11 dual-band role manual client-serving** 例： `Device# ap name ap-name dot11 dual-band role manual client-serving`	シスコ アクセス ポイントでクライアント サービング モードに切り替えます。
ステップ 6	**ap name** *ap-name* **dot11 dual-band band 24ghz** 例：	2.4 GHz 無線帯域に切り替えます。

	コマンドまたはアクション	目的
	`Device# ap name ap-name dot11 dual-band band 24ghz`	
ステップ 7	**ap name** *ap-name* **dot11 dual-band channel** *channel-number* 例： `Device# ap name ap-name dot11 dual-band channel 2`	デュアルバンドのチャネルを入力します。 *channel-number*：有効な範囲は 1 ～ 173 です。
ステップ 8	**ap name** *ap-name* **dot11 dual-band channel auto** 例： `Device# ap name ap-name dot11 dual-band channel auto`	デュアルバンドの自動チャネル割り当てを有効にします。
ステップ 9	**ap name** *ap-name* **dot11 dual-band channel width**{**20 MHz** | **40 MHz** | **80 MHz** | **160 MHz**} 例： `Device# ap name ap-name dot11 dual-band channel width 20 MHz`	デュアルバンドのチャネル幅を選択します。
ステップ 10	**ap name** *ap-name* **dot11 dual-band cleanair** 例： `Device# ap name ap-name dot11 dual-band cleanair`	デュアルバンド無線の Cisco CleanAir 機能を有効にします。
ステップ 11	**ap name** *ap-name* **dot11 dual-band cleanair band**{**24 GHz** | **5 GMHz**} 例： `Device# ap name ap-name dot11 dual-band cleanair band 5 GHz` `Device# ap name ap-name [no] dot11 dual-band cleanair band 5 GHz`	Cisco CleanAir 機能の帯域を選択します。 Cisco CleanAir 機能を無効にするには、このコマンドの **no** 形式を使用します。
ステップ 12	**ap name** *ap-name* **dot11 dual-band dot11n antenna** {**A** | **B** | **C** | **D**} 例： `Device# ap name ap-name dot11 dual-band dot11n antenna A`	特定のアクセス ポイントの 802.11n デュアルバンドパラメータを設定します。
ステップ 13	**show ap name** *ap-name* **auto-rf dot11 dual-band** 例： `Device# show ap name ap-name auto-rf dot11 dual-band`	シスコ アクセス ポイントの自動 RF 情報を表示します。

	コマンドまたはアクション	目的
ステップ 14	**show ap name** *ap-name* **wlan dot11 dual-band** 例： `Device# show ap name ap-name wlan dot11 dual-band`	シスコアクセスポイントの BSSID のリストを表示します。

指定したスロット番号に対する XOR 無線サポートの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Access Points]** の順にクリックします。

ステップ 2 [Dual-Band Radios] セクションで、デュアルバンド無線を設定する AP を選択します。

AP の AP 名、MAC アドレス、CleanAir 機能、およびスロット情報が表示されます。HyperLocation 方式が HALO の場合は、アンテナの PID とアンテナの設計情報も表示されます。

ステップ 3 [Configure] をクリックします。

ステップ 4 [General] タブで、必要に応じて [Admin Status] を設定します。

ステップ 5 [CleanAir Admin Status] フィールドを [Enable] または [Disable] に設定します。

ステップ 6 [Update & Apply to Device] をクリックします。

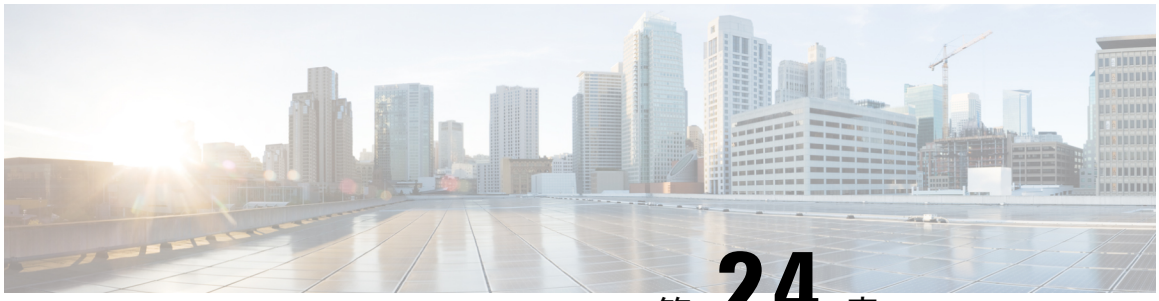
指定したスロット番号に対する XOR 無線サポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **dot11 dual-band slot 0 antenna ext-ant-gain** *external_antenna_gain_value* 例：	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンド アンテナを設定します。

	コマンドまたはアクション	目的
	`Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 antenna ext-ant-gain 2`	*external_antenna_gain_value*：外部アンテナ ゲイン値（.5 dBi の倍数単位）。有効な範囲は 0 ～ 40 です。
ステップ 3	**ap name** *ap-name* **dot11 dual-band slot 0 band** {**24ghz** | **5ghz**} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 band 24ghz`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線の現在の帯域を設定します。
ステップ 4	**ap name** *ap-name* **dot11 dual-band slot 0 channel** {*channel_number* | **auto** | **width** [**160** | **20** | **40** | **80**]} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 channel 3`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンド チャネルを設定します。 *channel_number*：有効な範囲は 1 ～ 165 です。
ステップ 5	**ap name** *ap-name* **dot11 dual-band slot 0 cleanair band** {**24Ghz** | **5Ghz**} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 cleanair band 24Ghz`	特定のアクセス ポイントのスロット 0 でホストされているデュアルバンド無線の CleanAir 機能を有効にします。
ステップ 6	**ap name** *ap-name* **dot11 dual-band slot 0 dot11n antenna** {**A** | **B** | **C** | **D**} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 dot11n antenna A`	特定のアクセス ポイントのスロット 0 でホストされている 802.11n デュアルバンド パラメータを設定します。 ここで、各変数は次のように定義されます。 **A**：アンテナ ポート A を有効にします。 **B**：アンテナ ポート B を有効にします。 **C**：アンテナ ポート C を有効にします。 **D**：アンテナ ポート D を有効にします。
ステップ 7	**ap name** *ap-name* **dot11 dual-band slot 0 role** {**auto** | **manual** [**client-serving** | **monitor**]} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 role auto`	特定のアクセス ポイントのスロット 0 でホストされている XOR 無線のデュアルバンドの役割を設定します。 デュアルバンドの役割は次のとおりです。 • **auto**：無線の役割を自動で選択することを指します。 • **manual**：無線の役割を手動で選択することを指します。

	コマンドまたはアクション	目的
ステップ 8	**ap name** *ap-name* **dot11 dual-band slot 0 shutdown** 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 shutdown` `Device# ap name AP-SIDD-A06 [no] dot11 dual-band slot 0 shutdown`	特定のアクセス ポイントのスロット 0 でホストされているデュアルバンド無線を無効にします。 デュアルバンド無線を有効にするには、このコマンドの **no** 形式を使用します。
ステップ 9	**ap name** *ap-name* **dot11 dual-band slot 0 txpower** {*tx_power_level* | **auto**} 例： `Device# ap name AP-SIDD-A06 dot11 dual-band slot 0 txpower 2`	特定のアクセスポイントのスロット 0 でホストされている XOR 無線のデュアルバンド送信電力を設定します。 • *tx_power_level*：送信電力レベルを dBm 単位で示します。有効な範囲は 1 ～ 8 です。 • **auto**：自動 RF を有効にします。



第 24 章

シスコ レシーバのパケット開始

レシーバのパケット検出開始しきい値について

レシーバのパケット検出開始（Rx SOP）しきい値機能は、アクセス ポイントの無線がパケットを復調してデコードする dBm 単位の Wi-Fi 信号レベルを決定します。Wi-Fi レベルが上がると、無線の受信感度が下がり、レシーバのセル サイズが小さくなります。セル サイズの減少は、ネットワークのクライアントの分散に影響します。

RF リンクが脆弱なクライアント、つなぎっぱなしのクライアント、およびアクセス ポイント全体で負荷分散しているクライアントに対処するために Rx SOP が使用されます。Rx SOP は、アクセス ポイントが最も近くにある最も強力なクライアントを最適化する必要のあるスタジアムやホールなどの高密度展開でネットワーク性能を最大限引き出すのに役立ちます。

Rx SOP の制約事項

RxSOP 設定は Cisco Aironet 3600 シリーズ AP でプラグ着脱可能なサードパーティの無線モジュールには適用できません。

次の表に、Rx SOP しきい値で許容される範囲を示します。

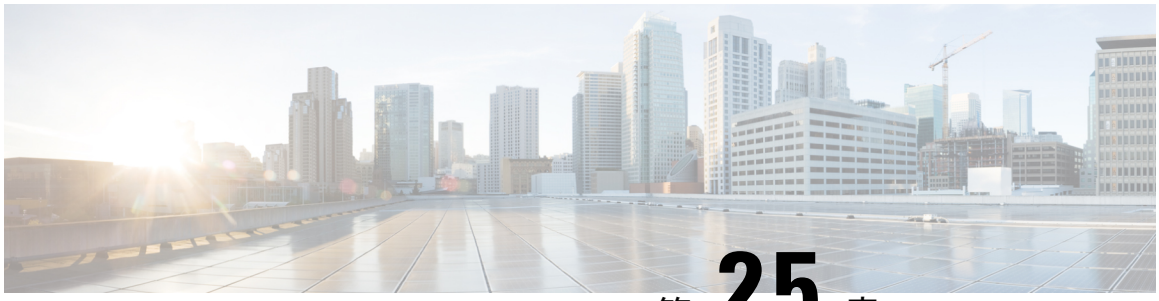
表 *6 : Rx SOP* しきい値

無線帯域	しきい値高	しきい値中	しきい値低
2.4 GHz	-79 dBm	-82 dBm	-85 dBm
5 GHz	-76 dBm	-78 dBm	-80 dBm

Rx SOP の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 {24ghz | 5ghz} rx-sop threshold {auto | high | low | medium}** 例： `Device(config)# ap dot11 5ghz rx-sop threshold high`	802.11a 無線 Rx SOP しきい値を設定します。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	**show ap dot11 {24ghz | 5ghz} high-density** 例： `Device# show ap dot11 5ghz high-density`	802.11ac 高密度パラメータを表示します。
ステップ 5	**show ap summary** 例： `Device# show ap summary`	接続されたすべての Cisco AP のサマリーを表示します。



第 25 章

クライアント リミット

クライアント リミットについて

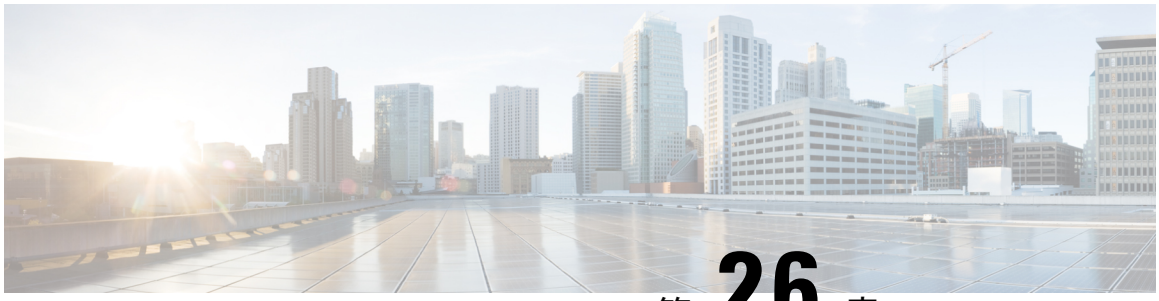
この機能により、アクセス ポイントに関連付けることができるクライアントの数に制限が適用されます。さらに、各アクセス ポイント無線に関連付けることができるクライアントの数を設定できます。

クライアント リミットの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device # 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 3	**wlan** *wlan-name* 例： `Device (config)# wlan ramban`	WLAN 名を指定します。
ステップ 4	**client association limit** *maximum-clients-per-WLAN(0—32000)* 例：	特定の WLAN に関連付けることができるクライアントの最大上限数を設定します。

	コマンドまたはアクション	目的
	`Device (config-wlan)# client association limit 110`	
ステップ 5	**client association limit ap** *maximum-clients-per-AP-per-WLAN(0—400)* 例： `Device (config-wlan) # client association limit ap 120`	WLAN 内の AP に関連付けることができるクライアントの最大上限数を設定します。
ステップ 6	**client association limit radio** *maximum-clients-per-AP-radio-per-WLAN(0—200)* 例： `Device (config-wlan) # client association limit radio 100`	WLAN 内の AP 無線に関連付けることができるクライアントの最大上限数を設定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show wlan id** *wlan-id* 例： `Device# show wlan id 2`	WLAN の現在の設定と、対応するクライアント関連付け制限を表示します。



第 26 章

IP 盗難

IP 盗難の概要

IP 盗難機能は、すでに別のデバイスに割り当てられている IP アドレスが使用されないようにします。2 つのワイヤレス クライアントが同じ IP アドレスを使用していることがコントローラによって検出された場合、コントローラは、優先順位が低い方のクライアントを IP 盗難者であると宣言し、他方のクライアントが継続できるようにします。ブラックリストが有効になっている場合は、そのクライアントが除外リストに登録され、追放されます。

コントローラでは、IP 盗難機能がデフォルトで有効になっています。クライアント（データベース内の新規および既存のクライアント）の優先順位レベルも IP 盗難の報告に使用されます。優先順位レベルは、Dynamic Host Configuration Protocol（DHCP）、Address Resolution Protocol（ARP）、データ収集（クライアントがどの IP アドレスを使用しているかを示す IP データ パケットを調べる）などの学習タイプまたは学習ソースです。有線クライアントは、常に他よりも高い優先順位レベルになります。ワイヤレス クライアントが有線 IP の盗難を試みると、そのクライアントは盗難者であると宣言されます。

IPv4 クライアントの優先順位は次のとおりです。

1. DHCPv4
2. ARP
3. データ パケット

IPv6 クライアントの優先順位は次のとおりです。

1. DHCPv6
2. NDP

3. データ パケット

（注） 静的な有線クライアントは、DHCP よりも優先順位が高くなります。

IP 盗難の設定

IP 盗難機能を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps client-exclusion ip-theft** 例： `Device(config)# wireless wps client-exclusion ip-theft`	クライアント除外ポリシーを設定します。

IP 盗難除外タイマーの設定

IP 盗難除外タイマーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**exclusionlist timeout** *time-in-seconds* 例： `Device(config-wireless-policy)# exclusionlist timeout 5`	タイムアウトを秒単位で指定します。有効な範囲は 0 ～ 2147483647 です。タイムアウトなしの場合は0を入力します。

有線ホストの静的エントリの追加

静的な有線バインディングを作成するには、次の手順に従います。

（注） 静的な有線バインディングとローカルに設定されたSVIIPアドレスは、DHCPよりも優先順位が高くなります。

手順

	コマンドまたはアクション	目的
ステップ1	**configure terminal** 例： `Device# 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	1番目のオプションを使用してIPv4スタティック エントリを設定するか、2番目のオプションを使用してIPv6スタティック エントリを作成します。 • **device-tracking binding vlan** *vlan-id ipv4-address* **interface gigabitEthernet***ge-intf-num hardware-or-mac-address* • **device-tracking binding vlan** *vlan-id ipv6-address* **interface gigabitEthernet***ge-intf-num hardware-or-mac-address* 例： `Device(config)# device-tracking binding vlan 20 20.20.20.5 interface gigabitEthernet 1 0000.1111.2222` 例： `Device(config)# device-tracking binding vlan 20 2200:20:20::6 interface gigabitEthernet 1 0000.444.3333`	IPv4またはIPv6スタティック エントリを設定します。

IP 盗難設定の確認

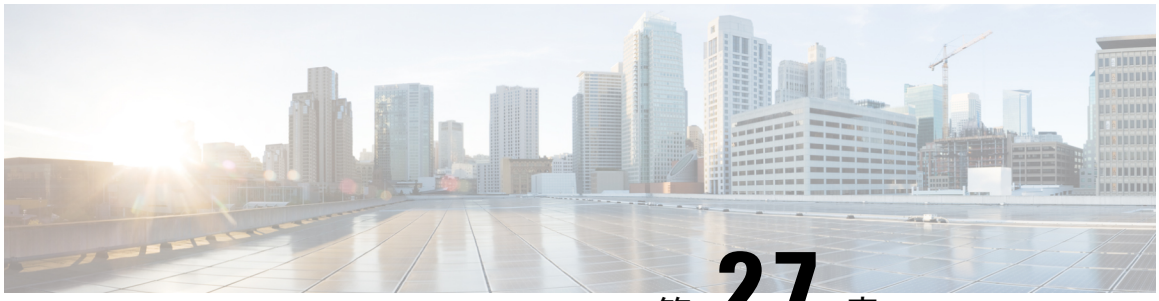
IP 盗難機能が有効になっているかどうかを確認するには、次のコマンドを使用します。

```
Device# show wireless wps summary

Client Exclusion Policy
```

```
  Excessive 802.11-association failures   : Enabled
  Excessive 802.11-authentication failures: Enabled
  Excessive 802.1x-authentication         : Enabled
  IP-theft                                : Enabled
  Excessive Web authentication failure    : Enabled
  Cids Shun failure                       : Enabled
  Misconfiguration failure                : Enabled
  Failed Qos Policy                       : Enabled
  Failed Epm                              : Enabled
```

IP 盗難機能に関するその他の詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless client summary

Number of Local Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method     Role
-------------------------------------------------------------------------------------
000b.bbb1.0001 SimAP-1                2    Run                11a      None       Local


Number of Excluded Clients: 1

MAC Address    AP Name                WLAN State              Protocol Method
-------------------------------------------------------------------------------------
10da.4320.cce9 charlie2               2    Excluded           11ac     None


Device# show wireless device-tracking database ip

IP                              VLAN  STATE       DISCOVERY   MAC
  ------------------------------------------------------------------------
  20.20.20.2                     20    Reachable   Local       001e.14cc.cbff
  20.20.20.6                     20    Reachable   IPv4 DHCP   000b.bbb1.0001


Device# show wireless exclusionlist

Excluded Clients

MAC Address       Description          Exclusion Reason               Time Remaining
-------------------------------------------------------------------------------------
10da.4320.cce9                         IP address theft                   59


Device# show wireless exclusionlist client mac 12da.4820.cce9 detail

Client State : Excluded
Client MAC Address : 12da.4820.cce9
Client IPv4 Address: 20.20.20.6
Client IPv6 Address: N/A
Client Username: N/A
Exclusion Reason : IP address theft
Authentication Method : None
Protocol: 802.11ac
AP MAC Address : 58ac.780e.08f0
AP Name: charlie2
AP slot : 1
Wireless LAN Id : 2
Wireless LAN Name: mhe-ewlc
VLAN Id : 20
```



第 27 章

不定期自動省電力配信

不定期自動省電力配信について

不定期自動省電力配信（U-APSD）は、モバイルクライアントのバッテリ寿命を延ばすQoS機能で、IEEE 802.11e で定義されています。この機能により、バッテリ寿命が延びるだけでなく、無線メディアで配信されるトラフィック フローの遅延時間が短縮されます。U-APSD では、クライアントはアクセスポイントでバッファされる個々のパケットをポーリングする必要がないため、単一のアップリンク トリガー パケットを送信して複数のダウンリンク パケットを配信することが可能になります。

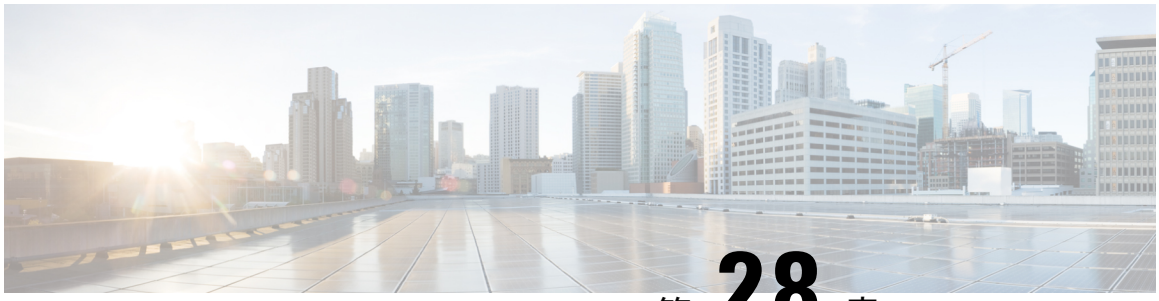
WMM が有効化されると、U-APSD は自動的に有効化されます。

不定期自動省電力配信の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**show wireless client mac-address** *client_mac***detail** 例： `Device(config)#show wireless client mac-address 2B:5B:B3:18:56:E9 detail` `Output Policy State : Unknown` `Output Policy Source : Unknown` `WMM Support : Enabled` `U-APSD Support : Enabled` `U-APSD value : 15` `APSD ACs : BK(T/D), BE, VI(T/D), VO(T/D)` `Power Save : OFF` `Current Rate :`	クライアントの詳細情報を Mac アドレス別に表示します。

	コマンドまたはアクション	目的
	`` -------------------------- BK : Background BE : Best Effort VI : Video VO : Voice. T: UAPSD Trigger Enabled D: UAPSD Delivery Enabled T/D : UAPSD Trigger and Delivery Enabled ```	



第 28 章

USB 電源のサポート

AP プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *ap-profile* 例： `Device(config)# ap profile xyz-ap-profile`	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。 （注） 名前付きプロファイルを削除した場合、そのプロファイルに関連付けられていた AP はデフォルト プロファイルに戻らなくなります。

シスコ AP プロファイルの USB の有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**usb-enable** 例： `Device(config-ap-profile)# usb-enable`	各 AP プロファイルの USB を有効にします。 （注） デフォルトでは、各 AP プロファイルの USB は有効になっています。
ステップ 2	**no usb-enable** 例： `Device(config-ap-profile)# no usb-enable`	各 AP プロファイルの USB を無効にします。
ステップ 3	**end** 例： `Device(config-ap-profile)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

各アクセスポイントでオーバーライドする USB ポートの有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **usb-module override** 例： `Device# ap name AP44d3.ca52.48b5 usb-module override`	USB のオーバーライドを有効にして、AP プロファイルの USB ステータスをオーバーライドし、AP によるローカル設定の取得を強制します。 （注） USB オーバーライドを有効にした場合にのみ、対応する AP の USB ステータスを設定できます。

	コマンドまたはアクション	目的
ステップ 3	**ap name** *ap-name* **no usb-module override** 例： `Device# ap name AP44d3.ca52.48b5 no usb-module override`	USB のオーバーライドを無効にして、AP プロファイルの USB ステータスをオーバーライドし、AP によるローカル設定の取得を強制します。

アクセス ポイントの USB ポートの有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **usb-module** 例： `Device# ap name AP44d3.ca52.48b5 usb-module`	アクセス ポイントの USB ポートを有効にします。
ステップ 3	**ap name** *ap-name* **no usb-module** 例： `Device# ap name AP44d3.ca52.48b5 no usb-module`	アクセス ポイントの USB ポートを無効にします。

シスコ アクセス ポイントの設定での USB の確認

シスコ AP のインベントリの詳細を表示するには、次のコマンドを使用します。

```
Device# show ap name <> inventory
NAME: AP2800    , DESCR: Cisco Aironet 2800 Series (IEEE 802.11ac) Access Point
PID: AIR-AP2802I-D-K9  ,  VID: 01,  SN: FGL2135A4GSAP2800
NAME: SanDisk    , DESCR: Cruzer Blade
PID: SanDisk  ,  SN: 4C530001151, MaxPower: 224
```

AP モジュールのサマリーを表示するには、次のコマンドを使用します。

```
Device# show ap module summary
AP Name               External Module       External Module PID   External Module
Description
-------------------------------------------------------------------------------------------
AP500F.8059.1620      Enable                SanDisk               Cruzer Blade
```

各 AP の設定の詳細を表示するには、次のコマンドを使用します。

```
Device# show ap config general
USB Module Type.............................. USB Module
```

```
USB Module Status.............................. Disabled
USB Module Operational State..................... Enabled
USB Override ……..... Enabled
```

設定の詳細を表示するには、次のコマンドを使用します。

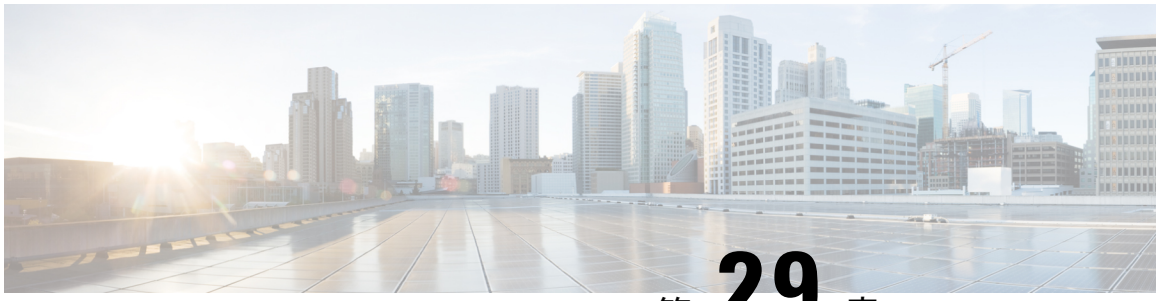
```
Device# show ap name < > config general
USB Module Type................................ USB Module
USB Module Status.............................. Disabled
USB Module Operational State..................... Enabled
USB Override ……..... Enabled
```

USB モジュールのステータスを表示するには、次のコマンドを使用します。

```
Device# show ap profile xyz detailed
USB Module                : ENABLED
```

第 IV 部

Network Management



第 29 章

AP パケット キャプチャ

AP クライアント パケット キャプチャの概要

AP クライアント パケット キャプチャ機能を使用すると、ワイヤレス クライアントのトラブルシューティングを目的として AP 上のパケットをキャプチャすることができます。パケット キャプチャ操作は、指定されたパケット キャプチャ フィルタに基づいて、AP が動作している現在のチャネルの無線ドライバによって、AP 上で実行されます。特定のクライアントについてキャプチャされたパケットはすべて、FTP サーバのファイルにアップロードされます。このファイルを Wireshark で開いてパケットを調べることができます。

AP クライアント パケット キャプチャの制限事項

- パケット キャプチャのタスクは、サイトごとに一度に 1 つのクライアントに対してのみ実行できます。
- パケット キャプチャは、スタティック モードを使用して、特定の AP または AP のセットで開始できます。キャプチャが進行中のときに、異なる AP 上の同じクライアントに対して開始または停止することができます。

  パケット キャプチャが自動モードで開始されると、一連の隣接する AP が自動的に選択されて特定のクライアントのパケット キャプチャが開始されます。このモードでは、個々の AP でパケット キャプチャを開始または停止することはできません。自動モードで開始されたパケット キャプチャを停止するには、**stop all** コマンドを使用します。
- SSO が完了すると、スイッチオーバー後にパケット キャプチャの動作は継続されません。

パケット キャプチャの有効化（GUI）

手順

ステップ 1 **[Troubleshooting]** > **[AP Packet Capture]** を選択します。

ステップ 2 [Troubleshooting] ページの [Start Packet Capture] セクションの [Client MAC Address] フィールドに、クライアントの MAC アドレスを入力します。

ステップ 3 [Capture Mode] オプションから [Auto] を選択します。

ステップ 4 [Start] をクリックします。

パケット キャプチャの有効化（CLI）

パケット キャプチャを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**ap packet-capture start** *client-mac-address* **auto** 例： `Device# ap packet-capture start 0011.0011.0011 auto`	一連の隣接するアクセス ポイントで、指定したクライアントのパケット キャプチャを有効にします。

AP パケット キャプチャ プロファイルの作成と AP 参加プロファイルへのマッピング（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[AP Join Profile]** をクリックします。

ステップ 2 [Add] をクリックして新しい AP join プロファイルを作成し、必要な詳細情報を入力します。

ステップ 3 [Add AP Join Profile] 領域で、**[AP]** > **[Packet Capture]** をクリックします。

ステップ 4 [+] アイコンをクリックして新しいパケット キャプチャ プロファイルを作成するか、またはドロップダウン メニューから 1 つ選択します。

ステップ 5 **[保存（Save）]** をクリックします。

AP パケット キャプチャ プロファイルの作成と AP join プロファイルへのマッピング

パケット キャプチャ プロファイルの設定は AP に使用されますが、パケット キャプチャ プロファイルは AP プロファイルにマッピングされます。AP プロファイルはさらにサイト タグにマッピングされます。

パケット キャプチャの開始時に、AP は、自身が属しているサイトと AP join プロファイルに基づいて、パケット キャプチャ プロファイルの設定を使用します。

AP パケット キャプチャ プロファイルを作成して AP join プロファイルにマッピングするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile ap packet-capture** *packet-capture-profile-name* 例： `Device(config)# wireless profile ap packet-capture test1`	AP プロファイルを設定します。
ステップ 3	**ap profile** *profile-name* 例： `Device(config)# ap profile default-ap-profile`	AP パケット キャプチャ プロファイルを設定します。
ステップ 4	**packet-capture** *profile-name* 例： `Device(config-ap-profile)# packet-capture capture-test`	AP プロファイルでパケット キャプチャを有効にします。
ステップ 5	**end** 例：	AP プロファイル コンフィギュレーション モードを終了します。

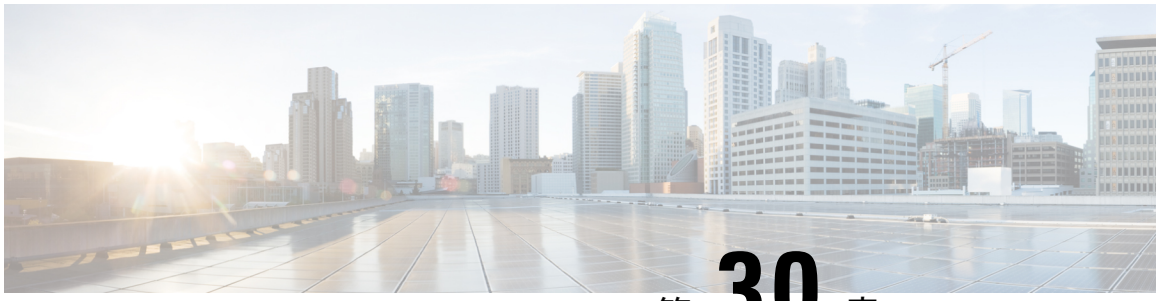
	コマンドまたはアクション	目的
	`Device(config-ap-profile)# end`	
ステップ 6	**show wireless profile ap packet-capture detailed** *profile-name* 例： `Device# show wireless profile ap packet-capture detailed test1`	選択した AP パケット キャプチャ プロファイルの詳細情報を表示します。

パケット キャプチャの開始または停止

パケット キャプチャの手順を開始または停止するには、次のいずれかの作業を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap packet-capture start** *client-mac-address* {**auto** | **static** *ap-name* } 例： `Device# ap packet-capture start 0011.0011.0011 auto`	クライアントのパケット キャプチャを有効にします。
ステップ 2	**ap packet-capture stop** *client-mac-address* {**all** | **static** *ap-name* } 例： `Device# ap packet-capture stop 0011.0011.0011 all`	クライアントのパケット キャプチャを無効にします。



第 30 章

スニファ モード

スニファについて

コントローラには、アクセスポイントの1つをネットワーク「スニファ」として設定する機能があります。スニファは、特定のチャネル上のパケットをすべてキャプチャして、パケットアナライザ ソフトウェアを実行しているリモートマシンに転送します。これらのパケットには、タイム スタンプ、信号強度、パケット サイズなどの情報が含まれます。

スニファを使用すると、ネットワーク アクティビティを監視して記録し、問題を検出できます。

スニファの前提条件

スニファを実行するには、次のハードウェアとソフトウェアが必要です。

- 専用アクセスポイント：スニファとして設定されたアクセスポイントは、そのネットワーク上で無線アクセス サービスを同時に提供できません。カバレッジの中断を回避するには、既存のワイヤレス ネットワークの一部ではないアクセス ポイントを使用します。
- リモート監視デバイス：アナライザ ソフトウェアを実行できるコンピュータ。
- ソフトウェアおよび関連ファイル、プラグイン、またはアダプタ：アナライザ ソフトウェアによっては、有効にするために特殊なファイルが必要となる場合があります。

スニファの制限事項

- サポートされているサードパーティ製のネットワーク アナライザ ソフトウェア アプリケーションは、次のとおりです。
  - Wildpackets Omnipeek または Airopeek
  - AirMagnet Enterprise Analyzer
  - Wireshark
- Wireshark の最新バージョンでは、Analyze モードでパケットをデコードできます。[decode as] を選択し、UDP5555 を PEEKREMOTE としてデコードするように切り替えます。

スニファの設定方法

スニファとして使用するアクセス ポイントの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [General] タブで、AP の名前を更新します。

ステップ 3 AP が存在する物理的な場所を指定します。

ステップ 4 AP を有効状態にする場合は、[Admin Status] として [Enabled] を設定します。

ステップ 5 AP のモードを [Sniffer] として選択します。

ステップ 6 [Tags] セクションで、[Configuration] > [Tags & Profiles] > [Tags] ページで作成した、該当するポリシー タグ、サイト タグ、および RF タグを指定します。

ステップ 7 [Update & Apply to Device] をクリックします。

スニファとして使用するアクセス ポイントの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**ap name** *ap-name* **mode sniffer** 例： `Device#ap name access1 mode sniffer`	アクセス ポイントをスニファとして設定します。 ここで、 *ap-name* は、Cisco Lightweight アクセス ポイントの名前です。

アクセス ポイントでのスニッフィングの有効化または無効化（GUI）

始める前に

アクセス ポイントの AP モードをスニファ モードに変更します。

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [Access Points] ページで、[5GHz] または [2.4 GHz] リストから AP 名をクリックします。

ステップ 3 **[Edit Radios]** > **[Configure]** > **[Sniffer Channel Assignment]** セクションで、[Sniffer Channel Assignment] チェックボックスをオンにして有効にします。

アクセス ポイントでスニッフィングを無効にするには、このチェックボックスをオフにします。

ステップ 4 [Sniff Channel] ドロップダウン リストからチャネルを選択します。

ステップ 5 [Sniffer IP] フィールドに IP アドレスを入力します。

ステップ 6 [Update & Apply to Device] をクリックします。

アクセス ポイントでのスニッフィングの有効化または無効化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**ap name** *ap-name* **sniff** {**dot11a** *channel server-ip-address* | **dot11b** *channel server-ip-address* | **dual-band** *channel server-ip-address*} 例： `Device#ap name access1 sniff dot11b 1 9.9.48.5`	アクセス ポイントでスニッフィングを有効にします。 • *channel* は、スニファされる有効なチャネルです。802.11a の場合、範囲は 36 ～ 165 です。802.11b の場合、範囲は 1 ～ 14 です。 • *server-ip-address* は、Omnipeek、Airopeek、AirMagnet、または Wireshark ソフトウェアを実行するリモート マシンの IP アドレスです。
ステップ 3	**ap name** *ap-name* **no sniff** {**dot11a** | **dot11b** | **dual-band**} 例： `Device#ap name access1 no sniff dot11b`	アクセス ポイントでスニッフィングを無効にします。

スニファの設定の確認

表 *7:* スニファの設定を確認するためのコマンド

コマンド	説明
show ap name *ap-name* **config dot11** {**24ghz** |**5ghz** | **dual-band**}	スニッフィングの詳細を表示します。
show ap name *ap-name* **config slot** *slot-ID*	スニッフィング設定の詳細を表示します。 *slot-ID* の範囲は 0 ～ 3 です。すべてのアクセス ポイントにはスロット 0 とスロット 1 があります。

スニファの設定とモニタリングの例

次に、アクセス ポイントをスニファとして設定する例を示します。

```
Device# ap name access1 mode sniffer
```

次に、アクセス ポイントでスニッフィングを有効にする例を示します。

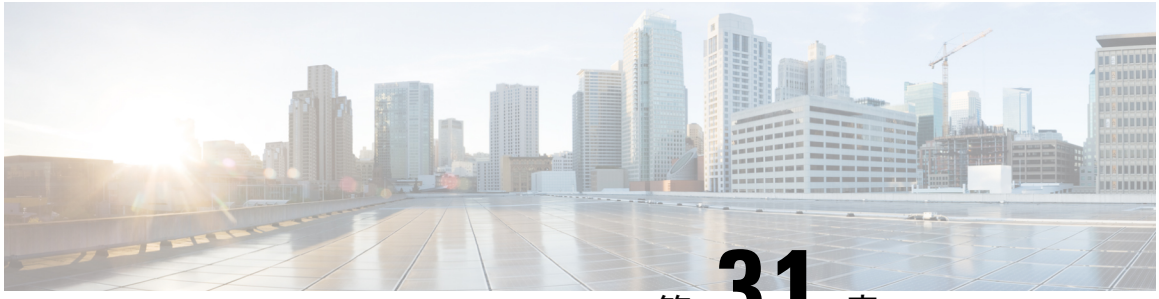
```
Device# ap name access1 sniff dot11b 1 9.9.48.5
```

次に、アクセス ポイントでスニッフィングを無効にする例を示します。

```
Device# ap name access1 no sniff dot11b
```

次に、スニッフィング設定の詳細を表示する例を示します。

```
Device# show ap name access1 config dot11 24ghz
Device# show ap name access1 config slot 0
```



第 31 章

DHCP オプション 82

DHCP オプション 82 について

DHCP オプション 82 は、リレー エージェントが認識する情報を含んだ単一の DHCP オプションとして構成されています。この機能により、DHCP を使用してネットワーク アドレスを割り当てる際のセキュリティが強化されます。また、シスコ コントローラを DHCP リレー エージェントとして機能させ、信頼できない送信元からの DHCP クライアント要求を防止できるようになります。

クライアントからの DHCP 要求にオプション 82 の情報を追加し、それからその要求を DHCP サーバに転送するように、コントローラを設定することができます。その後、DHCP オプション 82 に含まれている情報に基づいてワイヤレス クライアントに IP アドレスを割り当てるように、DHCP サーバを設定できます。

DHCP は、TCP/IP ネットワーク上のホストに設定情報を渡すフレームワークを提供します。設定パラメータやその他の制御情報は、DHCP メッセージのオプション フィールドに格納されたタグ付きデータ項目で伝送されます。これらのデータ項目自体もオプションと呼ばれます。オプション 82 には、リレー エージェントが認識する情報が含まれています。

リレー エージェント情報オプションは、1 つまたは複数のサブオプションを含む単一の DHCP オプションとして構成されています。このサブオプションによってリレー エージェントが認識する情報が伝達されます。オプション 82 は、DHCP リレー エージェントが DHCP サーバに転送中の要求に回線固有の情報を挿入できるようにすることを目的として設計されました。このオプションは、次の 2 つのサブオプションを設定することで機能します。

- 回線 ID
- リモート ID

回線 ID サブオプションには、要求が送信された回線に固有の情報が含まれます。このサブオプションはリレー エージェントに固有の識別子です。したがって、記述される回線はリレー エージェントによって異なります。

リモート ID サブオプションには、回線のリモート ホスト側の情報が含まれます。通常、このサブオプションには、リレー エージェントを識別する情報が含まれます。ワイヤレス ネットワークであれば、これはワイヤレス アクセス ポイントの固有識別子になります。

コントローラでは、DHCP オプション 82 の次のオプションを設定できます。

- DHCP 有効
- DHCP Opt82 有効
- DHCP Opt82 Ascii
- DHCP Opt82 RID
- DHCP Opt82 形式
- DHCP AP MAC
- DHCP SSID
- DHCP AP ETH MAC
- DHCP AP NAME
- DHCP ポリシー タグ
- DHCP AP ロケーション
- DHCP VLAN ID

DHCP オプション 82 グローバル インターフェイスの設定

サーバ オーバーライドによるグローバル設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ip dhcp-relay information option server-override** 例：	グローバル サーバ オーバーライドおよびリンク選択サブオプションを挿入します。

	コマンドまたはアクション	目的
	`Device(config)# ip dhcp-relay information option server-override`	

各種 SVI によるグローバル設定（GUI）

手順

ステップ 1 [Configuration] > [VLAN] を選択します。 >
ステップ 2 リストから VLAN を選択します。[Edit SVI] 画面が表示されます。
ステップ 3 [Advanced] タブをクリックします。
ステップ 4 [IPv4 Inbound ACL] ドロップダウン リストから必要なオプションを選択します。
ステップ 5 [IPv4 Outbound ACL] ドロップダウン リストから必要なオプションを選択します。
ステップ 6 [IPv6 Inbound ACL] ドロップダウン リストから必要なオプションを選択します。
ステップ 7 [IPv6 Outbound ACL] ドロップダウン リストから必要なオプションを選択します。
ステップ 8 [IPv4 Helper Address] フィールドに IP アドレスを入力します。
ステップ 9 [Relay Information Option] 設定を有効にする場合は、ステータスを [Enabled] に設定します。
ステップ 10 [Subscriber ID] を入力します。
ステップ 11 [Server ID Override] 設定を有効にする場合は、ステータスを [Enabled] に設定します。
ステップ 12 [Option Insert] 設定を有効にする場合は、ステータスを [Enabled] に設定します。
ステップ 13 [Source-Interface Vlan] ドロップダウン リストから必要なオプションを選択します。
ステップ 14 [Update & Apply to Device] ボタンをクリックします。

各種 SVI によるグローバル設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ip dhcp-relay source-interface vlan** *vlan-id* 例： `Device(config)# ip dhcp-relay source-interface vlan 74`	リレーされるメッセージのグローバル送信元インターフェイスを設定します。

プロファイル ポリシーによる DHCP オプション 82 の設定

ap_ethmac コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp7`	指定したポリシープロファイルの設定を有効にします。
ステップ 3	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	プロファイルのプロファイルポリシーをシャット ダウンします。
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	プロファイル ポリシーを VLAN に割り当てます。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッションタイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドルタイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。

	コマンドまたはアクション	目的
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format ap_ethmac** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format ap_ethmac`	対応する AP のイーサネット ポートで DHCP オプション 82 を有効にします。
ステップ 12	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

ap_location コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp2`	指定したプロファイル ポリシーの設定を有効にします。
ステップ 3	**shutdown** 例：	プロファイル ポリシーをシャットダウンします。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# shutdown`	
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	プロファイルポリシーを VLAN に割り当てます。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッションタイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドルタイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format ap_location** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format ap_location`	対応する AP で DHCP オプション 82 を有効にします。
ステップ 12	**no shutdown** 例：	プロファイル ポリシーを有効にします。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# no shutdown`	

ethmac コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp3`	指定したプロファイル ポリシーの設定を有効にします。
ステップ 3	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	プロファイル ポリシーをシャットダウンします。
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	プロファイル ポリシーを VLAN に割り当てます。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッション タイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドル タイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。

	コマンドまたはアクション	目的
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format apmac** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format apmac`	対応する AP で DHCP オプション 82 を有効にします。
ステップ 12	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

apname コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp7`	指定したプロファイルポリシーの設定を有効にします。
ステップ 3	**shutdown** 例：	プロファイルポリシーをシャットダウンします。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# shutdown`	
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	プロファイル ポリシーを VLAN に割り当てます。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッション タイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドル タイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format apname** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format apname`	AP で DHCP オプション 82 を有効にします。
ステップ 12	**no shutdown** 例：	プロファイル ポリシーを有効にします。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# no shutdown`	

ポリシー タグ コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp5`	指定したプロファイルポリシーの設定を有効にします。
ステップ 3	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	プロファイルポリシーをシャットダウンします。
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	プロファイルポリシーを VLAN に割り当てます。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッションタイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドルタイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。

	コマンドまたはアクション	目的
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format policy_tag** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format policy_tag`	ポリシー タグで DHCP オプション 82 を有効にします。
ステップ 12	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

SSID コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp6`	指定したプロファイル ポリシーの設定を有効にします。
ステップ 3	**shutdown** 例：	プロファイル ポリシーをシャットダウンします。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# shutdown`	
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	プロファイルポリシーを VLAN に割り当てます。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッションタイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドルタイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format ssid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format ssid`	SSID で DHCP オプション 82 を有効にします。
ステップ 12	**no shutdown** 例：	プロファイル ポリシーを有効にします。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# no shutdown`	

ap_ethmac および SSID コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp7`	指定したプロファイル ポリシーの設定を有効にします。
ステップ 3	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	プロファイル ポリシーをシャットダウンします。
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	VLAN を設定します。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッション タイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドル タイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。

	コマンドまたはアクション	目的
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format ap_ethmac** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format ap_ethmac`	AP イーサネット MAC で DHCP オプション 82 を有効にします。
ステップ 12	**ipv4 dhcp opt82 format ssid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format ssid`	SSID で DHCP オプション 82 を有効にします。
ステップ 13	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

ap_mac および vlan_id コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp8`	指定したプロファイルポリシーの設定を有効にします。
ステップ 3	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	プロファイルポリシーをシャットダウンします。
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	プロファイルポリシーを VLAN に割り当てます。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッションタイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドルタイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレスクライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。

	コマンドまたはアクション	目的
ステップ 11	**ipv4 dhcp opt82 format apmac** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format apmac`	AP で DHCP オプション 82 を有効にします。
ステップ 12	**ipv4 dhcp opt82 format vlan_id** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan_id`	VLAN で DHCP オプション 82 を有効にします。
ステップ 13	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

ap_name コマンドと VLAN ID を使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp9`	指定したプロファイルポリシーの設定を有効にします。
ステップ 3	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	プロファイルポリシーをシャットダウンします。
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	プロファイルポリシーを VLAN に割り当てます。

	コマンドまたはアクション	目的
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッションタイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドルタイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format apname** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format apname`	AP で DHCP オプション 82 を有効にします。
ステップ 12	**ipv4 dhcp opt82 format vlan_id** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan_id`	VLAN で DHCP オプション 82 を有効にします。
ステップ 13	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

ap_ethmacコマンドを使用しサーバオーバーライドを有効にしたDHCPオプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy pp10`	指定したプロファイルポリシーの設定を有効にします。
ステップ 3	**shutdown** 例： `Device(config-wireless-policy)# shutdown`	プロファイルポリシーをシャットダウンします。
ステップ 4	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 72`	プロファイルポリシーを VLAN に割り当てます。
ステップ 5	**session-timeout** *value-btwn-20-86400* 例： `Device(config-wireless-policy)# session-timeout 300`	（任意）セッションタイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 6	**idle-timeout** *value-btwn-15-100000* 例： `Device(config-wireless-policy)# idle-timeout 15`	（任意）アイドルタイムアウト値を秒単位で設定します。範囲は 15 ～ 100000 です。
ステップ 7	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 8	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。

	コマンドまたはアクション	目的
ステップ 9	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	（任意）DHCP オプション 82 機能で ASCII を有効にします。
ステップ 10	**ipv4 dhcp opt82 rid** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	（任意）DHCP オプション 82 機能に対してシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 11	**ipv4 dhcp opt82 format ap_ethmac** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format ap_ethmac`	AP のイーサネット ポートで DHCP オプション 82 を有効にします。
ステップ 12	**ipv4 dhcp server server-ipaddress** 例： `Device(config-wireless-policy)# ipv4 dhcp server 9.3.74.1`	DHCP オーバーライド サーバの IP アドレスを入力します。
ステップ 13	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

VLAN インターフェイスによる DHCP オプション 82 の設定

option-insert コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 72`	VLAN ID を設定します。
ステップ 3	**ip dhcp relay information option-insert** 例： `Device(config-if)# ip dhcp relay information option-insert`	BOOTREQUEST にリレー情報を挿入します。
ステップ 4	**ip address** *ip-address* 例： `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**ip helper-address** *ip-address* 例： `Device(config-if)# ip helper-address 9.3.72.1`	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 6	**[no] mop enabled** 例： `Device(config-if)# no mop enabled`	インターフェイスの MOP を無効にします。
ステップ 7	**[no] mop sysid** 例： `Device(config-apgroup)# [no] mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。

server-id-overrideコマンドを使用したDHCPオプション82の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 vlan** *vlan-id* 例： `Device(config)# interface vlan 72`	VLAN ID を設定します。

	コマンドまたはアクション	目的
ステップ 3	**ip dhcp relay information option server-id-override** 例： `Device(config-if)# ip dhcp relay information option server-id-override`	サーバ ID オーバーライドおよびリンク選択サブオプションを挿入します。
ステップ 4	**ip address** *ip-address* 例： `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**ip helper-address** *ip-address* 例： `Device(config-if)# ip helper-address 9.3.72.1`	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 6	**[no] mop enabled** 例： `Device(config-if)# no mop enabled`	インターフェイスの MOP を無効にします。
ステップ 7	**[no] mop sysid** 例： `Device(config-apgroup)# [no] mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。

サブスクライバ ID による DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 vlan** *vlan-id* 例： `Device(config)# interface vlan 72`	VLAN ID を設定します。
ステップ 3	**ip dhcp relay information option subscriber-id** *subscriber-id* 例：	サブスクライバ ID サブオプションを挿入します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip dhcp relay information option subscriber-id test10`	
ステップ 4	**ip address** *ip-address* 例： `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**ip helper-address** *ip-address* 例： `Device(config-if)# ip helper-address 9.3.72.1`	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 6	**[no] mop enabled** 例： `Device(config-if)# no mop enabled`	インターフェイスの MOP を無効にします。
ステップ 7	**[no] mop sysid** 例： `Device(config-apgroup)# [no] mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。

server-ID-override および subscriber-id コマンドを使用した DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 vlan** *vlan-id* 例： `Device(config)# interface vlan 72`	VLAN ID を設定します。
ステップ 3	**ip dhcp relay information option server-id-override** 例： `Device(config-if)# ip dhcp relay information option server-id-override`	サーバ ID オーバーライドおよびリンク選択サブオプションを挿入します。

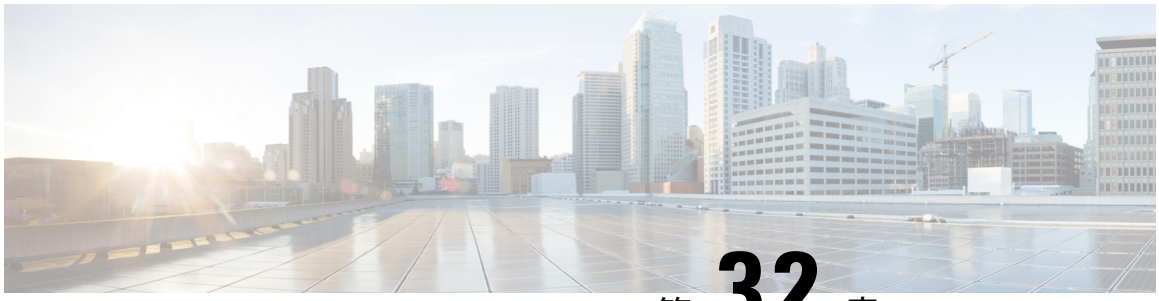
	コマンドまたはアクション	目的
ステップ 4	**ip dhcp relay information option subscriber-id** *subscriber-id* 例： `Device(config-if)# ip dhcp relay information option subscriber-id test10`	サブスクライバ ID サブオプションを挿入します。
ステップ 5	**ip address** *ip-address* 例： `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 6	**ip helper-address** *ip-address* 例： `Device(config-if)# ip helper-address 9.3.72.1`	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 7	**[no] mop enabled** 例： `Device(config-if)# no mop enabled`	インターフェイスの MOP を無効にします。
ステップ 8	**[no] mop sysid** 例： `Device(config-apgroup)# [no] mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。

各種 SVI による DHCP オプション 82 の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 vlan** *vlan-id* 例： `Device(config)# interface vlan 72`	VLAN ID を設定します。
ステップ 3	**ip dhcp relay source-interface vlan** *vlan-id* 例： `Device(config-if)# ip dhcp relay source-interface vlan 74`	VLAN ID でリレーされるメッセージの送信元インターフェイスを設定します。

	コマンドまたはアクション	目的
ステップ 4	**ip address** *ip-address* 例： `Device(config-if)# ip address 9.3.72.38 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 5	**ip helper-address** *ip-address* 例： `Device(config-if)# ip helper-address 9.3.72.1`	UDP ブロードキャストの宛先アドレスを設定します。
ステップ 6	**[no] mop enabled** 例： `Device(config-if)# no mop enabled`	インターフェイスの MOP を無効にします。
ステップ 7	**[no] mop sysid** 例： `Device(config-apgroup)# [no] mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。



第 32 章

RADIUS レルム

RADIUS レルムについて

RADIUS レルム機能は、ユーザのドメインに関連付けられています。クライアントはこの機能を使用して、認証とアカウンティングの処理に使用する RADIUS サーバを選択できます。

モバイル クライアントが WLAN に関連付けられている場合、Extensible Authentication Protocol Method for UMTS Authentication and Key Agreement（EAP-AKA）の ID 応答要求の一部として、認証要求パケット内で RADIUS レルムを受信します。WLAN のネットワーク アクセス ID（NAI）形式（EAP-AKA）は、*username@domain.com* として指定できます。NAI 形式のレルムは @ 記号の後ろに示され、domain.com として指定されます。ベンダー固有の属性が *test* として追加された場合は、NAI 形式は test@domain.com として表されます。

RADIUS レルム機能は、WLAN で有効または無効にすることができます。レルムが WLAN で有効になっている場合、対応するユーザはユーザ名を NAI 形式で送信する必要があります。コントローラは、クライアントから受信した NAI 形式のレルムが特定の標準に従っている場合にのみ、AAA サーバに認証要求を送信します。認証とは別に、アカウンティング要求もレルム フィルタリングに基づいて AAA サーバに送信する必要があります。

WLAN 上のレルム サポート

各 WLAN は NAI レルムをサポートするように設定されます。レルムが特定の SSID に対して有効になると、RADIUS サーバ上で設定されたレルムに対して EAP ID 応答で受信したレルムを照合するためのルックアップが実行されます。クライアントがレルムとともにユーザ名を送信しない場合は、WLAN で設定されているデフォルトの RADIUS サーバが認証に使用されます。クライアントから受信したレルムが、WLAN 上で設定されているレルムと一致しない場合、クライアントは認証解除され、ドロップされます。

RADIUS レルム機能が WLAN で有効になっていない場合は、EAP ID 要求の一部として受信したユーザ名がユーザ名として直接使用され、設定されている RADIUS サーバが認証およびアカウンティングに使用されます。デフォルトでは、RADIUS レルム機能は WLAN で無効になっています。

- **認証用のレルム照合**：EAP 方式を使用した dot1x（EAP AKA と同様）では、ユーザ名が EAP ID 応答の一部として受信されます。レルムはユーザ名から抽出され、対応する RADIUS 認証サーバですでに設定されているレルムと照合されます。一致した場合は、認証要求が RADIUS サーバに転送されます。一致しなかった場合は、クライアントが認証解除されます。
- **アカウンティング用のレルム照合**：クライアントのユーザ名が access-accept メッセージを通じて受信されます。アカウンティングメッセージがトリガーされると、対応するクライアントのユーザ名からレルムが抽出され、RADIUS アカウンティング サーバ上で設定されたアカウンティング レルムと比較されます。一致した場合は、アカウンティング要求が RADIUS サーバに転送されます。一致しなかった場合は、アカウンティング要求が破棄されます。

RADIUS レルムの有効化

RADIUS レルムを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# 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	**wireless aaa policy** *aaa-policy* **例：** `Device(config)# wireless aaa policy policy-1`	新しい AAA ポリシーを作成します。
ステップ 3	**aaa-realm enable** **例：** `Device(config-aaa-policy)# aaa-realm enable`	AAA RADIUS レルムの選択を有効にします。 （注） RADIUS レルムを無効にするには、**no aaa-realm enable** または **default aaa-realm enable** コマンドを使用します。

認証およびアカウンティング用に RADIUS サーバと照合するためのレルムの設定

認証およびアカウンティング用にRADIUSサーバと照合するようにレルムを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 認証モデルを作成します。
ステップ 3	**aaa authorization network default group** *radius-server-group* 例： `Device(config)# aaa authorization network default group aaa_group_name`	許可の方法を設定します。
ステップ 4	**aaa authentication dot1x** *realm* **group** *radius-server-group* 例： `Device(config)# aaa authentication dot1x cisco.com group cisco1`	dot1xがレルム グループRADIUSサーバを使用する必要があることを示します。
ステップ 5	**aaa authentication login** *realm* **group** *radius-server-group* 例： `Device(config)# aaa authentication login cisco.com group cisco1`	ログイン時の認証方法を定義します。
ステップ 6	**aaa accounting identity** *realm* **start-stop group** *radius-server-group* 例： `Device(config)# aaa accounting identity cisco.com start-stop group cisco1`	アカウンティングを有効にして、クライアントが承認されたときに start-record アカウンティング通知を送信し、最後に stop-record を送信できるようにします。

WLAN の AAA ポリシーの設定

WLAN の AAA ポリシーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless aaa policy** *aaa-policy-name* 例： `Device(config)# wireless aaa policy aaa-policy-1`	ワイヤレスの新しい AAA ポリシーを作成します。
ステップ 3	**aaa-realm enable** 例： `Device(config-aaa-policy)# aaa-realm enable`	レルム別の AAA RADIUS サーバの選択を有効にします。
ステップ 4	**exit** 例： `Device(config-aaa-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**wireless profile policy** *wlan-policy-profile* 例： `Device(config)# wireless profile policy wlan-policy-a`	WLAN ポリシープロファイルを設定します。
ステップ 6	**aaa-policy** *aaa-policy* 例： `Device(config-wireless-policy)# aaa-policy aaa-policy-1`	AAA ポリシーをマッピングします。
ステップ 7	**accounting-list** *acct-config-realm* 例： `Device(config-wireless-policy)# accounting-list cisco.com`	アカウンティング リストを設定します。
ステップ 8	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 9	**wlan** *wlan-name wlan-id ssid* 例： `Device(config)# wlan wlan2 14 wlan-aaa`	WLAN を設定します。
ステップ 10	**security dot1x authentication-list** *auth-list-realm* 例： `Device(config-wlan)# security dot1x authentication-list cisco.com`	IEEE 802.1x のセキュリティ認証リストを有効にします。
ステップ 11	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 12	**wireless tag policy** *policy* 例： `Device(config)# wireless tag policy tag-policy-1`	ポリシー タグを設定します。
ステップ 13	**wlan** *wlan-name* **policy** *policy-profile* 例： `Device(config-policy-tag)# wlan Abc-wlan policy wlan-policy-a`	ポリシープロファイルを WLAN にマッピングします。
ステップ 14	**exit** 例： `Device(config-policy-tag)# exit`	グローバル コンフィギュレーション モードに戻ります。

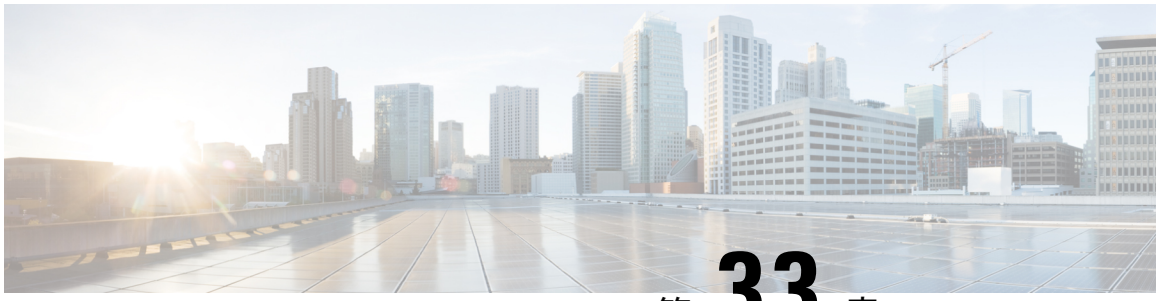
RADIUS レルム設定の確認

RADIUS レルム設定を確認するには、次のコマンドを使用します。

```
Device# show wireless client mac-address 14bd.61f3.6a24 detail


Client MAC Address : 14bd.61f3.6a24
Client IPv4 Address : 9.4.113.103
Client IPv6 Addresses : fe80::286e:9fe0:7fa6:8f4
Client Username : sacthoma@cisco.com
AP MAC Address : 4c77.6d79.5a00
AP Name: AP4c77.6d53.20ec
AP slot : 1
Client State : Associated
Policy Profile : name-policy-profile
Flex Profile : N/A
Wireless LAN Id : 3
Wireless LAN Name: ha_realm_WLAN_WPA2_AES_DOT1X
BSSID : 4c77.6d79.5a0f
```

```
Connected For : 26 seconds
Protocol : 802.11ac
Channel : 44
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Re-Authentication Timeout : 1800 sec (Remaining time: 1775 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 06/12/2018 19:52:35 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 25 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : PEAP
VLAN : 113
Multicast VLAN : 0
Access VLAN : 113
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_9040000f
  IIF ID           : 0x9040000F
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 097704090000000DF4607B3B
  Acct Session ID  : 0x00000fa2
  Aaa Server Details
  Server IP        : 9.4.23.50
  Auth Method Status List
       Method : Dot1x
              SM State         : AUTHENTICATED
              SM Bend State    : IDLE
  Local Policies:
       Service Template : wlan_svc_name-policy-profile_local (priority 254)
              Absolute-Timer   : 1800
              VLAN             : 113
  Server Policies:
  Resultant Policies:
```

```
              VLAN            : 113
              Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 0
  Number of Bytes Sent : 0
  Number of Packets Received : 0
  Number of Packets Sent : 0
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : 0 dBm
  Signal to Noise Ratio : 0 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```



第 33 章

Cisco StadiumVision

Cisco StadiumVision の概要

Cisco StadiumVision ソリューションは、実績のあるエンドツーエンドの高解像度 IPTV ソリューションです。デジタル コンテンツの高度な管理機能と配信機能によって、スタジアムの雰囲気を一変させます。このソリューションは Cisco Connected Stadium ソリューションの上層に構築され、StadiumVision Director を通じて一元管理されます。Cisco StadiumVision ソリューションでは、複数の送信元からスタジアムのさまざまなエリアに、カスタマイズされた動的なコンテンツをハイ デフィニション品質で統合的に自動配信できます。

このテクノロジーにより、ゲームの中でとてもエキサイティングで重要な瞬間を Wi-Fi 対応デバイス上でリプレイすることができます。

コントローラで Cisco StadiumVision ソリューションを有効にするには、次のパラメータを設定する必要があります。

1. ワイヤレス コントローラ：
   - マルチキャスト データ レート
   - RX 感度 SOP
   - マルチキャスト バッファ
2. CAPWAP
3. AP 無線ドライバとファームウェア：
   - マルチキャスト データ レート
   - RX 感度 SOP
   - マルチキャスト バッファ

Cisco StadiumVision のワイヤレス コントローラ パラメータの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Advanced] を選択します。

ステップ 2 [High Density] タブをクリックします

ステップ 3 [Multicast Data Rate] セクションで、ドロップダウンを使用して 5 GHz 無線または 2.4 GHz 無線のデータレートを設定します。

ステップ 4 [Apply] をクリックします。

Cisco StadiumVision のワイヤレス コントローラ パラメータの設定（CLI）

（注）

- マルチキャスト バッファおよびデータ レートの設定は、すべての AP モデルでサポートされています。
- Rx SOP 機能は、次のモデルでサポートされています。
  - Cisco Aironet 1570 シリーズ アクセス ポイント
  - Cisco Aironet 2700 シリーズ アクセス ポイント
  - Cisco Aironet 2800 シリーズ アクセス ポイント
  - Cisco Aironet 3700 シリーズ アクセス ポイント
  - Cisco Aironet 3800 シリーズ アクセス ポイント
  - Cisco Aironet 4800 シリーズ アクセス ポイント

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *wlan-name wlan-id* 例：	WLAN を設定します。

	コマンドまたはアクション	目的
	`Device(config)# wlan wlan1 10`	
ステップ 2	**multicast buffer** *multicast-buffer-number* 例： `Device(config-wlan)# multicast buffer 45`	WLAN で拡張マルチキャスト バッファ サイズを 30（デフォルト）～ 60 の範囲で設定します。 （注） 拡張マルチキャスト バッファについては、コントローラで設定されている 512 個の WLAN のうち 2 つのみを有効にすることができます。
ステップ 3	**ap dot11 [5ghz| 24ghz] multicast data-rate** *rate* 例： `Device(config)# ap dot11 [5ghz| 24ghz] rx-sop threshold custom -70`	無線受信感度 SOP のしきい値を -60 ～ -85 dB の範囲で設定します。この値は、5 GHz または 2.4 GHz 帯域に固有の事前定義された auto、low、high、medium の値として設定することもできます。 デフォルトでは、設定は無効になっており、値は [auto] に設定されています。*auto*（0）の RxSOP 値がプッシュされた場合、AP は、値を製造時に焼き付けされたものと見なします。

StadiumVision の設定の確認

- **show ap rf-profile name** *rf-name* **detail**
- **show ap dot11 5ghz** *high-density*

Rx SOP

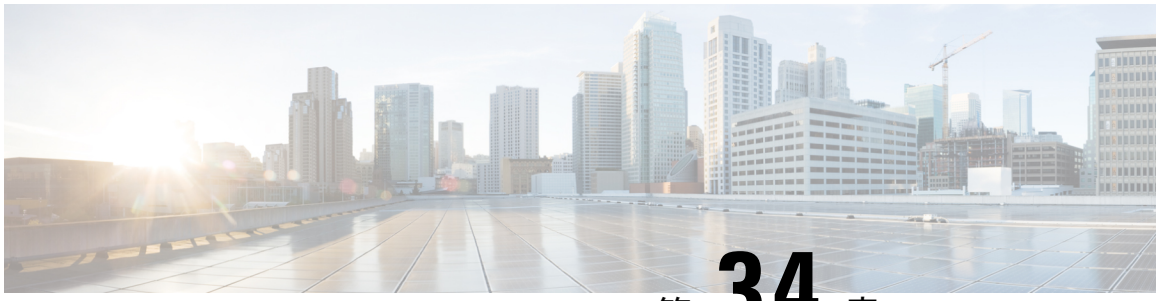
```
Device#show ap rf-profile name Typical_Client_Density_rf_5gh detail | i SOP
Rx SOP Threshold                : auto
```

マルチキャスト バッファ

```
Device#show wlan id 1 | sec Buffer
Multicast Buffer                                : Enabled
Multicast Buffer Size                           : 45

Device#

Device#sh wlan name vwlc-OpenAuth | inc Buffer
Multicast Buffer                                : Enabled
Multicast Buffer Size                           : 45
Device#
```

マルチキャスト データ レート

```
Device#sh ap dot11 24ghz high-density
AP Name                          Mac Address            Slot         Rxsop
Threshold Type Value (dbm)       Multicast Data Rate(Mbps)
-------------------------------------------------------------------------------------
-------------------------------------------------
test-1800-AP                      aaaa.bbbb.cccc            0         auto
        0                         54
AP4001.7AB2.BEB6                  aaab.bbbb.cccc            2         auto
        0                         54
AP70DF.2FA2.72EE                  aaac.bbbb.cccc            0         auto
        0                         0

Device#show ap dot11 5ghz high-density
AP Name                          Mac Address            Slot         Rxsop
Threshold Type Value (dbm)       Multicast Data Rate(Mbps)
-------------------------------------------------------------------------------------
-------------------------------------------------
Saji-1800-AP                      aaab.bbbb.cccc            1         auto
        0                         12
Saji-2802I-AP                     aaab.bbbb.cccc            0         custom
         -82                       12
Saji-2802I-AP                     aaac.bbbb.cccc            1         custom
         -82                       12
AP4001.7AB2.BEB6                  aaad.bbbb.cccc            0         custom
         -82                       12
AP4001.7AB2.BEB6                  aaae.bbbb.cccc            1         custom
         -82                       0
AP500F.8086.8B56                  aaaf.bbbb.cccc            0         custom
         -82                       12
AP500F.8086.8B56                  aaag.bbb.cccc            1         custom
         -82                       12
AP70DF.2FA2.72EE                  aaah.bbbb.cccc            1         auto
        0                         0

Device#
Device(config)#ap dot11 5ghz rf-profile test_5ghz_rf
Device(config-rf-profile)#high-density multicast data-rate RATE_18M


Device#  show ap rf-profile name test_5ghz_rf detail | inc Multicast
Multicast Data Rate               : 18 Mbps
Device#
```



第 34 章

永続的 SSID ブロードキャスト

永続的 SSID ブロードキャスト

メッシュ ネットワーク内のアクセス ポイントは、ルート アクセス ポイント（RAP）またはメッシュ アクセス ポイント（MAP）として動作します。RAP はコントローラへ有線で接続され、MAP はコントローラへ無線で接続されます。この機能は、Flex＋ブリッジ モードの Cisco Aironet 1542 アクセス ポイントにのみ適用されます。

この機能により、WAN 接続がダウンしている場合でも、ルート アクセス ポイント（RAP）とメッシュ アクセス ポイント（MAP）が SSID をブロードキャストします。このことは、障害の原因がバックホールにあるのかアクセス ワイヤレス ネットワークにあるのかにかかわらず、責任を分離するために必要です。なぜなら、ネットワークの各部分はさまざまな通信事業者が所有している可能性があるためです。

デフォルト ゲートウェイが到達可能である限り、RAP および MAP はスタンドアロン モード時は SSID をブロードキャストします。

永続的 SSID ブロードキャストの設定

手順

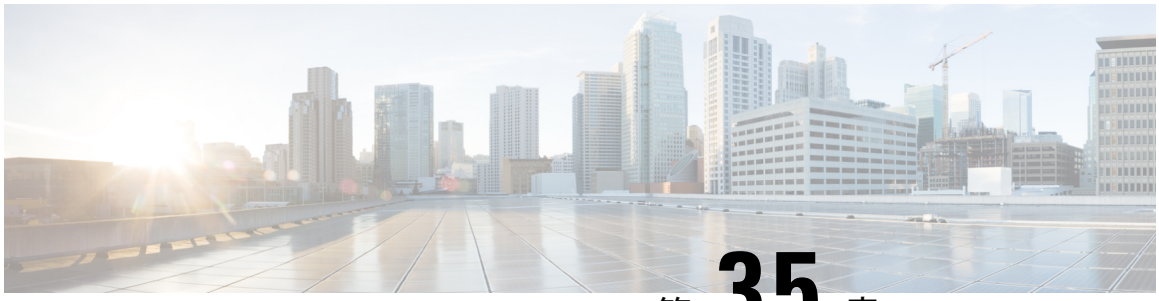
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**ap profile** *ap-profile-name* 例： `Device(config)# ap profile ap-profile-name`	AP プロファイルを設定します。
ステップ 3	**[no]ssid broadcast persistent** 例： `Device(config-ap-profile)# [no] ssid broadcast persistent`	**ssid broadcast** コマンドを実行すると、SSID ブロードキャスト モードが設定されます。**persistent** キーワードを指定すると、永続的 SSID ブロードキャストが有効になり、関連付けられた AP が再参加します。この機能を無効にするには、**[no]** コマンドを使用します。 （注） この機能を有効または無効にすると、AP が再参加します。

永続的 SSID ブロードキャストの確認

すべてのシスコ AP の設定を表示するには、次の **show** コマンドを使用します。

```
Device#show ap config general
Cisco AP Name   : AP4C77.6DF2.D598
=================================================
Office Extend Mode                              : Disabled
Persistent SSID Broadcast                       : Enabled
Remote AP Debug                                 : Disabled
```



第 35 章

ネットワーク モニタリング

ネットワーク モニタリング

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、この機能を使用して API を公開したり、サードパーティ システムにデータをプッシュしたりします。サードパーティ システムは、特定のパラメータ（たとえば、村の名前、各村のアクセスポイントなど）をモニタするアプリケーションの開発に使用されます。

サードパーティ システムへのデータの転送に使用されるメカニズムは、NETCONF/YANG です。YANG をネットワーク設定プロトコル（NETCONF）で使用すると、自動化されたプログラミング可能なネットワーク操作の望ましいソリューションが実現します。

次のリンクを使用して、NETCONF/YANG 機能の API または開発者のサポートに問い合わせることができます。

https://developer.cisco.com/site/support/#

次の 2 種類の情報が提供されます。

- 同期的に受信されるステータス情報：NETCONF はステータス情報に使用される管理インターフェイスであり、コントローラを含むデバイスの動作状態を公開できます。
- 非同期的に送信されるアラームおよびイベント情報：NETCONF/YANG のプッシュは、アラームおよびイベント情報に使用されるソリューションであり、サブスクライブ対象の NETCONF 通知を送信するメカニズムを提供します。

同期的に受信されるステータス情報：設定例

NETCONF/YANG インターフェイスは、顧客の要求に応えることを目的として使用されます。

ステータス情報およびアラーム/イベント情報の前提条件となる設定として、次のコマンドを使用してコントローラ上で NETCONF サーバを有効にする必要があります。

netconf-yang

「同期的に受信されるステータス情報」タイプでは、次の情報が NETCONF を介してエクスポートされます。

- 村の名前
- 各村の AP
- 各 AP のステータス
- 各村と各 AP で現在接続してログオンしているクライアントの数

上記の項目のデータはすべて、すでに参照可能です。これは、コントローラの動作データが NETCONF によってエクスポートされているためです。以下の例では、リストされているデータ項目が参照可能な場所について説明します。

次のコマンドをコントローラで使用します。

```
wireless tag site village_name_1
```

サイト タグは、 **get config** 操作を使用して NETCONF によって取得できます。

村の名前の出力例：

```
<site-cfg-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-site-cfg">
[...]
<site-tag-configs>
  <site-tag-config>
    <site-tag-name>village_name_1</site-tag-name>
    <description>custom user site tag for a village</description>
  </site-tag-config>
[...]
</site-tag-configs>
```

コントローラの動作データには、接続されている（join している）AP がすべて含まれており、サイト タグがリストされています。出力例には、AP とサイト タグに関する詳細情報が表示されています。次の例では、関連するフィールドと対応するコントローラの show コマンドを示します。

村ごとのアクセス ポイントの出力例：

```
<data>
    <access-point-oper-data
xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-oper">
    [...]
      <radio-oper-data>
        <wtp-mac>00:1b:0c:00:02:00</wtp-mac>      #show ap dot11 {24ghz|5ghz} summary
"MAC Address"
        <radio-slot-id>0</radio-slot-id>          #show ap dot11 {24ghz|5ghz} summary
"Slot"
        <ap-mac>00:1b:0c:00:02:00</ap-mac>
        <slot-id>0</slot-id>
        <radio-type>1</radio-type>                # 1 - 2.4GHz, 2 - 5GHz
        <admin-state>enabled</admin-state>        #show ap dot11 {24ghz|5ghz} summary
"Admin State"
        <oper-state>radio-up</oper-state>         #show ap dot11 {24ghz|5ghz} summary
```

```
"Oper State"
    [...]
[...]
      <capwap-data>
        <wtp-mac>00:1b:0c:00:02:00</wtp-mac>                #show ap summary  "Radio
MAC"
        <ap-operation-state>registered</ap-operation-state> #show ap summary  "State"
       <ip-addr>10.102.140.10</ip-addr>                  #show ap summary  "IP Address"

        [...]
       <admin-state>1</admin-state>             #show ap status   "Status", 1 - Enabled,
 2 - Disabled
        <location>default-location </location>    #show ap summary  "Location"
        <country-code>CH </country-code>
        <name>AP_A-1</name>                        #show ap summary  "AP Name"
 [...]
        <tag-info>
          [...]
          <site-tag>
            <site-tag-name>village_name_1</site-tag-name> #show ap name AP_A-1 config
general "Site Tag Name"
            [...]
          </site-tag>
[...]
```

コントローラの動作データには、接続されているすべてのワイヤレス クライアントの情報が含まれています。これには、MAC アドレス、IP アドレス、状態、AP 名などの詳細なクライアント デバイス情報が含まれます。

現在オンラインで、各村と各 AP にログインしているクライアントの数の出力例：

```
<data>
   <client-oper-data xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-client-oper">
      <common-oper-data>
       <client-mac>00:00:1a:04:00:02</client-mac>     #show wireless client summary  "MAC
 Address"
        <ap-name>AP_A-1</ap-name>                      #show wireless client summary  "AP
 Name"
        [...]
        <co-state>client-status-run</co-state>         #show wireless client
summary  "State"
```

非同期的に受信されるアラームおよびイベント情報：設定例

アラームおよびイベント情報のプッシュ機能は、XMLエンコーディングを使用したNETCONF ダイナミック サブスクリプションによる変更通知によって実行されます。

AP のアップ/ダウン イベント：サブスクリプションの出力例

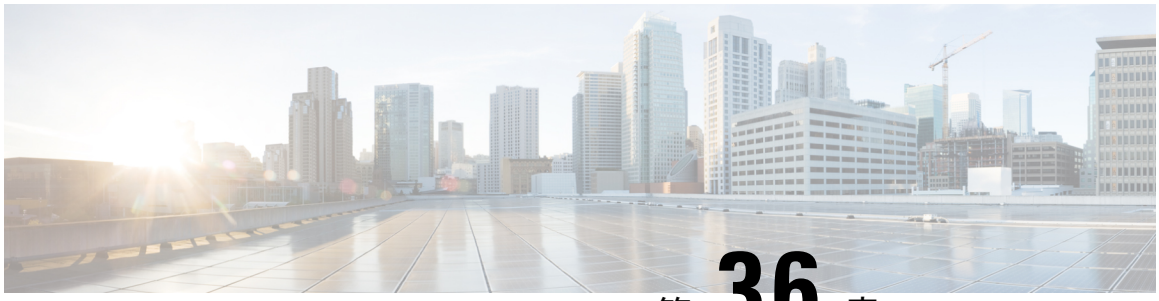
```
Request:

<?xml version="1.0" encoding="UTF-8"?>
<rpc message-id="urn:uuid:b0c581c9-ff5a-4352-9e64-7f2ce1ec603a"
xmlns="urn:ietf:params:xml:ns:netconf:base:1.0">
 <establish-subscription xmlns="urn:ietf:params:xml:ns:yang:ietf-event-notifications"
   xmlns:yp="urn:ietf:params:xml:ns:yang:ietf-yang-push">
  <stream>yp:yang-push</stream>
```

```
  <yp:xpath-filter>/access-point-oper-data/capwap-data/ap-operation-state</yp:xpath-filter>

  <yp:dampening-period>0</yp:dampening-period>
 </establish-subscription>
</rpc>

Reply:

<?xml version="1.0" encoding="UTF-8"?>
<rpc-reply xmlns="urn:ietf:params:xml:ns:netconf:base:1.0"
message-id="urn:uuid:673b42b2-e988-4e20-a6c3-0679c08e6114"><subscription-result
xmlns='urn:ietf:params:xml:ns:yang:ietf-event-notifications'
xmlns:notif-bis="urn:ietf:params:xml:ns:yang:ietf-event-notifications">notif-bis:ok</subscription-result>
<subscription-id
xmlns='urn:ietf:params:xml:ns:yang:ietf-event-notifications'>2147483652</subscription-id>
</rpc-reply>
-->>
(Default Callback)
Event time      : 2018-03-09 15:08:21.880000+00:00
Subscription Id : 2147483651
Type            : 2
Data            :
<datastore-changes-xml xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-push">
  <yang-patch xmlns="urn:ietf:params:xml:ns:yang:ietf-yang-patch">
    <patch-id>null</patch-id>
    <edit>
      <edit-id>edit1</edit-id>
      <operation>merge</operation>
      <target>/access-point-oper-data/capwap-data</target>
      <value>
        <capwap-data
xmlns="http://cisco.com/ns/yang/Cisco-IOS-XE-wireless-access-point-oper">
          <ap-operation-state>registered</ap-operation-state>
          <wtp-mac>00ab11006600</wtp-mac>
        </capwap-data>
      </value>
    </edit>
  </yang-patch>
</datastore-changes-xml>
<<--
```

第 V 部

システム管理

- ソフトウェア メンテナンス アップグレード （503 ページ）



第 36 章

Network Mobility Services Protocol（ネットワーク モビリティ サービス プロトコル）

Network Mobility Services Protocol について

Cisco Network Mobility Services Protocol（NMSP）は、コネクション型（TLS）またはコネクションレス型（DTLS）の転送を介して実行できる、セキュアな双方向プロトコルです。ワイヤレス インフラストラクチャで NMSP サーバを実行し、Cisco Connected Mobile Experiences（Cisco CMX）が NMSP クライアントとして機能します。コントローラは複数のサービスをサポートし、複数の Cisco CMX が NMSP サーバに接続して、NMSP セッションを介して各種サービスのデータを取得できます（ワイヤレス デバイスの場所、プローブ RSSI、HyperLocation、wIPS など）。

NMSP は、Cisco CMX とコントローラ間の相互通信を定義します。Cisco CMX は、ルーテッド IP ネットワークを介してコントローラと通信します。publish-subscribe と request-reply の両方の

通信モデルがサポートされています。通常、Cisco CMXは、コントローラから定期的な更新の形式でサービス データを受信するためのサブスクリプションを確立します。コントローラはデータ パブリッシャとして機能し、複数の CMX にサービス データをブロードキャストします。サブスクリプションに加えて、Cisco CMXはコントローラが応答を送り返すようにコントローラに要求を送信することもできます。

NMSPは基本的に、外部との通信手段をコントローラのアプリケーションに提供します。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの NMSP は、外部と通信するようにプロトコルを変更する柔軟性も備えています。

Network Mobility Services Protocol の機能の一覧を次に示します。

- NMSP はデフォルトで無効になっています。
- NMSP は TCP を使用して Cisco CMX と通信し、暗号化に TLS を使用します。
- ワイヤレス侵入防御システム（wIPS）は TCP および TLS を介した場合のみサポートされます。
- Web ソケットを使用すると、双方向通信がサポートされ、Cisco CMX は確立されたチャネルを介して非同期的にメッセージを送信できます。

（注） HTTPS は、コントローラと Cisco CMX 間のデータ転送ではサポートされていません。

NMSP オンプレミス サービスの有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**nmsp enable** 例： `Device(config)# nmsp enable`	NMSP オンプレミス サービスを有効にします。 （注） デフォルトでは、NMSP はコントローラで有効になっています。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クライアント、RFID タグ、および不正デバイスの NMSP 通知間隔の変更

NMSP は、Cisco モビリティ サービス エンジン（Cisco MSE）とコントローラ間の発着信トラフィックに関する通信を管理します。高い頻度でのロケーション更新を必要とするアプリケーションがある場合は、クライアント、アクティブな RFID タグ、および不正なアクセス ポイント/クライアントの NMSP 通知間隔を 1 ～ 180 秒の範囲内で変更できます。

（注） NMSP が機能するためには、コントローラと Cisco MSE の間にあるすべてのファイアウォールで、コントローラと Cisco MSE 間の通信に使用される TCP ポート（16113）が開いている（ブロックされていない）必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**nmsp notification interval** {**rssi** {**clients** | **rfid** | **rogues** {**ap** | **client** } | **spectrum interferers** } *interval*} 例： `Device(config)# nmsp notification interval rssi rfid 50`	クライアント、RFID タグ、不正クライアント、およびアクセス ポイントの NMSP 通知間隔の値を設定します。 *interval*：RSSI 測定の NMSP 通知間隔の値（秒単位）。有効な範囲は 1 ～ 180 です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クライアント、RFID タグ、および不正デバイスの NMSP 通知しきい値の変更（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**location notify-threshold** {**clients** | **rogues ap** | **tags** } *threshold* 例： `Device(config)# location notify-threshold clients 5`	クライアント、RFID タグ、不正クライアント、およびアクセス ポイントの NMSP 通知しきい値を設定します。 *threshold*：RSSI しきい値（db 単位）。有効な範囲は 0 ～ 10 です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

NMSP の強力な暗号の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**nmsp strong-cipher** 例： `Device(config)# nmsp strong-cipher`	NMSP サーバの強力な暗号を有効にします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

NMSP 設定の表示

コントローラの NMSP 機能を表示するには、次のコマンドを使用します。

```
Device# show nmsp capability
Service            Subservice
----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum           Aggregate Interferer, Air Quality, Interferer,
Info               Rogue, Mobile Station,
Statistics         Rogue, Tags, Mobile Station,
AP Monitor         Subscription
On Demand Services Device Info
AP Info            Subscription
```

NMSP 通知間隔を表示するには、次のコマンドを使用します。

```
Device# show nmsp notification interval
NMSP Notification Intervals
---------------------------

RSSI Interval:
  Client              : 2 sec
  RFID                : 50 sec
  Rogue AP            : 2 sec
  Rogue Client        : 2 sec
  Spectrum            : 2 sec
```

すべての CMX 接続における接続固有の統計カウンタを表示するには、次のコマンドを使用します。

```
Device# show nmsp statistics connection
NMSP Connection Counters
------------------------
 CMX IP Address: 10.22.244.31, Status: Active
 State:
      Connections : 1
      Disconnections : 0
      Rx Data Frames : 13
      Tx Data Frames : 99244
      Unsupported messages : 0
  Rx Message Counters:
     ID  Name                                  Count
    ---------------------------------------------
      1  Echo Request                          6076
      7  Capability Notification                  2
     13  Measurement Request                      5
     16  Information Request                      3
     20  Statistics Request                       2
     30  Service Subscribe Request                1

  Tx Message Counters:
     ID  Name                                  Count
    ---------------------------------------------
      2  Echo Response                         6076
      7  Capability Notification                  1
     14  Measurement Response                    13
     15  Measurement Notification              91120
     17  Information Response                     6
     18  Information Notification              7492
     21  Statistics Response                      2
     22  Statistics Notification                305
```

```
     31  Service Subscribe Response              1
     67  AP Info Notification                  304
```

コントローラのNMSPサービスにおける共通の統計カウンタを表示するには、次のコマンドを使用します。

```
Device# show nmsp statistics summary
NMSP Global Counters
--------------------
Number of restarts                :

SSL Statistics
--------------------
Total amount of verifications      : 6
Verification failures              : 6
Verification success               : 0
Amount of connections created      : 8
Amount of connections closed       : 7
Total amount of accept attempts    : 8
Failures in accept                 : 0
Amount of successful accepts       : 8
Amount of failed registrations     : 0

AAA Statistics
--------------------
Total amount of AAA requests       : 7
Failed to send requests            : 0
Requests sent to AAA               : 7
Responses from AAA                 : 7
Responses from AAA to validate     : 7
Responses validate error           : 6
Responses validate success         : 1
```

NMSP の全体的な接続を表示するには、次のコマンドを使用します。

```
Device# show nmsp status
NMSP Status
-----------

CMX IP Address   Active    Tx Echo Resp  Rx Echo Req   Tx Data     Rx Data     Transport
-------------------------------------------------------------------------------------------
127.0.0.1        Active    6             6             1           2           TLS
```

すべてのCMXによってサブスクライブされているすべてのモビリティ サービスを表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription detail
CMX IP address 127.0.0.1:
Service            Subservice
-----------------------------
RSSI               Rogue, Tags, Mobile Station,
Spectrum
Info               Rogue, Mobile Station,
Statistics         Tags, Mobile Station,
AP Info            Subscription
```

特定の CMX によってサブスクライブされているすべてのモビリティ サービスを表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription detail <ip_addr>
CMX IP address 127.0.0.1:
Service            Subservice
-----------------------------
```

```
RSSI                Rogue, Tags, Mobile Station,
Spectrum
Info                Rogue, Mobile Station,
Statistics          Tags, Mobile Station,
AP Info             Subscription
```

すべての CMX によってサブスクライブされているモビリティ サービス全体を表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription summary
Service             Subservice
-----------------------------
RSSI                Rogue, Tags, Mobile Station,
Spectrum
Info                Rogue, Mobile Station,
Statistics          Tags, Mobile Station,
AP Info             Subscription
```

例：NMSP の設定

次に、RFID タグの NMSP 通知間隔を設定する例を示します。

```
Device# configure terminal
Device(config)# nmsp notification interval rssi rfid 50
Device(config)# end
Device# show nmsp notification interval
```

次に、クライアントの NMSP 通知間隔を設定する例を示します。

```
Device# configure terminal
Device(config)# nmsp notification interval rssi clients 180
Device(config)# end
Device# show nmsp notification interval
```

CMX からのサブスクリプション リストがある AP グループ別の NMSP

Cisco CMX グループのサポートにより、必要な Network Mobility Services Protocol（NMSP）データだけを Cisco CCMX に送信できます（オンプレミスとクラウド ベースの CMX の両方に適用可能）。Cisco CMX は、ワイヤレス コントローラ内のアクティブなサービスに基づいて、特定の AP または AP グループの NMSP データをサブスクライブできます。

この機能は、AP が異なる CMX サーバにわたって分散されているときの、データ フローの負荷のロード バランシングと最適化に役立ちます。Cisco CMX サーバは、CMX AP グループを作成し、一意の名前を付け、その配下の AP をグループ化します。

（注） Cisco CMX AP グループは、ロケーション サービスのために Cisco CMX によって管理されている Cisco AP のリストです。この AP グループは、ワイヤレス コントローラの AP グループと同じではありません。

この機能は次のサービスをサポートしています。

- クライアント
- プローブ クライアントのフィルタリング
- HyperLocation
- BLE サービス

（注） NMSP サブスクリプションが使用できるのは、ワイヤレス コントローラで有効状態になっているサービスの場合のみです。

CMX からのサブスクリプション リストがある AP グループ別の NMSP の確認

すべての CMX 接続におけるモビリティ サービス グループのサブスクリプションの概要を表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription group summary

CMX IP address: 127.0.0.1
  Groups subscribed by this CMX server:
  Group name: Group1
```

AP グループにサブスクライブされているサービスを CMX 接続別に表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription group details services group-name cmx-IP-addrress

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group filtered services:
Service            Subservice
-----------------------------
RSSI               Mobile Station,
Spectrum
Info
Statistics
```

AP グループにサブスクライブされている AP MAC リストを CMX 接続別に表示するには、次のコマンドを使用します。

```
Device show nmsp subscription group detail ap-list group-name  cmx-IP-addrress

CMX IP address: 127.0.0.1
CMX Group name: Group1
CMX Group AP MACs:
: 00:00:00:00:70:02  00:00:00:00:66:02  00:99:00:00:00:02  00:00:00:bb:00:02
  00:00:00:00:55:02  00:00:00:00:50:02  00:33:00:00:00:02  00:d0:00:00:00:02
  00:10:00:10:00:02  00:00:00:06:00:02  00:00:00:02:00:02  00:00:00:00:40:02
  00:00:00:99:00:02  00:00:00:00:a0:02  00:00:77:00:00:02  00:22:00:00:00:02
  00:00:00:00:00:92  00:00:00:00:00:82  00:00:00:00:03:02  aa:00:00:00:00:02
  00:00:00:50:00:42  00:00:0d:00:00:02  00:00:00:00:00:32  00:00:00:cc:00:02
  00:00:00:88:00:02  20:00:00:00:00:02  10:00:00:00:00:02  01:00:00:00:00:02
  00:00:00:00:00:02  00:00:00:00:00:01  00:00:00:00:00:00
```

すべての CMX における CMX-AP グループ化の詳細を表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription group detail all
CMX IP address: 127.0.0.1
  Groups subscribed by this CMX server:
  Group name: Group1
    CMX Group filtered services:
    Service            Subservice
    ----------------------------
    RSSI               Mobile Station,
    Spectrum
    Info
    Statistics

    CMX Group AP MACs:
    : 00:00:00:00:00:03  00:00:00:00:00:02  00:00:00:00:00:01

  Group name: Group2
    CMX Group filtered services:
    Service            Subservice
    ----------------------------
    RSSI               Tags,
    Spectrum
    Info
    Statistics

    CMX Group AP MACs:
    : 00:00:00:00:03:00  00:00:00:00:02:00  00:00:00:00:01:00

  Group name: Group3
    CMX Group filtered services:
    Service            Subservice
    ----------------------------
    RSSI               Rogue,
    Spectrum
    Info
    Statistics

    CMX Group AP MACs:
    : 00:00:00:03:00:00  00:00:00:02:00:00  00:00:00:01:00:00
```

プローブ RSSI ロケーション

プローブ RSSI ロケーション機能を使用すると、ワイヤレス コントローラと Cisco CMX で次の動作をサポートできます。

- ロード バランシング
- カバレッジ ホールの検出
- CMX へのロケーションの更新

ワイヤレス クライアントが有効な場合、ワイヤレス クライアントから、近くにあるワイヤレス ネットワークを識別すると同時に、識別されたサービス セット識別子（SSID）に関連付けられた受信信号強度表示（RSSI）を検出するための、プローブ要求が送信されます。

ワイヤレス クライアントは、アクセス ポイントに接続した後も、定期的にバックグラウンドでアクティブ スキャンを実行します。これにより、ワイヤレス クライアントは、接続に最も適した信号強度を持つアクセス ポイントのリストを更新できるようになります。アクセス ポイントに接続できなくなると、ワイヤレス クライアントは、保存されているアクセス ポイント リストを使用して、最適な信号強度を提供する別のアクセスポイントに接続します。WLAN 内のアクセス ポイントは、これらのプローブ要求、RSSI、およびワイヤレス クライアントの MAC アドレスを収集し、それらをワイヤレス コントローラに転送します。Cisco CMX は、これらのデータをワイヤレスコントローラから収集し、それらを使用して、ネットワークをローミングする際にワイヤレス クライアントの更新後のロケーションを計算します。

プローブ RSSI の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# 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	**wireless probe filter** **例：** `Device(config)# wireless probe filter`	AP から受け取る未応答のプローブ要求のフィルタリングを有効にして、ロケーションの精度を向上させます。 この機能を無効にするには、このコマンドの **no** 形式を使用します。この結果、応答済みと未応答の両方のプローブ要求がコントローラに転送されます。

	コマンドまたはアクション	目的
ステップ 3	**wireless probe limit** *limit-value interval* 例： `Device(config)# wireless probe limit 10 100`	同じクライアントに対して、指定した間隔で AP からワイヤレス コントローラに報告されるプローブ要求の数を設定します。 デフォルトの制限（500 ミリ秒の間隔で 2 つのプローブ）に戻すには、このコマンドの **no** 形式を使用します。
ステップ 4	**location algorithm rssi-average** 例： `Device(config)# location algorithm rssi-average`	プローブ RSSI 測定の更新を、より正確なアルゴリズムに設定します。ただし、CPU のオーバーヘッドは高くなります。
ステップ 5	**location algorithm simple** 例： `Device(config)# location algorithm simple`	（任意）プローブ RSSI 測定の更新を、より高速なアルゴリズムに設定します。CPU のオーバーヘッドは小さくなりますが、精度は低くなります。 アルゴリズム タイプをデフォルト（*rssi-average*）に戻すには、このコマンドの **no** 形式を使用します。
ステップ 6	**location expiry client** *interval* 例： `Device(config)# location expiry client 300`	RSSI 値のタイムアウトを設定します。 このコマンドの **no** 形式を指定すると、デフォルト値の 15 に設定されます。
ステップ 7	**location notify-threshold client** *threshold-db* 例： `Device(config)# location notify-threshold client 5`	クライアントの通知しきい値を設定します。 このコマンドの **no** 形式を指定すると、デフォルト値の 0 に設定されます。
ステップ 8	**location rssi-half-life client** *time-in-seconds* 例： `Device(config)# location rssi-half-life client 20`	2 つの RSSI 測定値を平均するときの半減期を設定します。 このオプションを無効にするには、値を 0 に設定します。

次のタスク

各プローブ クライアント（関連付けられていて、プローブのみ）を 10 個の MAC アドレスの集まりで表示するには、**show wireless client probing** コマンドを使用します。

RFID タグのサポート

コントローラでは、無線周波数ID（RFID）タグの追跡を設定できます。RFIDタグは、独自の信号を継続的にブロードキャストし、リアルタイムのロケーション トラッキングのためにアセットに付加される小型のワイヤレスバッテリ電源タグです。これらのタグは、自身の位置を専用の802.11パケットを使用してアドバタイズします。アドバタイズされたパケットは、アクセス ポイント、コントローラ、およびCisco CMXによって処理されます。アクティブなRFIDのみがサポートされています。アクティブなRFIDタグとワイヤレス コントローラの組み合わせにより、機器の現在の場所を追跡できます。「アクティブ」なタグは、一般には「クローズドループ」システム（タグがタグの所有者または発信者が管理する施設から物理的に離れることを前提としないシステム）での高価値資産のリアルタイム追跡に使用されます。

RFIDタグの詳細については、『Wi-Fi Location-Based Services 4.1 Design Guide』の「*Active RFID tags*」の項を参照してください。

一般的な注意事項

- シスコ準拠の「アクティブ RFID タグ」のみがサポートされています。
- コントローラで RFID タグを確認できます。
- RFID タグのハイ アベイラビリティがサポートされています。

RFID タグのサポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless rfid** 例： `Device(config)# wireless rfid`	RFID タグ追跡をイネーブルにします。 デフォルト値はイネーブルです。 RFID タグ追跡をディセーブルにするには、このコマンドの **no** 形式を使用します。
ステップ 3	**wireless rfid timeout** *timeout-value* 例： `Device(config)# wireless rfid timeout 90`	テーブルをクリーンアップするための RFID タグ データ タイムアウト値を設定します。

	コマンドまたはアクション	目的
		タイムアウト値は、タグを失効させるまでコントローラが保持する時間の長さです。たとえば、タグが 30 秒ごとにビーコンするよう設定されている場合は、タイムアウト値を 90 秒（ビーコン値の約 3 倍）に設定することをお勧めします。デフォルト値は 1200 秒です。

RFID タグのサポートの確認

クライアントである RFID タグのサマリーを表示するには、次のコマンドを使用します。

```
Device# show wireless rfid client
```

RFID タグの詳細情報を表示するには、次のコマンドを使用します。

```
Device# show wireless rfid detail <rfid-mac-address>

RFID address  000c.cc96.0001
Vendor Cisco
Last Heard 6 seconds  ago
Packets Received 187
Bytes Received 226

Content Header
==============
  CCX Tag Version 0
  Tx power: 12
  Channel: 11
  Reg Class: 4
CCX Payload
==============
  Last Sequence Control 2735
  Payload length 221
  Payload Data Hex Dump:
  00000000  00 02 00 00 01 09 00 00  00 00 0c b8 ff ff ff 02  |................|
  00000010  07 42 03 20 00 00 0b b8  03 4b 00 00 00 00 00 00  |.B. .....K......|
  00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
  00000030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
  00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
```

既知のすべての RFID タグについてそれらのサマリー情報を表示するには、次のコマンドを使用します。

```
Device# show wireless rfid summary

Total RFID entries: : 16
Total Unique RFID entries : 16
RFID ID VENDOR Closet AP RSSI Time Since Last Heard
0012.b80a.c791 Cisco 7069.5a63.0520 -31 3 minutes 30 seconds ago
0012.b80a.c953 Cisco 7069.5a63.0460 -33 4 minutes 5 seconds ago
0012.b80b.806c Cisco 7069.5a63.0520 -46 15 seconds ago
0012.b80d.e9f9 Cisco 7069.5a63.0460 -38 4 minutes 28 seconds ago
0012.b80d.ea03 Cisco 7069.5a63.0520 -43 4 minutes 29 seconds ago
0012.b80d.ea6b Cisco 7069.5a63.0460 -39 4 minutes 26 seconds ago
```

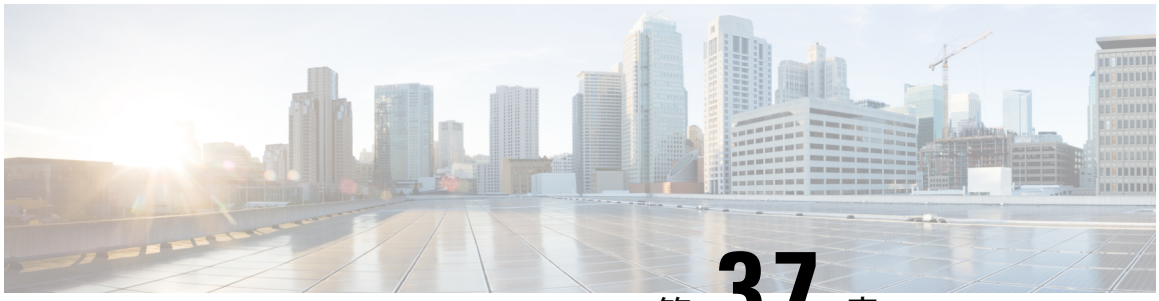
```
0012.b80d.ebe8 Cisco 7069.5a63.0520 -43 3 minutes 21 seconds ago
0012.b80d.ebeb Cisco 7069.5a63.0520 -43 4 minutes 28 seconds ago
0012.b80d.ec48 Cisco 7069.5a63.0460 -42 4 minutes 7 seconds ago
0012.b80d.ec55 Cisco 7069.5a63.0520 -41 1 minute 52 seconds ago
```

ロケーションベースのシステム RFID 統計情報を表示するには、次のコマンドを使用します。

```
Device# show wireless rfid stats

RFID stats :
==============
RFID error db full : 0
RFID error invalid paylod : 0
RFID error invalid tag : 0
RFID error dot11 hdr : 0
RFID error pkt len : 0
RFID error state drop : 0
RFID total pkt received : 369
RFID populated error value : 0
RFID error insert records : 0
RFID error update records : 0
RFID total insert record : 16
RFID ccx payload error : 0
RFID total delete record : 0
RFID error exceeded ap count : 0
RFID error record remove : 0
RFID old rssi expired count: 0
RFId smallest rssi expireed count : 0
RFID total query insert : 0
RFID error invalid rssi count : 0
```

NMSP 通知間隔を表示するには、次のコマンドを使用します。

```
Device# show nmsp notification interval

NMSP Notification Intervals
---------------------------

RSSI Interval:
  Client              : 2 sec
  RFID                : 50 sec
  Rogue AP            : 2 sec
  Rogue Client        : 2 sec
  Spectrum            : 2 sec
```



第 37 章

Application Visibility and Control（アプリケーションの可視化と制御）

Application Visibility and Control について

Application Visibility and Control（AVC）は、トラフィック情報を提供できる Flexible NetFlow（FNF）パッケージ全体のサブセットです。AVC 機能では、アクセス ポイント（AP）またはコントローラで実行される NBAR のメリットをもたらす分散型アプローチが利用されており、ディープ パケット インスペクション（DPI）を実行してその結果を FNF メッセージで報告することを目的としています。

AVC により、リアルタイム分析を実施し、ネットワークの輻輳、コストのかかるネットワーク リンクの使用、およびインフラストラクチャの更新を削減するためのポリシーを作成できます。トラフィック フローが NBAR2 エンジンを使用して分析および認識され、認識されたプロトコルまたはアプリケーションと一緒に、特定のフローがマークされます。このフロー単位の情報を、FNF によるアプリケーションの可視化に使用できます。アプリケーションの可視化が確立されると、ユーザはクライアントのポリシング メカニズムを使用してコントロール ルールを定義できます。

AVC ルールを使用すると、WLAN 上で join しているすべてのクライアントに対して、特定アプリケーションの帯域幅を制限できます。これらの帯域幅コントラクトは、アプリケーション単位のレート制限より優先されるクライアント単位のダウンストリーム レート制限と共存します。

FNF はワイヤレスでサポートされる機能であり、コントローラのすべてのモード（フレックス、ローカル、ファブリック）で NetFlow が有効になっている必要があります。

ローカル モードでは、NBAR はコントローラ ハードウェア上で実行され、プロセスのクライアント トラフィックは AP CAPWAP トンネルを使用してコントローラのデータプレーンを経由して流れます。

FlexConnect またはファブリック モードでは、NBAR は AP 上で動作し、統計情報のみがコントローラに送信されます。これら 2 つのモードで動作している場合、AP は定期的に FNFv9 レポートをコントローラに送り返します。コントローラの FNF 機能は、これらの FNFv9 レポートを使用して、AVC が表示するアプリケーション統計情報を提供します。

ファブリック モードの動作では、FNF キャッシュは設定されません。FNFv9 レポートを着信時にリレーします。その結果、フロー モニタの設定の一部（たとえば、キャッシュ タイムアウトなど）は考慮されません。

AVC ソリューションの動作は、ワイヤレスの展開に基づいて変わります。ここでは、すべてのシナリオにおける共通点と相違点について説明します。

ローカル モード

- NBAR はコントローラで有効になっています。
- AVC は、FNF 設定を AP にプッシュしません。
- ローミング イベントは無視されます。

  ただし、AVC は、トラフィックがアンカー コントローラ（クライアントが join したときのトラフィックを NBAR が最初に処理した場所）を通過する際に、ローカル モードでの L3 ローミングをサポートします。
- IOSd が NBAR 接続をトリガーする必要があります。
- フロー モニタ キャッシュをサポートします。
- NetFlow エクスポータをサポートします。

フレックス モード

- NBAR は AP で有効になっています。
- AVC は、FNF 設定を AP にプッシュします。
- AVC-FNF で、ローミングのコンテキスト転送をサポートします。
- フロー モニタ キャッシュをサポートします。
- NetFlow エクスポータをサポートします。

ファブリック モード

- NBAR は AP で有効になっています。
- AVC は、FNF 設定を AP にプッシュします。
- AVC-FNF で、ローミングのコンテキスト転送をサポートします。
- フロー モニタ キャッシュはサポートされません。
- 限定された、NetFlow エクスポータのサポートのみ提供します。

関連トピック

無線ゲスト アクセス （1119 ページ）

Application Visibility and Control の前提条件

- アクセスポイントは、AVC 対応である必要があります

  ただし、ローカル モードではこの要件は適用されません。
- AVC（QoS）の制御部分を機能させるには、FNF 付きのアプリケーションの可視化機能を設定する必要があります。

Application Visibility and Control の制限

- IPv6（ICMPv6 トラフィックを含む）のパケット分類は、FlexConnect モードおよびファブリック モードではサポートされません。ただし、ローカル モードではサポートされます。
- レイヤ 2 ローミングは、コントローラでサポートされていません。
- マルチキャスト トラフィックはサポートされていません。
- AVC は次のアクセス ポイントでのみサポートされます。
  - Cisco Aironet 1800 シリーズ アクセス ポイント
  - Cisco Aironet 2700 シリーズ アクセス ポイント
  - Cisco Aironet 2800 シリーズ アクセス ポイント

- Cisco Aironet 3700 シリーズ アクセス ポイント
- Cisco Aironet 3800 シリーズ アクセス ポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント

- AVC は、Cisco Aironet 702W、702I（128 M メモリ）、および 1530 シリーズ アクセス ポイントではサポートされません。
- App の可視性と認識されているアプリケーションのみ、QoS 制御の適用に使用できます。
- データリンクは AVC の NetFlow フィールドではサポートされません。
- AVC 非対応ポリシープロファイルと AVC 対応ポリシープロファイルの両方に同じ WLAN プロファイルをマッピングすることはできません。
- AVC は管理ポート（Gig 0/0）ではサポートされません。
- NBAR 対応 QoS ポリシー設定は有線物理ポートでのみ許可されます。ポリシー設定は、たとえば、VLAN、ポート チャネル、および他の論理インターフェイスなどの仮想インターフェイスではサポートされていません。

AVC が有効になっている場合、AVC プロファイルは、デフォルトの DSCP ルールを含む最大 23 個のルールのみをサポートします。ルールが 23 個を超えている場合、AVC ポリシーは AP までプッシュされません。

AVC の設定の概要

AVC を設定するには、次の手順に従います。

1. **record wireless avc basic** コマンドを使用してフロー モニタを作成します。
2. ワイヤレス ポリシー プロファイルを作成します。
3. フロー モニタをワイヤレス ポリシー プロファイルに適用します。
4. ワイヤレス ポリシー タグを作成します。
5. WLAN をポリシー プロファイルにマッピングします。
6. ポリシー タグを AP に接続します。

フロー モニタの作成

NetFlow の設定には、フロー レコード、フロー モニタ、およびフロー エクスポータが必要です。この設定は、AVC 全体の設定における最初のステップとして行ってください。

（注） Flex モードおよびローカル モードでは、**cache timeout active** および **cache timeout inactive** コマンドのデフォルト値は AVC に最適ではありません。フロー モニタでは、両方の値を 60 に設定することを推奨します。

ファブリック モードの場合、キャッシュ タイムアウト設定は適用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	**flow monitor** *monitor-name* **例：** `Cisco(config)# flow monitor fm_avc`	フロー モニタを作成します。
ステップ 2	**record wireless avc basic** **例：** `Cisco(config-flow-monitor)# record wireless avc basic`	基本的なワイヤレス AVC テンプレートを指定します。
ステップ 3	**cache timeout active** *value* **例：** `Cisco(config-flow-monitor)# cache timeout active 60`	アクティブ フロー タイムアウトを秒単位で設定します。
ステップ 4	**cache timeout inactive** *value* **例：** `Cisco(config-flow-monitor)# cache timeout inactive 60`	非アクティブ フロー タイムアウトを秒単位で設定します。

フロー レコードの作成

デフォルトのフロー レコードは、編集も削除もできません。新しいフロー レコードが必要な場合、1 つを作成し、CLI からのフロー モニタにマップする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**flow record** *flow_record_name* **例：**	フロー レコードを作成します。

	コマンドまたはアクション	目的
	`Device(config)# flow record record1`	（注） カスタムのフローレコードがFlexおよびファブリック モードで設定されている場合、オプション フィールド（record wireless avc basic にないフィールド）は無視されます。
ステップ 2	**description** *string* 例： `Device(config-flow-record)# description IPv4flow`	（任意）最大 63 文字で、このフローレコードの説明を指定します。
ステップ 3	**match ipv4 protocol** 例： `Device(config-flow-record)# match ipv4 protocol`	IPv4 プロトコルとの一致を指定します。
ステップ 4	**match ipv4 source address** 例： `Device(config-flow-record)# match ipv4 source address`	IPv4 送信元アドレス ベースのフィールドとの一致を指定します。
ステップ 5	**match ipv4 destination address** 例： `Device(config-flow-record)# match ipv4 destination address`	IPv4 宛先アドレス ベースのフィールドとの一致を指定します。
ステップ 6	**match transport source-port** 例： `Device(config-flow-record)# match transport source-port`	トランスポート層の発信元ポートのフィールドとの一致を指定します。
ステップ 7	**match transport destination-port** 例： `Device(config-flow-record)# match transport destination-port`	トランスポート層の宛先ポートのフィールドとの一致を指定します。
ステップ 8	**match flow direction** 例： `Device(config-flow-record)# match flow direction`	フローがモニタされる方向との一致を指定します。
ステップ 9	**match application name** 例：	アプリケーション名との一致を指定します。

	コマンドまたはアクション	目的
	`Device(config-flow-record)# match application name`	（注） この操作は、AVC サポートでは必須です。フローがアプリケーションと一致することが可能になるためです。
ステップ 10	**match wireless ssid** 例： `Device(config-flow-record)# match wireless ssid`	ワイヤレス ネットワークを特定する SSID 名との一致を指定します。
ステップ 11	**collect counter bytes long** 例： `Device(config-flow-record)# collect counter bytes long`	カウンタ フィールドの合計バイト数を収集します。
ステップ 12	**collect counter packets long** 例： `Device(config-flow-record)# collect counter bytes long`	カウンタ フィールドの合計パケット数を収集します。
ステップ 13	**collect wireless ap mac address** 例： `Device(config-flow-record)# collect wireless ap mac address`	ワイヤレス クライアントが関連付けられているアクセス ポイントの MAC アドレスを持つ BSSID を収集します。
ステップ 14	**collect wireless client mac address** 例： `Device(config-flow-record)# collect wireless client mac address`	ワイヤレス ネットワークのクライアントの MAC アドレスを収集します。

フロー エクスポータの作成

フロー エクスポータを作成すると、フローのエクスポート パラメータを定義できます。これは、フローのエクスポート パラメータを設定するためのオプションの手順です。

（注） AVC 統計情報がコントローラに表示されるようにするには、次のコマンドを使用してローカルのフロー エクスポータを設定する必要があります。

- **flow exporter** *my_local*
- **destination local wlc**

また、フローモニタでは、統計情報をコントローラに表示するためにこのローカルのエクスポータを使用する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**flow exporter** *flow-export-name* 例： `Device(config)# flow exporter export-test`	フロー モニタを作成します。
ステップ 2	**description** *string* 例： `Device(config-flow-exporter)# description IPv4flow`	最大 63 文字で、フロー レコードの説明を示します。
ステップ 3	**destination** {*hostname/ipv4address [vrf] | hostname/ipv6address [vrf] |local {wlc}*} 例： `Device(config-flow-exporter) # destination 10.99.1.4`	エクスポータでデータを送信する宛先のシステムまたはローカル WLC のホスト名または IPv4 アドレスを指定します。
ステップ 4	**transport udp** *port-value* 例： `Device(config-flow-exporter) # transport udp 2`	UDP プロトコルのポートの値を設定します。
ステップ 5	**option application-table timeout** *seconds* 例： `Device(config-flow-exporter)# option application-table timeout 500`	（任意）アプリケーション テーブルのタイムアウト オプションを秒単位で指定します。有効な範囲は 1 ～ 86400 です。
ステップ 6	**option usermac-table timeout** *seconds* 例： `Device(config-flow-exporter)# option usermac-table timeout 1000`	（任意）ワイヤレスのユーザ MAC からユーザ名へのテーブルのオプションを秒単位で指定します。有効な範囲は 1 ～ 86400 です。

	コマンドまたはアクション	目的
ステップ 7	**show flow exporter** 例： `Device # show flow exporter`	（任意）設定を確認します。

AVC の WLAN の設定

AVC の WLAN を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *wlan-avc* **1** *ssid-avc* 例： `Device(config)# wlan wlan1 1 ssid1`	WLAN を設定します。
ステップ 2	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をシャット ダウンします。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化を無効にします。

ポリシー タグの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless tag policy** *policy-tag-name* 例： `Device(config-policy-tag)# wireless tag policy rr-xyz-policy-tag`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**end** 例： `Device(config-policy-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

WLAN インターフェイスへのポリシー プロファイルのアタッチ（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。

ステップ 2 [Manage Tags] ページで、[Policy] タブをクリックします。

ステップ 3 [Add] をクリックして、[Add Policy Tag] ウィンドウを表示します。

ステップ 4 ポリシー タグの名前と説明を入力します。

ステップ 5 [Add] をクリックして、WLAN とポリシーをマッピングします。

ステップ 6 適切なポリシープロファイルを使用してマッピングするWLANプロファイルを選択し、チェック アイコンをクリックします。

ステップ 7 [Save & Apply to Device] をクリックします。

WLAN インターフェイスへのポリシー プロファイルのアタッチ（CLI）

始める前に

- 異なるポリシー タグ間で同じ WLAN に異なる AVC ポリシー プロファイルを適用しないでください。

  次に、正しくない設定例を示します。

```
wireless profile policy avc_pol1
   ipv4 flow monitor fm-avc1 input
   ipv4 flow monitor fm-avc1 output
   no shutdown
```

```
wireless profile policy avc_pol2
 ipv4 flow monitor fm-avc2 input
 ipv4 flow monitor fm-avc2 output
 no shutdown
wireless tag policy avc-tag1
 wlan wlan1 policy avc_pol1
wireless tag policy avc-tag2
 wlan wlan1 policy avc_pol2
```

この例は前述の制限に反しています。つまり、WLAN *wlan1* を 2 つのポリシー プロファイル（*avc_pol1* と *avc_pol2*）にマッピングしています。したがって、WLAN *wlan1* をすべての場所で *avc_pol1* または *avc_pol2* にマッピングする必要があるため、この設定は正しくありません。

- 同じ WLAN でのポリシー プロファイルの競合はサポートされていません。たとえば、ポリシー プロファイルを（AVC の有無にかかわらず）異なるポリシー タグ内の同じ WLAN に適用する場合などです。

  次に、正しくない設定例を示します。

```
wireless profile policy avc_pol1
   no shutdown
  wireless profile policy avc_pol2
   ipv4 flow monitor fm-avc2 input
   ipv4 flow monitor fm-avc2 output
   no shutdown
  wireless tag policy avc-tag1
   wlan wlan1 policy avc_pol1
  wireless tag policy avc-tag2
   wlan wlan1 policy avc_pol2
```

この例では、AVC の有無にかかわらずポリシープロファイルを異なるタグ内の同じ WLAN に適用しています。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless tag policy** *avc-tag* 例： `Device(config)# wireless tag policy avc-tag`	ポリシー タグを作成します。
ステップ 2	**wlan** *wlan-avc* **policy** *avc-policy* 例： `Device(config-policy-tag)# wlan wlan_avc policy avc_pol`	WLAN プロファイルにポリシー プロファイルをアタッチします。

次のタスク

- 設定が完了したら、WLAN で **no shutdown** コマンドを実行します。

- WLAN がすでに **no shutdown** モードになっている場合は、 **shutdown** コマンドを実行し、その後に **no shutdown** コマンドを実行します。

AP へのポリシー プロファイルのアタッチ

手順

	コマンドまたはアクション	目的
ステップ 1	**ap** *ap-ether-mac* 例： `Device(config)# ap 34a8.2ec7.4cf0`	AP 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	**policy-tag** *policy-tag* 例： `Device(config)# policy-tag avc-tag`	アクセス ポイントにアタッチするポリシー タグを指定します。

AVC の設定の確認

手順

	コマンドまたはアクション	目的
ステップ 1	**show avc wlan** *wlan-name* **top** *num-of-applications* **applications {aggregate | downstream | upstream}** 例： `Device# show avc wlan wlan_avc top 2 applications aggregate`	これらのアプリケーションを使用している上位のアプリケーションとユーザに関する情報を表示します。 （注） ワイヤレス クライアントが WLAN に関連付けられていて、トラフィックが生成されていることを確認し、その後 90 秒間待ってからコマンドを実行してください（統計情報を確実に参照できるようにするため）。
ステップ 2	**show avc client** *mac* **top** *num-of-applications* **applications {aggregate | downstream | upstream}**	上位の数のアプリケーションに関する情報を表示します。

	コマンドまたはアクション	目的
	例： `Device# show avc client 9.3.4 top 3 applications aggregate`	（注） ワイヤレス クライアントが WLAN に関連付けられていて、トラフィックが生成されていることを確認し、その後 90 秒間待ってからコマンドを実行してください（統計情報を確実に参照できるようにするため）。
ステップ 3	**show avc wlan** *wlan-name* **application** *app-name* **top** *num-of-clients* **aggregate** 例： `Device# show avc wlan wlan_avc application app top 4 aggregate`	これらのアプリケーションを使用している上位のアプリケーションとユーザに関する情報を表示します。
ステップ 4	**show ap summary** 例： `Device# show ap summary`	コントローラに接続しているすべてのアクセス ポイントのサマリーを表示します。
ステップ 5	**show ap tag summary** 例： `Device# show ap tag summary`	ポリシー タグを持つすべてのアクセス ポイントのサマリーを表示します。

AVC のデフォルト DSCP

AVC プロファイル用のデフォルト DSCP の設定

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、ポリシーで指定できるフィルタの数は 最大32 個のみです。フィルタで指定されていないパケットを分類する手段がありませんでしたが、ポリシーでこれらのパケットにマークを付けられるようになりました。

マーク付けの操作は、クラスマップの作成時やポリシーマップの作成時にトラフィックに適用できます。

クラス マップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**Configure Terminal** 例： `Device# 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	**class** *class-map-name*] 例： `Device(config-pmap)# class-map avc-class`	クラス マップを作成します。
ステップ 3	**match protocol** { *application-name* | **attribute category** *category-name* | **attribute sub-category** *sub-category-name* | **attribute application-group** *application group-name* 例： `Device(config)# class-map avc-class` `Device(config-cmap)# match protocol avc-media` `Device(config)# class-map class-avc-category` `Device(config-cmap)# match protocol attribute category avc-media` `Device# class-map class-avc-sub-category` `Device(config-cmap)# match protocol attribute sub-category avc-media` `Device# class-map avcS-webex-application-group` `Device(config-cmap)# match protocol attribute application-group webex-media`	アプリケーション名、カテゴリ名、サブカテゴリの名前、またはアプリケーション グループに一致するものを指定します。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー マップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**Configure Terminal** 例： `Device# 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	**policy-map** *policy-map-name* 例： `Device(config)#policy-map avc-policy`	ポリシーマップ名を入力することによってポリシー マップを作成し、ポリシー マップ コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップは定義されていません。 ポリシー マップのデフォルトの動作では、パケットが IP パケットの場合は DSCP が 0 に設定され、パケットがタグ付きの場合は CoS が 0 に設定されます。ポリシングは実行されません。 （注） 既存のポリシー マップを削除するには、no policy-map policy-map-name グローバル コンフィギュレーション コマンドを使用します。
ステップ 3	**class** [*class-map-name* | **class-default**] 例： `Device(config-pmap)# class-map avc-class`	トラフィックの分類を定義し、ポリシー マップ クラス コンフィギュレーション モードを開始します。 デフォルトでは、ポリシー マップおよびクラスマップは定義されていません。 すでに class-map 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トラフィック クラスが定義されている場合は、このコマンドで class-map-name にその名前を指定します。 class-default トラフィック クラスは定義済みで、どのポリシーにも追加できます。このトラフィック クラスは、常にポリシーマップの最後に配置されます。暗黙の match any が class-default クラス

	コマンドまたはアクション	目的
		に含まれている場合、他のトラフィック クラスと一致しないパケットはすべて class-default と一致します。 （注） 既存のクラス マップを削除するには、no class class-map-name ポリシー マップ コンフィギュレーション コマンドを使用します。
ステップ 4	**set dscp** *new-dscp* 例： `Device(config-pmap-c)# set dscp 45`	パケットに新しい値を設定することによって、IP トラフィックを分類します。**dscp new-dscp** には、分類されたトラフィックに割り当てる新しい DSCP 値を入力します。指定できる範囲は 0 ～ 63 です。
ステップ 5	**class** *class-default*	ポリシーを設定または変更できるようデフォルト クラスを指定します。
ステップ 6	**set dscp default**	デフォルトの DSCP を設定します。
ステップ 7	**end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AVC ベースの選択的リアンカー

AVC ベースの選択的リアンカー機能は、クライアントが一方のコントローラから他方のコントローラにローミングするときにクライアントをリアンカーすることを目的としています。クライアントをリアンカーすることで、Cisco WLC の新しいクライアントで使用可能な IP アドレスが枯渇するのを防ぎます。クライアントをリアンカーするか保留するかを決めるために、AVC プロファイル ベースの統計情報が使用されます。この機能は、AVC ルールで定義されている音声またはビデオアプリケーションをクライアントが積極的に実行している場合に便利です。

リアンカーのプロセスでは、アンカーされたクライアントの認証解除も伴います。クライアントは、WLC 間をローミングしている時に、AVC ルールにリストされているアプリケーションのトラフィックを送信していない場合に、認証解除されます。

AVC ベースの選択的リアンカーの制限事項

- この機能はローカル モードでのみサポートされています。FlexConnect モードおよびファブリック モードはサポートされていません。
- この機能は、ゲスト トンネリングおよびエクスポート アンカーのシナリオではサポートされていません。
- 古い IP アドレスは、IP アドレスのリース期間が終了するまで、リアンカー後も解放されません。

フロー エクスポータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**flow exporter** *name* 例： `Device(config)# flow exporter avc-reanchor`	フロー エクスポータを作成し、フロー エクスポータ コンフィギュレーション モードを開始します。 （注） このコマンドを使用して既存のフロー エクスポータを変更することもできます。
ステップ 3	**destination local wlc** 例： `Device(config-flow-exporter)# destination local wlc`	エクスポータをローカルとして設定します。

フロー モニタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**flow monitor** *monitor-name* 例： `Device(config)# flow monitor fm_avc`	フローモニタを作成し、Flexible NetFlow フロー モニタ コンフィギュレーション モードを開始します。 （注） このコマンドを使用して既存のフロー モニタを変更することもできます。
ステップ 3	**exporter** *exporter-name* 例： `Device(config-flow-monitor)# exporter avc-reanchor`	フロー エクスポータの名前を指定します。
ステップ 4	**record wireless avc basic** 例： `Device(config-flow-monitor)# record wireless avc basic`	キャッシュの定義に使用するフロー レコードを指定します。
ステップ 5	**cache timeout active** *value* 例： `Device(config-flow-monitor)# cache timeout active 60`	アクティブ フロー タイムアウトを秒単位で設定します。
ステップ 6	**cache timeout inactive** *value* 例： `Device(config-flow-monitor)# cache timeout inactive 60`	非アクティブ フロー タイムアウトを秒単位で設定します。

AVC リアンカー プロファイルの設定

始める前に

- AVC-Reanchor-Class クラス マップを使用していることを確認します。それ以外のクラス マップ名はすべて、選択的リアンカーでは無視されます。
- システムの起動中に、AVC-Reanchor-Class クラス マップが存在するかどうかがチェックされます。見つからなかった場合は、デフォルトのプロトコル（jabber-video、wifi-calling など）が作成されます。AVC-Reanchor-Class クラス マップが見つかった場合、設定の変更は行われず、スタートアップ コンフィギュレーションに保存されているプロトコルの更新はリブート後も維持されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**class-map** *cmap-name* 例： `Device(config)# class-map AVC-Reanchor-Class`	クラス マップを設定します。
ステップ 3	**match any** 例： `Device(config-cmap)# match any`	デバイスを通過するいずれかのプロトコルと照合するようにデバイスに指示します。
ステップ 4	**match protocol jabber-audio** 例： `Device(config-cmap)# match protocol jabber-audio`	アプリケーション名との一致を指定します。 必要に応じて、後でクラスマップ設定を編集し、jabber-video や wifi-calling などのプロトコルを追加または削除することができます。

ワイヤレス WLAN プロファイル ポリシーの設定

WLAN プロファイル ポリシーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。

	コマンドまたはアクション	目的
ステップ 4	**ipv4 flow monitor** *monitor-name***input** 例： `Device(config-wireless-policy)# ipv4 flow monitor fm_avc input`	入力フローモニタの名前を指定します。
ステップ 5	**ipv4 flow monitor** *monitor-name* **output** 例： `Device(config-wireless-policy)# ipv4 flow monitor fm_avc output`	出力フローモニタの名前を指定します。
ステップ 6	**reanchor class** *class-name* 例： `Device(config-wireless-policy)# reanchor class AVC-Reanchor-Class`	選択的リアンカー機能のプロトコルを使用してクラス マップを設定します。

AVC リアンカーの確認

AVC リアンカーの設定を確認するには、次のコマンドを使用します。

```
Device# show wireless profile policy detailed avc_reanchor_policy

Policy Profile Name           : avc_reanchor_policy
Description                   :
Status                        : ENABLED
VLAN                          : 1
Wireless management interface VLAN        : 34
!
.
.
.
AVC VISIBILITY                : Enabled
Flow Monitor IPv4
  Flow Monitor Ingress Name   : fm_avc
  Flow Monitor Egress Name    : fm_avc
Flow Monitor IPv6
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
NBAR Protocol Discovery       : Disabled
Reanchoring                   : Enabled
Classmap name for Reanchoring
  Reanchoring Classmap Name   : AVC-Reanchor-Class
!
.
.
.
  ------------------------------------------------------


Device# show platform software trace counter tag wstatsd chassis active R0 avc-stats
debug

Counter Name Thread ID Counter Value
-----------------------------------------------------------------------------
```

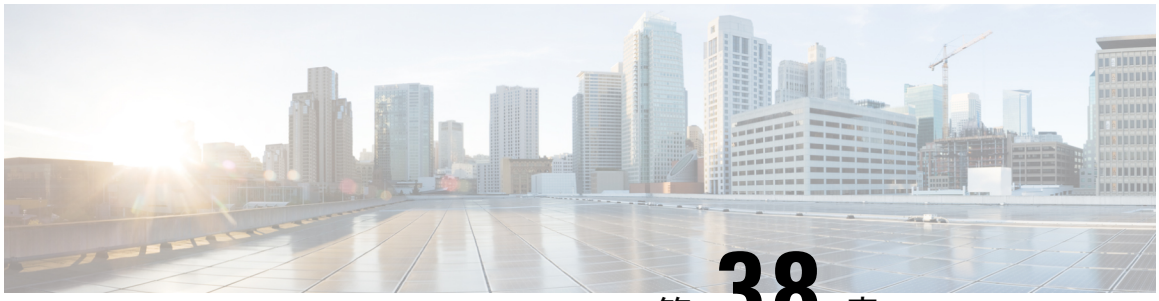
```
Reanch_deassociated_clients 28340 1
Reanch_tracked_clients 28340 4
Reanch_deleted_clients 28340 3
```

```
Device# show platform software trace counter tag wncd chassis active R0 avc-afc debug

Counter Name Thread ID Counter Value
-----------------------------------------------------------------------------
Reanch_co_ignored_clients 30063 1
Reanch_co_anchored_clients 30063 5
Reanch_co_deauthed_clients 30063 4
```

```
Device# show platform software wlavc status wncd

Event history of WNCD DB:

AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.630342 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822780 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822672 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172073 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738367 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738261 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.162689 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757643 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757542 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.468749 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18857 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18717 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164304 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163877 2 :READY 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593257 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:18.593152 1 :INIT 24:CREATE_FSM 0 0

AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.664772 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822499 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822222 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.207605 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738105 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.737997 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164225 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757266 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757181 2 :READY 2 :FSM_AFM_UNBIND 0 0
```

```
06/12/2018 16:44:04.472778 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.15413 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.15263 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164254 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163209 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163189 1 :INIT 24:CREATE_FSM 0 0

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.630764 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:28.822621 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:28.822574 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:15.172357 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:45:12.738212 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:12.738167 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:45:01.164048 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:55.757403 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:55.757361 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:04.472561 3 :ZOMBIE 1 :FSM_AFM_BIND 0 2
06/12/2018 16:44:02.18660 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:44:02.18588 2 :READY 2 :FSM_AFM_UNBIND 0 0
06/12/2018 16:38:20.164293 2 :READY 3 :FSM_AFM_SWEEP 0 2
06/12/2018 16:35:20.163799 1 :INIT 1 :FSM_AFM_BIND 0 2
06/12/2018 16:35:20.163773 1 :INIT 24:CREATE_FSM 0 0


Device# show platform software wlavc status wncmgrd

Event history of WNCMgr DB:

AVC key: [1,wlan_avc,N/A,Reanc,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Reanchoring
Flow-mon-name : N/A
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------- ------------------- -------------------------- ---- ----
06/12/2018 16:45:30.629278 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629223 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629179 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510867 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510411 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510371 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886377 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
!

AVC key: [1,wlan_avc,fm_avc,v4-In,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Ingress
```

```
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------- ------------------ ------------------------- ---- ----
06/12/2018 16:45:30.664032 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.663958 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.663921 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.511151 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510624 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510608 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.810867 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807239 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807205 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806734 4 :READY 3 :FSM_WLAN_DOWN 0 0
!

AVC key: [1,wlan_avc,fm_avc,v4-Ou,default-policy-tag]
Current state : READY
Wlan-id : 1
Wlan-name : wlan_avc
Feature type : Flow monitor IPv4 Egress
Flow-mon-name : fm_avc
Policy-tag : default-policy-tag
Switching Mode : CENTRAL
Policy-profile : AVC_POL_PYATS

Timestamp FSM State Event RC Ctx
------------------------- ------------------ ------------------------- ---- ----
06/12/2018 16:45:30.629414 3 :WLAN_READY 24:BIND_WNCD 0 0
06/12/2018 16:45:30.629392 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.629380 3 :WLAN_READY 4 :FSM_BIND_ACK 0 0
06/12/2018 16:45:30.510954 2 :PLUMB_READY 22:BIND_IOSD 0 0
06/12/2018 16:45:30.510572 2 :PLUMB_READY 2 :FSM_WLAN_UP 0 0
06/12/2018 16:45:30.510532 2 :PLUMB_READY 1 :FSM_WLAN_FM_PLUMB 0 0
06/12/2018 16:45:28.886293 2 :PLUMB_READY 20:UNBIND_ACK_IOSD 0 0
06/12/2018 16:45:28.807844 4 :READY 25:UNBIND_WNCD 0 0
06/12/2018 16:45:28.807795 4 :READY 23:UNBIND_IOSD 0 0
06/12/2018 16:45:28.806990 4 :READY 3 :FSM_WLAN_DOWN 0 0
!
```



第 38 章

Cisco Hyperlocation

Cisco Hyperlocation について

Cisco Hyperlocation は、ワイヤレス クライアントの場所を追跡できる超高精度のロケーション ソリューションです。このソリューションを可能にしているのは、Cisco Aironet 3600、3700、および 4800 シリーズ アクセス ポイントに搭載されている Cisco Hyperlocation 無線モジュールです。Cisco Hyperlocation モジュールと Wi-Fi および Bluetooth Low Energy（BLE）技術との組み合わせにより、ビーコン、インベントリおよび個人のモバイルデバイスの位置を正確に特定できます。

HyperLocation はファブリック モードでもサポートされています。特に、ワイヤレス コントローラがスイッチ上で実行されている場合、コントローラは AP のプロビジョニングに必要な手順を実行します。これにより、AP はファブリック インフラストラクチャを利用してファブリック ネットワークを通過できる HyperLocation VxLAN パケットを生成し、宛先の CMX に正しく配信できるようになります。

Hyperlocation の VxLAN パケットは、SGT 0 でマークされた特殊なパケットであり、AP の L3VNID を使用します。詳細については、SDA のマニュアルを参照してください。

Cisco Hyperlocation の無線モジュールには、以下の機能があります。

- 以下の拡張性を備えた WSM または WSM2 無線モジュール機能：
  - 802.11ac
  - Wi-Fi 送信

- 20 MHz、40 MHz、および 80 MHz のチャネル帯域幅

- 拡張ロケーション機能：
  - 低遅延ロケーション最適化チャネルのスキャン
  - 32 アンテナ到達角度（AoA）。WSM2 モジュールでのみ使用できます。

（注） WSM2 モジュール（WSM モジュールとアンテナ アドオンを含む）を使用すると、ワイヤレス クライアントの位置を追跡する精度を 1 m にまで高めることができます。

Cisco Hyperlocation は Cisco Connected Mobile Experiences（CMX）と連携して機能します。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの Cisco Hyperlocation 機能と CMX デバイスを組み合わせることで、ロケーション精度が向上し、ユーザに提供するコンテンツを絞り込むことができます。Cisco CleanAir の周波数スキャンとともに CMX を使用する場合は、失敗したビーコン、失われたビーコン、また不正なビーコンでさえ見つけることが簡単です。

内蔵型 BLE 無線を備えた Cisco Hyperlocation 無線モジュールでは、最大 5 台の Bluetooth Low Energy（BLE）トランスミッタを使用して BLE ブロードキャスト メッセージを伝送できます。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを使用して、ビーコンのインターバル、汎用一意識別子（UUID）、送信電力などの伝送パラメータを、すべてのアクセスポイントに対してビーコン別にグローバルに設定します。また、コントローラでは各アクセス ポイントのメジャー、マイナー、および送信電力の値を設定できるため、ビーコンの精度が高まります。

（注） BLE を機能させるには、コントローラと CMX で Cisco Hyperlocation 機能が有効になっている必要があり、CMX が接続されている必要があります。

Cisco Hyperlocation 無線モジュールが存在しない場合でも、HyperLocation は「HyperLocation ローカル モード」と呼ばれるモードで機能します。これにより、5 ～ 7 メートルの範囲内で精度がわずかに低下した位置精度が保証されます。このモードは CPU サイクルの借用によって実現され、次の AP に適用されます。

- Cisco Aironet 700 シリーズ AP
- Cisco Aironet 1700 シリーズ AP
- Cisco Aironet 2600 シリーズ AP
- Cisco Aironet 2700 シリーズ AP
- Cisco Aironet 3600 シリーズ AP
- Cisco Aironet 3700 シリーズ AP

コントローラを使用し、AP のプロファイルに基づいて AP の Cisco Hyperlocation を設定できます。

ネットワーク タイム プロトコル サーバ

Cisco Hyperlocation では、時間に関して AP を同期させる必要があります。これを行うために、コントローラからネットワーク タイム プロトコル（NTP）情報が AP に送信されます。NTP 情報を受信した AP は、NTP サーバを使用して自身のクロックを同期させます。そのため、AP から NTP サーバに接続できることが必要になります。

AP は地理的に分散する場合があります。したがって、AP ごとに異なる NTP サーバを提供する必要があります。これを実現するため、NTP サーバ情報を AP プロファイルごとに設定できるようになっています。NTP 情報が AP プロファイルで設定されていない場合、コントローラは、自身の設定で定義されているグローバル NTP ピアのいずれかを使用します。または、コントローラが NTP サーバとして機能している場合に使用する NTP サーバとして、管理 IP アドレスが送信されます。NTP サーバが使用できない場合、Cisco Hyperlocation は無効になります。

Bluetooth Low Energy（BLE）の設定

BLE の設定は、AP プロファイルごとと AP ごとの 2 つの部分に分かれています。BLE 機能は、AP プロファイルから部分的に設定でき（デフォルトでは、AP プロファイルの BLE 設定が適用されます）、AP ごとに部分的に設定できます（一部またはすべての属性が適用されます）。

表 *8 : BLE* の設定の詳細

属性	AP プロファイルごとの BLE の設定	AP ごとの BLE の設定
AP ごとの精度を持つ属性（すべてのビーコンに対してグローバル）	• インターバル • アドバタイズされる送信電力	• インターバル • アドバタイズされる送信電力
AP ごとおよび 0 ビーコンごとの精度を持つ属性	• 送信電力 • UUID • Status（ステータス）	• 送信電力 • UUID • Status（ステータス） • Major（やや重大） • Minor（比較的重大でない）

（注） *default-ap-profile* BLE 設定はデフォルトの BLE 設定と見なすことができます。これは、他のプロファイルが削除された場合にすべての AP が *default-ap-profile* AP プロファイルに join するためです。

Cisco Hyperlocation の詳細については、以下の文書を参照してください。

- 『Cisco Hyperlocation Solution』
- 『Cisco CMX Configuration Guide to enable Cisco Hyperlocation』
- 『Cisco CMX Release Notes』

Cisco Hyperlocation の制約事項

- 現在のところ Cisco Hyperlocation は IPv4 ソリューションであるため、ワイヤレス管理、CMX、および NTP サーバのアドレスは IPv4 形式のみである必要があります。
- HyperLocation が有効状態になっている間は、検出、トリガー、およびリセットのしきい値を変更することはできません。
- リセットしきい値の変更が許される値の範囲は、0 ～ 現在のしきい値よりも 1 少ない値までです。たとえば、現在のしきい値のリセット値が 10 の場合、リセットしきい値の変更は 0 ～ 9 の範囲の値に対して許されます。
- 非ファブリック展開の Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで Cisco Hyperlocation を使用している場合、 SVI インターフェイス（VLAN）を介して CMX に到達できる必要があります。L3 ポートを介して CMX に到達できる展開では、エラーが発生します。
- ファブリック展開では、ワイヤレス管理インターフェイス（通常はループバック インターフェイス）をファブリック内に配置することはできません。
- 非ファブリック展開で、ワイヤレス管理インターフェイスをループバック インターフェイスに設定することはできません。

Cisco Hyperlocation の設定（GUI）

Cisco Hyperlocation は、ワイヤレス クライアントの場所を 1 メートルの精度で追跡できるロケーション ソリューションです。このオプションを選択すると、NTP サーバを除く画面内の他のすべてのフィールドが無効になります。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] を選択します。

ステップ 2 [Add] ボタンをクリックします。[Add AP Join Profile] ダイアログボックスが表示されます。

ステップ 3 [AP] タブをクリックし、[Hyperlocation] タブをクリックします。

ステップ 4 [Enable Hyperlocation] チェックボックスをオンにします。

ステップ 5 RSSI が低いパケットを除外するには、[Detection Threshold (dBm)] フィールドに値を入力します。値は -100 ～ -50 dBm の範囲で入力する必要があります。

ステップ 6 クライアントに BAR を送信するまでのスキャン サイクル数を設定するには、[Trigger Threshold (cycles)] フィールドに値を入力します。0 ～ 99 の値を入力する必要があります。

ステップ 7 トリガー後のスキャン サイクルの値をリセットするには、[Reset Threshold is required] フィールドに値を入力します。0 ～ 99 の値を入力する必要があります。

ステップ 8 [Save & Apply to Device] ボタンをクリックします。

Cisco Hyperlocation の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *profile-name* 例： `Device(config)# ap profile profile-name`	指定した AP プロファイル名に関連付けられているすべての AP について設定を有効にします。
ステップ 3	**[no] hyperlocation** 例： `Device(config-ap-profile)# [no] hyperlocation`	この AP プロファイルに関連付けられているすべてのサポート対象の AP で、HyperLocation を有効または無効にします。
ステップ 4	**[no] hyperlocation threshold detection** *value-in-dBm* 例： `Device(config-ap-profile)# [no] hyperlocation threshold detection -100`	低い RSSI を持つパケットを除外するためのしきい値を設定します。このコマンドの **no** 形式を使用すると、しきい値がデフォルト値にリセットされます。有効な範囲は -100 ～ -50 です。

	コマンドまたはアクション	目的
ステップ 5	**[no] hyperlocation threshold reset** *value-btwn-0-99* 例： `Device(config-ap-profile)# [no] hyperlocation threshold reset 8`	トリガー後のスキャン サイクルの値をリセットします。このコマンドの **no** 形式を使用すると、しきい値がデフォルト値にリセットされます。
ステップ 6	**[no] hyperlocation threshold trigger** *value-btwn-1-100* 例： `Device(config-ap-profile)# [no] hyperlocation threshold trigger 10`	Block Acknowledgment Request（BAR）をクライアントに送信する前のスキャン サイクルの数を設定します。このコマンドの **no** 形式を使用すると、しきい値がデフォルト値にリセットされます。
ステップ 7	**[no] ntp ip** *ipv4-address-of-ntp-server* 例： `Device(config-ap-profile)# [no] ntp ip 9.0.0.4`	アクセス ポイントによって直接到達可能な、NTP サーバの IPv4 アドレスを設定します。このコマンドの **no** 形式を使用すると NTP サーバが削除されます。

Cisco Hyperlocation の確認

すべての AP プロファイルについて HyperLocation のステータスとパラメータの値を表示するには、次のコマンドを使用します。

```
Device# show ap hyperlocation summary

Profile Name: custom-profile

Hyperlocation operational status: Down
Reason: Hyperlocation is administratively disabled
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Disabled
Hyperlocation detection threshold (dBm): -100
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8


Profile Name: default-ap-profile

Hyperlocation operational status: Up
Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 22
Hyperlocation reset threshold: 8
```

全体の設定値と AP ごとの設定値の両方と動作ステータスを表示する場合です。HyperLocation のステータスとパラメータに表示される値には、すべての AP プロファイルの値が反映されます。次のコマンドを使用します。

```
Device# show ap hyperlocation detail

Profile Name: house

Hyperlocation operational status: Up
 Reason: N/A
Hyperlocation NTP server: 1.0.1.0
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7

AP Name                  Radio MAC         Method      CMX IP             AP Profile
-------------------------------------------------------------------------------------------------


Profile Name: house24

Hyperlocation operational status: Up
 Reason: NTP server is not properly configured
Hyperlocation NTP server: 0.0.0.0
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7

AP Name                  Radio MAC         Method      CMX IP             AP Profile
-------------------------------------------------------------------------------------------------
APe865.49d9.bfe0         e865.49ea.a4b0    WSM2+Ant    10.0.0.1         house24

APa89d.21b9.69d0         a89d.21b9.69d0    Local       10.0.0.1         house24

APe4aa.5d3f.d750         e4aa.5d5f.3630    WSM         10.0.0.1         house24



Profile Name: default-ap-profile

Hyperlocation operational status: Up
 Reason: CMX is not subscribed to AP Monitor and RSSI services, or NMSP connection is
down
Hyperlocation NTP server: 1.3.3.1
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7

AP Name                  Radio MAC         Method      CMX IP             AP Profile
-------------------------------------------------------------------------------------------------
T3-1                     0a0b.0c00.0200    WSM2+Ant    N/A         default-ap-profile
T3-2                     0a0b.0c00.0300    Local       N/A         default-ap-profile
T3-3                     0a0b.0c00.0400    WSM         N/A         default-ap-profile
```

特定のプロファイルについて全体の（プロファイル固有の）設定値と動作ステータスを表示するには、次のコマンドを使用します。

```
Device# show ap profile profile-name hyperlocation summary

Profile Name: profile-name
Hyperlocation operational status: Up
   Reason: N/A
```

```
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -100
Hyperlocation trigger threshold: 10
Hyperlocation reset threshold: 8
```

特定のプロファイルについて全体（プロファイル固有）と AP ごとの両方の設定値と動作ステータスを表示するには、次のコマンドを使用します。

リストされる AP は、指定した join プロファイルに属する AP のみです。

```
Device# show ap profile profile-name hyperlocation detail
```

```
Profile Name: profile-name
Hyperlocation operational status: Up
 Reason: N/A
Hyperlocation NTP server: 209.165.200.224
Hyperlocation admin status: Enabled
Hyperlocation detection threshold (dBm): -90
Hyperlocation trigger threshold: 8
Hyperlocation reset threshold: 7

AP Name                  Radio MAC         Method      CMX IP
-----------------------------------------------------------------
APf07f.0635.2d40         f07f.0635.2d40    WSM2+Ant    1.2.3.4
APf07f.0635.2d41         f07f.0635.2d41    Local       1.2.3.4
APf07f.0635.2d42         f07f.0635.2d42    WSM         1.2.3.4
```

AP プロファイルの設定値を表示する場合です。HyperLocation 設定のセクションがあります。このセクションには、PAK RSSI などの HyperLocation しきい値パラメータの値が表示されます。次のコマンドを使用します。

```
Device# show ap profile profile-name detailed
```

```
Hyperlocation :
  Admin State             : ENABLED
  PAK RSSI Threshold Detection: -100
  PAK RSSI Threshold Trigger  : 10
  PAK RSSI Threshold Reset    : 8
...
```

どの CMX が正しく join されていて HyperLocation によって使用されているかを確認するには、次のコマンドを使用します。

```
Device# show ap hyperlocation cmx summary

Hyperlocation-enabled CMXs

IP         Port    Dest MAC       Egress src MAC    Egress VLAN   Ingress src MAC  Join
time
-------------------------------------------------------------------------------------------------
1.2.3.4  2003    aaaa.bbbb.cccc    aabb.ccdd.eeff      2       0000.0001.0001   12/14/18
 09:27:14
```

Cisco Hyperlocation のクライアントの統計情報を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary

Client Type Abbreviations:
  RG - REGULAR BL - BLE
  HL - HALO    LI - LWFL INT
Auth State Abbreviations:
  UK - UNKNOWN IP - LEARN IP IV - INVALID
  L3 - L3 AUTH RN - RUN
Mobility State Abbreviations:
  UK - UNKNOWN IN - INIT
  LC - LOCAL   AN - ANCHOR
  FR - FOREIGN MT - MTE
  IV - INVALID
EoGRE Abbreviations:
  N - NON EOGRE Y - EOGRE
 CPP IF_H     DPIDX      MAC Address    VLAN  CT  MCVL  AS  MS  E        WLAN
          POA
-----------------------------------------------------------------------------------------------

   0X32     0XF0000001  0000.0001.0001   9    HL   0    RN  LC  N
         NULL
```

統計情報を開始するには、インターフェイス ハンドルの値を使用します。

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
cpp-if-handle 0x32 statistics start
```

記録されたフローを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
cpp-if-handle 0X32 statistics

                                                          Pkts                Bytes
Rx                                                         26                  3628
```

統計情報のキャプチャを停止するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
cpp-if-handle 0x32 statistics stop
```

AP グループを持つ CMX がサポートされている場合に、AP が CMX によって要求されたかどうかを確認するには、次のコマンドを使用します。

```
Device# show nmsp subscription group summary

CMX IP address: 10.0.0.1
  Groups subscribed by this CMX server:
  Group name: CMX_10.0.0.1

Device# show nmsp subscription group detail ap-list CMX_10.0.0.1 10.0.0.1

CMX IP address: 10.0.0.1
CMX Group name: CMX_10.0.0.1
CMX Group AP MACs:
: aa:bb:cc:dd:ee:01 aa:bb:cc:dd:ee:02 aa:bb:cc:dd:ee:03 aa:bb:cc:dd:ee:03
```

APのHyperLocationBLEビーコンパラメータの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] を選択します。 >

ステップ 2 [Add] をクリックします。[Add AP Join Profile] ダイアログボックスが表示されます。

ステップ 3 [AP] タブを選択し、[BLE] をクリックします。

ステップ 4 [Beacon Interval (Hz)] フィールドに値を入力します。

ステップ 5 [Advertised Attenuation Level (dBm)] フィールドに値を入力します。

ステップ 6 各 ID に対してチェックボックスをオンにし、必要に応じて [Reset] ボタンをクリックします。

ステップ 7 （任意）ID をクリックして、次のフィールドの値を編集します。

- **Status**
- **Tx Power (dBm)**
- **UUID**

[Save] をクリックします。

ステップ 8 [Save & Apply to Device] ボタンをクリックします。

HyperLocation BLE ビーコン パラメータの設定（CLI）

始める前に

HyperLocation BLE を有効にするには、CMX が HyperLocation に対して完全に join されていて有効になっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap profile** *profile-name* 例： `Device(config)# ap profile profile-name`	指定したAPプロファイル名に関連付けられているすべてのAPについて設定を有効にします。

	コマンドまたはアクション	目的
ステップ 2	**hyperlocation ble-beacon** *beacon-id* 例： `Device(config)# hyperlocation ble-beacon 3`	BLE ビーコン パラメータを指定して、BLE コンフィギュレーション モードを開始します。
ステップ 3	**default** {**enabled** | **txpwr** | **uuid** } | **enabled** | **exit** | **no** {**enabled** | **txpwr** | **uuid** } | **txpwr** *att-value* | **uuid** *uuid-value* 例： `Device(config-halo-ble)# enabled`	指定したビーコン ID の BLE を有効にします。
ステップ 4	**hyperlocation ble-beacon interval** *value-in-hertz* 例： `Device(config-ap-profile)# hyperlocation ble-beacon interval 1`	選択したプロファイルについて、BLE ビーコン間隔を 1 Hz に設定します。
ステップ 5	**hyperlocation ble-beacon advpwr** *value-in-dBm* 例： `Device(config-ap-profile)# hyperlocation ble-beacon advpwr 40`	BLE ビーコンのアドバタイズされる減衰レベルを設定します。有効な範囲は -40 ～ -100 dBm です。デフォルト値は -59 dBm です。

HyperLocation BLE ビーコン設定のモニタリング

手順

	コマンドまたはアクション	目的
ステップ 1	**show ap profile** *profile-name* **hyperlocation ble-beacon** 例： `Device# show ap profile ap-profile-name hyperlocation ble-beacon` `BLE Beacon interval (Hz): 1` `BLE Beacon advertised attenuation value (dBm): -59` `ID UUID` `TX Power(dBm) Status` `----------------------------------------` `0 ffffffff-aaaa-aaaa-aaaa-aaaaaaaaaaaa` `0 Enabled` `1 ffffffff-bbbb-bbbb-bbbb-bbbbbbbbbbbb` `0 Enabled` `2 ffffffff-gggg-gggg-gggg-gggggggggggg` `0 Enabled`	設定済み BLE ビーコンのリストを表示します。

	コマンドまたはアクション	目的
	3 ffffffff-dddd-dddd-dddd-dddddddddddd 0 Enabled 4 ffffffff-eeee-eeee-eeee-eeeeeeeeeeee 0 Enabled	

APのHyperLocationBLEビーコンパラメータの設定（CLI）

AP の HyperLocation BLE ビーコン パラメータを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap-name* [**no**] **hyperlocation ble-beacon** *beacon-id* {**enable** | **major** *major-value* | **minor** *minor-value* | **txpwr** *value-in-dBm* | **uuid** *uuid-value* } 例： `Device# ap name test-ap hyperlocation ble-beacon 3 major 65535`	AP および指定したビーコン ID について、Hyperlocation および関連パラメータを設定します。 • **enable**：AP で BLE ビーコンを有効にします。 • **major** *major-value*：BLE ビーコンの major パラメータを設定します。有効な値は 0 ～ 65535 です。デフォルト値は 0 です。 • **minor** *minor-value*：BLE ビーコンの minor パラメータを設定します。有効な値は 0 ～ 65535 です。デフォルト値は 0 です。 • **txpwr** *value-in-dBm*：BLE ビーコン減衰レベルを設定します。有効な値は -52 ～ 0 dBm です。 • **uuid** *uuid-value*：UUID を設定します。
ステップ 2	**ap name** *ap-name* **hyperlocation ble-beacon** {**advpwr** *value-in-dBm* | **global** | **interval** *value-in-hertz*} 例： `Device# ap name test-ap hyperlocation ble-beacon advpwr 90`	AP の Hyperlocation および関連パラメータを設定します。 • **advpwr** *value-in-dBm*：BLE ビーコンのアドバタイズされる減衰レベルを設定します。有効な範囲は -40 ～ -100 dBm です。デフォルト値は -59 dBm です（値はすべて正の整数として入力する必要があります）。

	コマンドまたはアクション	目的
		• **global**: AP 固有の設定を削除し、AP にグローバル設定を適用します。 • **interval** *value-in-hertz*：BLE ビーコン間隔の値をヘルツ単位で設定します。有効な値は 1 ～ 10 です。デフォルト値は 1 です。

AP の HyperLocation BLE ビーコン設定のモニタリング

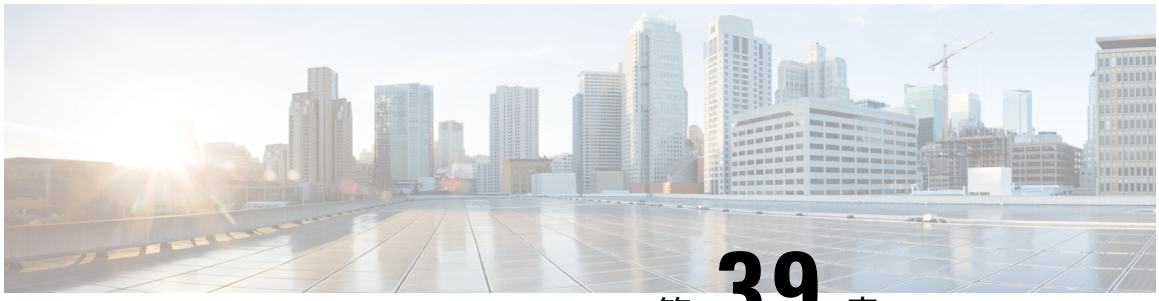
次に、AP の HyperLocation BLE ビーコン設定をモニタする方法の例を示します。

手順

設定した BLE ビーコンのリストを表示するには、**show ap name** *ap-name* **hyperlocation ble-beacon** コマンドを使用します。

例：

```
Device# show ap name test-ap hyperlocation ble-beacon

BLE Beacon interval (Hz): 1
BLE Beacon advertised attenuation value (dBm): -60

ID Status UUID Major Minor TXPower(dBm)
------------------------------------------------------------------------------
0 Enabled 99999999-9999-9999-9999-999999999999 8 0 -0
1 Enabled bbbbbbbb-bbbb-bbbb-bbbb-bbbbbbbbbbbb 8 1 -0
2 Enabled 88888888-8888-8888-8888-888888888888 8 2 -0
3 Enabled dddddddd-dddd-dddd-dddd-dddddddddddd 8 3 -0
4 Enabled eeeeeeee-eeee-eeee-eeee-eeeeeeeeeeee 8 4 -0
```



第 39 章

Cisco Connected Mobile Experiences クラウド

Cisco Connected Mobile Experiences（CMX）は、コネクション型（TLS）トランスポート経由で動作する を使用して、シスコ ワイヤレス コントローラと通信します。このトランスポートではセキュアな双方向接続が提供されます。コントローラと CMX の両方がオンプレミスで、それらの間に直接 IP 接続がある場合に便利です。

Cisco CMX クラウドは、オンプレミス CMX のクラウドによって提供されるバージョンです。Cisco CMX クラウド サービスにアクセスする場合、HTTPS がトランスポート プロトコルとして使用されます。

Cisco CMX クラウド の設定

CMX クラウド を設定するには、次の手順に従います。

始める前に

- **DNS の設定**：NMSP クラウドサービスで使用される完全修飾ドメイン名を解決するには、ステップ 2 に示すように、**ip name-server** *server_address* コンフィギュレーション コマンドを使用して **DNS** を設定します。
- **サード パーティのルート CA のインポート**：コントローラは、接続確立時に CMX から送信される証明書に基づいてピアとホストを確認します。ただし、ルート CA はコントローラに事前にインストールされていません。ステップ 3 に示すように、**crypto pki trustpool import url <url>** コンフィギュレーション コマンドを使用して、シスコが信頼するルート CA のセットを crypto PKI の trustpool にインポートする必要があります。
- この設定の完了に必要な **server url** および **server token** パラメータの設定を有効にするには、Cisco DNA Spaces への登録が成功している必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ip name-server** *namesvr-ip-addr* 例： `Device(config)#ip name-server 10.10.10.205`	NMSP クラウドサービスで使用される FQDN名を解決するようにコントローラの DNS を設定します。
ステップ 3	**crypto pki trustpool import url** *url* 例： `Device(config)#crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`	サードパーティのルート CA をインポートします。コントローラは、インポートされた証明書を使用してピアを確認します。
ステップ 4	**[no] nmsp cloud-services server url** *url* 例： `Device(config)# nmsp cloud-services server url https://cisco.com`	クラウド サービスに使用する URL を設定します。コンフィギュレーションからサーバ URL を削除するには、このコマンドの **no** 形式を使用します。
ステップ 5	**[no] nmsp cloud-services server token** *token* 例： `Device(config)# nmsp cloud-services server token test`	NMSP クラウド サービスの認証トークンを設定します。コンフィギュレーションからサーバ トークンを削除するには、このコマンドの **no** 形式を使用します。
ステップ 6	**[no] nmsp cloud-services http-proxy** *proxy-server port* 例： `Device(config)# nmsp cloud-services http-proxy 10.0.0.1 10`	（任意）NMSP クラウド サービスの HTTP プロキシの詳細を設定します。HTTP プロキシの使用を無効にするには、このコマンドの **no** 形式を使用します。
ステップ 7	**[no] nmsp cloud-services enable** 例： `Device(config)# nmsp cloud-services enable`	NMSP クラウド サービスを有効にします。この機能を無効にするには、このコマンドの **no** 形式を使用します。

Cisco CMX Cloud の設定の確認

CMX Cloud の設定を確認するには、次のコマンドを使用します。

アクティブな NMSP 接続のステータスを表示するには、、次のコマンドを使用します。

```
Device# show nmsp status

MSE IP Address   Tx Echo Resp  Rx Echo Req   Tx Data     Rx Data   Transport
------------------------------------------------------------------------------
9.9.71.78        0             0             1           1         TLS
64.103.36.133    0             0             1230        2391      HTTPs
```

NMSP クラウド サービスのステータスを表示するには、次のコマンドを使用します。

```
Device# show nmsp cloud-services summary

CMX Cloud-Services Status
-------------------------

   Server:                                 https://yenth8.cmxcisco.com
   IP Address:                             64.103.36.133
   Cmx Service:                            Enabled
   Connectivity:                           https: UP
   Service Status:                         Active
   Last Request Status:                    HTTP/1.1 200 OK
   Heartbeat Status:                       OK
```

NMSP クラウド サービスの統計情報を表示するには、次のコマンドを使用します。

```
Device# show nmsp cloud-services statistics

CMX Cloud-Services Statistics
-----------------------------

   Tx DataFrames:                           3213
   Rx DataFrames:                           1606
   Tx HeartBeat Req:                       31785
   Heartbeat Timeout:                          0
   Rx Subscr Req:                           2868
   Tx DataBytes:                           10069
   Rx DataBytes:                           37752
   Tx HeartBeat Fail:                          2
   Tx Data Fail:                               0
   Tx Conn Fail:                               0
```

モビリティ サービスのサマリーを表示するには、次のコマンドを使用します。

```
Device# show nmsp subscription summary

Mobility Services Subscribed:
Index Server IP Services
----- --------- --------
1 209.165.200.225 RSSI, Info, Statistics, AP Monitor, AP Info
2 209.165.200.225 RSSI, Statistics, AP Info
```

第 40 章

EDCA パラメータ

InformationEnhanced Distributed Channel Access（EDCA）パラメータについて

Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）パラメータは、音声、ビデオ、およびその他の Quality of Service（QoS）トラフィックに優先的な無線チャネル アクセスを提供するように設計されています。

EDCA パラメータの設定（GUI）

手順

ステップ 1 [Configuration] > [Radio Configuration] > [Parameters] を選択します。このページを使用して、802.11a/n/ac（5 GHz）および 802.11b/g/n（2.4 GHz）無線のグローバル パラメータを設定できます。

（注） 無線ネットワークが有効になっている場合、パラメータを設定または変更することはできません。続行する前に、[Configuration] > [Radio Configuration] > [Network] ページでネットワーク ステータスを無効にしてください。

ステップ 2 [EDCA Parameters] セクションで、[EDCA Profile] ドロップダウン リストから EDCA プロファイルを選択します。Enhanced Distributed Channel Access（EDCA; 拡張型分散チャネル アクセス）パラメータは、音声、ビデオ、およびその他の Quality-of-Service（QoS）トラフィックに優先的な無線チャネル アクセスを提供するように設計されています。

ステップ 3 802.11a/n/ac（5 GHz）無線の場合は、[(DFS 802.11h)] セクションで、ローカル電力制限を入力します。[Configuration] > [Radio Configuration] > [Network] ページの [DTPC Support] チェックボックスがオンになっている場合は、電力制限を設定できません。有効な範囲は 0 ～ 30 dBm です。

ステップ 4 AP が新しいチャネルと新しいチャネル番号に切り替わるときにアナウンスされるようにするには、[Channel Switch Announcement Mode] チェックボックスをオンにします。デフォルト値は [disabled] です。

ステップ 5 動的周波数選択（DFS）を有効にしてレーダー信号による干渉を回避するには、[Smart DFS] チェックボックスをオンにします。

ステップ 6 [Apply] をクリックします。

EDCA パラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 {5ghz | 24ghz } shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	無線ネットワークをディセーブルにします。
ステップ 3	**ap dot11 {5ghz | 24ghz} edca-parameters {custom-voice | fastlane | optimized-video-voice | optimized-voice | svp-voice | wmm-default}** 例： `Device(config)# ap dot11 5ghz edca-parameters optimized-voice`	802.11a または 802.11b/g ネットワークに対する特定の EDCA パラメータを有効にします。 （注） **custom-voice** オプションは Cisco Catalyst 9800 シリーズ ワイヤレス コントローラではサポートされていません。 • **custom-voice**：802.11a または 802.11b/g ネットワークのカスタム音声パラメータを有効にします。 • **fastlane**：802.11a または 802.11b/g ネットワークの fastlane パラメータを有効にします。 • **optimized-video-voice**：802.11a または 802.11b/g ネットワークの EDCA

	コマンドまたはアクション	目的
		音声およびビデオ最適化パラメータを有効にします。ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。 • **optimized-voice**：802.11a または 802.11b/g ネットワークで、SpectraLink 以外の音声用に最適化されたプロファイル パラメータを有効にします。ネットワーク上で SpectraLink 以外の音声サービスを展開する場合に、このオプションを選択します。 • **svp-voice**：802.11a または 802.11b/g ネットワークの SpectraLink 音声優先パラメータをイネーブルにします。コールの品質を向上させるためにネットワーク上で SpectraLink の電話を展開する場合に、このオプションを選択します。 • **wmm-default**：802.11a または 802.11b/g ネットワークの Wi-Fi Multimedia（WMM）デフォルト パラメータを有効にします。これがデフォルトのオプションです。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。
ステップ 4	**no ap dot11 {5ghz | 24ghz} shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	無線ネットワークを再度イネーブルにします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show ap dot11 {5ghz | 24ghz} network** 例： `Device# show ap dot11 5ghz network`	音声用の MAC 最適化の現在のステータスを表示します。

第 41 章

802.11 パラメータおよび帯域選択

帯域選択の制約事項、802.11 帯域とパラメータ

- 帯域選択が有効になっている WLAN では、ローミングの遅延が発生するため、音声やビデオなどの時間的に制約があるアプリケーションはサポートされません。
- 帯域選択は、Cisco Aironet 1140、1250、1260、1550、1800、2600、2700、2800、3500、3600、3700、3800 シリーズ アクセス ポイントでのみ使用できます。
- Mid-RSSI は、Cisco Aironet 1600 シリーズ アクセス ポイントではサポートされていません。
- 帯域選択は、Cisco Aironet 1040、OEAP 600 シリーズ アクセスポイントではサポートされていません。
- 帯域選択が動作するのは、コントローラに接続されたアクセス ポイントに対してのみです。コントローラに接続しない FlexConnect アクセス ポイントは、リブート後に帯域選択を実行しません。
- 帯域選択アルゴリズムによるデュアル バンド クライアントの誘導は、同じアクセス ポイントの 2.4 GHz 無線から 5 GHz 無線に限られます。このアルゴリズムが機能するのは、アクセス ポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。
- コントローラ上で帯域選択とアグレッシブ ロード バランシングの両方を有効にすることができます。これらは独立して動作し、相互に影響を与えることはありません。
- コントローラ GUI またはコントローラ CLI を使用して、帯域選択とクライアント ロード バランシングをグローバルで有効または無効にすることはできません。ただし、特定の WLAN の帯域選択とクライアント ロード バランシングを有効または無効にできます。帯

域選択とクライアント ロード バランシングは、デフォルトではグローバルで有効になっています。

帯域選択、802.11 帯域およびパラメータについて

バンドの選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、輻輳の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャネル干渉も受けます。これは、802.11b/g では、重複しないチャネルの数が 3 つに制限されているためです。このような干渉源を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、deviceで帯域選択を設定します。

クライアントに対するプローブ応答を調整すると帯域選択が機能し、WLAN 単位で有効にできます。5 GHz チャネルへクライアントを誘導するために、2.4 GHz チャネルでのクライアントへのプローブ応答を遅らせます。アクセス ポイントでは、**show dot11 band-select** コマンドを実行して帯域選択表を表示できます。また、**show cont d0/d1 | begin Lru** コマンドを実行して表示することもできます。

（注） WMM のデフォルト設定は、**show running-config** コマンドの出力には表示されません。

帯域選択アルゴリズム

帯域選択アルゴリズムは2.4 GHz GHz 帯を使用するクライアントに反映されます。最初に、クライアントがアクセス ポイントにプローブ要求を送信すると、対応するクライアント プローブのアクティブ値とカウント値（帯域選択表に表示）が1になります。以下のシナリオによるアルゴリズム機能を示します。

- シナリオ 1：クライアント RSSI（**show cont d0/d1 | begin RSSI** コマンドの出力に表示）は、中間 RSSI と受け入れ可能クライアント RSSI のどちらよりも強い。
  - デュアルバンド クライアント：2.4 GHz プローブ応答は常に表示されず、すべての 5 GHz プローブ要求に 5 GHz プローブ応答が表示されます。
  - シングルバンド（2.4 GHz）クライアント：プローブ抑制サイクル後にのみ2.4 GHzプローブ応答が表示されます。
  - 設定したプローブ サイクル カウントにクライアントのプローブ カウントが達すると、アルゴリズムはエージング アウト抑止時間を待ち、プローブのアクティブ値を 0 にマークします。そして、アルゴリズムが再起動します。

- シナリオ 2：クライアント RSSI（**show cont d0/d1 | begin RSSI** で表示）は、中間 RSSI と受け入れ可能クライアント RSSI の間に位置します。
  - 2.4 GHz プローブ要求と 5 GHz プローブ要求はすべて制限なしで応答します。
  - このシナリオは、帯域選択無効時と似ています。

（注） クライアントの RSSI 値（**sh cont d0 | begin RSSI** コマンドの出力で表示）は、受信したクライアント パケットの平均値であり、中間 RSSI 機能はプローブ パケットの RSSI の瞬時値です。結果として、クライアント RSSI は設定した中間 RSSI 値（7 dB デルタ）より弱くなります。クライアントからのプローブ 802.11b は、802.11a バンドに関連付けるためクライアントをプッシュするように抑制されます。

802.11 帯域

自国の法的な規制基準を遵守するために、コントローラの 802.11b/g/n（2.4 GHz）帯域と 802.11a/n（5 GHz）帯域を設定できます。デフォルトでは、802.11b/g/n と 802.11a/n の両方が有効になっています。

コントローラが 802.11g トラフィックだけを許可するように設定されている場合、802.11b クライアント デバイスはアクセス ポイントに正常に接続できますが、トラフィックを送信できません。コントローラを 802.11g トラフィック専用に設定する場合、11g レートを必須としてマークする必要があります。

（注） Cisco 2800、3800、1560 AP のブロック ACK は、2.4 GHz 無線に対して Cisco WLC で設定されている必須データ レートで送信されます。

802.11n パラメータ

ここでは、ネットワーク上の 802.11n アクセス ポイントの管理手順について説明します。802.11n デバイスは、2.4 GHz 帯域と 5 GHz 帯域をサポートしており、高スループット データ レートを提供します。

802.11n の高スループット レートは、WMM を使用している WLAN のすべての 802.11n アクセス ポイントで使用できます。この場合、レイヤ 2 暗号化を使用していないか、WPA2/AES 暗号化が有効になっている必要があります。

（注） Cisco 802.11n AP は、偽の wIPS アラームをトリガーする可能性がある誤ったビーコン フレームを断続的に送信する場合があります。これらのアラームを無視することをお勧めします。この問題は Cisco 802.11n AP の 2600、3500、および 3600 で確認されています。

802.11h パラメータ

802.11h では、チャネルの変更がクライアント デバイスに通知されます。また、クライアント デバイスの送信電力を制限できるようになっています。

802.11 帯域とそのパラメータを設定する方法

帯域選択の設定（GUI）

始める前に

プライマリ コントローラとバックアップ コントローラを設定する前に、AP 参加プロファイルがすでに設定済みであることを確認します。

手順

ステップ 1 **[Configuration]** > **[Wireless Advanced]** > **[Band Select]** を選択します。

ステップ 2 [Cycle Count] フィールドに、1 ～ 10 の値を入力します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。デフォルトのサイクル回数は 2 です。

ステップ 3 [Cycle Threshold (milliseconds)] フィールドに、スキャン サイクル期間しきい値を 1 ～ 1000 ミリ秒の値で入力します。この設定は、クライアントからの新しいプローブ要求が新しいスキャン サイクルから送信される間の時間しきい値を決定します。デフォルトのサイクルしきい値は 200 ミリ秒です。

ステップ 4 [Age Out Suppression (seconds)] フィールドに、10 ～ 200 秒の値を入力します。エージング アウト抑制は、以前に認識されていた 802.11b/g/n クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 20 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 5 [Age Out Dual Band (seconds)] フィールドに、10 ～ 300 秒の値を入力します。エージング アウト期間は、以前に認識されていたデュアルバンド クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 50 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 6 [Client RSSI (dbm)] フィールドに、-90 ～ -20 の値を入力します。これは、受信するクライアント パケットの平均です。

ステップ 7 [Client Mid RSSI (dbm)] フィールドに、-90 ～ -20 の値を入力します。これは、プローブパ ケットの瞬間 RSSI 値です。

ステップ 8 [AP Join Profile] ページで、AP 参加プロファイル名をクリックします。

ステップ 9 [Apply] をクリックします。

帯域選択の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless client band-select cycle-count** *cycle_count* 例： `Device(config)# wireless client band-select cycle-count 3`	帯域選択のプローブ サイクル カウントを設定します。 有効な範囲は 1 ～ 10 です。
ステップ 3	**wireless client band-select cycle-threshold** *milliseconds* 例： `Device(config)# wireless client band-select cycle-threshold 5000`	新規スキャン周期の時間のしきい値を設定します。 有効な範囲は 1 ～ 1000 です。
ステップ 4	**wireless client band-select expire suppression** *seconds* 例： `Device(config)# wireless client band-select expire suppression 100`	抑制の期限切れを帯域幅選択に設定します。 有効な範囲は 10 ～ 200 です。
ステップ 5	**wireless client band-select expire dual-band** *seconds* 例： `Device(config)# wireless client band-select expire dual-band 100`	デュアル バンドの期限を設定します。 有効な範囲は 10 ～ 300 です。
ステップ 6	**wireless client band-select client-rssi** *client_rssi* 例： `Device(config)# wireless client band-select client-rssi 40`	クライアント RSSI しきい値を設定します。 有効な範囲は 20 ー 90 です。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

	コマンドまたはアクション	目的
ステップ 8	**wlan** *wlan_profile_name wlan_ID SSID_network_name* **band-select** 例： `Device(config)# wlan wlan1 25 ssid12` `Device(config-wlan)# band-select`	特定の WLAN で帯域選択を設定します。 有効な範囲は 1 ～ 512 です。 *SSID_network_name* パラメータには、最大 32 文字の英数字を入力できます。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 帯域の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[Network]** を選択します。

ステップ 2 [5 GHz Band] または [2.4 GHz Band] のいずれかをクリックします。

ステップ 3 ネットワーク パラメータを設定できるようにするには、[Network Status] チェックボックスをオフにしてネットワークを無効にします。

ステップ 4 [Beacon Interval] フィールドに、AP による SSID のブロードキャスト レートを 100 ～ 600 ミリ秒の範囲で入力します。デフォルトは 100 ミリ秒です。

ステップ 5 802.11b/g/n（2.4 GHz）無線の場合、無線でショート プリアンブルを有効にするには、[Short Preamble] チェックボックスをオンにします。ショート 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。

ステップ 6 [Fragmentation Threshold (in bytes)] フィールドに、256 ～ 2346 バイトの値を入力します。ここで指定したサイズよりも大きいパケットはフラグメント化されます。

ステップ 7 ビーコンおよびプローブ応答で無線の送信電力レベルをアドバタイズするには、[DTPC Support] チェックボックスをオンにします。Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）を使用するクライアント デバイスは、アクセス ポイントからチャネルおよび電力レベル情報を受信して、自身の設定を自動的に調整します。たとえば、主に日本で使用されているクライアントデバイスをイタリアに移送し、そこのネットワークに追加した場合、チャネルと電力設定の自動調整を DTPC に任せることができます。[DTPC Support] チェックボックスをオンにした場合、802.11a/n/ac（5 GHz）無線ネットワークで電力制限値を設定することはできません。

ステップ 8 [Apply] をクリックします。

ステップ 9 ネットワークの CCX 無線管理をグローバルに有効にするには、[CCX Location Measurement] セクションで、[Mode] チェックボックスをオンにします。このパラメータによって、このデバイスに接続されている AP から、CCX v2 以降のリリースを実行しているクライアントに対してブロードキャスト無線測定要求が発行されます。

ステップ 10 [Interval] フィールドに値を入力して、AP がブロードキャスト無線測定要求を発行する頻度を指定します。

ステップ 11 [Apply] をクリックします。

ステップ 12 アクセス ポイントとクライアントとの間で可能なデータ送信レートを指定するには、[Data Rates] セクションでその値を選択します。

- [Mandatory]：クライアントは、このコントローラ上のアクセス ポイントにアソシエートするにはこのデータ レートをサポートしている必要があります。
- [Supported]：アソシエートしたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセス ポイントと通信することができます。
- [Disabled]：通信に使用するデータ レートは、クライアントが指定します。

ステップ 13 [Apply] をクリックします。

ステップ 14 設定を保存します。

802.11 帯域の設定（CLI）

802.11 の帯域とパラメータを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 5ghz shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	802.11a 帯域をディセーブルにします。 （注） 802.11a ネットワーク パラメータを設定する前に、802.11a 帯域をディセーブルにする必要があります。
ステップ 3	**ap dot11 24ghz shutdown** 例： `Device(config)# ap dot11 24ghz shutdown`	802.11b 帯域をディセーブルにします。 （注） 802.11b ネットワーク パラメータを設定する前に、802.11b 帯域をディセーブルにする必要があります。
ステップ 4	**ap dot11 {5ghz | 24ghz} beaconperiod** *time_unit* 例：	対応するアクセス ポイントによる SSID のブロードキャスト レートを指定します。

	コマンドまたはアクション	目的
	`Device(config)# ap dot11 5ghz beaconperiod 500`	ビーコン間隔は時間単位（TU）で測定されます。1 TU は 1024 マイクロ秒です。20 ～ 1000 ミリ秒ごとにビーコンを送信するように、アクセスポイントを設定できます。
ステップ 5	**ap dot11 {5ghz | 24ghz} fragmentation** *threshold* 例： `Device(config)# ap dot11 5ghz fragmentation 300`	パケットを断片化するサイズを指定します。 しきい値は、256 ～ 2346 バイト（両端の値を含む）です。接続不良や多くの無線干渉が発生している領域では、この値を小さくします。
ステップ 6	**ap dot11 {5ghz | 24ghz} dtpc** 例： `Device(config)# ap dot11 5ghz dtpc` `Device(config)# no ap dot11 24ghz dtpc`	アクセスポイントによる、チャネルのアドバタイズ、ビーコンの電力レベル送信、応答プローブを有効にします。 デフォルト値はイネーブルです。Dynamic Transmit Power Control（DTPC; 送信電力の動的制御）を使用するクライアントデバイスは、アクセスポイントからチャネルレベルおよび電力レベルの情報を受信して、自身の設定を自動的に調整します。たとえば、主に日本で使用されているクライアントデバイスをイタリアに移送し、その場所のネットワークに参加させた場合、チャネルと電力の設定の自動調整を DTPC に任せることができます。 このコマンドの **no** 形式は、802.11a または 802.11b DTPC 設定をディセーブルにします。
ステップ 7	**wireless client association limit** *number* **interval** *milliseconds* 例： `Device(config)# wireless client association limit 50 interval 1000`	設定できるクライアントの最大数を指定します。 単一アクセスポイントスロットの、所定の間隔内におけるアソシエーション要求の最大数を設定できます。設定できるアソシエーション制限の範囲は 1 ～ 100 です。 アソシエーション要求制限間隔は 100 ～ 10000 ミリ秒です。

	コマンドまたはアクション	目的
ステップ 8	**ap dot11 {5ghz | 24ghz} rate** *rate* {**disable** | **mandatory** | **supported**} 例： `Device(config)# ap dot11 5ghz rate 36 mandatory`	データをコントローラとクライアント間で送信できる速度を指定します。 • *disable*：クライアントが通信に使用するデータ レートを指定するように定義します。 • *mandatory*：クライアントがコントローラのアクセス ポイントにアソシエートするにはこのデータ レートをサポートする必要があると定義します。 • *supported*：アソシエートしたクライアントは、このデータ レートをサポートしていれば、このレートを使用してアクセス ポイントと通信することができます。ただし、クライアントがこのレートを使用できなくても、アソシエートは可能です。 • *rate*：データが送信されるレートを指定します。802.11a、802.11b 帯域では、データは 1、2、5.5、6、9、11、12、18、24、36、48、または 54 Mbps のレートで送信されます。
ステップ 9	**no ap dot11 5ghz shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	802.11a 帯域をイネーブルにします。 （注） デフォルト値はイネーブルです。
ステップ 10	**no ap dot11 24ghz shutdown** 例： `Device(config)# no ap dot11 24ghz shutdown`	802.11b 帯域をイネーブルにします。 （注） デフォルト値はイネーブルです。
ステップ 11	**ap dot11 24ghz dot11g** 例： `Device(config)# ap dot11 24ghz dot11g`	802.11g ネットワークのサポートをイネーブルまたはディセーブルにします。 デフォルト値はイネーブルです。このコマンドは、802.11b帯域が有効になっている場合のみ使用できます。この機

	コマンドまたはアクション	目的
		能を無効にすると、802.11b 帯域は 802.11g をサポートせずに有効になります。
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

帯域選択 RF プロファイルの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Advanced]** を選択します。

ステップ 2 [Band Select] タブで、[Cycle Count] フィールドに 1 ～ 10 の値を入力します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。デフォルトのサイクル回数は 2 です。

ステップ 3 [Cycle Threshold] フィールドに、スキャン サイクル期間しきい値を 1 ～ 1000 ミリ秒の値で入力します。この設定は、クライアントからの新しいプローブ要求が新しいスキャンサイクルから送信される間の時間しきい値を決定します。デフォルトのサイクルしきい値は200ミリ秒です。

ステップ 4 [Age Out Suppression] フィールドに、10 ～ 200 秒の値を入力します。エージング アウト抑制は、以前に認識されていた 802.11b/g/n クライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 20 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 5 [Age Out Dual Band] フィールドに、10 ～ 300 秒の値を入力します。エージング アウト期間は、以前に認識されていたデュアルバンドクライアントをプルーニングするための期限切れ時間を設定します。デフォルト値は 50 秒です。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。

ステップ 6 [Client RSSI] フィールドに、-90 ～ -20 dBm の値を入力します。クライアントがプローブに応答するための最大 RSSI です。

ステップ 7 [Client Mid RSSI] フィールドに、-20 ～ -90 dBm の値を入力します。このパラメータは mid-RSSI を設定します。この値を使用して RSSI 値に基づき 2.4 GHz プローブの抑制をトグルできます。

ステップ 8 [Apply] をクリックします。

帯域選択 RF プロファイルの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz rf-profile** *rf-profile* 例： `Device(config)# ap dot11 24ghz rf-profile test1`	RF プロファイル名を設定し、RF プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**band-select client** {**mid-rssi** | **rssi** }*dbm* 例： `Device(config-rf-profile)# band-select client rssi -90`	帯域選択のクライアントしきい値を設定します。
ステップ 4	**band-select cycle** {**count** | **threshold**}*count* 例： `Device(config-rf-profile)# band-select cycle count 10`	帯域選択のサイクル パラメータを設定します。
ステップ 5	**band-select expire** {**dual-band** | **suppression** }*time* 例： `Device(config-rf-profile)# band-select expire dual-band 100`	RF プロファイルの帯域選択の有効期間を設定します。
ステップ 6	**band-select probe-response** 例： `Device(config-rf-profile)# band-select probe-response`	RF プロファイルの帯域選択のプローブ応答を有効にします。

802.11n のパラメータの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [RF] を選択します。 > >

ステップ 2 [Add] をクリックして、[Add RF Profile] ウィンドウを表示します。

ステップ 3 [802.11] タブで、次の手順を実行します。

a) 必要な動作レートを選択します。

b) 対応するチェックボックスをオンにして、必要な [802.11n MCS Rates] を選択します。

ステップ 4 [Save & Apply to Device] をクリックします。

802.11n のパラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 {5ghz | 24ghz} dot11n** 例： `Device(config)# ap dot11 5ghz dot11n`	ネットワークで 802.11n サポートを有効にします。 このコマンドの **no** 形式は、ネットワークでの 802.11n サポートを無効にします。
ステップ 3	**ap dot11 {5ghz | 24ghz} dot11n mcs tx** *rtu* 例： `Device(config)# ap dot11 5ghz dot11n mcs tx 20`	データをアクセスポイントとクライアント間で送信できる変調および符号化方式（MCS）レートを指定します。 *rtu*：有効な範囲は 0 ～ 23 です。 このコマンドの **no** 形式は、設定された MCS レートを無効にします。
ステップ 4	**wlan***wlan_profile_name wlan_ID SSID_network_name* **wmm require** 例： `Device(config)# wlan wlan1 25 ssid12` `Device(config-wlan)# wmm require`	WLAN で WMM をイネーブルにし、設定した 802.11n データ レートを使用します。 **require** キーワードは、クライアント デバイスに WMM の使用を要求します。WMM をサポートしていないデバイスは WLAN に接続できません。
ステップ 5	**ap dot11 {5ghz | 24ghz} shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	ネットワークをディセーブルにします。
ステップ 6	**{ap | no ap} dot11 {5ghz | 24 ghz} dot11n a-mpdu tx priority {all | 0-7}** 例：	802.11n パケットに使用する集約方法を指定します。 集約は、パケット データ フレームを個別に伝送するのではなく、グループに

	コマンドまたはアクション	目的
	`Device(config)# ap dot11 5ghz dot11n a-mpdu tx priority all`	まとめるプロセスです。集約方法には、Aggregated MAC Protocol Data Unit（A-MPDU）と Aggregated MAC Service Data Unit（A-MSDU）の 2 種類があります。A-MPDU と A-MSDU は、両方ともソフトウェアで実行されます。 集約方法は、アクセスポイントからクライアントへのトラフィックのタイプごとに指定できます。 リストでは、トラフィック タイプごとに割り当てられる優先レベル（0～7）を定義します。 • 0：ベスト エフォート • 1：バックグラウンド • 2：スペア • 3：エクセレント エフォート • 4：制御ロード • 5：ビデオ（100 ms 未満の遅延およびジッタ） • 6：音声（100 ms 未満の遅延およびジッタ） • 7：ネットワーク コントロール 各優先レベルを個別に設定するか、all パラメータを使用して一度にすべての優先レベルを設定できます。トラフィックが A-MPDU 送信または A-MSDU 伝送を使用するよう、プライオリティ レベルを設定できます。 • 他のオプションとともに **ap** コマンドを使用すると、そのプライオリティ レベルに関連付けられたトラフィックは、A-MPDU 送信に関連付けらます。 • 他のオプションとともに **no ap** コマンドを使用すると、そのプライオリティ レベルに関連付けられた

	コマンドまたはアクション	目的
		トラフィックは、A-MSDU 送信に関連付けられます。 クライアントが使用する集約方法に合わせて優先度を設定します。デフォルトでは、A-MPDU は、優先レベル 0、4、および 5 に対して有効になっており、それ以外は無効になっています。デフォルトでは、A-MPDU は、6 と 7 以外のすべての優先度に対して有効になっています。
ステップ 7	**no ap dot11 {5ghz | 24ghz} shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	ネットワークを再度イネーブルにします。
ステップ 8	**ap dot11 {5ghz | 24ghz} dot11n guard-interval {any | long}** 例： `Device(config)# ap dot11 5ghz dot11n guard-interval long`	ネットワークのガード間隔を設定します。
ステップ 9	**ap dot11 {5ghz | 24ghz} dot11n rifs rx** 例： `Device(config)# ap dot11 5ghz dot11n rifs rx`	ネットワークの Reduced Interframe Space（RIFS）を設定します。
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11h のパラメータの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**ap dot11 5ghz shutdown** 例： `Device(config)# ap dot11 5ghz shutdown`	802.11a ネットワークをディセーブルにします。

	コマンドまたはアクション	目的
ステップ 2	**{ap | no ap} dot11 5ghz channelswitch mode** *switch_mode* 例： `Device(config)# ap dot11 5ghz channelswitch mode 0`	アクセス ポイントの、新しいチャネルに切り替わった際のアナウンス機能をイネーブルまたはディセーブルにします。 *switch_mode*：0 または 1 を入力して、チャネルが実際に切り替えられるまで送信を制限する（0）か、制限しない（1）かを指定します。デフォルト値は [disabled] です。
ステップ 3	**ap dot11 5ghz power-constraint** *value* 例： `Device(config)# ap dot11 5ghz power-constraint 200`	802.11h の電力制限値を dB 単位で設定します。有効範囲は 0 ～ 255 です。 デフォルト値は 3 です。
ステップ 4	**no ap dot11 5ghz shutdown** 例： `Device(config)# no ap dot11 5ghz shutdown`	802.11a ネットワークを再度イネーブルします。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

帯域選択、802.11 帯域およびパラメータの設定のモニタリング

帯域選択と 802.11 帯域を使用した設定の確認コマンド

次のコマンドは、の帯域選択と 802.11 帯域、およびパラメータの確認に使用できます。

表 *9 :* 帯域選択と *802.11* 帯域を使用した設定のモニタリング コマンド

コマンド	目的
show ap dot11 5ghz network	802.11a 帯域ネットワーク パラメータ、802.11a 運用率、802.11n MCS 設定および 802.11n ステータス情報を表示します。
show ap dot11 24ghz network	802.11b 帯域ネットワーク パラメータ、802.11b/g 運用率、802.11n MCS 設定および 802.11n ステータス情報を表示します。

show wireless dot11h	802.11h 設定パラメータを表示します。
show wireless band-select	帯域選択の設定を表示します。

例：5 GHz 帯域の設定の確認

```
Device# show ap dot11 5ghz network
802.11a Network : Enabled
11nSupport : Enabled
  802.11a Low Band : Enabled
  802.11a Mid Band : Enabled
  802.11a High Band : Enabled

802.11a Operational Rates
  802.11a 6M : Mandatory
  802.11a 9M : Supported
  802.11a 12M : Mandatory
  802.11a 18M : Supported
  802.11a 24M : Mandatory
  802.11a 36M : Supported
  802.11a 48M : Supported
  802.11a 54M : Supported
802.11n MCS Settings:
  MCS 0 : Supported
  MCS 1 : Supported
  MCS 2 : Supported
  MCS 3 : Supported
  MCS 4 : Supported
  MCS 5 : Supported
  MCS 6 : Supported
  MCS 7 : Supported
  MCS 8 : Supported
  MCS 9 : Supported
  MCS 10 : Supported
  MCS 11 : Supported
  MCS 12 : Supported
  MCS 13 : Supported
  MCS 14 : Supported
  MCS 15 : Supported
  MCS 16 : Supported
  MCS 17 : Supported
  MCS 18 : Supported
  MCS 19 : Supported
  MCS 20 : Supported
  MCS 21 : Supported
  MCS 22 : Supported
  MCS 23 : Supported
802.11n Status:
  A-MPDU Tx:
    Priority 0 : Enabled
    Priority 1 : Disabled
    Priority 2 : Disabled
    Priority 3 : Disabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
  A-MSDU Tx:
    Priority 0 : Enabled
```

```
    Priority 1 : Enabled
    Priority 2 : Enabled
    Priority 3 : Enabled
    Priority 4 : Enabled
    Priority 5 : Enabled
    Priority 6 : Disabled
    Priority 7 : Disabled
Guard Interval : Any
  Rifs Rx : Enabled
Beacon Interval : 100
CF Pollable mandatory : Disabled
CF Poll Request Mandatory : Disabled
CFP Period : 4
CFP Maximum Duration : 60
Default Channel : 36
Default Tx Power Level : 1
DTPC Status : Enabled
Fragmentation Threshold : 2346
Pico-Cell Status : Disabled
Pico-Cell-V2 Status : Disabled
TI Threshold : 0
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type check : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

例：24 GHz 帯域の設定の確認

```
Device# show ap dot11 24ghz network
802.11b Network : Enabled
11gSupport : Enabled
11nSupport : Enabled

  802.11b/g Operational Rates
  802.11b 1M : Mandatory
  802.11b 2M : Mandatory
  802.11b 5.5M : Mandatory
  802.11g 6M : Supported
  802.11g 9M : Supported
  802.11b 11M : Mandatory
  802.11g 12M : Supported
  802.11g 18M : Supported
  802.11g 24M : Supported
```

```
    802.11g 36M : Supported
    802.11g 48M : Supported
    802.11g 54M : Supported
  802.11n MCS Settings:
    MCS 0 : Supported
    MCS 1 : Supported
    MCS 2 : Supported
    MCS 3 : Supported
    MCS 4 : Supported
    MCS 5 : Supported
    MCS 6 : Supported
    MCS 7 : Supported
    MCS 8 : Supported
    MCS 9 : Supported
    MCS 10 : Supported
    MCS 11 : Supported
    MCS 12 : Supported
    MCS 13 : Supported
    MCS 14 : Supported
    MCS 15 : Supported
    MCS 16 : Supported
    MCS 17 : Supported
    MCS 18 : Supported
    MCS 19 : Supported
    MCS 20 : Supported
    MCS 21 : Supported
    MCS 22 : Supported
    MCS 23 : Supported
  802.11n Status:
    A-MPDU Tx:
      Priority 0 : Enabled
      Priority 1 : Disabled
      Priority 2 : Disabled
      Priority 3 : Disabled
      Priority 4 : Enabled
      Priority 5 : Enabled
      Priority 6 : Disabled
      Priority 7 : Disabled
    A-MSDU Tx:
      Priority 0 : Enabled
      Priority 1 : Enabled
      Priority 2 : Enabled
      Priority 3 : Enabled
      Priority 4 : Enabled
      Priority 5 : Enabled
    Priority 6 : Disabled
      Priority 7 : Disabled
    Guard Interval : Any
    Rifs Rx : Enabled
  Beacon Interval : 100
  CF Pollable Mandatory : Disabled
  CF Poll Request Mandatory : Disabled
  CFP Period : 4
  CFP Maximum Duration : 60
  Default Channel : 11
  Default Tx Power Level : 1
  DTPC Status : true
  Call Admission Limit : 105
  G711 CU Quantum : 15
  ED Threshold : -50
  Fragmentation Threshold : 2346
  PBCC Mandatory : Disabled
  Pico-Cell Status : Disabled
  Pico-Cell-V2 Status : Disabled
```

```
RTS Threshold : 2347
Short Preamble Mandatory : Enabled
Short Retry Limit : 7
Legacy Tx Beamforming setting : Disabled
Traffic Stream Metrics Status : Disabled
Expedited BW Request Status : Disabled
EDCA profile type : default-wmm
Call Admision Control (CAC) configuration
Voice AC
  Voice AC - Admission control (ACM) : Disabled
  Voice Stream-Size : 84000
  Voice Max-Streams : 2
  Voice Max RF Bandwidth : 75
  Voice Reserved Roaming Bandwidth : 6
  Voice Load-Based CAC mode : Enabled
  Voice tspec inactivity timeout : Enabled
CAC SIP-Voice configuration
  SIP based CAC : Disabled
  SIP Codec Type : CODEC_TYPE_G711
  SIP call bandwidth : 64
  SIP call bandwith sample-size : 20
Video AC
  Video AC - Admission control (ACM) : Disabled
  Video max RF bandwidth : Infinite
  Video reserved roaming bandwidth : 0
```

例：802.11h パラメータの状態の確認

```
Device# show wireless dot11h
Power Constraint: 0
Channel Switch: 0
Channel Switch Mode: 0
```

例: 帯域選択の設定の確認

次に、帯域選択の設定を表示する例を示します。

```
Device# show wireless band-select

Band Select Probe Response   : per WLAN enabling
Cycle Count                  : 2
Cycle Threshold (millisec)   : 200
Age Out Suppression (sec)    : 20
Age Out Dual Band (sec)      : 60
Client RSSI (dBm)            : -80
Client Mid RSSI (dBm)        : -80
```

次に、AP RF プロファイルの詳細を表示する例を示します。

```
Device# show ap rf-profile name vid detail

Description                     :
RF Profile Name                 : vid
Band                            : 2.4 GHz
802.11n client only             : Disabled
Transmit Power Threshold v1     : -70 dBm
Min Transmit Power              : -10 dBm
Max Transmit Power              : 30 dBm
Operational Rates
```

```
    802.11b 1M Rate                 : Mandatory
    802.11b 2M Rate                 : Mandatory
    802.11b 5.5M Rate               : Mandatory
    802.11b 11M Rate                : Mandatory
    802.11b 6M Rate                 : Supported
    802.11b 9M Rate                 : Supported
    802.11b 12M Rate                : Supported
    802.11b 18M Rate                : Supported
    802.11b 24M Rate                : Supported
    802.11b 36M Rate                : Supported
    802.11b 48M Rate                : Supported
    802.11b 54M Rate                : Supported
  Max Clients                       : 200
  Trap Threshold
    Clients                         : 12 clients
    Interference                    : 10%
    Noise                           : -80 dBm
    Utilization                     : 10%
  Multicast Data Rate               : auto
  Rx SOP Threshold                  : auto
  Band Select
    Probe Response                  :  Disabled
    Cycle Count                     :  2 cycles
    Cycle Threshold                 :  200 milliseconds
    Expire Suppression              :  20 seconds
    Expire Dual Band                :  60 seconds
    Client RSSI                     :  -80 dBm
    Client Mid RSSI                 :  -80 dBm
  High Speed Roam
    hsr mode                        :  Disabled
    hsr neighbor timeout            :  5
  Load Balancing
    Window                          :  5 clients
    Denial                          :  3 count
  Coverage Data
    Data                            : -62 dBm
    Voice                           : -80 dBm
    Minimum Client Level            : 12 clients
    Exception Level                 : 48%
  DCA Channel List                  : 1,6,11
  Unused Channel List               : 2,3,4,5,7,8,9,10
  DCA Foreign AP Contribution       : Enabled
  802.11n MCS Rates
    MCS  0                          : Enabled
    MCS  1                          : Enabled
    MCS  2                          : Enabled
    MCS  3                          : Enabled
    MCS  4                          : Enabled
    MCS  5                          : Enabled
    MCS  6                          : Enabled
    MCS  7                          : Enabled
    MCS  8                          : Enabled
    MCS  9                          : Enabled
    MCS 10                          : Enabled
    MCS 11                          : Enabled
    MCS 12                          : Enabled
    MCS 13                          : Enabled
    MCS 14                          : Enabled
    MCS 15                          : Enabled
    MCS 16                          : Enabled
    MCS 17                          : Enabled
    MCS 18                          : Enabled
    MCS 19                          : Enabled
    MCS 20                          : Enabled
```

```
  MCS 21                          : Enabled
  MCS 22                          : Enabled
  MCS 23                          : Enabled
  MCS 24                          : Enabled
  MCS 25                          : Enabled
  MCS 26                          : Enabled
  MCS 27                          : Enabled
  MCS 28                          : Enabled
  MCS 29                          : Enabled
  MCS 30                          : Enabled
  MCS 31                          : Enabled
State                             : Up
Client Network  Preference        : connectivity
```

帯域選択、802.11 帯域およびパラメータの設定例

例：帯域選択の設定

次に、帯域選択の新規スキャン周期のプローブ サイクル カウントおよび時間しきい値を設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select cycle-count 3
Device(config)# wireless client band-select cycle-threshold 5000
Device(config)# end
```

次に、抑制の期限を帯域選択に設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select expire suppression 100
Device(config)# end
```

次に、デュアル バンドの期限を帯域選択に設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select expire dual-band 100
Device(config)# end
```

次に、クライアント RSSI しきい値を帯域選択に設定する例を示します。

```
Device# configure terminal
Device(config)# wireless client band-select client-rssi 40
Device(config)# end
```

次に、特定の WLAN 上で帯域選択を設定する例を示します。

```
Device# configure terminal
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# band-select
Device(config)# end
```

例：802.11 帯域設定

次に、ビーコン間隔、フラグメンテーション、および動的な送信電力コントロールを使用して 802.11 帯域を設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 24ghz shutdown
Device(config)# ap dot11 5ghz beaconperiod 500
Device(config)# ap dot11 5ghz fragmentation 300
Device(config)# ap dot11 5ghz dtpc
Device(config)# wireless client association limit 50 interval 1000
Device(config)# ap dot11 5ghz rate 36 mandatory
Device(config)# no ap dot11 5ghz shutdown
Device(config)# no ap dot11 24ghz shutdown
Device(config)# ap dot11 24ghz dot11g
Device(config)#end
```

例：802.11n 設定

次に、集約方法を使って 5 GHz 帯域の802.11n パラメータを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n a-mpdu tx priority all
Device(config)# no ap dot11 5ghz shutdown
Device(config)#exit
```

次に、5 GHz 帯域でガード インターバルを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# no ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz dot11n guard-interval long
Device(config)#end
```

次に、5 GHz 帯域で RIFS を設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz dot11n
Device(config)# ap dot11 5ghz dot11n mcs tx 20
Device(config)# wlan wlan1 25 ssid12
Device(config-wlan)# wmm require\
Device(config-wlan)# exit
Device(config)# ap dot11 5ghz shutdown
```

```
Device(config)# ap dot11 5ghz dot11n rifs rx
Device(config)#end
```

例：802.11h 設定

次に、制限伝送を使用して、アクセスポイントをいつ新しいチャネルに切り替えるかをアナウンスするために、そのアクセスポイントを設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz channelswitch mode 0
Device(config)# no ap dot11 5ghz shutdown
Device(config)#end
```

次に、5 GHz 帯域で 802.11h 電力制限を設定する例を示します。

```
Device# configure terminal
Device(config)# ap dot11 5ghz shutdown
Device(config)# ap dot11 5ghz power-constraint 200
Device(config)# no ap dot11 5ghz shutdown
Device(config)#end
```

第 42 章

アクセス ポイントへのイメージのプレダウンロード

アクセスポイントへのイメージのプレダウンロードについて

ネットワークの停止を最小限に抑えるため、アクセスポイントをリセットしたり、ネットワーク接続を切断したりせずに、deviceからのアクセスポイントにアップグレードイメージをダウンロードしてください。以前は、アップグレードイメージをdeviceにダウンロードしてコントローラをリセットすると、アクセス ポイントがディスカバリ モードに移行してしまう場合がありました。アクセスポイントで新しいイメージを含むコントローラが検出されると、新しいイメージがダウンロードされ、アクセス ポイントがリセットされ、ディスカバリ モードに移行し、deviceに再 join されていました。

これで、コントローラにアップグレードイメージをダウンロードできるようになります。コントローラがアップグレード イメージを使用して起動すると、AP はコントローラに参加し、Registered（登録済み）状態に移行します。これは、すでに AP イメージが AP にプレダウンロードされているためです。

アクセスポイントへのイメージのプレダウンロードの制限

以下は、アクセス ポイントにイメージをプレダウンロードする際の制約事項です。

- 同時プレダウンロードの最大数は、コントローラの wncd インスタンスごとに 100 個に制限されています。ただし、プレダウンロードは、開始時に wncd インスタンスごとに 16 のセットでトリガーされ、60 秒ごとに繰り返されます。
- アクセス ポイントの使用可能なメモリの全容量が 16 MB の場合は、アップグレード イメージをダウンロードすると空き容量が不足するおそれがあるため、クラッシュ情報ファイル、無線ファイル、およびバックアップイメージが存在する場合、それらはすべて自動的に削除され、空き容量が確保されます。ただし、プレダウンロードイメージはアクセスポイントのバックアップイメージがあればそれらに置き換えられるため、この制限はプレダウンロード プロセスには影響しません。
- すべてのプライマリ、セカンダリ、ターシャリ コントローラで、同じイメージを実行する必要があります。そうしないと、この機能は有効になりません。
- リセット時に、すべてのアクセス ポイントでイメージのダウンロードが完了していることを確認する必要があります。
- アクセス ポイントには、2 種類のソフトウェア イメージだけを保存できます。
- Cisco Wave 1 AP は、Cisco AireOS リリース 8.3 から Cisco IOS XE Gibraltar 16.10.1 への移行中にイメージを 2 回ダウンロードする場合があります。これにより、移行中の AP のダウンタイムが増大します。

アクセスポイントへのイメージのプレダウンロード方法

アクセス ポイントへのイメージのプレダウンロード（CLI）

始める前に

イメージをアクセス ポイントにプレダウンロードする際に、覚えておく必要がある前提条件があります。

- プレダウンロードは、deviceがインストール モードで起動している場合にのみ可能です。
- TFTP サーバ、フラッシュ イメージ、またはUSBから新しいイメージをコピーできます。
- 新しいイメージをプレダウンロードする前に、**software install** コマンドを使用して新しいソフトウェアをインストールし、**reload** オプションでは **no** を選択します。
- すでに最新のアップグレード イメージが AP に存在する場合、プレダウンロードはトリガーされません。**show ap image** コマンドを使用して、プライマリ イメージとバックアップイメージのバージョンがアップグレードイメージと同じであるかどうかを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap image predownload** or **ap name** *ap-name* **image predownload** 例： `Device# ap image predownload` `Device# ap name ap1 image predownload`	すべてのアクセス ポイントに、または deviceに接続している特定のアクセス ポイントに、新しいイメージをダウンロードします。
ステップ 2	**show ap image** 例： `Device# show ap image`	アクセス ポイントのプレダウンロード ステータスを確認します。 このコマンドでは、最初にステータスが Predownloading として表示され、ダウンロードが完了すると Completed に移行します。
ステップ 3	**show ap name** *ap-name* **image** 例： `Device# show ap name ap1 image`	特定の AP におけるイメージの詳細を提供します。
ステップ 4	**ap image swap** or **ap name** *ap-name* **image swap** or **ap image swap completed** 例： `Device# ap image swap`	プレダウンロードが完了した AP どうしのイメージを交換します。
ステップ 5	**ap image reset** or **ap name** *ap-name* **reset** 例： `Device# ap image reset`	アクセス ポイントをリセットします。
ステップ 6	**reload** 例： `Device# reload`	システムをリセットします。

アクセス ポイント プレダウンロード プロセスのモニタリング

このセクションでは、アクセス ポイントのプレダウンロード プロセスのモニタリングに使用できるコマンドについて説明します。

アクセス ポイント のプレダウンロード イメージのダウンロード中に、対応するアクセス ポイントのプレダウンロードの進捗を確認するには、**show ap image** コマンドを入力します。

```
Device# show ap image
Total number of APs  : 1
```

```
Number of APs
       Initiated                   : 1
       Predownloading              : 1
       Completed predownloading    : 0
       Not Supported               : 0
       Failed to Predownload       : 0

AP Name                            Primary Image   Backup Image    Predownload Status
 Predownload Ver...  Next Retry Time    Retry Count
-------------------------------------------------------------------------------------------
AP1                                10.0.1.66       10.0.1.66       Predownloading
 10.0.1.67           NA                             0


Device# show ap image

Total number of APs  : 1

Number of APs
       Initiated                   : 1
       Predownloading              : 0
       Completed predownloading    : 1
       Not Supported               : 0
       Failed to Predownload       : 0

AP Name                            Primary Image   Backup Image    Predownload Status
 Predownload Ver...  Next Retry Time    Retry Count
-------------------------------------------------------------------------------------------
AP1                                10.0.1.66       10.0.1.67       Complete
 10.0.1.67           NA
                        0
```

特定の AP におけるイメージの詳細を表示するには、次のコマンドを使用します。

```
Device# show ap name APe4aa.5dd1.99b0 image

AP Name : APe4aa.5dd1.99b0
Primary Image : 16.6.230.46
Backup Image : 3.0.51.0
Predownload Status : None
Predownload Version : 000.000.000.000
Next Retry Time : N/A
Retry Count : 0
```

第 43 章

イメージの効率的なアップグレード

イメージの効率的なアップグレード

「イメージの効率的なアップグレード」は、AP にイメージをプレダウンロードするための効率的な方法です。この機能はマスター/スレーブモデルと同様に機能します。モデルごとの AP がマスター AP になり、WAN リンクを介してコントローラからイメージをダウンロードします。マスター AP にイメージがダウンロードされると、スレーブ AP はマスター AP からのイメージのダウンロードを開始します。この方法では WAN の遅延が減少します。マスター AP の選択は動的かつランダムに行われます。AP モデルごとに最大 3 つのスレーブ AP が、マスター AP からイメージをダウンロードできます。

（注）

- イメージの効率的なアップグレードは、flex モードでのみ機能します。
- イメージの効率的なアップグレードは、default-site-tag とは連動しません。

プレダウンロードの有効化（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [Access Points] ページで、[All Access Points] セクションを展開し、編集する AP の名前をクリックします。

ステップ 3 [Edit AP] ページで、[Advanced] タブをクリックし、[AP Image Management] セクションで [Predownload] をクリックします。

ステップ 4 [Update & Apply to Device] をクリックします。

プレダウンロードの有効化（(CLI)）

始める前に

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex rr-xyz-flex-profile`	RF プロファイルを設定し、rf プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**predownload** 例： `Device(config-wireless-flex-profile)# predownload`	イメージのプレダウンロードを有効にします。
ステップ 4	**end** 例： `Device(config-wireless-flex-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

サイト タグの設定（CLI）

サイト タグを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site rr-xyz-site`	サイト タグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**flex-profile** *flex-profile-name* 例： `Device(config-site-tag)# flex-profile rr-xyz-flex-profile`	flex プロファイルを設定します。 （注） サイト タグでローカル サイトが設定されている場合、flex プロファイル設定をサイト タグから削除することはできません。 （注） サイト タグを Flexconnect として設定するには、**no local-site** コマンドを使用する必要があります。そうしないと flex プロファイル設定が有効になりません。
ステップ 4	**description** *site-tag-name* 例： `Device(config-site-tag)# description "default site tag"`	サイト タグの説明を追加します。
ステップ 5	**end** 例： `Device(config-site-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 6	**show wireless tag site summary** 例： `Device# show wireless tag site summary`	（任意）サイト タグの数を表示します。 （注） タグに関する詳細情報を表示するには、**show wireless tag site detailed** *site-tag-name* コマンドを使用します。

	コマンドまたはアクション	目的
		（注） サイトタグとポリシータグの両方が設定されていない場合、**show wireless loadbalance tag affinity wncd** *wncd-instance-number* コマンドの出力にはデフォルト タグ（サイトタグ）タイプが表示されます。

AP へのポリシー タグとサイト タグの付加（CLI）

ポリシー タグとサイト タグを AP に付加するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap** *mac-address* 例： `Device(config)# ap F866.F267.7DFB`	Cisco AP を設定し、AP プロファイル コンフィギュレーション モードを開始します。 （注） *mac-address* 有線 mac アドレスである必要があります。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag rr-xyz-policy-tag`	ポリシー タグを AP にマッピングします。
ステップ 4	**site-tag** *site-tag-name* 例： `Device(config-ap-tag)# site-tag rr-xyz-site`	サイト タグを AP にマッピングします。
ステップ 5	**rf-tag** *rf-tag-name* 例： `Device(config-ap-tag)# rf-tag rf-tag1`	RF タグを関連付けます。

	コマンドまたはアクション	目的
ステップ 6	**end** 例： `Device(config-ap-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 7	**show ap tag summary** 例： `Device# show ap tag summary`	（任意）AP の詳細と AP に関連付けられているタグを表示します。
ステップ 8	**show ap name** <*ap-name*> **tag info** 例： `Device# show ap name ap-name tag info`	（任意）AP 名とタグ情報を表示します。
ステップ 9	**show ap name** <*ap-name*> **tag detail** 例： `Device# show ap name ap-name tag detail`	（任意）AP 名とタグの詳細を表示します。

サイト タグへのプレダウンロードのトリガー

サイト タグへのイメージのダウンロードをトリガーするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> configure terminal`	特権 EXEC モードを開始します。
ステップ 2	**ap image predownload site-tag** *site-tag* **start** 例： `Device# ap image predownload site-tag rr-xyz-site start`	イメージのプレダウンロードを開始するようマスター AP に指示します。
ステップ 3	**show ap master list** 例： `Device# show ap master list`	サイトタグごとにAPモデルごとのマスター AP のリストを表示します。
ステップ 4	**show ap image** 例：	マスター AP とスレーブ AP のプレダウンロード状態を表示します。

	コマンドまたはアクション	目的
	Device# show ap image	（注） lexefficient イメージのアップグレードが AP で有効になっているかどうかを確認するには、AP コンソールで **show capwap client rcb** コマンドを使用します。

次に、イメージの効率的なアップグレード機能の機能状態を表示する出力例を示します。

次の出力は、マスター AP を示しています。

```
Device# show ap master list
AP Name                          WTP Mac           AP Model          Site Tag
-------------------------------------------------------------------------------
AP0896.AD9D.3124                 f80b.cb20.2460    AIR-AP2802I-D-K9 ST1
```

次の出力は、マスター AP がイメージのプレダウンロードを開始したことを示しています。

```
Device# show ap image
Total number of APs: 6

AP Name            Primary Image   Backup Image  Predownload Status   Predownload Version
  Next Retry Time   Retry Count
-------------------------------------------------------------------------------------------
APE00E.DA99.687A    16.6.230.37     0.0.0.0       None                 0.0.0.0
     N/A              0
AP188B.4500.4208    16.6.230.37     8.4.100.0     None                 0.0.0.0
     N/A              0
AP188B.4500.4480    16.6.230.37     0.0.0.0       None                 0.0.0.0
     N/A              0
AP188B.4500.5E28    16.6.230.37     16.4.230.35   None                 0.0.0.0
     N/A              0
AP0896.AD9D.3124    16.6.230.37     8.4.100.0     Predownloading       16.6.230.36
     0                0
AP2C33.1185.C4D0    16.6.230.37     8.4.100.0     None                 0.0.0.0
     N/A              0
```

次の出力は、マスター AP がプレダウンロードを完了し、スレーブ AP でプレダウンロードが開始されたことを示しています。

```
Device# show ap image

Total number of APs: 6
AP Name            Primary Image   Backup Image  Predownload Status   Predownload Version
  Next Retry Time   Retry Count
-------------------------------------------------------------------------------------------
APE00E.DA99.687A    16.6.230.37     0.0.0.0       Initiated            16.6.230.36
     N/A              0
AP188B.4500.4208    16.6.230.37     8.4.100.0     None                 0.0.0.0
     N/A              0
AP188B.4500.4480    16.6.230.37     0.0.0.0       None                 0.0.0.0
     N/A              0
AP188B.4500.5E28    16.6.230.37     16.4.230.35   None                 0.0.0.0
     N/A              0
```

```
AP0896.AD9D.3124    16.6.230.37     8.4.100.0     Complete             16.6.230.36
     0                 0
AP2C33.1185.C4D0    16.6.230.37     8.4.100.0     Initiated            16.6.230.36
     0                 0
```

次の出力は、特定の AP のイメージ ステータスを示しています。

```
Device# show ap name APe4aa.5dd1.99b0 image
AP Name : APe4aa.5dd1.99b0
Primary Image : 16.6.230.46
Backup Image : 3.0.51.0
Predownload Status : None
Predownload Version : 000.000.000.000
Next Retry Time : N/A
Retry Count : 0
```

次の出力は、すべての AP でのプレダウンロードの完了を示しています。

```
Device# show ap image
Total number of APs: 6

Number of APs
        Initiated                 : 0
        Predownloading            : 0
        Completed predownloading  : 3
        Not Supported             : 0
        Failed to Predownload     : 0

AP Name            Primary Image   Backup Image  Predownload Status   Predownload Version
  Next Retry Time   Retry Count
------------------------------------------------------------------------------------------
APE00E.DA99.687A    16.6.230.37     16.6.230.36   Complete             16.6.230.36
     N/A               0
AP188B.4500.4208    16.6.230.37     8.4.100.0     None                 0.0.0.0
     N/A               0
AP188B.4500.4480    16.6.230.37     0.0.0.0       None                 0.0.0.0
     N/A               0
AP188B.4500.5E28    16.6.230.37     16.4.230.35   None                 0.0.0.0
     N/A               0
AP0896.AD9D.3124    16.6.230.37     16.6.230.36   Complete             16.6.230.36
     0                 0
AP2C33.1185.C4D0    16.6.230.37     16.6.230.36   Complete             16.6.230.36
     0                 0
```

第 44 章

ヒットレス アップグレード

N+1 ヒットレス ローリング AP アップグレード

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでの既存の CAPWAP の実装では、コントローラとそれに関連付けられているすべての AP のソフトウェア バージョンが同じである必要があります。N+1 ヒットレス ローリング AP アップグレード機能を使用することで、一連の AP をアップグレードすることができます。ただし、ネットワークのダウンタイムを発生させずにすべての AP を同時にアップグレードすることはできません。

コントローラと AP 間で同じバージョン スキューがサポートされている場合は、ネットワークのダウンタイムを伴わずにワイヤレス ネットワークをアップグレードできます。これにより、同じコントローラに接続している間も AP を段階的にアップグレードできます。バージョン スキューの方法では、N+1 ヒットレス ローリング AP アップグレード機能とスペア コントローラを使用することで、N+1 ネットワークの場合でもアップグレードのダウンタイムを回避できます。

次に、N+1 ヒットレス ローリング AP アップグレード機能のワークフローを示します。

1. コントローラ（WLC1）からモビリティ メンバ（WLC2）へのモビリティ トンネルを確立します。
2. **install add file bootflash:***new_version.bin* を使用して、コントローラソフトウェア（WLC1）をアップグレードします。
3. （任意）AP イメージをアップグレードすることもできます。詳細については、「アクセス ポイントへのイメージのプレダウンロード」の項を参照してください。
4. **ap image upgrade destination** *controller-name controller-ip report-name* 特権 EXEC コマンドを使用して、すべての AP をアップグレードし、WLC1（送信元）から WLC2（宛先）に移動します。
5. **install activate** コマンドを使用して、WLC1 の新しいイメージをアクティブにします。

6. **install commit** コマンドを使用して、変更を確定します。
7. **ap image move destination** *controller-name controller-ip report-name* コマンドを使用して、APを WLC2 から WLC1 に移動して戻します。

ヒットレス アップグレードの設定

N+1 展開でゼロ ダウンタイム ネットワーク アップグレードを実現するには、次の手順に従います。

始める前に

- 宛先コントローラのホスト名とワイヤレス管理 IP が、特権 EXEC コマンドで指定されていることを確認します。
- アクセス ポイントが、宛先コントローラで実行されているイメージとともにプレダウンロードされていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**ap image upgrade destination** *wlc-name wlc-ip* 例： `Device# ap image upgrade destination wlc2 10.7.8.9`	swap および reset コマンドを使用して、指定した宛先コントローラに AP を移動します。この後、親コントローラは新しいイメージをアクティブ化し、新しいイメージを使用してリロードします。モビリティ トンネルが起動すると、APはスワップとリセットなしで親コントローラに戻されます。 （注） イメージをアップグレードする前に、コントローラ（WLC1）からモビリティ メンバ（WLC2）へのモビリティ トンネルを確立していることを確認します。
ステップ 2	**ap image upgrade destination** *wlc-name wlc-ip* 例： `Device# ap image upgrade destination wlc2 10.7.8.9`	（任意）swap および reset コマンドを使用して、指定した宛先コントローラに AP を移動します。 （注） ステップ 1 を実行していない場合にのみ、ステップ 2 ～ 4 を実行します。

	コマンドまたはアクション	目的
ステップ 3	**ap image move destination** *wlc-name wlc-ip* 例： `Device# ap image move destination wlc1 10.7.8.6`	AP を親コントローラに戻します。

ヒットレス アップグレードの確認

ヒットレス アップグレードを確認するには、次の **show** コマンドを使用します。

すべてのアップグレード レポート名を表示するには、次のコマンドを使用します。

```
Device# show ap upgrade summary

Report Name      Start time
-------------------------------------------------------------------------------------------------
AP_upgrade_from_VIGK_CSR_2042018171639 05/20/2018 17:16:39 UTC
```

アップグレード レポート名に基づいて AP のアップグレード情報を表示するには、次のコマンドを使用します。

```
Device# show ap upgrade name test-report

AP upgrade is complete
From version: 16.10.1.4
To version: 16.10.1.4
Started at: 05/20/2018 17:16:39 UTC
Percentage complete: 100
End time: 05/20/2018 17:25:39 UTC
Progress Report
---------------
Iterations
----------
Iteration Start time End time AP count
-------------------------------------------------------------------------------------------------
0 05/20/2018 17:16:39 UTC 05/20/2018 17:16:39 UTC 0
1 05/20/2018 17:16:39 UTC 05/20/2018 17:25:39 UTC 1
Upgraded
--------
Number of APs: 1
AP Name Ethernet MAC Iteration Status
-------------------------------------------------------------------------------------------------
AP-SIDD-CLICK 70db.9848.8f60 1 Joined
In Progress
-----------
Number of APs: 0
AP Name Ethernet MAC
-----------------------------------------------
Remaining
---------
Number of APs: 0
AP Name Ethernet MAC
-----------------------------------------------
```

第 45 章

スイッチのワイヤレス サブパッケージ

ワイヤレス サブパッケージの概要

ワイヤレスのみのファブリックでは、ファブリックの利点を活かすためにファブリック構造が使用されます。このアーキテクチャでは、既存の従来型ネットワーク設計（マルチ階層、ルーテッド アクセス、VSS ネットワークなど）の上層にファブリックが構築されます。LISP コントロール プレーンとともに、オーバーレイ データ プレーン トラフィックの VXLAN カプセル化も使用されます。ワイヤレス コントロール プレーンはそのまま維持され、CAPWAP トンネルは AP を始点とし、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラまたは AireOS を終点とします。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、専用のアプライアンス内、スイッチ内、または VM 内で機能できます。

スイッチ用の Cisco Catalyst 9800 ワイヤレス コントローラ では、コントロール プレーンと管理プレーンの一元管理（設定、アップグレード、トラブルシューティングなどが簡単に行える）、分散型フォワーディング プレーンのスループットやパフォーマンスの最大化といったメリットがすべて実現されます。分散型データ プレーンにより、AVC などのサービスの拡張が可能になります。この新しいモデルでは、ワイヤレス コントロール プレーンは MC や MA との間で分割されません。スイッチがワイヤレス コントロール プレーンから切り離され、コントローラがワイヤレス機能を処理し、トラフィックのスイッチングがシスコのアクセス スイッチによって実行されます。

ワイヤレス機能を有効にする必要があるのはネットワークの少数のノードに限られるため、必要に応じて Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを個別のパッケージとしてスイッチにインストールできます。サブパッケージはベースイメージの上層にインストールされます。サブパッケージをアクティブ化するにはリロードが必要です。

（注） サブパッケージは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ソフトウェア全体を含むオプションのバイナリです。

（注） Cisco Catalyst 9300 スイッチ上の Cisco Catalyst 9800 ワイヤレス コントローラ ソフトウェアは、Cisco DNA Center を使用してスイッチにプロビジョニングおよび展開する必要があり、スタンドアロン コントローラとして設定することはできません。詳細については、『Cisco Catalyst 9300 Series Switches Hardware Installation Guide』を参照してください。

ワイヤレス パッケージのインストール方法

1. スイッチにベース イメージ（ワイヤレスなし）をインストールします。
2. スイッチにワイヤレス パッケージをインストールします。
3. AP イメージをアップグレードします。
4. スイッチをリロードします。
5. **wireless-controller** コンフィギュレーション コマンドを使用してスイッチでワイヤレスを有効にし、ワイヤレス機能を設定します。

ワイヤレス パッケージの削除方法

1. スイッチからワイヤレス パッケージをアンインストールします。
2. スイッチをリロードします。
3. **write** コマンドを実行します。これで、スタートアップコンフィギュレーションからワイヤレス設定が削除されます。

新しいバージョンのワイヤレス パッケージへのアップグレード方法

1. スイッチにベース イメージ（ワイヤレスなし）をインストールします。
2. スイッチをリロードします。
3. 更新されたワイヤレス パッケージをインストールします。
4. スイッチをリロードします。

インストール モードでのスイッチの起動

次に示す手順を使用して、スイッチをインストールモードで起動します。

始める前に

サブパッケージはバンドルモードでは機能しません。**show version** コマンドを使用してブートモードを検証します。

手順

ステップ 1 **install add file** *image.bin location* **activate commit**

このコマンドは、スイッチをバンドルモードからインストールモードに移行します。ここで *image.bin* はベース イメージです。

ステップ 2 すべてのプロンプトで [yes] をクリックします。

ステップ 3 **reload**

スイッチをリロードします。*flash:packages.conf* から起動していることを確認します。リロード後に、スイッチはインストールモードになります。

（注） インストール モードでのイメージのアップグレード/ダウングレード中、flash:<file_name> を使用した「Install add file」コマンドは使用できません。代わりに「bootflash:<filename>」を使用する必要があります。

```
Install add file bootflash:<file_name>  activate commit
```

次のタスク

show version コマンドを使用してブート モードを確認します。

1 ステップでのサブパッケージのインストール

次の手順を使用して、1 ステップでサブパッケージをインストールします。

始める前に

- スイッチがインストールモードであることを確認します。
- *flash:packages.conf* からのみ起動していることを確認します。

手順

ステップ 1 **install add file** *flash:<controller>_pkg.bin* **activate commit**

スイッチ用の Cisco Catalyst 9800 ワイヤレス コントローラのサブパッケージをインストールします。

（注） サブパッケージ（flash:<controller>_pkg.bin）は www.cisco.com で入手できます。また、TFTP サーバからサブパッケージを直接インストールすることもできます。

ステップ 2 すべてのプロンプトで [yes] をクリックします。

ステップ 3 スイッチをリロードします。

次のタスク

インストールされているイメージまたはパッケージを確認するには、**show install summary** コマンドを使用します。

複数ステップでのサブパッケージのインストール

次の手順を使用してサブパッケージをインストールします。

始める前に

- スイッチがインストールモードであることを確認します。
- *flash:packages.conf* からのみ起動していることを確認します。

手順

ステップ 1 **install add file** *flash:<controller>_pkg.bin*

サブパッケージがフラッシュに追加されて展開されます。

ステップ 2 **install activate file** *flash:<controller>_pkg.bin*

サブパッケージをインストールし、リロードをトリガーします。ただし、リロード後に以前の状態にロールバックすることもできます。

ステップ 3 **install commit**

ファイルの書き込みを実行してインストールを完了します。

次のタスク

インストールされているイメージまたはパッケージを確認するには、**show install summary** コマンドを使用します。

スタックへのインストール

1 ステップでのサブパッケージのインストールまたは複数ステップでのサブパッケージのインストール （426 ページ）を使用して、パッケージをスタックにインストールできます。

新しいメンバがスタックに加わる場合、次の 2 つのシナリオが考えられます。

- **自動アップグレードが有効になっている場合**：必要なソフトウェアが新しいメンバにインストールされます。この場合、ワイヤレスパッケージだけでなく、スタックで実行されているソフトウェアについても、バージョンが一致します。
- **自動アップグレードが無効になっている場合**：ソフトウェアのバージョンがスタック内のものと同じではないため、新しいメンバはバージョン不一致状態のままになり、スタックに加わりません。自動アップグレード手順を開始するには、EXEC モードで手動で **install autoupgrade** コマンドを実行する必要があります。

ワイヤレス パッケージの非アクティブ化

ワイヤレス サブパッケージを非アクティブ化するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**install deactivate file** *flash:<controller>_pkg.bin* 例： `Device# install deactivate file flash:<controller>_pkg.bin`	パッケージを削除し、スイッチを強制的にリブートします。
ステップ 2	**install commit** 例： `Device# install commit`	ワイヤレス パッケージを使用せずにスイッチをコミットします。

自動アップグレードの有効化または無効化

自動アップグレードを有効または無効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**software auto-upgrade enable** 例： `Device(config)# software auto-upgrade enable`	ソフトウェアの自動アップグレードを有効にします。
ステップ 2	**software auto-upgrade disable** 例： `Device(config)# software auto-upgrade disable`	ソフトウェアの自動アップグレードを無効にします。

第 46 章

NBAR Protocol Discovery

NBAR Protocol Discovery の概要

NBAR Protocol Discovery 機能により、インターフェイスをパススルーするアプリケーション プロトコルを容易に検出できます。Network Based Application Recognition（NBAR）は、どのプロトコルやアプリケーションが現在ネットワークで動作しているかを調べます。Protocol Discovery を使用すると、NBAR でサポートされるすべてのプロトコル トラフィックを検出し、そのプロトコルに関連する統計情報を取得できます。

NBAR は、レイヤ 4 ～ レイヤ 7 のアプリケーションとプロトコルを識別するいくつかの分類機能を導入しています。NBAR は、Cisco Application Visibility and Control（AVC）でも使用されます。AVC を使用して、NBAR は、より適切な QoS とポリシングを通してアプリケーション パフォーマンスを向上させ、使用されているネットワークに関する可視性を高めます。

NBAR Protocol Discovery の設定

プロトコルの検出を有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy nbar-proto-policy`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングのワイヤレスポリシープロファイルを設定します。 （注） NBAR Protocol Discovery は、ローカル モード（中央スイッチング）および FlexConnect（中央スイッチング）モードでサポートされています。
ステップ 4	**ip nbar protocol-discovery** 例： `Device(config-wireless-policy)# ip nbar protocol-discovery`	NBAR2 エンジンをアクティブ化することで、ワイヤレス ポリシー プロファイルでアプリケーションの認識を有効にします。

Protocol Discovery の統計情報の確認

Protocol Discovery の統計情報を表示するには、次のコマンドを使用します。

```
Device# show ip nbar protocol-discovery wlan wlan-profile-name

wlan_profile_name (iif_id 0xF0400002)

Last clearing of "show ip nbar protocol-discovery" counters 00:07:12


                           Input                     Output
                           -----                     ------
   Protocol                Packet Count              Packet Count
                           Byte Count                Byte Count
                           5min Bit Rate (bps)       5min Bit Rate (bps)
                           5min Max Bit Rate (bps)   5min Max Bit Rate (bps)
   ------------------------ ------------------------ ------------------------
   unknown                 22                        0
                           4173                      0
                           0                         0
                           2000                      0
   dhcp                    3                         2
                           1166                      724
                           0                         0
                           0                         0
   ping                    2                         2
                           204                       236
                           0                         0
                           0                         0
   Total                   27                        4
                           5543                      960
```

```
0                       0
2000                    0
```

Protocol Discovery の統計情報をクリアするには、次のコマンドを使用します。

```
Device# clear ip nbar protocol-discovery wlan wlan-profile-name
```

第 47 章

NBAR プロトコル パックの動的アップグレード

NBAR プロトコル パックの動的アップグレード

プロトコル パックは、は、デバイスのシスコ ソフトウェアを置き換えることなく、デバイスでの Network Based Application Recognition（NBAR）エンジン プロトコルのサポートを更新するソフトウェア パッケージです。プロトコル パックには、NBAR によって公式にサポートされている、コンパイル済みでパック済みのアプリケーションに関する情報が含まれています。各アプリケーションについて、プロトコル パックには、アプリケーション署名とアプリケーション属性の情報が含まれています。各ソフトウェア リリースには、組み込みのプロトコル パックがバンドルされています。

Application Visibility and Control（AVC）機能（ディープ パケット インスペクション（DPI）に使用）は分散型アプローチを使用してワイヤレス製品に対応します。このアプローチでは、DPI を実行して Netflow メッセージで結果を報告するために、アクセス ポイント（AP）またはコントローラ上で実行されている NBAR が活用されます。

AVC DPI テクノロジーは、認識されたトラフィックを更新し、カスタム タイプのトラフィック（カスタム アプリケーションと呼ばれます）を定義する機能をサポートしています。NBAR は、ローカル モードではコントローラ上で実行され、Flex モードおよびファブリック モードでは AP 上で実行されます。ローカル モードでは、AP から着信するすべてのトラフィックがワイヤレス コントローラにトンネリングされます。

（注）

- NBAR はすべてのモードでサポートされていますが、NBAR プロトコル パックのアップグレードはローカル モード（中央スイッチング）と FlexConnect モード（中央スイッチング）でのみサポートされています。
- カスタム アプリケーションは、ローカル モード（中央スイッチング）と FlexConnect モード（中央スイッチング）でのみ使用できます。

プロトコル パックには次の特長があります。

- 簡単かつ迅速にロードできます。
- 新バージョンのプロトコルパックにアップグレードしたり旧バージョンのプロトコルパックに戻したりできます。
- デバイスのリロードは必要ありません。
- サービスを中断することはありません。

プロトコル パックのアップグレード

プロトコル パックのアップグレードを使用すると、スイッチ全体やアプライアンス イメージ全体を更新することなく、NBARエンジンを更新して、新しいタイプのプロトコルやトラフィックを認識することができます。また、システム全体を再起動する必要もなくなります。

NBAR2 プロトコル パックは Cisco Software Center で次の URL からダウンロードできます：https://software.cisco.com/download/navigator.html

カスタム アプリケーション

カスタム アプリケーションを使用すると、宛先 IP、ホスト名、URL などの一連のカスタムルールに基づいてトラフィックを認識するよう NBAR エンジンに強制することができます。

カスタム アプリケーション名は Web UI または NetFlow コレクタに表示されます。

NBAR2 プロトコル パックのアップグレード

NBAR2 プロトコル パックをアップグレードするには、次の手順に従います。

始める前に

[Software Download] ページからプロトコル パックをダウンロードし、ブートフラッシュにコピーします。https://software.cisco.com/download/home

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ip nbar protocol-pack bootflash:***pack-name* 例： `Device(config)# ip nbar protocol-pack bootflash:mypp.pack`	プロトコル パックをロードします。

カスタム アプリケーションの設定

カスタム アプリケーションを設定するには、次の手順に従います。

（注） カスタム アプリケーション ルールを追加すると、それらのルールに一致する新しいフローのみが表示されます。既存のフローは、引き続きデフォルトの NBAR ルールで識別されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ip nbar custom** *custom-protocol* **http host** *host-string* 例： `Device(config)# ip nbar custom myapp`	カスタム プロトコルを設定し、HTTP ホストを設定します。 （注） カスタム アプリケーションは、組み込みプロトコルより優先されます。
ステップ 3	次のコマンドの 1 つを実行します。 • **http host** *host-name* • **ip address** *ip-address* 例： `Device(config-custom)# http host www.cisco.com` `Device(config-custom)# ip address 8.9.71.50 8.9.71.11 8.9.71.14`	IP プロトコルに基づいて HTTP ホストまたはカスタム プロトコルを設定します。

	コマンドまたはアクション	目的
ステップ 4	**port** *port-no* 例： `Device(config-custom)# port 1111`	使用するポート番号を設定します。
ステップ 5	**dscp** *dscp-value* 例： `Device(config-custom)# dscp 0`	DSCP を設定します。
ステップ 6	**direction any** 例： `Device(config-custom)# direction any`	フローの方向を設定します。

次のタスク

NBAR2 の詳細については、次の「NBAR Configuration Guide」を参照してください：
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_nbar/configuration/xe-3s/qos-nbar-xe-3s-book.html

第 48 章

条件付きデバッグとラジオアクティブ トレース

条件付きデバッグの概要

条件付きデバッグ機能によって、定義した条件に基づき、特定の機能のデバッグおよびロギングを選択して有効にすることができます。この機能は、多くの機能がサポートされているシステムで有用です。

条件付きデバッグでは、多数の機能が導入されていて大規模に稼働しているネットワークにおけるきめ細かなデバッグが可能です。これにより、システム内の細かなインスタンスに対しても、詳細なデバッグを実行できます。これは、何千ものセッションのうちの特定のセッションのみをデバッグするような場合に、非常に有用です。条件は複数指定することもできます。

条件とは、機能またはアイデンティティをいいます。アイデンティティは、インターフェイス、IP アドレス、MAC アドレスなどです。

これは、処理する機能オブジェクトを区別せずに出力を生成する、一般的なデバッグ コマンドとは対照的です。一般的なデバッグ コマンドは、多数のシステム リソースを消費し、システム パフォーマンスに影響します。

ラジオアクティブ トレースの概要

ラジオアクティブ トレース（RA）により、冗長性のレベルを高めた状態で、システムの全体にわたって目的とする動作を連鎖的に実行できます。また、複数のスレッド、プロセス、および関数呼び出しにわたって、デバッグ情報を条件に基づいて（DEBUG レベルまで、または指定のレベルまで）出力する方法を提供します。

（注）

- ラジオアクティブ トレースではファーストホップ セキュリティ（FHS）がサポートされています。

  ファースト ホップ セキュリティ機能の詳細については、[System Management] > [Wireless Multicast] > [Information About Wireless Multicast] > [Information About IPv6 Snooping] を参照してください。

- 証明書が有効でない場合、ラジオアクティブ トレース フィルタは機能しません。
- メッシュ機能の問題を効果的にデバッグできるようにするため、ログの収集時に、イーサネット アドレスと無線 MAC アドレスの両方を RA トレースの条件付き MAC として追加してください。
- ワイヤレス IP のデバッグを有効にするには、**debug platform condition feature wireless ip** *ip-address* コマンドを使用します。

表 *10*：無線アクティブ トレースをサポートするコンポーネント

コンポーネント	詳細
SISF または FHS	ファーストホップ セキュリティ機能。Pv6 アドレス収集とIPv6デバイス トラッキングを含みます。詳細については、「IPv6 スヌーピングに関する情報」を参照してください。
LISP	Locator/ID Separation Protocol。

条件付きデバッグおよび放射線トレース

条件付きデバッグと組み合わせた放射線トレースによって、条件に関連するすべての実行コンテキストをデバッグする単一のデバッグCLIを取得できます。これは、ボックス内の機能のさまざまな制御フロー プロセスを認識していなくても行うことができ、これらのプロセスでデバッグを個別に発行する必要もありません。

トレースファイルの場所

デフォルトでは、トレースファイル ログは各プロセスで生成され、**/tmp/rp/trace** または **/tmp/fp/trace** ディレクトリに保存されます。この一時ディレクトリで、トレース ログがファイルに書き込まれます。各ファイルは 1 MB サイズです。これらのログ（プロセス単位）は **show platform software trace message** *process_name* **chassis active R0** コマンドを使用して確認できます。このディレクトリでは、特定のプロセスのこうしたファイルを、最大 25 件保持できます。**/tmp** ディレクトリのトレースファイルがその 1 MB 制限またはブート時に設定されたサイズに達した場合、ローテーションから外れ、**tracelogs** ディレクトリの **/crashinfo** パーティションの下にあるアーカイブの場所に移動します。

/tmp ディレクトリが 1 つのプロセスで保持するトレースファイルは 1 つのみです。ファイルがそのファイル サイズの制限に達すると、ローテーションから外れ、**/crashinfo/tracelogs** に移動します。アーカイブ ディレクトリに蓄積されるファイルは最大 25 ファイルであり、その後は最も古いものから順に、**/tmp** から新たにローテーションされたファイルに置換されます。

crashinfo ディレクトリ内のトレースファイルは次の形式で配置されます。

1. Process-name_Process-ID_running-counter.timestamp.gz

   例：IOSRP_R0-0.bin_0.14239.20151101234827.gz

2. Process-name_pmanlog_Process-ID_running-counter.timestamp.bin.gz

   例：wncmgrd_R0-0.27958_1.20180902081532.bin.gz

条件付きデバッグの設定

条件付きデバッグを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例**： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**debug platform condition mac** {*mac-address*} **例**： `Device# debug platform condition mac bc16.6509.3314`	ワイヤレス フローで指定された MAC アドレスの条件付きデバッグを設定します。

	コマンドまたはアクション	目的
ステップ 3	**debug platform condition feature wireless mac** {*mac-address*} 例： `Device# debug platform condition feature wireless mac b838.61a1.5433`	指定された MAC アドレスを使用する機能の条件付きデバッグを設定します。
ステップ 4	**debug platform condition start** 例： `Device# debug platform condition start`	条件付きデバッグを開始します（上記のいずれかの条件に一致すると放射線トレースを開始します）。
ステップ 5	**show platform condition** または **show debug** 例： `Device# show platform condition` `Device# show debug`	現在設定されている条件を表示します。
ステップ 6	**debug platform condition stop** 例： `Device# debug platform condition stop`	条件付きデバッグを停止します（放射線トレースを停止します）。
ステップ 7	**request platform software trace archive** [**last** {*number*} **days**] [**target** {*crashinfo:* | *flashinfo:*}] 例： `Device# request platform software trace archive last 2 days`	（任意）システムのマージされたトレースファイルの履歴ログを表示します。日数またはロケーションの組み合わせのフィルタ。
ステップ 8	**request platform software trace filter-binary** {*wire* | *wireless*} [**context** {*mac-address*} | **level** | **module**] 例： `Device# request platform software trace filter-binary wireless context bc16.6509.3314`	（任意）指定された MAC アドレスのコンテキストと情報（ネットワークまたはワイヤレス）を照合するには、モジュールをフィルタリングします。これらのログはオフラインで確認できます。
ステップ 9	**show platform software trace filter-binary wireless** 例： `Device# show platform software trace filter-binary wireless`	（任意）すべての機能によって生成された統合ログを表示します。
ステップ 10	**show platform software trace** [**counter** | **filter-binary**| **level** | **message**] 例： `Device# show platform software trace message`	（任意）最新のトレースファイルからマージされたログを表示します。アプリケーションの状態、トレース モジュール名およびトレース レベルをさ

	コマンドまたはアクション	目的
		まざまな組み合わせでフィルタリングします。 （注） このコマンドは、関係のあるすべてのプロセスから生成されるすべてのログファイルを順に並べて 1 つのログ出力にします。
ステップ 11	**clear platform condition all** 例： `Device# clear platform condition all`	すべての条件をクリアします。

次のタスク

（注） **request platform software trace filter-binary** コマンドと **show platform software trace filter-binary** コマンドは同様の動作をします。唯一の違いは次のとおりです。

- **request platform software trace filter-binary**：データ ソースとして履歴ログを使用します。
- **show platform software trace filter-binary**：データ ソースとしてフラッシュの一時ディレクトリを使用します。

（注） コマンド **request platform software trace filter-binary wireless** {*mac-address*} は次の 3 つのフラッシュファイルを生成します。

- *collated_log_<.date..>*
- *mac_log <..date..>*
- *mac_database .. file*

その中でも、*mac_log <..date..>* は、デバッグする MAC 用のメッセージを伝えるため、最も重要なファイルです。コマンド **show platform software trace filter-binary** も同じフラッシュ ファイルを生成し、また、画面に mac_log を出力します。

L2 マルチキャストの放射線トレース

特定のマルチキャスト受信者を特定するには、参加者または受信側クライアントの MAC アドレス、グループのマルチキャスト IP アドレスおよびスヌーピング VLAN を指定します。また、

デバッグのトレース レベルを有効にします。デバッグ レベルでは、詳細なトレースとシステムへの高い可視性が提供されます。

debug platform condition feature multicast controlplane mac *client MAC address* **ip** *Group IP address* **vlan** *id* **level** *debug level*

トレース ファイルの推奨ワークフロー

トレース ファイルの推奨ワークフローの概要は次のとおりです。

1. 特定の時間帯のトレースログを要求する場合。

   たとえば 1 日。

   使用するコマンドは、次のとおりです。

   Device#**request platform software trace archive last 1 day**

2. システムは、/flash: ロケーション内のトレースログの tar ball（.gz ファイル）を生成します。
3. スイッチ外にファイルをコピーします。ファイルをコピーすることによって、オフラインでトレースログが使用できます。ファイルのコピーについての詳細は、次のセクションを参照してください。
4. /flash: location からトレースログファイル（.gz）ファイルを削除します。これにより、他の操作に十分な領域がスイッチに確保されます。

ボックス外へのトレース ファイルのコピー

トレース ファイルの例を以下に示します。

```
Device# dir crashinfo:/tracelogs
Directory of crashinfo:/tracelogs/

50664 -rwx 760 Sep 22 2015 11:12:21 +00:00 plogd_F0-0.bin_0.gz
50603 -rwx 991 Sep 22 2015 11:12:08 +00:00 fed_pmanlog_F0-0.bin_0.9558.20150922111208.gz
50610 -rw- 11 Nov 2 2015 00:15:59 +00:00 timestamp
50611 -rwx 1443 Sep 22 2015 11:11:31 +00:00
auto_upgrade_client_sh_pmanlog_R0-.bin_0.3817.20150922111130.gz
50669 -rwx 589 Sep 30 2015 03:59:04 +00:00 cfgwr-8021_R0-0.bin_0.gz
50612 -rwx 1136 Sep 22 2015 11:11:46 +00:00 reflector_803_R0-0.bin_0.1312.20150922111116.gz
50794 -rwx 4239 Nov 2 2015 00:04:32 +00:00 IOSRP_R0-0.bin_0.14239.20151101234827.gz
50615 -rwx 131072 Nov 2 2015 00:19:59 +00:00 linux_iosd_image_pmanlog_R0-0.bin_0
```

トレース ファイルは、次に示すさまざまなオプションのいずれかを使用して、コピーできます。

```
Device# copy crashinfo:/tracelogs ?
  crashinfo: Copy to crashinfo: file system
```

```
  flash: Copy to flash: file system
  ftp: Copy to ftp: file system
  http: Copy to http: file system
  https: Copy to https: file system
  null: Copy to null: file system
  nvram: Copy to nvram: file system
  rcp: Copy to rcp: file system
  running-config Update (merge with) current system configuration
  scp: Copy to scp: file system
  startup-config Copy to startup configuration
  syslog: Copy to syslog: file system
  system: Copy to system: file system
  tftp: Copy to tftp: file system
  tmpsys: Copy to tmpsys: file system
```

TFTP サーバにコピーするための一般的な構文は次のとおりです。

```
Device# copy source: tftp:
Device# copy crashinfo:/tracelogs/IOSRP_R0-0.bin_0.14239.20151101234827.gz tftp:
Address or name of remote host []? 2.2.2.2
Destination filename [IOSRP_R0-0.bin_0.14239.20151101234827.gz]?
```

（注） tracelogおよび他の目的に使用可能な空き容量があることを確認するために、生成されたレポート/アーカイブ ファイルをスイッチからクリアすることが重要です。

条件付きデバッグの設定例

次に、*show platform condition* コマンドの出力例を示します。

```
Device# show platform condition
Conditional Debug Global State: Stop
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|-----------------------|---------------------------------
Device#
```

次に、*show debug* コマンドの出力例を示します。

```
Device# show debug
IOSXE Conditional Debug Configs:
Conditional Debug Global State: Start
Conditions Direction
------------------------------------------------------------------------------------------|---------
MAC Address 0024.D7C7.0054 N/A
Feature Condition Type Value
----------------------|-----------------------|---------------------------------
Packet Infra debugs:
Ip Address Port
------------------------------------------------------|----------
Device#
```

条件付きデバッグの確認

次の表に、条件付きデバッグの確認に使用できる各種コマンドを示します。

コマンド	目的
show platform condition	現在設定されている条件を表示します。
show debug	現在設定されているデバッグ条件を表示します。
show platform software trace filter-binary	最新のトレース ファイルからマージされたログを表示します。
request platform software trace filter-binary	システムにマージされたトレース ファイルの履歴ログを表示します。

例：SISF のラジオアクティブ トレース ログの確認

次に、*show platform software trace message ios chassis active R0 | inc sisf* コマンドの出力例を示します。

```
Device# show platform software trace message ios chassis active R0 | inc sisf

2017/10/26 13:46:22.104 {IOSRP_R0-0}{1}: [parser]: [5437]:  UUID: 0, ra: 0 (note):  CMD:
 'show platform software trace message ios switch active R0 | inc sisf' 13:46:22 UTC Thu
 Oct 26 2017
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):   FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Unlocking, count is now 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):   FF8E802918 semaphore system unlocked
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Unlocking, count is now 1
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Setting State to 2
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Start timer 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc  Timer value/granularity for 0 :299998/1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Updated Mac Timer : 299998
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Before Timer :  350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Timer 0, default value is 350000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):   Allocating timer wheel for 0
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc No timer running
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
(debug):  Granularity for timer MAC_T1  is 1000
2017/10/26 13:46:10.667 {IOSRP_R0-0}{1}: [sisf]: [5437]:  UUID: 4800000000060, ra: 7
```

```
(debug):  Gi1/0/5 vlan 10 aaaa.bbbb.cccc Current State :MAC-STALE, Req Timer : MAC_T1
Current Timer MAC_T1
```

第 49 章

アグレッシブ クライアント ロード バランシング

アグレッシブ クライアント ロード バランシングの設定について

シスコ ワイヤレス コントローラでアグレッシブ ロード バランシングを有効にすると、ワイヤレス クライアントの負荷を Lightweight アクセス ポイント間で分散することができます。

ワイヤレス クライアントが Lightweight アクセス ポイントへのアソシエートを試みると、アソシエートされた応答パケットとともに 802.11 応答パケットがクライアントに送信されます。この 802.11 応答パケットの中にステータス コード 17 があります。このコード 17 は AP がビジー状態であることを示します。AP のしきい値に達成しなければ、AP からは「success」を示す応答は返りません。AP 使用率のしきい値を超えると、コード 17（AP ビジー）が返り、処理能力に余裕がある別の AP がクライアント要求を受け取ります。

たとえば、AP1 上のクライアント数が、AP2 のクライアント数とロード バランシング ウィンドウを上回っている場合は、AP1 の負荷は AP2 よりも高いと判断されます。クライアントは、AP1 にアソシエートしようとするときに、ステータス コード 17 が含まれている 802.11 応答パケットを受け取ります。アクセス ポイントの負荷が高いことがこのステータス コードからわかるので、クライアントは別のアクセス ポイントへのアソシエーションを試みます。

コントローラは、クライアントアソシエーションを 10 回まで拒否するように設定できます（クライアントがアソシエーションを 11 回試みた場合、11 回目の試行時にアソシエーションが許可されます）。また、特定の WLAN 上でロード バランシングを有効にするか、無効にするかも指定できます。これは、特定のクライアント グループ（遅延に敏感な音声クライアントなど）に対してロード バランシングを無効にする場合に便利です。

（注） 300 ミリ秒を超えて遅延を設定すると、音声クライアントは認証しません。これを避けるには、中央認証（Cisco Centralized Key Management（CCKM）による WLAN のローカルスイッチング）を設定し、AP と WLC 間に遅延 600 ms（UP と DOWN それぞれ 300 ms）の pagent ルータを設定して、音声クライアントのアソシエートを試みます。

（注） FlexConnect AP の場合は、アソシエーションがローカルに処理されます。ロードバランシングの判断は、Cisco WLC で行われます。FlexConnect AP は、Cisco WLC の計算結果を確認する前に、最初の応答をクライアントに返します。FlexConnect AP がスタンドアロン モードの場合は、ロード バランシングが適用されません。

FlexConnect AP は、ローカル モードの AP と同様のロード バランシング用のステータス 17 で（再）アソシエーション応答を送信しません。代わりに、ステータス 0（成功）で（再）アソシエーションを送信してから、理由 5 で認証解除を送信します。

アグレッシブ クライアント ロード バランシングの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [WLANs] > [Wireless Networks] の順に選択します。

ステップ 2 [WLAN] を選択して、[Edit WLAN] ウィンドウを表示します。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [Load Balance] チェックボックスをオンにして機能を有効にします。

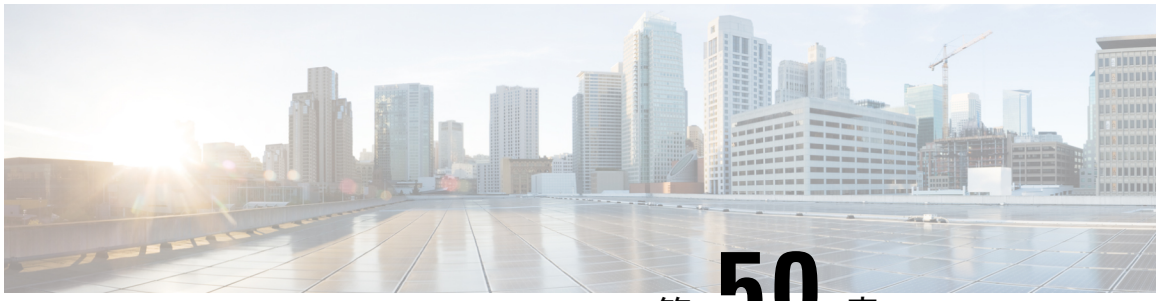
ステップ 5 [Update & Apply to Device] をクリックします。

アグレッシブ クライアント ロード バランシングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device # 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 3	**wlan** *wlan-name* 例： `Device (config)# wlan test-wlan`	*wlan-name* には WLAN 名を入力します。
ステップ 4	**shutdown** 例： `Device (config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 5	**load-balance** 例： `Device (config-wlan) # load-balance`	特定の WLAN へのクライアント ロードバランスを有効にするために、ゲスト コントローラをモビリティ コントローラとして設定します。 WLAN の要件として WLAN のセキュリティ設定を設定します。
ステップ 6	**no shutdown** 例： `Device (config-wlan)# no shutdown`	WLAN を有効にします。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**configure terminal** 例： `Device # 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。

	コマンドまたはアクション	目的
ステップ 9	**wireless load-balancing window** *number-of-clients(0-20)* 例： `Device (config) # wireless load-balancing window 2`	クライアント数を [Aggressive Load Balancing] ウィンドウで設定します。
ステップ 10	**wireless load-balancing denial** *load-balancing-denial-count(1-10)* 例： `Device (config) # wireless load-balancing denial 5`	ロードバランシングのクライアント拒否回数を設定します。ロードバランシングの拒否回数を入力します。
ステップ 11	**end** 例： `Device (config-wlan) # end`	特権 EXEC モードに戻ります。
ステップ 12	**show running-config | section** *wlan-name* 例： `Device# show running-config | section test-wlan`	現在の設定のフィルタリングされたセクションを表示します。



第 50 章

アカウンティング ID リスト

アカウンティング ID リストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。

ステップ 2 [Accounting] セクションで、[Add] をクリックします。

ステップ 3 表示される [Quick Setup: AAA Accounting] ウィンドウに、メソッド リストの名前を入力します。

ステップ 4 [Type] ドロップダウン リストで、認証タイプとして ID を選択します。

ステップ 5 [Available Server Groups] リストで、ネットワークへのアクセスの認証に使用するサーバ グループを選択し、[>] アイコンをクリックして [Assigned Server Groups] リストに移動します。

ステップ 6 [Save & Apply to Device] をクリックします。

アカウンティング ID リストの設定（CLI）

アカウンティングは、ユーザの操作をロギングしてユーザのネットワーク使用状況を追跡するプロセスです。ユーザによる操作が正常に実行されるとそのたびに、RADIUS アカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明が、ログに記録されます。

アカウンティング ID リストを設定するには、次の手順に従います。

始める前に

RADIUS サーバと AAA サーバ グループを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa accounting identity** *named-list* **start-stop group** *server-group-name* 例： `Device(config)# aaa accounting identity user1 start-stop group aaa-test`	アカウンティングを有効にして、クライアントが承認されたときに start-record アカウンティング通知を送信し、最後に stop-record を送信できるようにします。 （注） 名前付きリストの代わりにデフォルトのリストを使用することもできます。

クライアント属性が変更された場合（たとえば、IPアドレスの変更、クライアントのローミングなど）はそのたびに、アカウンティングの中間アップデートがRADIUSサーバに送信されます。

クライアント アカウンティングの設定（GUI）

手順

	コマンドまたはアクション	目的
ステップ 1	**[Configuration]** > **[Security]** > **[AAA]** の順にクリックします。	
ステップ 2	**[AAA Method List]** > **[Accounting]** をクリックし、[Add] をクリックします。	
ステップ 3	表示される [Quick Setup: AAA Accounting] ウィンドウに、メソッド リストの名前を入力します。	
ステップ 4	ネットワークへのアクセスを許可する前に実行するアカウンティングのタイプを [Type] ドロップダウン リストから選択します。	
ステップ 5	[Type] ドロップダウン リストから、サーバのグループをアクセス サーバとして割り当てるか、またはローカル サーバを使用してアクセスを許可するかを選択します。	

	コマンドまたはアクション	目的
ステップ 6	[Available Server Groups] リストで、ネットワークへのアクセスの追跡に使用するサーバ グループを選択し、クリックして [Assigned Server Groups] リストに移動します。	
ステップ 7	[Save & Apply to Device] をクリックします。	

クライアント アカウンティングの設定（CLI）

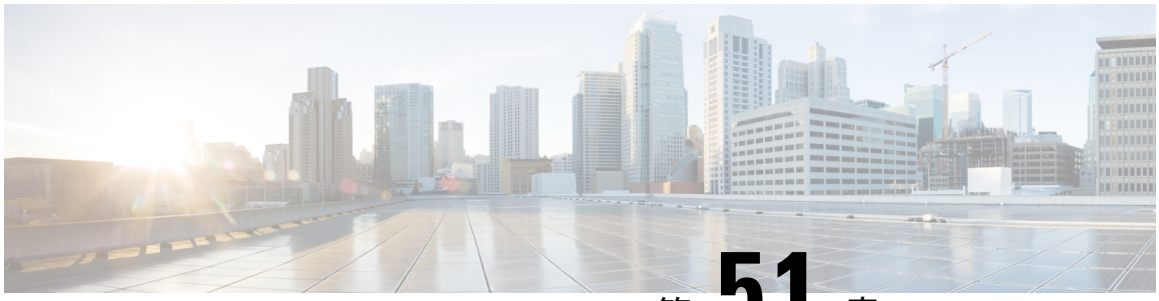
クライアント アカウンティングを設定するには、次の手順に従います。

始める前に

RADIUS アカウンティングが設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *profile-name wlan-identifier ssid* 例： `Device(config)# wlan user1_dot1x 2 user1_network`	WLAN を作成します。 （注） ここでは dot1x WLAN を例として使用します。RADIUS サーバが設定されていれば、他のセキュリティ方式に対してもアカウンティングを有効にすることができます。
ステップ 2	**security dot1x authentication-list** *auth-list-name* 例： `Device(config)# security dot1x authentication-list user1-ext`	dot1x セキュリティ用のセキュリティ認証リストを有効にします。
ステップ 3	**no shutdown** 例： `Device(config)# no shutdown`	WLAN をイネーブルにします。



第 51 章

ワイヤレス マルチキャスト

ワイヤレス マルチキャストに関する情報

ネットワークがパケットのマルチキャストをサポートしている場合は、deviceが使用するマルチキャストの方法を設定できます。deviceは次の2つのモードでマルチキャストを実行します。

- ユニキャスト モード：deviceは、deviceにアソシエートしているすべてのアクセス ポイントに、すべてのマルチキャストパケットをユニキャストします。このモードは非効率的ですが、マルチキャストをサポートしていないネットワークでは必要です。
- マルチキャスト モード：deviceは、マルチキャスト パケットを CAPWAP マルチキャスト グループに送信します。この方法では、device プロセッサのオーバーヘッドが軽減され、パケット レプリケーションの処理がネットワークに移されます。これは、ユニキャストを使った方法よりはるかに効率的です。

Flexconnect モードには、ローカル スイッチングと中央スイッチングという 2 つのサブモードがあります。ローカル スイッチング モードでは、データ トラフィックは AP レベルでスイッチングされ、コントローラはマルチキャスト トラフィックを認識しません。中央スイッチング モードでは、マルチキャスト トラフィックがコントローラに到達します。ただし、IGMP スヌーピングは AP で行われます。

マルチキャスト モードが有効な場合に、deviceがマルチキャスト パケットを有線 LAN から受信すると、deviceは CAPWAP を使用してパケットをカプセル化し、CAPWAP マルチキャスト グループ アドレスへ転送します。deviceは、必ず管理 VLAN を使用してマルチキャスト パケットを送信します。マルチキャスト グループのアクセス ポイントはパケットを受け取り、クラ

イアントがマルチキャスト トラフィックを受信する LAN にマップされたすべての BSSID にこれを転送します。

deviceは、マルチキャスト リスナー検出（MLD）v1 スヌーピングを含む IGMP v1 のすべての機能をサポートしますが、IGMP v2 および IGMP v3 の機能は制限されます。この機能により、IPv6 マルチキャスト フローが追跡され、フローを要求したクライアントにそれらが配信されます。IPv6 マルチキャストをサポートするには、グローバル マルチキャスト モードを有効にする必要があります。

マルチキャスト パケットのダイレクトを向上させるために、インターネット グループ管理プロトコル（IGMP）スヌーピングを導入しています。この機能が有効になっている場合、device スヌーピングは IGMP レポートをクライアントから収集して処理し、レイヤ 3 マルチキャスト アドレスと VLAN 番号に基づいて一意なマルチキャスト グループ ID（MGID）を作成し、その IGMP レポートを IGMP クエリアへ送信します。次に、deviceは、アクセス ポイント上のアクセス ポイント MGID テーブルを、クライアント MAC アドレスを使用して更新します。device は、特定のマルチキャスト グループのマルチキャスト トラフィックを受信すると、それをすべてのアクセス ポイントに転送します。ただし、アクティブなクライアントでリッスンしているアクセス ポイント、またはそのマルチキャスト グループへ加入しているアクセス ポイントだけは、その特定の WLAN 上でマルチキャスト トラフィックを送信します。IP パケットは、入力 VLAN および宛先マルチキャスト グループの一意の MGID を使用して転送されます。レイヤ 2 マルチキャスト パケットは、入力 VLAN の一意の MGID を使用して転送されます。

MGID は、CAPWAP ヘッダー内のワイヤレス情報の 16 ビットの予約済みフィールドに入力された 14 ビットの値です。残りの 2 ビットはゼロに設定する必要があります。

マルチキャスト最適化

マルチキャストは、マルチキャスト アドレスと VLAN を 1 つのエンティティ（MGID）としてグループ化することを基本としていました。VLAN グループで、重複したパケットが増加する可能性があります。VLAN グループ機能を使用して、すべてのクライアントがそれぞれ異なる VLAN 上でマルチキャスト ストリームをリッスンします。そのため、deviceは、マルチキャスト アドレスと VLAN の組み合わせごとに異なる MGID を作成します。したがって、アップストリーム ルータは VLAN ごとにコピーを 1 つ送信します。結果的に、グループ内に存在する VLAN の数だけコピーが作成されます。WLAN はすべてのクライアントに対して同じままなので、マルチキャスト パケットの複数のコピーがワイヤレス ネットワークで送信されます。deviceとアクセス ポイント間のワイヤレス メディアでマルチキャスト ストリームの重複を抑制する目的で、マルチキャスト最適化機能を使用できます。

マルチキャスト最適化では、マルチキャスト トラフィック用に使用可能なマルチキャスト VLAN を作成できます。device内の VLAN の 1 つを、マルチキャスト グループが登録されるマルチキャスト VLAN として設定できます。クライアントは、マルチキャスト VLAN 上でマルチキャスト ストリームをリッスンできます。MGID は、マルチキャスト VLAN とマルチキャスト IP アドレスを使用して生成されます。同じ WLAN の異なる VLAN 上にある複数のクライアントが単一のマルチキャスト IP アドレスをリッスンしている場合、単一の MGID が生成されます。deviceは、この VLAN グループ上のクライアントからのすべてのマルチキャスト ストリームが常にマルチキャスト VLAN 上に送出されるようにして、その VLAN グループのすべての VLAN に対し、アップストリーム ルータに登録されるエントリが 1 つになるようにしま

す。クライアントが異なる VLAN 上にあっても、1 つのマルチキャスト ストリームだけが VLAN グループにヒットします。したがって、ネットワークで送信されるマルチキャスト パケットは、1 つのストリームだけになります。

IPv6 グローバル ポリシー

IPv6 グローバル ポリシーは、ストレージおよびアクセス ポリシー データベースのサービスを提供します。IPv6 ND 検査と IPv6 RA ガードは、IPv6 グローバル ポリシー機能です。ND インスペクションまたは RA ガードをグローバルに設定するたびに、ポリシーの属性が、ソフトウェア ポリシー データベースに保存されます。その後ポリシーはインターフェイスに適用され、ポリシーが適用されたこのインターフェイスを含めるためにソフトウェア ポリシー データベース エントリが更新されます。

IPv6 スヌーピングに関する情報

IPv6 ネイバー ディスカバリ ネイバー インスペクション

IPv6 ネイバー探索インスペクション、または IPv6「スヌーピング」機能によって、複数のレイヤ 2 IPv6 ファーストホップ セキュリティ機能（IPv6 アドレス収集と IPv6 デバイス トラッキングを含む）がバンドルされます。IPv6 ネイバー探索（ND）インスペクションは、レイヤ 2（またはレイヤ 2 とレイヤ 3 の間）で動作し、IPv6 の機能にセキュリティと拡張性を提供します。この機能によって、Duplicate Address Detection（DAD）、アドレス解決、デバイス検出やネイバー キャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

IPv6 ND インスペクションは、レイヤ 2 ネイバー テーブルのステートレス自動設定アドレスのバインディングを学習して保護し、信頼できるバインディング テーブルを構築するために ND メッセージを分析します。有効なバインディングのない IPv6 ND メッセージはドロップされます。ND メッセージは、その IPv6 から MAC へのマッピングが検証可能な場合に信頼できると見なされます。この機能によって、Duplicate Address Detection（DAD）、アドレス解決、デバイス検出やネイバー キャッシュに対する攻撃といった、ネイバー探索メカニズムに固有のいくつかの脆弱性が軽減されます。

ターゲット（プラットフォームのターゲット サポートによって異なり、デバイス ポート、スイッチ ポート、レイヤ 2 インターフェイス、レイヤ 3 インターフェイス、および VLAN が含まれることがある）に IPv6 ND インスペクションが設定されている場合、IPv6 トラフィックの ND プロトコルと Dynamic Host Configuration Protocol（DHCP）をルーティング デバイスのスイッチ統合セキュリティ機能（SISF）インフラストラクチャにリダイレクトするためのキャプチャ命令がハードウェアにダウンロードされます。ND トラフィックの場合、NS、NA、RS、RA、REDIRECT などのメッセージが SISF にリダイレクトされます。DHCP の場合、ポート 546 または 547 から送信された UDP メッセージがリダイレクトされます。

IPv6 ND インスペクションはその「キャプチャ ルール」を分類子に登録します。分類子では、特定のターゲットにあるすべての機能のルールがすべて集約され、対応する ACL がプラットフォーム依存モジュールにインストールされます。分類子は、リダイレクトされたトラフィックを受信すると、（トラフィックを受信しているターゲットに対して）登録されているすべて

の機能からすべてのエントリ ポイント（IPv6 ND インスペクションのエントリ ポイントを含む）を呼び出します。このエントリ ポイントは最後に呼び出されるため、他の機能によって行われた決定が IPv6 ND インスペクションの決定よりも優先されます。

IPv6 デバイス トラッキング

IPv6 デバイス トラッキングは、IPv6 ホストが非表示になったときにネイバー テーブルを即時に更新できるように、IPv6 ホストの活性トラッキングを提供します。

IPv6 ファーストホップ セキュリティ バインディング テーブル

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能を使用すると、デバイスのリブート時にバインディング テーブルをリカバリできます。デバイスに接続されている IPv6 ネイバーのデータベース テーブルは、ND スヌーピングなどの情報源から作成されます。このデータベース（またはバインディング）テーブルは、スプーフィングやリダイレクト攻撃を防止するために、リンク層アドレス（LLA）、IPv4 または IPv6 アドレス、およびネイバーのプレフィックス バインディングを検証するためにさまざまな IPv6 ガード機能によって使用されます。

このメカニズムにより、デバイスのリブート時にバインディング テーブルをリカバリできます。リカバリ メカニズムは、不明な送信元、（バインディング テーブルにまだ指定されていない送信元や、ND または DHCP グリーニングを使用して学習されていない送信元）からのデータ トラフィックをブロックします。この機能は、宛先ガードで宛先アドレスの解決に失敗したときに、不足しているバインディング テーブルのエントリをリカバリします。障害が発生すると、バインディング テーブルのエントリは、設定に応じて、DHCP サーバまたは宛先ホストにクエリを実行することでリカバリできます。

リカバリ プロトコルとプレフィックス リスト

IPv6 ファーストホップ セキュリティ バインディング テーブルのリカバリ メカニズム機能は、DHCP と NDP の両方でリカバリを試みる前に、一致するプレフィックス リストを提供する機能を導入します。

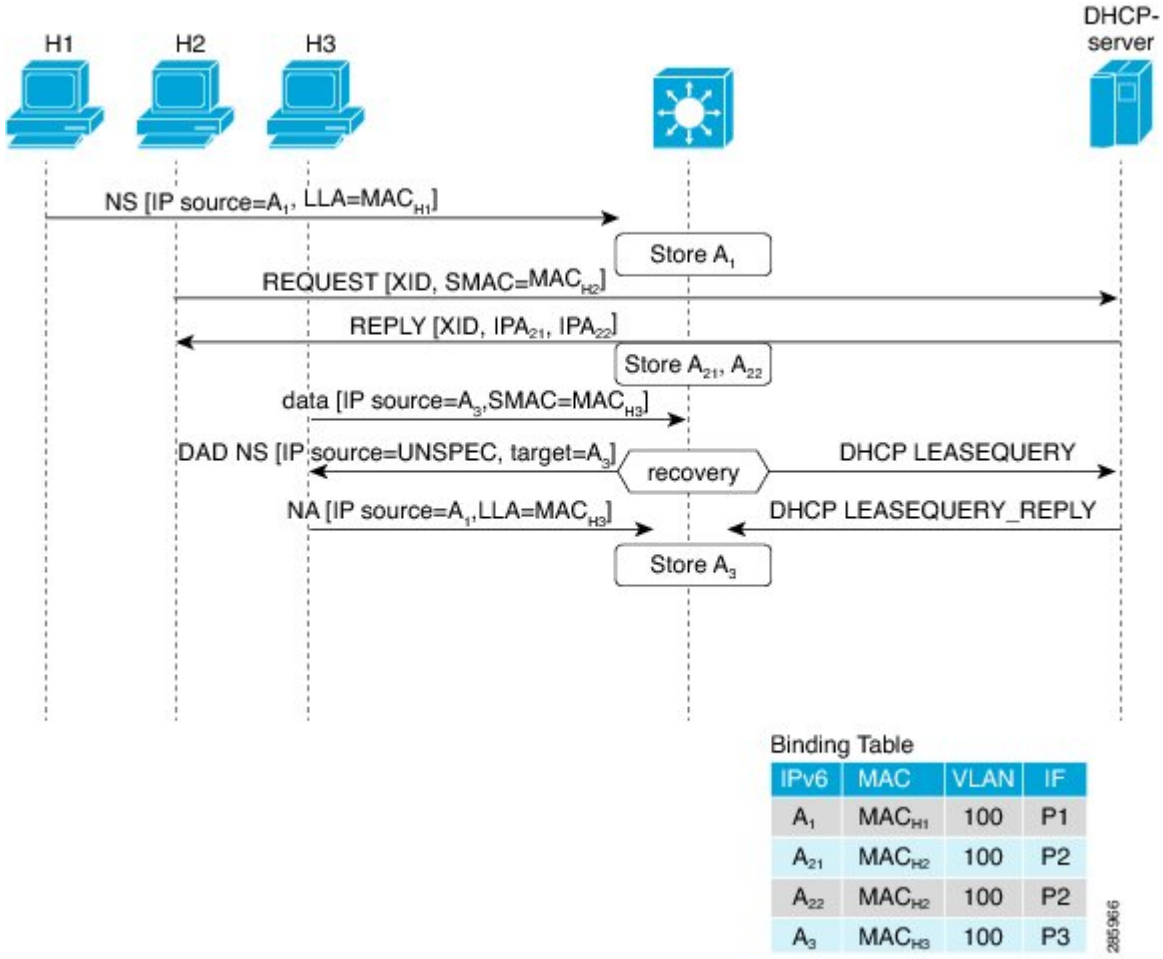
アドレスがプロトコルと関連付けられているプレフィックス リストと一致しない場合、そのプロトコルではバインディング テーブル エントリのリカバリは試行されません。プレフィックス リストは、プロトコルを使用してレイヤ 2 ドメインに割り当てられているアドレスに対して有効なプレフィックスに対応している必要があります。デフォルトではプレフィックス リストは存在せず、すべてのアドレスのリカバリが試行されます。プロトコルにプレフィックス リストを関連付けるコマンドは、**protocol** {**dhcp** | **ndp**} [**prefix-list** *prefix-list-name*] です。

IPv6 アドレス収集

IPv6 アドレス収集は、正確なバインディング テーブルに依存するその他多くの IPv6 の機能の基盤です。この機能は、アドレス収集のためにリンク上の ND および DHCP メッセージを検査した後に、それらのアドレスをバインディング テーブルに入力します。また、この機能は、アドレスの所有権を強制し、特定のノードが要求可能なアドレスの数を制限します。

次の図は、IPv6 アドレス収集の仕組みを示しています。

図 *5 : IPv6* アドレス収集



IPv6 RA ガード

IPv6 RA ガード機能は、ネットワーク デバイス プラットフォームに到着した不要または不正なRAガードメッセージを、ネットワーク管理者がブロックまたは拒否できるようにするためのサポートを提供します。RA は、リンクで自身をアナウンスするためにデバイスによって使用されます。IPv6 RA ガード機能は、それらの RA を分析して、承認されていないデバイスから送信された RA を除外します。ホスト モードでは、ポート上の RA とルータ リダイレクト メッセージはすべて許可されません。RA ガード機能は、レイヤ 2（L2）デバイスの設定情報を、受信した RA フレームで検出された情報と比較します。L2 デバイスは、RA フレームとルータ リダイレクト フレームの内容を設定と照らし合わせて検証した後で、RA をユニキャストまたはマルチキャストの宛先に転送します。RA フレームの内容が検証されない場合は、RA はドロップされます。

ワイヤレス展開では、ワイヤレス ポートで受信したRAはドロップされます。ルータはこれらのインターフェイスに存在できないためです。

ワイヤレス マルチキャスト設定の前提条件

- IP マルチキャスティングに加入するには、マルチキャスト ホスト、ルータ、およびマルチレイヤ スイッチで IGMP が動作している必要があります。
- device上でマルチキャスト モードを有効にする場合は、CAPWAP マルチキャスト グループアドレスも設定する必要があります。アクセス ポイントは、IGMP を使用して CAPWAP マルチキャスト グループをリッスンします。

ワイヤレス マルチキャスト設定の制約事項

次は、IP マルチキャスト ルーティングの設定の制約事項です。

- 監視モード、スニファ モード、または不正検出モードのアクセス ポイントは、CAPWAP マルチキャスト グループ アドレスには加入しません。
- 上で設定されている CAPWAP マルチキャスト グループは、devicesごとに異なっている必要があります。
- マルチキャスト ルーティングは、管理インターフェイスには有効にしないでください。

IPv6 スヌーピングの制限

IPv6 スヌーピング機能は、EtherChannel ポートではサポートされません。

IPv6 RA ガードの制限

- IPv6 RA ガード機能は、IPv6 トラフィックがトンネリングされる環境では保護を行いません。
- この機能は、TCAM（Ternary Content Addressable Memory）がプログラムされているハードウェアでのみサポートされています。
- この機能は、入力方向のスイッチ ポート インターフェイスで設定できます。
- この機能は、ホスト モードとルータ モードをサポートしています。
- この機能は、入力方向だけでサポートされます。出力方向ではサポートされません。
- この機能は、EtherChannel および EtherChannel ポート メンバーではサポートされません。
- この機能は、マージ モードのトランク ポートではサポートされません。
- この機能は、補助 VLAN およびプライベート VLAN（PVLAN）でサポートされています。PVLAN の場合、プライマリ VLAN の機能が継承され、ポート機能とマージされます。

- IPv6 RA ガード機能によってドロップされたパケットはスパニングできます。
- **platform ipv6 acl icmp optimize neighbor-discovery command** が設定されている場合、IPv6 RA ガード機能は設定できず、エラー メッセージが表示されます。このコマンドは、RA ガードの ICMP エントリを上書きするデフォルトのグローバル Internet Control Message Protocol（ICMP）エントリを追加します。

ワイヤレス マルチキャストの設定

ここでは、ワイヤレス マルチキャストのさまざまな設定作業について説明します。

ワイヤレス マルチキャスト MCMC モードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wireless multicast** 例： `Device(config)# wireless multicast` `Device(config)# no wireless multicast`	ワイヤレスクライアントへのマルチキャスト トラフィックを有効にします。デフォルトでは、マルチキャストは無効状態になっています。ワイヤレス クライアントへのマルチキャスト トラフィックを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**wireless multicast** *ip-addr* 例： `Device(config)# wireless multicast 231.1.1.1` `Device(config)# no wireless multicast 231.1.1.1`	マルチキャストオーバーマルチキャストを有効にします。この機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。
ステップ 5	**end** 例：	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押し

	コマンドまたはアクション	目的
	`Device(config)# end`	てコンフィギュレーション モードを終了します。

ワイヤレス マルチキャスト MCUC モードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wireless multicast** 例： `Device(config)# wireless multicast`	ワイヤレスクライアントへのマルチキャスト トラフィックを有効にして、mDNS ブリッジングを有効にします。デフォルトでは、この機能は無効の状態です。ワイヤレス クライアントへのマルチキャスト トラフィックを無効にして、mDNS ブリッジングを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**wireless multicast** *ip-addr* 例： `Device(config)# wireless multicast 231.1.1.1` `Device(config)# no wireless multicast 231.1.1.1`	マルチキャストオーバーマルチキャストを有効にします。この機能をディセーブルにする場合は、このコマンドの **no** 形式を使用します。
ステップ 5	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

IPv6 スヌーピングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ipv6 mld snooping** 例： `Device(config)# ipv6 mld snooping`	MLD スヌーピングをイネーブルにします。

IPv6 スヌーピング ポリシーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ipv6 snooping policy** *policy-name* 例： `Device(config)# ipv6 snooping policy mypolicy`	名前付きの IPv6 スヌーピング ポリシーを設定します。
ステップ 4	**security-level guard** 例： `Device(config-ipv6-snooping)# security-level guard`	未承認のメッセージがある場合にそれらを検査してドロップするためのセキュリティ レベルを設定します。

	コマンドまたはアクション	目的
ステップ5	**device-role node** 例： `Device(config-ipv6-snooping)# device-role node`	接続されたポートに、デバイスのロール（つまり、ノード）を設定します。
ステップ6	**protocol** {**dhcp** | **ndp**} 例： `Device(config-ipv6-snooping)# protocol ndp`	DHCP パケット内または NDP パケット内のいずれかのアドレスを収集するためのプロトコルを設定します。

マルチキャスト ルータ ポートとしてのレイヤ 2 ポートの設定

手順

	コマンドまたはアクション	目的
ステップ1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ2	**configure terminal** 例： `Device# 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3	**ipv6 mld snooping vlan** *vlan-id* **mrouter interface Port-channel** *port-channel-interface-number* 例： `Device(config)# ipv6 mld snooping vlan 2 mrouter interface Port-channel 22`	レイヤ 2 ポートをマルチキャスト ルータ ポートとして設定します。VLAN はクライアント VLAN です。

IPv6 RA ガードの設定

手順

	コマンドまたはアクション	目的
ステップ1	**enable** 例：	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
	`Device> enable`	
ステップ 2	**configure terminal** 例： `Device# 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 3	**ipv6 nd raguard policy** *policy-name* 例： `Device(config)# ipv6 nd raguard policy myraguardpolicy`	RA ガードのポリシーを設定します。
ステップ 4	**trusted-port** 例： `Device(config-nd-raguard)# trusted-port`	信頼できるポートを設定します。
ステップ 5	**device-role** {**host** | **monitor** | **router** | **switch**} 例： `Device(config-nd-raguard)# device-role router`	ポートに接続されているデバイスのロールを設定します。

非 IP ワイヤレス マルチキャストの設定

始める前に

- 非 IP マルチキャスト機能は、デフォルトではグローバルに無効になっています。
- 非 IP マルチキャストの場合、トラフィックが通過できるように、グローバルのワイヤレス マルチキャストを有効にする必要があります。
- ファブリックまたは Flex の展開ではこの機能はサポートされません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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 3	**wireless multicast non-ip** 例： `Device(config)# wireless multicast non-ip` `Device(config)# no wireless multicast non-ip`	すべての VLAN で非 IP マルチキャストを有効にします。デフォルトでは、すべての VLAN の非 IP マルチキャストは無効状態になっています。トラフィックが通過できるように、ワイヤレス マルチキャストを有効にしておく必要があります。すべての VLAN で非 IP マルチキャストを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**wireless multicast non-ip vlan** *vlanid* 例： `Device(config)# wireless multicast non-ip vlan 5` `Device(config)# no wireless multicast non-ip vlan 5`	VLAN ごとに非 IP マルチキャストを有効にします。デフォルトでは、VLAN ごとの非 IP マルチキャストは無効状態になっています。トラフィックが通過できるように、ワイヤレス マルチキャストおよびワイヤレス マルチキャスト非 IP の両方を有効にする必要があります。VLAN ごとに非 IP マルチキャストを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 5	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

ワイヤレス ブロードキャストの設定

始める前に

- この機能は、非 ARP および DHCP ブロードキャスト パケットにのみ適用されます。
- この機能はデフォルトでグローバルに無効に設定されています。
- ファブリックまたは Flex の展開ではこの機能はサポートされません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wireless broadcast** 例： `Device(config)# wireless broadcast` `Device(config)# no wireless broadcast`	ワイヤレス クライアントへのブロードキャスト パケットを有効にします。デフォルトでは、ワイヤレスク ライアントのブロードキャスト パケットは無効状態になっています。**wireless broadcast** を有効にすると、各 VLAN へのブロードキャスト トラフィックが有効になります。ブロードキャスト パケットを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**wireless broadcast vlan** *vlanid* 例： `Device(config)# wireless broadcast vlan 3` `Device(config)# no wireless broadcast vlan 3`	単一の VLAN へのブロードキャスト パケットを有効にします。デフォルトでは、単一の VLAN 機能のブロードキャスト パケットは無効状態になっています。ワイヤレス ブロードキャストは、ブロードキャスティングに対して有効にする必要があります。各 VLAN へのブロードキャスト トラフィックを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 5	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

WLAN の IP マルチキャスト VLAN の設定

始める前に

- ファブリックまたは Flex の展開ではこの機能はサポートされません。

- マルチキャスト VLAN は、AP への IPv4 と IPv6 の両方のマルチキャスト転送に使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**central association** 例： `Device(config-wireless-policy)# central association`	ローカルにスイッチされるクライアントの中央アソシエーションを設定します。
ステップ 4	**central switching** 例： `Device(config-wireless-policy)# central switching`	WLAN を中央スイッチング用に設定します。
ステップ 5	**description** *policy-profile-name* 例： `Device(config-wireless-policy)# description "default policy profile"`	（任意）ポリシー プロファイルの説明を追加します。
ステップ 6	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 32`	プロファイル ポリシーを VLAN に割り当てます。
ステップ 7	**multicast vlan** *vlan-id* 例： `Device(config-wireless-policy)# multicast vlan 84`	WLAN へのマルチキャスト VLAN を設定します。
ステップ 8	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイルポリシーを有効にします。

ワイヤレス マルチキャストの確認

表 *11 :* ワイヤレス マルチキャストを確認するためのコマンド

コマンド	説明
show wireless multicast	マルチキャスト ステータスと IP マルチキャスト モード、各 VLAN のブロードキャストおよび非 IP マルチキャスト ステータスを表示します。また、マルチキャスト ドメイン ネーム システム（mDNS）のブリッジング状態も表示します。
show wireless multicast group summary	すべての（グループおよび VLAN）リストおよび対応する MGID 値を表示します。
show wireless multicast [**source** *source*] **group** *group* **vlan** *vlanid*	指定した (S,G,V) の詳細を表示し、それに関連付けられているすべてのクライアントおよび MC2UC ステータスを示します。
show ip igmp snooping wireless mcast-ipc-count	ワイヤレス コントローラ モジュールに送信される MGID ごとのマルチキャスト IPC の数を表示します。
show ip igmp snooping wireless mgid	MGID マッピングを表示します。
show ip igmp snooping igmpv2-tracking	クライアントから SGV への間マッピングおよび SGV からクライアントへのマッピングを表示します。
show ip igmp snooping querier vlan *vlanid*	指定した VLAN の IGMP クエリア情報を表示します。
show ip igmp snooping querier detail	すべての VLAN の IGMP クエリアについて詳細情報を表示します。
show ipv6 mld snooping querier vlan *vlanid*	指定した VLAN の MLD クエリア情報を表示します。
show ipv6 mld snooping wireless mgid	IPv6 マルチキャスト グループの MGID を表示します。

マルチキャスト VLAN 設定の確認

ポリシー プロファイルに関連付けられているマルチキャスト VLAN と、そのプロファイルに割り当てられている VLAN を表示するには、次のコマンドを使用します。

```
Device# show wireless profile policy detail default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : vlan-pool1
Multicast VLAN        : 84
Client count                  : 0
```

```
Passive Client                  : DISABLED
```

クライアントに関連付けられているマルチキャスト VLAN を表示するには、次のコマンドを使用します。

```
Device# show wireless client mac ac2b.6e4b.551e detail

Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 84.84.0.20
…….
VLAN : 82
Access VLAN : 82
Multicast VLAN: 84
```

マルチキャストを介した IPv6 マルチキャスト

IPv6 マルチキャストオーバーマルチキャスト

IPv6 マルチキャストでは、ホストから単一データ ストリームをすべてのホストのサブネットに同時に送信する（グループ伝送）ことができます。IPv6 マルチキャスト オーバー マルチキャストが設定されると、、すべての AP が IPv6 マルチキャスト アドレスに join し、ワイヤレス コントローラから AP へのマルチキャスト トラフィックが IPv6 マルチキャスト トンネル経由で流れます。

混在環境（IPv4 および IPv6）では、AP が IPv4 または IPv6 を介してワイヤレス コントローラに参加する可能性があります。混在環境でマルチキャストオーバーマルチキャストを有効にするには、IPv4 と IPv6 の両方のマルチキャスト トンネルを設定します。IPv4 AP にはユニキャスト IPv4 CAPWAP トンネルがあり、IPv4 マルチキャスト グループに参加します。IPv6 AP は、ユニキャスト IPv6 CAPWAP トンネルを持ち、IPv6 マルチキャスト グループに参加します。

（注） IPv4 と IPv6 を介したマルチキャスト オーバー ユニキャストとマルチキャスト オーバー マルチキャストの混合モードは、Cisco IOS XE Gibraltar 16.10.1 ではサポートされていません。

表 *12:* プラットフォームごとのマルチキャストのサポート

プラットフォーム	マルチキャストのサポート：マルチキャスト オーバー ユニキャスト	マルチキャストのサポート：マルチキャスト オーバー マルチキャスト
Cisco Catalyst 9800-40 ワイヤレス コントローラ	なし	あり

プラットフォーム	マルチキャストのサポート：マルチキャストオーバーユニキャスト	マルチキャストのサポート：マルチキャストオーバー マルチキャスト
Cisco Catalyst 9800-80 ワイヤレス コントローラ	なし	あり
クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ ：小規模テンプレート	対応	対応
クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ ：中規模テンプレート	なし	あり
クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ ：大規模なテンプレート	なし	あり

IPv6 マルチキャストオーバーマルチキャストの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless multicast** {*ipv4-address* | **ipv6** *ipv6-address*) 例： `Device(config)# wireless multicast ipv6 ff45:1234::86`	IPv6マルチキャストオーバーマルチキャスト アドレスを設定します。

IPv6 マルチキャストオーバーマルチキャストの確認

IPv6マルチキャストオーバーマルチキャストの設定を確認するには、次のコマンドを使用します。

```
Device# show wireless multicast

Multicast : Enabled
AP Capwap Multicast : Multicast
AP Capwap IPv4 Multicast group Address : 231.1.1.1
AP Capwap IPv6 Multicast group Address : ff45:1234::86
Wireless Broadcast : Disabled
Wireless Multicast non-ip-mcast : Disabled
```

```
Device# show running-configuration | inc multicast

show run | inc multicast:--

wireless multicast
wireless multicast ipv6 ff45:1234::86
wireless multicast 231.1.1.1
```

Directed Multicast Service

Directed Multicast Service

クライアントで Directed Multicast Service（DMS）機能を使用すると、マルチキャスト パケットをユニキャスト フレームとして送信するようにアクセス ポイント（AP）に要求できます。AP は、この要求を受信すると、クライアントのマルチキャスト トラフィックをバッファリングし、クライアントが起動したときにユニキャストフレームとして送信します。これにより、クライアントはスリープモード（バッテリ電力の節約のため）では無視されていたマルチキャストパケットを受信できるようになり、レイヤ2の信頼性も保証されます。また、ユニキャスト フレームができるだけ高いワイヤレス リンク レートでクライアントに送信されるため、クライアントは無線の持続期間を短縮してパケットをすばやく受信できるようになり、バッテリ電力がさらに節約されます。DMS を使用しない場合、クライアントはマルチキャスト トラフィックを受信するために、Delivery Traffic Indication Map（DTIM）間隔ごとに起動する必要があります。

この機能は次の AP でサポートされています。

- Cisco Aironet 2700 シリーズ AP
- Cisco Aironet 2800 シリーズ AP
- Cisco Aironet 3700 シリーズ AP
- Cisco Aironet 3800 シリーズ AP
- Cisco Aironet 4800 シリーズ AP

Directed Multicast Service の設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [WLANs] > [Wireless Networks] の順に選択します。

ステップ 2 [WLAN] を選択して、[Edit WLAN] ウィンドウを表示します。

ステップ 3 [Advanced] タブをクリックします。

ステップ 4 [Directed Multicast Service] チェック ボックスをオンにして機能を有効にします。

ステップ 5 [Update & Apply to Device] をクリックします。

Directed Multicast Service の設定

始める前に

- この機能は、クライアントからの要求を受信すると有効になります。この機能が WLAN で設定されていることを確認します。
- この機能は、Apple iPad や Apple iPhone などの 802.11v 対応クライアントでのみサポートされています。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name* 例： `Device(config)# wlan test5`	WLAN プロファイルを設定し、WLAN プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN プロファイルを無効にします。
ステップ 4	**dms** 例： `Device(config-wlan)# dms`	WLAN ごとの DMS 処理を設定します。
ステップ 5	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN プロファイルを有効にします。

Directed Multicast Service の設定の確認

コントローラの DMS 設定のステータスを確認するには、次の **show** コマンドを使用します。[IEEE 802.11v Parameters] の下に、DMS ステータスが表示されます。

```
Device# show wlan id 5

WLAN Profile Name     : test
================================================
```

```
Identifier                                      : 5
Network Name (SSID)                             : test
Status                                          : Disabled
Broadcast SSID                                  : Enabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
!
.
.
.
Assisted-Roaming
    Neighbor List                               : Disabled
    Prediction List                             : Disabled
    Dual Band Support                           : Disabled

! DMS status is displayed below.

IEEE 802.11v parameters
    Directed Multicast Service                  : Enabled
    BSS Max Idle                                : Disabled
        Protected Mode                          : Disabled
    Traffic Filtering Service                   : Disabled
    BSS Transition                              : Enabled
        Disassociation Imminent                 : Disabled
            Optimised Roaming Timer             : 40
            Timer                               : 200
    WNM Sleep Mode                              : Disabled
802.11ac MU-MIMO                                : Disabled
802.11ax paramters
    OFDMA Downlink                              : unknown
    OFDMA Uplink                                : unknown
    MU-MIMO Downlink                            : unknown
    MU-MIMO Uplink                              : unknown
    BSS Color                                   : unknown
    Partial BSS Color                           : unknown
    BSS Color Code
```

クライアントのコントローラにおける DMS 設定のステータスを確認するには、次のコマンドを使用します。

```
Device# show wireless client mac-address 6c96.cff2.83a0 detail | inc 11v

11v BSS Transition : implemented
11v DMS Capable : Yes
```

DMS の要求と応答の統計情報を確認するには、次のコマンドを使用します。

```
Device# show wireless stats client detail | inc DMS

Total DMS requests received in action frame      : 0
Total DMS responses sent in action frame         : 0
Total DMS requests received in Re-assoc Request  : 0
Total DMS responses sent in Re-assoc Response    : 0
```

Cisco Aironet 2700 および 3700 シリーズ AP の DMS の設定を確認するには、次のコマンドを使用します。

```
AP# show controllers dot11Radio 0/1 | begin Global DMS

Global DMS - requests:0 uc:0 drop:408
```

```
DMS enabled on WLAN(s): dms-open
 test-open
```

Cisco Aironet 2800、3800、および 4800 シリーズ AP の DMS の設定を確認するには、次のコマンドを使用します。

```
AP# show multicast dms all

 vapid    client               dmsid        TClas
 0       1C:9E:46:7C:AF:C0     1    mask:0x55, version:4, proto:0x11, dscp:0x0, sport:0,
 dport:9, sip:0.0.0.0, dip:224.0.0.251
```

ワイヤレス ブロードキャスト、非IPマルチキャストおよびマルチキャスト VLAN

非 IP ワイヤレス マルチキャストの設定

始める前に

- 非 IP マルチキャスト機能は、デフォルトではグローバルに無効になっています。
- 非 IP マルチキャストの場合、トラフィックが通過できるように、グローバルのワイヤレス マルチキャストを有効にする必要があります。
- ファブリックまたは Flex の展開ではこの機能はサポートされません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wireless multicast non-ip** 例： `Device(config)# wireless multicast non-ip` `Device(config)# no wireless multicast non-ip`	すべての VLAN で非 IP マルチキャストを有効にします。デフォルトでは、すべての VLAN の非 IP マルチキャストは無効状態になっています。トラフィックが通過できるように、ワイヤレス マルチキャストを有効にしておく必要があります。すべての VLAN で非 IP マルチキャ

	コマンドまたはアクション	目的
		ストを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**wireless multicast non-ip vlan** *vlanid* 例： `Device(config)# wireless multicast non-ip vlan 5` `Device(config)# no wireless multicast non-ip vlan 5`	VLAN ごとに非 IP マルチキャストを有効にします。デフォルトでは、VLAN ごとの非 IP マルチキャストは無効状態になっています。トラフィックが通過できるように、ワイヤレス マルチキャストおよびワイヤレス マルチキャスト非 IP の両方を有効にする必要があります。VLAN ごとに非 IP マルチキャストを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 5	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

ワイヤレス ブロードキャストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Services]** > **[Multicast]** を選択します。

ステップ 2 [Multicast] ページで、ワイヤレス クライアントのブロードキャスト パケットを有効にするには、[Wireless Broadcas] のステータスを [enabled] にします。

デフォルト値は [disabled] です。

ステップ 3 VLAN のブロードキャスト パケットを有効にするには、[Disabled VLAN] テーブルから、[Disabled] 状態になっている VLAN ID の隣にある矢印をクリックして [Enabled] 状態にします。

デフォルト値は [disabled] です。

ステップ 4 設定を保存します。

ワイヤレス ブロードキャストの設定

始める前に

- この機能は、非 ARP および DHCP ブロードキャスト パケットにのみ適用されます。

- この機能はデフォルトでグローバルに無効に設定されています。
- ファブリックまたは Flex の展開ではこの機能はサポートされません。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wireless broadcast** 例： `Device(config)# wireless broadcast` `Device(config)# no wireless broadcast`	ワイヤレス クライアントへのブロードキャスト パケットを有効にします。デフォルトでは、ワイヤレスク ライアントのブロードキャスト パケットは無効状態になっています。**wireless broadcast** を有効にすると、各 VLAN へのブロードキャスト トラフィックが有効になります。ブロードキャスト パケットを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 4	**wireless broadcast vlan** *vlanid* 例： `Device(config)# wireless broadcast vlan 3` `Device(config)# no wireless broadcast vlan 3`	単一の VLAN へのブロードキャスト パケットを有効にします。デフォルトでは、単一の VLAN 機能のブロードキャスト パケットは無効状態になっています。ワイヤレス ブロードキャストは、ブロードキャスティングに対して有効にする必要があります。各 VLAN へのブロードキャスト トラフィックを無効にするには、このコマンドの **no** 形式を使用します。
ステップ 5	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了します。あるいは、**Ctrl+Z** キーを押してコンフィギュレーション モードを終了します。

すべてのAPマルチキャストグループに対するマルチキャストオーバーマルチキャストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Services]** > **[Multicast]** を選択します。

ステップ 2 [Multicast] ページで、[P CAPWAP Multicast] ドロップダウン リストから [Multicast] を選択します。これで、すべての AP に単一のパケットを送信するように、すべての AP マルチキャスト グループが設定されます。

ステップ 3 有効な IPv4 または IPv6 AP CAPWAP マルチキャスト グループ アドレスを入力します。これにより、基盤となるすべての AP マルチキャスト グループを介して、すべての AP にクライアント マルチキャスト グループ トラフィックをマルチキャストするためのマルチキャストオーバーマルチキャストが可能になります。

ステップ 4 設定を保存します。

すべてのAPマルチキャストグループに対するマルチキャストオーバーマルチキャストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap capwap multicast** *IP address* 例： `Device(config)# ap capwap multicast 239.4.4.4`	すべての AP に単一のパケットを送信するように、すべての AP マルチキャスト グループを設定します。
ステップ 3	**wireless multicast** *IP address* 例： `Device(config)# wireless multicast 239.4.4.4`	基盤となるすべての AP マルチキャスト グループを介して、すべての AP にクライアント マルチキャスト グループ トラフィックをマルチキャストするためのマルチキャストオーバーマルチキャストを有効にします。 *IP address*：マルチキャストオーバーマルチキャストの IP アドレス。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ワイヤレス マルチキャストの確認

表 *13*：ワイヤレス マルチキャストを確認するためのコマンド

コマンド	説明
show wireless multicast	マルチキャスト ステータスと IP マルチキャスト モード、各 VLAN のブロードキャストおよび非 IP マルチキャスト ステータスを表示します。また、マルチキャスト ドメイン ネーム システム（mDNS）のブリッジング状態も表示します。
show wireless multicast group summary	すべての（グループおよび VLAN）リストおよび対応する MGID 値を表示します。
show wireless multicast [**source** *source*] **group** *group* **vlan** *vlanid*	指定した (S,G,V) の詳細を表示し、それに関連付けられているすべてのクライアントおよび MC2UC ステータスを示します。
show ip igmp snooping wireless mcast-ipc-count	ワイヤレス コントローラ モジュールに送信される MGID ごとのマルチキャスト IPC の数を表示します。
show ip igmp snooping wireless mgid	MGID マッピングを表示します。
show ip igmp snooping igmpv2-tracking	クライアントから SGV への間マッピングおよび SGV からクライアントへのマッピングを表示します。
show ip igmp snooping querier vlan *vlanid*	指定した VLAN の IGMP クエリア情報を表示します。
show ip igmp snooping querier detail	すべての VLAN の IGMP クエリアについて詳細情報を表示します。
show ipv6 mld snooping querier vlan *vlanid*	指定した VLAN の MLD クエリア情報を表示します。
show ipv6 mld snooping wireless mgid	IPv6 マルチキャスト グループの MGID を表示します。

マルチキャスト最適化

マルチキャストは、マルチキャスト アドレスと VLAN を 1 つのエンティティ（MGID）としてグループ化することを基本としていました。VLAN グループで、重複したパケットが増加する可能性があります。VLAN グループ機能を使用して、すべてのクライアントがそれぞれ異なる VLAN 上でマルチキャスト ストリームをリッスンします。そのため、deviceは、マルチキャスト アドレスと VLAN の組み合わせごとに異なる MGID を作成します。したがって、アップストリーム ルータは VLAN ごとにコピーを 1 つ送信します。結果的に、グループ内に存在する VLAN の数だけコピーが作成されます。WLAN はすべてのクライアントに対して同じままなので、マルチキャスト パケットの複数のコピーがワイヤレス ネットワークで送信されます。deviceとアクセス ポイント間のワイヤレス メディアでマルチキャスト ストリームの重複を抑制する目的で、マルチキャスト最適化機能を使用できます。

マルチキャスト最適化では、マルチキャスト トラフィック用に使用可能なマルチキャスト VLAN を作成できます。device内の VLAN の 1 つを、マルチキャスト グループが登録されるマルチキャスト VLAN として設定できます。クライアントは、マルチキャスト VLAN 上でマルチキャスト ストリームをリッスンできます。MGID は、マルチキャスト VLAN とマルチキャスト IP アドレスを使用して生成されます。同じ WLAN の異なる VLAN 上にある複数のクライアントが単一のマルチキャスト IP アドレスをリッスンしている場合、単一の MGID が生成されます。deviceは、この VLAN グループ上のクライアントからのすべてのマルチキャスト ストリームが常にマルチキャスト VLAN 上に送出されるようにして、その VLAN グループのすべての VLAN に対し、アップストリーム ルータに登録されるエントリが 1 つになるようにします。クライアントが異なる VLAN 上にあっても、1 つのマルチキャスト ストリームだけが VLAN グループにヒットします。したがって、ネットワークで送信されるマルチキャスト パケットは、1 つのストリームだけになります。

WLAN の IP マルチキャスト VLAN の設定

始める前に

- ファブリックまたは Flex の展開ではこの機能はサポートされません。
- マルチキャスト VLAN は、AP への IPv4 と IPv6 の両方のマルチキャスト転送に使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**central association** 例： `Device(config-wireless-policy)# central association`	ローカルにスイッチされるクライアントの中央アソシエーションを設定します。
ステップ 4	**central switching** 例： `Device(config-wireless-policy)# central switching`	WLAN を中央スイッチング用に設定します。
ステップ 5	**description** *policy-profile-name* 例： `Device(config-wireless-policy)# description "default policy profile"`	（任意）ポリシー プロファイルの説明を追加します。
ステップ 6	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 32`	プロファイル ポリシーを VLAN に割り当てます。
ステップ 7	**multicast vlan** *vlan-id* 例： `Device(config-wireless-policy)# multicast vlan 84`	WLAN へのマルチキャスト VLAN を設定します。
ステップ 8	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイルポリシーを有効にします。

マルチキャスト VLAN 設定の確認

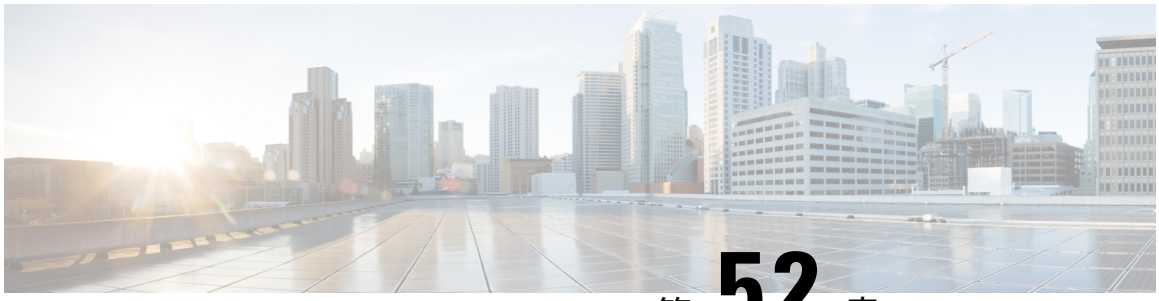
ポリシー プロファイルに関連付けられているマルチキャスト VLAN と、そのプロファイルに割り当てられている VLAN を表示するには、次のコマンドを使用します。

```
Device# show wireless profile policy detail default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : vlan-pool1
Multicast VLAN        : 84
```

```
Client count                  : 0
Passive Client                : DISABLED
```

クライアントに関連付けられているマルチキャスト VLAN を表示するには、次のコマンドを使用します。

```
Device# show wireless client mac ac2b.6e4b.551e detail

Client MAC Address : ac2b.6e4b.551e
Client IPv4 Address : 84.84.0.20
…….
VLAN : 82
Access VLAN : 82
Multicast VLAN: 84
```



第 52 章

サイトごとのマップサーバのサポート

サイトごとのマップ サーバのサポートについて

サイトごとのマップ サーバ機能により、サイトごとのマップサーバと、クライアントのサブネットに基づくマップ サーバの選択がサポートされます。これにより、コントローラは複数のサイトをサポートし、各サイトのトラフィックを分離することができます。

この機能は、Enterprise と Guest の両方のマップ サーバに適用されます。レイヤ 2 仮想拡張可能 LAN ネットワーク識別子ベース（L2VNID ベース）のマップ サーバでは、L2 VNID に基づいて適切なマップ サーバを選択する必要があります。

次のリストに、AP のクエリとクライアントの登録におけるマップ サーバの選択順序を示します。

- L3 ごとの VNID マップ サーバ
- サイトごとの（AP グループ）マップ サーバ
- デフォルトまたはグローバル マップ サーバ

利点

サイトごとのマップ サーバ機能を使用すると次のような利点があります。

- マップ サーバとボーダー ノードの水平スケーリングによる、単一の大規模なサイトを使用できます。
- 複数のサイト間でコントローラを共有できます。各サイトでは、独自のマップサーバと仮想ネットワークまたはVNIDを持つことができ、引き続き各サイトからトラフィックをセグメント化できます。
- Enterpriseマップサーバを分離したまま、複数のサイト間でGuestマップサーバを共有できます。
- 同じ SSID を異なるサイトにわたって使用できます。サイト内では、別の仮想ネットワーク ドメインに属することができます。

デフォルト マップ サーバの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Fabric]** を選択します。
ステップ 2 [Fabric] ページで、[Control Plane] タブをクリックします。
ステップ 3 [Control Plane Name] リストで、[default-control-plane] をクリックします。
ステップ 4 表示される [Edit Control Plane] ウィンドウで、[Add] をクリックします。
ステップ 5 マップ サーバの IP アドレスを入力します。
ステップ 6 [Password Type] を [Unencrypted] または [AES] のいずれかに設定します。
ステップ 7 [Pre Shared Key] を入力します。
ステップ 8 [Save] をクリックします。
ステップ 9 [Update & Apply to Device] をクリックします。

デフォルト マップ サーバの設定（CLI）

デフォルト マップ サーバを設定するには、次の手順に従います。

始める前に

- グローバル マップ サーバは、AP クエリ（AP の join 時）とクライアント登録（クライアントの join 時）の両方に使用されるデフォルトのマップ サーバです。
- LISP コントロールプレーンは本質的に冗長性をサポートしていないため、冗長性を確保するためにマップ サーバをペアで設定することを推奨します。

- マップ サーバ セットを共有するにはマップ サーバ グループを作成します。このグループは、サイト プロファイル、ファブリック プロファイル、レイヤ 2 およびレイヤ 3 VNID 間で共有できるほか、デフォルト マップ サーバとも共有できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless fabric control-plane** *control-plane-name* 例： `Device(config)# wireless fabric control-plane test-map`	コントロールプレーン名を設定します。 コントロール プレーン名を指定しない場合は、自動生成されるデフォルトのコントロール プレーンが使用されます。
ステップ 3	**ip address** *ip-address* **key** *pre-shared-key* 例： `Device((config-wireless-cp)#ip address 10.12.13.14 key secret`	コントロール プレーンの IP アドレスとキーを設定します。

サイトごとのマップ サーバの設定（GUI）

始める前に

プライマリ コントローラとバックアップ コントローラを設定する前に、AP 参加プロファイルがすでに設定済みであることを確認します。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。

ステップ 2 [AP Join Profile] ページで、AP 参加プロファイル名をクリックします。

ステップ 3 [Edit AP Join Profile] ウィンドウで [CAPWAP] タブをクリックします。

ステップ 4 [Backup Controller Configuration] の [High Availability] タブで、[Enable Fallback] チェック ボックスをオンにします。

ステップ 5 プライマリ コントローラとセカンダリ コントローラの名前および IP アドレスを入力します。

ステップ 6 [Update & Apply to Device] をクリックします。

サイトごとのマップ サーバの設定（CLI）

サイトタグの下にサイトごとの MAP サーバを設定するには、次の手順に従います。

始める前に

各サイトまたは各 AP グループに対してマップ サーバを設定できます。. マップ サーバが各 VNID またはサブネットに対して設定されていない場合は、サイトごとのマップ サーバが AP のクエリとクライアントの登録に使用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag site** *site-tag* 例： `Device(config)# wireless tag site test-site`	サイト タグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 3	**fabric control-plane** *map-server-name* 例： `Device(config-wireless-site)# fabric control-plane test-map`	ファブリック コントロール プレーン名をサイト タグに関連付けます。

各 VNID のマップ サーバの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless Plus]** > **[Fabric]** > **[Fabric Configuration]** をクリックします。
ステップ 2 [Profiles] タブで、[Add] をクリックして新しいファブリック プロファイルを追加します。
ステップ 3 表示される [Add New Profile] ウィンドウに、プロファイルの名前と説明を入力します。
ステップ 4 L2 VNID および SGT タグの詳細を指定します。
ステップ 5 [Map Servers] セクションで、サーバ 1 の IP アドレスと事前共有キーの詳細を指定します。
ステップ 6 必要に応じて、サーバ 2 の IP アドレスと事前共有キーの詳細を指定できます。
ステップ 7 [Save & Apply to Device] をクリックします。

各 VNID のマップ サーバの作成

レイヤ 2 およびレイヤ 3 内の各 VNID のマップ サーバ、またはクライアント VNID のマップ サーバを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# 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	次のいずれかを選択します。 • **wireless fabric name** *vnid-map* **l2-vnid** *l2-vnid* **l3-vnid** *l3vnid* **ip** *network-ip subnet-mask* **control-plane** *control-plane-name* • **wireless fabric name** *vnid-map* **l2-vnid** *l2-vnid* **control-plane** *control-plane-name* **例：** `Device(config)# wireless fabric name test1 l2-vnid 12 l3-vnid 10 ip 10.8.6.2 255.255.255.236 control-plane cp1` **例：** `Device(config)# wireless fabric name test1 l2-vnid 22 control-plane cp1`	レイヤ 2 およびレイヤ 3 内の各 VNID のマップ サーバ、またはクライアント VNID のマップ サーバを設定します。

ファブリック プロファイルの作成とタグおよび VNID の関連付け（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Fabric]** をクリックします。

ステップ 2 [Fabric Configuration] ページの [Profiles] タブで、[Add] をクリックして新しいプロファイルを追加します。

ステップ 3 表示される [Add New Profile] ウィンドウに、プロファイルの名前と説明を入力します。

ステップ 4 L2 VNID および SGT タグの詳細を指定します。

ステップ 5 [Save & Apply to Device] をクリックします。

ファブリック プロファイルの作成とタグおよび VNID の関連付け（CLI）

ファブリック プロファイルを作成し、クライアントが属する VNID と SGT タグをこのプロファイルに関連付けます。

手順

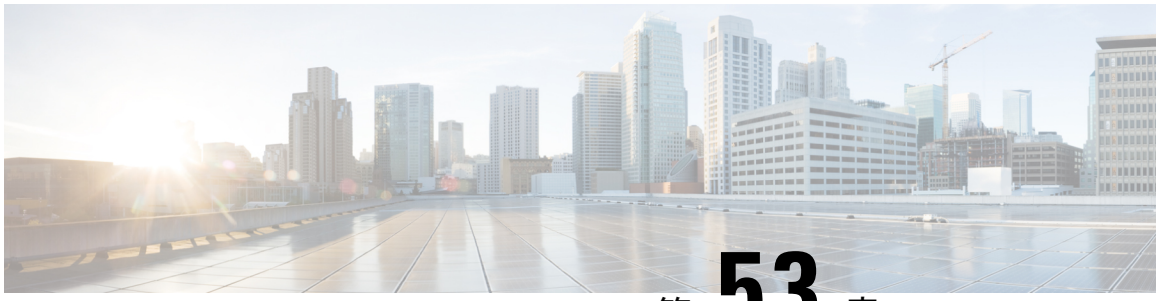
	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless profile fabric** *fabric-profile-name* **例：** `Device(config)# wireless profile fabric test-fabric`	ファブリック プロファイルを設定します。
ステップ 3	**sgt-tag** *value* **例：** `Device(config-wireless-fabric)# sgt-tag 5`	SGT タグを設定します。
ステップ 4	**client-l2-vnid** *vnid* **例：** `Device(config-wireless-fabric)# client-l2-vnid 10`	クライアントのレイヤ 2 VNID を設定します。

マップ サーバの設定の確認

マップ サーバの設定を確認するには、次のコマンドを使用します。

```
Device# show wireless fabric summary

Fabric Status      : Enabled


Control-plane:
Name                              IP-address        Key
Status
-------------------------------------------------------------------------------------
test-map                          10.12.13.14       test1                           Down
```

```
Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address              Subnet
 Control plane name
------------------------------------------------------------------------------------------------

  test1               12             10             10.6.8.9            255.255.255.236
    test2


Device# show wireless fabric vnid mapping

Fabric VNID Mapping:
  Name               L2-VNID        L3-VNID        IP Address              Subnet
Control Plane Name
------------------------------------------------------------------------------------------------

  fabric1             1              0              9.6.51.0            255.255.255.0
        map-server-name

Device# show wireless profile fabric detailed profile-name

Profile-name      : fabric-ap
VNID              : 1
SGT               : 500
Type              : Guest

Control Plane Name       Control-Plane IP   Control-Plane Key
------------------------------------------------------------------------------
 Ent-map-server           5.4.3.2                guest_1

Device# show ap name ap-name config general

Fabric status                                  : Enabled
RLOC                                           : 2.2.2.2
Control Plane Name  : ent-map-server

Device# show wireless client mac mac-address detail

Fabric status : Enabled
RLOC                   : 2.2.2.2
Control Plane Name  : ent-map-server

Device# show wireless tag site detailed site-tag

Site Tag Name        : default-site-tag
Description          : default site tag
--------------------------------------
AP Profile           : default-ap-profile
Local-site           : Yes
Fabric-control-plane: Ent-map-server
```



第 53 章

ボリューム測定

ボリューム測定機能を使用すると、アクセス ポイント（AP）がクライアント アカウンティング統計情報をコントローラに対して更新し、さらにRADIUSサーバに対して更新する間隔を設定できます。現在、レポートは 90 秒ごとに AP からコントローラに送信されます。この機能を使用することで、5～90秒の時間を設定できます。これにより、デバイスでのアカウンティング データの使用における遅延が削減されます。

（注） この機能は Wave 2 AP でのみサポートされています。

• ボリューム測定の設定 （491 ページ）

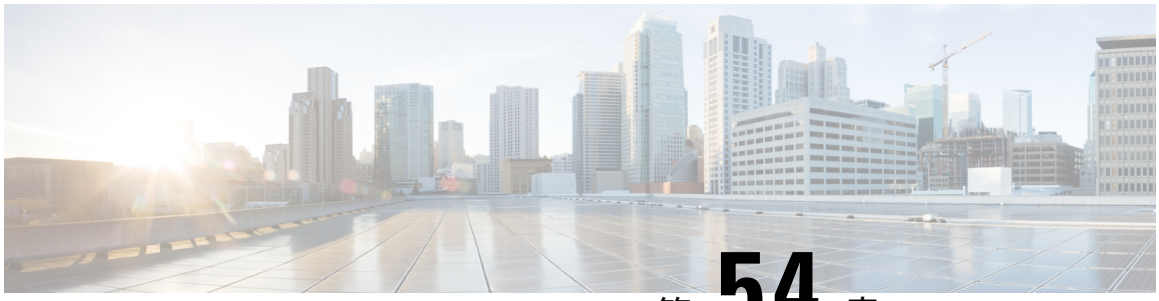
ボリューム測定の設定

ボリューム測定を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# 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	**ap profile** *profile-name* **例：** `Device(config)# ap profile yy-ap-profile`	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。
ステップ 3	**dot11 24ghz reporting-interval** *reporting-interval* **例：**	dot11 パラメータを設定します。

	コマンドまたはアクション	目的
	`Device(config-ap-profile)# dot11 24ghz reporting-interval 60`	
ステップ 4	**dot11 5ghz reporting-interval** *reporting-interval* 例： `Device(config-ap-profile)# dot11 5ghz reporting-interval 60`	dot11 パラメータを設定します。
ステップ 5	**exit** 例： `Device(config-ap-profile)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 6	**aaa accounting update periodic** *interval-in-minutes* 例： `Device(config)# aaa accounting update periodic 75`	コントローラがクライアントの中間アカウンティング更新を RADIUS サーバに送信する時間間隔（分単位）を設定します。
ステップ 7	**exit** 例： `Device(config)# exit`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。



第 54 章

Syslog サーバ用のアクセス ポイントとコントローラでの Syslog メッセージの有効化

Syslog サーバ用のアクセス ポイントとコントローラでの Syslog メッセージの有効化に関する情報

（注） AP が参加した後にのみ、Syslog サーバ メッセージを表示できるようになります。

アクセス ポイントおよびコントローラの Syslog サーバには、数多くのレベルとファシリティがあります。

Syslog レベルは次のとおりです。

- Emergencies
- Alerts
- Critical
- Errors
- Warnings
- [Notifications]
- Informational

- Debugging

Syslog ファシリティでは次のオプションを使用できます。

- auth：認可システム。
- cron：Cron/at ファシリティ。
- daemon：システム デーモン。
- kern：カーネル。
- local0：ローカル用。
- local1：ローカル用。
- local2：ローカル用。
- local3：ローカル用。
- local4：ローカル用。
- local5：ローカル用。
- local6：ローカル用。
- local7：ローカル用。
- lpr：ライン プリンタ システム。
- mail：メール システム。
- news：USENET ニュース。
- sys10：システム用。
- sys11：システム用。
- sys12：システム用。
- sys13：システム用。
- sys14：システム用。
- sys9：システム用。
- syslog：Syslog それ自体。
- user：ユーザ プロセス。
- uucp：Unix-to-Unix コピー システム。

AP プロファイルの Syslog サーバの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *ap-profile* 例： `Device(config)# ap profile xyz-ap-profile`	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。
ステップ 3	**syslog facility** 例： `Device(config-ap-profile)# syslog facility`	Syslog メッセージのファシリティ パラメータを設定します。
ステップ 4	**syslog host** *ip-address* 例： `Device(config-ap-profile)# syslog host 9.3.72.1`	Syslog サーバの IP アドレスとパラメータを設定します。
ステップ 5	**syslog level** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} 例： `Device(config-ap-profile)# syslog level`	Syslog サーバのロギング レベルを設定します。 Syslog サーバのロギング レベルは次のとおりです。 • **emergencies**：重大度 0 を示します。システムが使用できないことを意味します。 • **alerts**：重大度 1 を示します。ただちに対処する必要があることを意味します。 • **critical**：重大度 2 を示します。クリティカルな状態を意味します。 • **errors**：重大度 3 を示します。エラー状態を意味します。 • **warnings**：重大度 4 を示します。警告状態を意味します。

	コマンドまたはアクション	目的
		• **notifications**：重大度 5 を示します。正常ですが、注意を必要とする状態であることを意味します。 • **informational**：重大度 6 を示します。情報メッセージを意味します。 • **debugging**：重大度 7 を示します。デバッグメッセージを意味します。 （注） サポートされる Syslog レベルの数を確認するには、Syslog レベルを選択する必要があります。Syslog レベルを選択すると、それ以下のすべてのレベルも有効になります。 「critical」Syslog レベルを有効にすると、その下のすべてのレベルも有効になります。したがって、「critical」、「alerts」、「emergencies」の 3 つすべてが有効になります。
ステップ 6	**end** 例： `Device(config-ap-profile)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

コントローラの Syslog サーバの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**logging host** {*hostname* | *ipv6*} 例： `Device(config)# logging host 124.3.52.62`	Syslog サーバの IP アドレスとパラメータを有効にします。

	コマンドまたはアクション	目的
ステップ 3	**logging facility** {**auth** | **cron** | **daemon** | **kern** | **local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7** | **lpr** | **mail** | **news** | **sys10** | **sys11** | **sys12** | **sys13** | **sys14** | **sys9** | **syslog** | **user** | **uucp**} 例： `Device(config)# logging facility syslog`	Syslog メッセージのファシリティ パラメータを有効にします。 Syslog メッセージに対して次のファシリティ パラメータを有効にすることができます。 • **auth**：認可システム。 • **cron**：cron ファシリティ。 • **daemon**：システム デーモン。 • **kern**：カーネル。 • **local0** ～ **local7**：ローカル用。 • **lpr**：ライン プリンタ システム。 • **mail**：メール システム。 • **news**：USENET ニュース。 • **sys10** ～ **sys14** および **sys9**：システム用。 • **syslog**：Syslog それ自体。 • **user**：ユーザ プロセス。 • **uucp**：UNIX から UNIX へのコピー システム。
ステップ 4	**logging trap** {*severity-level* | **alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} 例： `Device(config)# logging trap 2`	Syslog サーバのロギング レベルを有効にします。 *severity-level*：ロギングの重大度レベルを示します。有効範囲は 0 ～ 7 です。 Syslog サーバのロギング レベルは次のとおりです。 • **emergencies**：重大度 0 を示します。システムが使用できないことを意味します。 • **alerts**：重大度 1 を示します。ただちに対処する必要があることを意味します。 • **critical**：重大度 2 を示します。クリティカルな状態を意味します。

	コマンドまたはアクション	目的
		• **errors**：重大度 3 を示します。エラー状態を意味します。 • **warnings**：重大度 4 を示します。警告状態を意味します。 • **notifications**：重大度 5 を示します。正常ですが、注意を必要とする状態であることを意味します。 • **informational**：重大度 6 を示します。情報メッセージを意味します。 • **debugging**：重大度 7 を示します。デバッグメッセージを意味します。 （注） サポートされる Syslog レベルの数を確認するには、Syslog レベルを選択する必要があります。Syslog レベルを選択すると、それ以下のすべてのレベルも有効になります。 「critical」Syslog レベルを有効にすると、その下のすべてのレベルも有効になります。したがって、「critical」、「alerts」、「emergencies」の 3 つすべてが有効になります。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Syslog サーバの設定の確認

すべてのアクセス ポイントに対するグローバルな Syslog サーバの設定の確認

コントローラに join しているすべてのアクセス ポイントに対するグローバルな Syslog サーバの設定を表示するには、次のコマンドを使用します。

```
Device# show ap config general
Cisco AP Name : APA0F8.4984.5E48
================================================
```

```
Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
```

```
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone flexconnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```

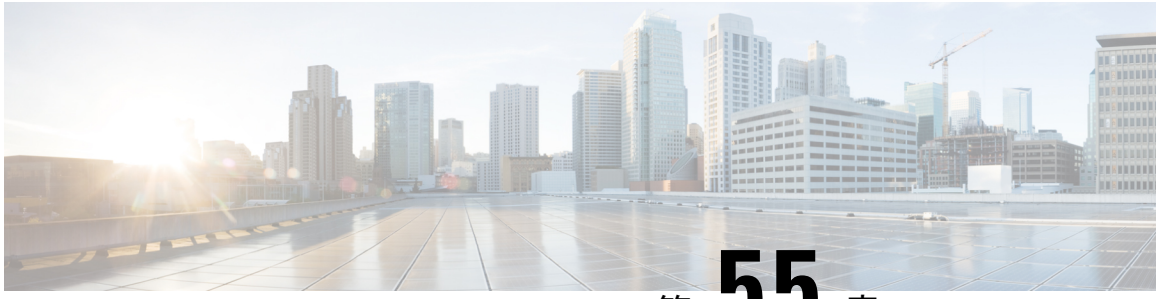
特定のアクセス ポイントに対する Syslog サーバの設定の確認

特定のアクセス ポイントに対する Syslog サーバの設定を表示するには、次のコマンドを使用します。

```
Device# show ap name <ap-name> config general
show ap name APA0F8.4984.5E48 config general
Cisco AP Name : APA0F8.4984.5E48
================================================

Cisco AP Identifier : a0f8.4985.d360
Country Code : IN
Regulatory Domain Allowed by Country : 802.11bg:-A 802.11a:-DN
AP Country Code : IN - India
AP Regulatory Domain
Slot 0 : -A
Slot 1 : -D
MAC Address : a0f8.4984.5e48
IP Address Configuration : DHCP
IP Address : 9.4.172.111
IP Netmask : 255.255.255.0
Gateway IP Address : 9.4.172.1
Fallback IP Address Being Used :
Domain :
Name Server :
CAPWAP Path MTU : 1485
Telnet State : Disabled
SSH State : Disabled
Jumbo MTU Status : Disabled
Cisco AP Location : default location
Site Tag Name : ST1
RF Tag Name : default-rf-tag
Policy Tag Name : PT3
```

```
AP join Profile : default-ap-profile
Primary Cisco Controller Name : WLC2
Primary Cisco Controller IP Address : 9.4.172.31
Secondary Cisco Controller Name : Not Configured
Secondary Cisco Controller IP Address : 0.0.0.0
Tertiary Cisco Controller Name : Not Configured
Tertiary Cisco Controller IP Address : 0.0.0.0
Administrative State : Enabled
Operation State : Registered
AP Certificate type : Manufacturer Installed Certificate
AP Mode : Local
AP VLAN tagging state : Disabled
AP VLAN tag : 0
CAPWAP Preferred mode : Not Configured
AP Submode : Not Configured
Office Extend Mode : Disabled
Remote AP Debug : Disabled
Logging Trap Severity Level : notification
Software Version : 16.10.1.24
Boot Version : 1.1.2.4
Mini IOS Version : 0.0.0.0
Stats Reporting Period : 180
LED State : Enabled
PoE Pre-Standard Switch : Disabled
PoE Power Injector MAC Address : Disabled
Power Type/Mode : PoE/Full Power (normal mode)
Number of Slots : 3
AP Model : AIR-AP1852I-D-K9
IOS Version : 16.10.1.24
Reset Button : Disabled
AP Serial Number : KWC212904UB
Management Frame Protection Validation : Disabled
AP User Mode : Automatic
AP User Name : Not Configured
AP 802.1X User Mode : Global
AP 802.1X User Name : Not Configured
Cisco AP System Logging Host : 9.4.172.116
AP Up Time : 11 days 1 hour 15 minutes 52 seconds
AP CAPWAP Up Time : 6 days 3 hours 11 minutes 6 seconds
Join Date and Time : 09/05/2018 04:18:52
Join Taken Time : 3 minutes 1 second
Join Priority : 1
Ethernet Port Duplex : Auto
Ethernet Port Speed : Auto
AP Link Latency : Disable
AP Lag Configuration Status : Disabled
AP Lag Operational Status : Disabled
Lag Support for AP : Yes
Rogue Detection : Enabled
Rogue Containment auto-rate : Disabled
Rogue Containment of standalone flexconnect APs : Disabled
Rogue Detection Report Interval : 10
Rogue AP minimum RSSI : -90
Rogue AP minimum transient time : 0
AP TCP MSS Adjust : Enabled
AP TCP MSS Size : 1250
AP IPv6 TCP MSS Adjust : Enabled
AP IPv6 TCP MSS Size : 1250
Hyperlocation Admin Status : Disabled
Retransmit count : 5
Retransmit interval : 3
Fabric status : Disabled
FIPS status : Disabled
WLANCC status : Disabled
```

```
USB Module Type : USB Module
USB Module State : Enabled
USB Operational State : Disabled
USB Override : Disabled
Lawful-Interception Admin status : Disabled
Lawful-Interception Oper status : Disabled
```



第 55 章

ソフトウェア メンテナンス アップグレード

ソフトウェア メンテナンス アップグレードの概要

ソフトウェア メンテナンス アップグレード（SMU）は、システムにインストールしてパッチ修正やセキュリティ解決をリリースされたイメージに提供できるパッケージです。SMU パッケージはリリースごとおよびコンポーネントごとに提供され、プラットフォームに固有です。

SMU はネットワークの問題に迅速に対応できるようにするとともに、必要なテストの時間と範囲を削減するため、従来の IOS ソフトウェアには多大なメリットがあります。Cisco IOS XE プラットフォームでは SMU の互換性を内部的に検証し、互換性のない SMU はインストールできません。

すべて SMU が後続の Cisco IOS XE ソフトウェア メンテナンス リリースに統合されています。SMU は独立した自己完結型パッケージであり、前提条件や依存関係はありません。SMU はどのような順序でもインストールまたはアンインストールできます。

SMU インフラストラクチャは、ワイヤレスの状況における次の要件を満たすために使用できます。

- コントローラのバグ修正または PSIRT。
- AP のバグ修正、PSIRT、またはコントローラの変更を必要としないマイナー機能など、既存の SMU ガイドラインに反すること。
- 新しいハードウェアまたはソフトウェアの機能を導入しない、新しい AP モデルのサポート。

SMU のワークフロー

SMU プロセスは、SMU Committee への要求によって開始されます。カスタマー サポートに連絡し、SMU 要求を行います。SMU パッケージがリリースされると [シスコ ソフトウェアのダ

ウンロード（Cisco Software Download）]ページに掲載されます。そのパッケージをダウンロードし、インストールします。

SMU パッケージ

SMU パッケージには、SMU が要求されている報告済みの問題のメタデータと修正が含まれています。

SMU のリロード

SMUのタイプは、SMUのインストール後のシステムへの影響を説明します。SMUはトラフィックに影響を与えない場合もありますが、デバイスの再起動、リロード、スイッチオーバーを引き起こす可能性もあります。

すべての SMU で、アクティブ化中にシステムをコールド リロードする必要があります。コールド リロードは、オペレーティング システムを完全にリロードします。このアクションは、リロードの間（現在は最大 5 分間）、トラフィック フローに影響します。このリロードにより、SMU の一部としてインストールされている正しいライブラリとファイルですべてのプロセスが起動します。

ホット パッチのサポートにより、システムをリロードすることなく、SMU をアクティブ化の直後に実行できます。SUM がコミットされると、リロードが繰り返されてもアクティブ化の変更が持続します。ホット パッチ SMU パッケージには、SMU をアクティブにするために再起動する必要があるすべてのプロセスをリストするメタデータが含まれています。SMU のアクティブ化の間、SMU が完全に適用されるまで、このリスト内の各プロセスが一度に 1 つずつ再起動されます。

AP イメージの SMU

AP イメージを SMU としてサポートするには、AP またはコントローラが、SMU にバンドルされているさまざまなバージョンの AP イメージを認識している必要があります。このことは、コントローラまたは AP から AP イメージのプレダウンロードを開始して、コントローラから新しい AP イメージをダウンロードするために必要です。

AP イメージがバンドルされている SMU が存在する場合、AP またはコントローラは、さまざまなバージョンの AP イメージが SUM の一部となっていることを認識する必要があります。

AP SMU パッケージの管理

手順

	コマンドまたはアクション	目的
ステップ 1	**Configure Terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**install add file bootflash:** *filename* 例： `Device# install add file bootflash:<Filename>`	メンテナンス更新プログラム パッケージをリモート ロケーションからデバイスにコピーし、プラットフォームとイメージのバージョンの互換性チェックを実行します。 このコマンドは、ファイルで基本的な互換性チェックを実行し、SMU パッケージがプラットフォームでサポートされていることを確認します。また、パッケージ/SMU.sta ファイル内にエントリを追加することで、ステータスを監視し、維持できるようにします。
ステップ 3	**install activate file bootflash:** *filename* 例： `Device# install activate file bootflash:<Filename>`	互換性チェックを実行し、パッケージをインストールして、パッケージのステータスの詳細を更新します。 再起動可能なパッケージの場合、このコマンドは適切なポストインストール スクリプトをトリガーして必要なプロセスを再起動します。また、再起動できないパッケージの場合は、リロードをトリガーします。
ステップ 4	**install commit file bootflash:** *filename* 例： `Device# install activate file bootflash:<Filename>`	リロードが繰り返されても持続するようにアクティブ化の変更をコミットします。 アクティブ化の後で、システムがアップしている間、または最初のリロード後にコミットできます。パッケージがアクティブになっていてもコミットされていない場合は、最初のリロード後はアクティブの状態を保ちますが、2回目のリロード後はアクティブ状態を保ちません。
ステップ 5	**install rollback to** {**base** | **committed** | **id** | **committed** } *committed ID* 例： `Device# install rollback to id 1234`	デバイスを以前のインストール状態に戻します。ロールバック後にリロードする必要があります。
ステップ 6	**install deactivate file bootflash:** *filename* 例：	アクティブなパッケージを非アクティブ化し、パッケージステータスを更新し、

	コマンドまたはアクション	目的
	`Device# install deactivate file bootflash:<Filename>`	再起動またはリロードするプロセスをトリガーします。
ステップ 7	**show version** 例： `Device# show version`	デバイスのイメージ バージョンを表示します。
ステップ 8	**show installsummary** 例： `Device# show version`	アクティブ パッケージに関する情報を表示します。 このコマンドの出力は、設定されている install コマンドに応じて変化します。

SMU の設定例

次に、show install summary コマンドの出力例を示します。

show install summary コマンドの出力には、image2 の Install add が実行された後の進行状況のステータスが表示されています。

```
Device#show install summary

[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------------------
IMG   I    16.9.1.0.40038
IMG   C    16.8.1.0.39751

--------------------------------------------------------------------
Auto abort timer: inactive
--------------------------------------------------------------------
```

install activate issu の実行後は次のようになります。

```
Device# show install summary
[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
--------------------------------------------------------------------
Type  St   Filename/Version
--------------------------------------------------------------------
IMG   U    16.9.1.0.40038
IMG   C    16.8.1.0.39751

Auto abort timer: active on install_activate, time before rollback - 01:59:47
--------------------------------------------------------------------
```

install commit の実行後は次のようになります。

```
Device #show install summary
[ Chassis 1 2 ] Installed Package(s) Information:
State (St): I - Inactive, U - Activated & Uncommitted,
            C - Activated & Committed, D - Deactivated & Uncommitted
```

```
----------------------------------------------------------------------
Type  St   Filename/Version
----------------------------------------------------------------------
IMG   C    16.9.1.0.40038
IMG   C    16.8.1.0.39751

----------------------------------------------------------------------
Auto abort timer: inactive
----------------------------------------------------------------------
```

ローリング AP アップグレード

APのローリングアップグレードは、いくつかのAPをネットワーク内で常にアップ状態にし、他の AP がアップグレード対象として選択されている状態で、クライアントにシームレスなカバレッジを提供するように、段階的な方法で AP をアップグレードする方法です。

（注） ローリング アップグレードがトリガーされる前に、AP イメージがダウンロードされている必要があります。これにより、アップグレード対象のすべての AP に新しいイメージバージョンが用意されます。

ローリング AP アップグレードのプロセス

AP のローリング アップグレードはコントローラ単位で実行されます。特定の時間にアップグレードされる AP の数は、コントローラに接続している AP の総数のパーセンテージになります。パーセンテージは、ユーザが設定した値を上限とします。デフォルトのパーセンテージは 15 です。AP の実際のアップグレードが開始される前に、クライアント以外の AP がアップグレードされます。

アップグレード プロセスは次のようになります。

1. **候補となる AP セットの選択**

   この段階では、隣接 AP の情報に基づいて一連の AP の候補が選択されます。たとえば、ある AP をアップグレード対象として特定した場合、そのネイバーの特定の番号（N）が候補の選択から除外されます。この N の値は次の方法で生成されます。

   ユーザが設定可能な上限値が 25% の場合、N = 6（想定される反復回数 = 5）

   ユーザが設定可能な上限値が 15% の場合、N = 12（想定される反復回数 = 12）

   ユーザが設定可能な上限値が 5% の場合、N = 24（想定される反復回数 = 22）

   隣接 AP の情報を使用して候補を選択できない場合は、間接のネイバーから候補を選択します。それでも候補を選択できない場合、AP は失敗せずに正常にアップグレードされます。

（注） 候補が選択された後、候補の数が設定されたパーセンテージの値を超えると、追加の候補が削除され、パーセンテージの上限が維持されます。

2. クライアントのステアリング

   AP の候補に接続しているクライアントは、AP の候補を再起動する前に、AP の候補のリストにない AP にステアリングされます。AP は、自身に関連付けられた各クライアントに対して、最適な AP のリストを求めるための要求を送信します。これには AP の候補は含まれません。AP の候補は、ネイバー リストで使用不可としてマークされます。その後、AP の再 join とリロードのプロセスでマーキングがリセットされます。

3. AP の再 join とリロードのプロセス

   クライアントのステアリングの完了後もクライアントが AP の候補に接続している場合、クライアントに認証解除が送信され、AP は新しいイメージをリロードします。AP が再 join するために 3 分間のタイマーが設定されます。このタイマーが経過すると、すべての候補は、コントローラまたはモビリティ ピアのいずれかに join したかどうがかチェックされ、マークされます。AP の候補の 90% が join を完了すると、反復が完了します。join を完了していない場合はタイマーがさらに 3 分間延長され、3分 後に同じチェックが繰り返されます。チェックが 3 回繰り返されると、反復が終了し、次の反復が開始されます。反復はそれぞれ 10 分ほど続く場合があります。

   AP のローリング アップグレードの場合、必要な設定は 1 つだけです。それは、一度にアップグレードする AP の数であり、ネットワークにある AP の総数のパーセンテージとして表されます。

   デフォルト値は 15 になります。

```
Device (config)#ap upgrade staggered <25 | 15 | 5>
```

AP のローリング アップグレードをトリガーするには、次のコマンドを使用します。

```
Device#ap image upgrade [test]
```

コントローラでの AP のアップグレードの確認

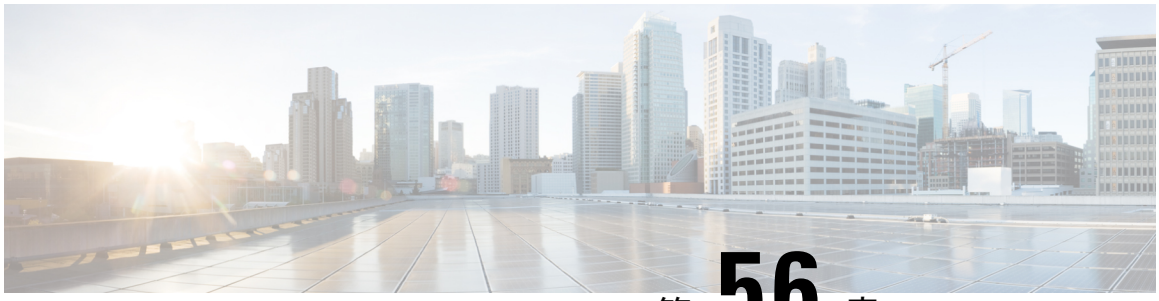
コントローラでの AP のアップグレードを確認するには、次の **show** コマンドを使用します。

```
Device #show ap upgrade


AP upgrade is in progress

From version: 8 16.9.1.6
To version: 9 16.9.1.30
Started at: 03/09/2018 21:33:37 IST
Percentage complete: 0
Expected time of completion: 03/09/2018 22:33:37 IST

Progress Report
---------------
```

```
Iterations
----------

Iteration    Start time                 End time            AP count
-------------------------------------------------------------------

0            03/09/2018 21:33:37 IST   03/09/2018 21:33:37 IST     0
1            03/09/2018 21:33:37 IST   ONGOING                     0


Upgraded
--------
Number of APs: 0

AP Name           Ethernet MAC            Iteration       Status
-------------------------------------------------------------------


In Progress
-----------
Number of APs: 1

AP Name                           Ethernet MAC
-------------------------------------------------
APf07f.06a5.d78c                  f07f.06cf.b910


Remaining
---------
Number of APs: 3

AP Name                           Ethernet MAC
-------------------------------------------------
APCC16.7EDB.6FA6                  0081.c458.ab30
AP38ED.18CA.2FD0                  38ed.18cb.25a0
AP881d.fce7.5ee4                  d46d.50ee.33a0
```

第 VI 部

セキュリティ



第 56 章

IPv4 ACL

ACL によるネットワーク セキュリティに関する情報

この章では、アクセス コントロール リスト（ACL）を使用して、スイッチのネットワーク セキュリティを設定する方法について説明します。コマンドや表では、ACL をアクセス リストと呼ぶこともあります。

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACLはルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスを通過するパケットを許可または拒否します。ACLは、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。パケットがインターフェイスに着信すると、スイッチはパケット内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。スイッチは、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ3スイッチにアクセス リストを設定します。ACL を設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送また

はブロックされるトラフィックの種類を決定したりできます。たとえば、電子メール トラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。

アクセス コントロール エントリ

ACL には、アクセス コントロール エントリ（ACE）の順序付けられたリストが含まれています。各 ACE には、*permit* または *deny* と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。*permit* または *deny* の意味は、ACL が使用されるコンテキストによって変わります。

ACL でサポートされるタイプ

スイッチは、IP ACL とイーサネット（MAC）ACL をサポートしています。

- IP ACL は、TCP、ユーザ データグラム プロトコル（UDP）、インターネット グループ管理プロトコル（IGMP）、およびインターネット制御メッセージプロトコル（ICMP）などの IPv4 トラフィックをフィルタリングします。
- イーサネット ACL は非 IP トラフィックをフィルタリングします。

このスイッチは、Quality of Service（QoS）分類 ACL もサポートしています。

サポートされる ACL

スイッチでは、トラフィックをフィルタリングするために、次に示す 3 種類の ACL がサポートされています。

- ポート ACL は、レイヤ 2 インターフェイスに入るトラフィックをアクセス コントロールします。IPv4 と MAC どちらのアクセス リスト タイプのどの方向に対してでも、レイヤ 2 インターフェイスにポート ACL を適応できます。
- ルータ ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御し、レイヤ 3 インターフェイスで特定の方向（着信または発信）に適用されます。

ACL 優先順位

、ポート ACL、およびルータ ACL が同じスイッチに設定されている場合、入力トラフィックの場合のフィルタの優先順位は上からポート ACL、、およびルータ ACL です。出力トラフィックの場合、フィルタの優先順位は、ルータ ACL、ポート ACL です。

次の例で、簡単な使用例を説明します。

- スイッチ仮想インターフェイス（SVI）に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。他のポートで受信した着信のルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。

- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートにパケットが着信すると、このパケットはポート ACL によってフィルタリングされます。発信するルーティング IP パケットには、ルータ ACL のフィルタが適用されます。他のパケットはフィルタリングされません。

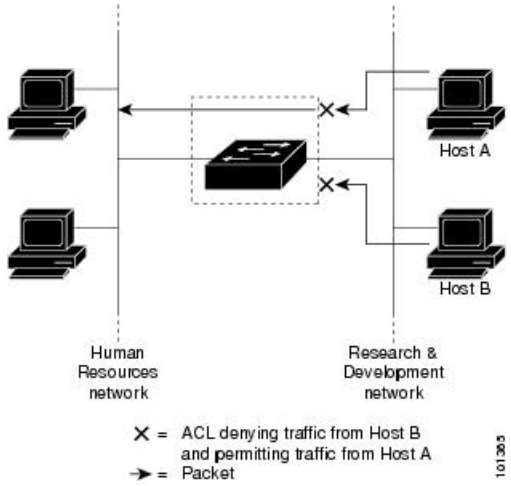
ポート ACL

- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

スイッチは、インターフェイス上の ACL を調べ、パケットが ACL 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、ACL がネットワークまたはネットワークの部分へのアクセスを制御します。

図 *6 : ACL* によるネットワーク内のトラフィックの制御

次に、すべてのワークステーションが同じ VLAN にある場合にポート ACL を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 の着信方向に適用された ACL は、ホスト A がヒューマン リソース ネットワークにアクセスすることを許可しますが、ホスト B が同一のネットワークにアクセスすることは拒否します。ポート ACL は、着信方向のレイヤ 2



インターフェイスだけに適用できます。

ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。

（注） レイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに、新しい IP アクセス リストまたは MAC アクセス リストを適用すると、前に設定した ACL が新しい ACL に置き換わります。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスであるスイッチ仮想インターフェイス（SVI）、物理層 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向（着信または発信）に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

スイッチは、IPv4 トラフィックの次のアクセス リストをサポートしています。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチはインターフェイスに設定されている機能に関連付けられている ACL が照合されます。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてからネクストホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセス コントロールが行えます。

VLAN マップ

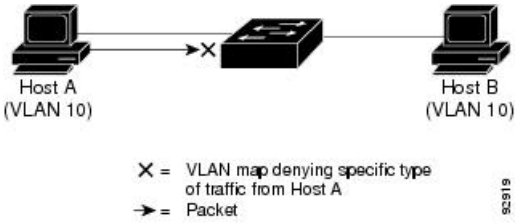
VLAN ACL または VLAN マップは、VLAN 内のネットワーク トラフィックを制御するために使用されます。スイッチまたはスイッチ スタックの VLAN 内でブリッジングされるすべてのパケットに VLAN マップを適用できます。VACL は、セキュリティ パケット フィルタリングおよび特定の物理インターフェイスへのトラフィックのリダイレクトだけを目的としたものです。VACL は方向（入力または出力）で定義されることはありません。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、MAC アドレスおよび Ethertype によってアクセス コントロールされます（IP トラフィックは、MAC VACL マップではアクセス制御されません）。VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。

図 *7: VLAN* マップによるトラフィックの制御

次の図に、VLAN マップを適用して、特定のトラフィック タイプを VLAN 10 のホスト A から転送できないように設定する例を示します。各 VLAN には、VLAN マップを 1 つだけ適用できます。



ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィック

IP パケットは、ネットワークを通過するときにフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

アクセス コントロール エントリ（ACE）には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報（TCP や UDP などのプロトコル タイプを含む）をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。

（注） L4 Ops をともなう ACE の TCP では、フラグメント化パケットは RFC 1858 ごとにドロップします。

- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

ACE およびフラグメント化されたトラフィックとフラグメント化されていないトラフィックの例

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
Device(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Device(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Device(config)# access-list 102 permit tcp any host 10.1.1.2
```

```
Device(config)# access-list 102 deny tcp any any
```

（注） 最初の 2 つの ACE には宛先アドレスの後に *eq* キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれシンプル メール転送プロトコル（SMTP）および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE（permit）と一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ 3 情報だけをチェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。
- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが 2 つめの ACE（deny）と一致します。残りのフラグメントは、レイヤ 4 情報が含まれていないため、2 つめの ACE と一致しません。残りのフラグメントは 3 つめの ACE（permit）と一致します。

  最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。
- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE（deny）と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の permit ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

標準 IPv4 ACL および拡張 IPv4 ACL

ここでは、IP ACL について説明します。

ACL は、許可条件と拒否条件の順序付けられた集まりです。スイッチは、アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、IPv4 について次の ACL（アクセス リスト）をサポートします。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。

- 拡張 IP アクセス リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることもできます。

IPv4 ACL スイッチでサポートされていない機能

このスイッチで IPv4 ACL を設定する手順は、他の Cisco スイッチやルータで IPv4 ACL を設定する手順と同じです。

以下の ACL 関連の機能はサポートされていません。

- 非 IP プロトコル ACL または
- IP アカウンティング
- 再帰 ACL およびダイナミック ACL はサポートされていません。

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。

次の一覧に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト（1 ～ 199 および 1300 ～ 2699）をサポートします。

表 *14*：アクセス リスト番号

アクセス リスト番号	タイプ	サポートあり
1 ～ 99	IP 標準アクセス リスト	Yes
100 ～ 199	IP 拡張アクセス リスト	Yes
200 ～ 299	プロトコル タイプコード アクセス リスト	なし
300 ～ 399	DECnet アクセス リスト	なし
400 ～ 499	XNS 標準アクセス リスト	なし
500 ～ 599	XNS 拡張アクセス リスト	なし
600 ～ 699	AppleTalk アクセス リスト	なし
700 ～ 799	48 ビット MAC アドレス アクセス リスト	なし
800 ～ 899	IPX 標準アクセス リスト	なし
900 ～ 999	IPX 拡張アクセス リスト	なし
1000 ～ 1099	IPX SAP アクセス リスト	なし

アクセス リスト番号	タイプ	サポートあり
1100 ～ 1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	なし
1200 ～ 1299	IPX サマリー アドレス アクセス リスト	なし
1300 ～ 1999	IP 標準アクセス リスト（拡張範囲）	Yes
2000 ～ 2699	IP 拡張アクセス リスト（拡張範囲）	Yes

番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 ACL および名前付き拡張 ACL も作成できます。標準 IP ACL の名前は 1 ～ 99 で、拡張 IP ACL の名前は 100 ～ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

番号付き標準 IPv4 ACL

ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

スイッチは、**host** 一致条件があるエントリと *don't care* マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の *don't care* マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準 IPv4 ACL を 、端末回線、またはインターフェイスに適用できます。

番号付き拡張 IPv4 ACL

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

このスイッチは、ダイナミックまたはリフレクシブ アクセス リストをサポートしていません。また、タイプ オブ サービス（ToS）の minimize-monetary-cost ビットに基づくフィルタリングもサポートしていません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

拡張 TCP、UDP、ICMP、IGMP、またはその他の IP ACL を定義できます。また、このスイッチはこれらの IP プロトコルをサポートします。

これらの IP プロトコルがサポートされます。

- 認証ヘッダー プロトコル（**ahp**）
- Encapsulation Security Payload（**esp**）
- Enhanced Interior Gateway Routing Protocol（**eigrp**）
- 総称ルーティング カプセル化（**gre**）
- インターネット制御メッセージ プロトコル（**icmp**）
- インターネット グループ管理プロトコル（**igmp**）
- すべての内部プロトコル（**ip**）
- IP-in-IP トンネリング（**ipinip**）
- KA9Q NOS 互換 IP over IP トンネリング（**nos**）
- Open Shortest Path First ルーティング（**ospf**）
- ペイロード圧縮プロトコル（**pcp**）
- プロトコル独立マルチキャスト（**pim**）
- 伝送制御プロトコル（**tcp**）
- ユーザ データグラム プロトコル（**udp**）

名前付き IPv4 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング（名前）を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセス リストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。

（注） 標準 ACL または拡張 ACL に指定する名前は、アクセス リスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ～ 99 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定するときには、次の注意事項に留意してください。

- また、番号付き ACL も使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。

ACL ロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、syslog メッセージを管理する **logging console** コマンドで管理されます。

（注） ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可（*permit*）または拒否（*deny*）ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

（注） ロギング メッセージが多すぎて処理できない場合、または 1 秒以内に処理する必要があるロギング メッセージが複数ある場合、ロギング設備ではロギング メッセージ パケットの一部をドロップすることがあります。この動作によって、ロギング パケットが多すぎてルータがクラッシュすることを回避します。そのため、課金ツールや、アクセス リストと一致する数の正確な情報源としてロギング設備をを使用しないでください。

ハードウェアおよびソフトウェアによる IP ACL の処理

ACL 処理はハードウェアで実行されます。ハードウェアで ACL の設定を保存する領域が不足すると、そのインターフェイス上のすべてのパケットがドロップします。

（注） スイッチまたはスタック メンバーのリソース不足が原因でハードウェアに ACL を設定できない場合、影響を受けるのは、スイッチに着信した該当 VLAN 内のトラフィックだけです。

show ip access-lists 特権 EXEC コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチド パケットおよびルーテッド パケットに関するハードウェアの ACL の基本的な統計情報を取得する場合は、 特権 EXEC コマンドを使用します。

IPv4 ACL のインターフェイスに関する注意事項

着信 ACL の場合、パケットの受信後スイッチはパケットを ACL と照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信 ACL の場合、パケットを受信し制御対象インターフェイスにルーティングしたあと、スイッチはパケットを ACL と照合します。ACL がパケットを許可した場合は、スイッチはパケットを送信します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。

未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワーク セキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

IPv4 アクセス コントロール リストを設定するための前提条件

ここでは、アクセス コントロール リスト（ACL）によるネットワーク セキュリティの設定の前提条件を示します。

- LAN ベース フィーチャ セットを実行しているスイッチでは、VLAN マップがサポートされます。

IPv4 アクセス コントロール リストの設定に関する制約事項

一般的なネットワーク セキュリティ

次は、ACL によるネットワーク セキュリティの設定の制約事項です。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- **appletalk** は、コマンドラインのヘルプ ストリングに表示されますが、**deny** および **permit** MAC アクセスリスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。
- ACL ワイルドカードは、ダウンストリーム クライアント ポリシーではサポートされていません。

IPv4 ACL ネットワーク インターフェイス

次の制限事項が、ネットワーク インターフェイスへの IPv4 ACL に適用されます。

- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。

レイヤ 2 インターフェイスの MAC ACL

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。IP アクセス リストは IP パケットだけをフィルタリングし、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

（注） **mac access-group** インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用される場合のみ有効です。このコマンドは、EtherChannel ポート チャネルでは使用できません。

IP アクセス リスト エントリ シーケンス番号

- この機能は、ダイナミック アクセス リスト、再帰アクセス リスト、またはファイアウォール アクセス リストをサポートしていません。

ACL の設定方法

IPv4 ACL の設定

スイッチで IP ACL を使用するには、次の手順に従います。

手順

ステップ 1 アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。

ステップ 2 その ACL をインターフェイスまたは端末回線に適用します。

番号付き標準 ACL の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[ACL]** の順に選択します。

ステップ 2 [ACL] ページで、[Add] をクリックします。

ステップ 3 [Add ACL Setup] ウィンドウで、次のパラメータを入力します。

- [ACL Name]：ACL の名前を入力します。
- [ACL Type]：[IPv4 Standard]。
- [Sequence]：有効な範囲は 1 ～ 99 または 1300 ～ 1999 です。
- [Action]：ドロップダウン リストからアクセスの [Permit] または [Deny] を選択します。
- [Source Type]：[any]、[Host]、または [Network] を選択します。
- [Log]：ロギングを有効または無効にします。これは、レイヤ 3 インターフェイスに関連付けられている ACL のみに限定されます。

ステップ 4 [Add] をクリックします。

ステップ 5 [Save & Apply to Device] をクリックします。

番号付き標準 ACL の作成（CLI）

番号付き標準 ACL を作成するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} *source source-wildcard*] 例： `Device(config)# access-list 2 deny your_host`	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 *access-list-number* には、1 ～ 99 または 1300 ～ 1999 の 10 進数を指定します。 条件が一致した場合にアクセスを拒否する場合は **deny** を指定し、許可する場合は **permit** を指定します。 *source* には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • キーワード **any** は 0.0.0.0 255.255.255.255 という *source* および *source-wildcard* の省略形です。source-wildcard を入力する必要はありません。 • キーワード **host** は送信元および *source* 0.0.0.0 の *source-wildcard* の省略形です。 （任意）*source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 （注） ロギングは、レイヤ 3 インターフェイスに割り当てられた ACL でだけサポートされます。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 6	**copy running-config startup-config** 例： `Device# 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。

番号付き拡張 ACL の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[ACL]** の順に選択します。

ステップ 2 [ACL] ページで、[Add] をクリックします。

ステップ 3 [Add ACL Setup] ウィンドウで、次のパラメータを入力します。

- [ACL Name]：ACL の名前を入力します。
- [ACL Type]：[IPv4 Extended]。
- [Sequence]：有効な範囲は 100 ～ 199 または 2000 ～ 26991 です。
- [Action]：ドロップダウン リストからパケット フローの [Permit] または [Deny] を選択します。
- [Source Type]：パケットの送信元として [any]、[Host]、または [Network] を選択します。
- [Destination Type]：パケットの宛先として [any]、[Host]、または [Network] を選択します。
- [Protocol]：ドロップダウン リストからプロトコルを選択します。
- [Log]：ロギングを有効または無効にします。
- [DSCP]：パケットを DSCP 値に合わせる場合に入力します。

ステップ 4 [Add] をクリックします。

ステップ 5 [Save & Apply to Device] をクリックします。

番号付き拡張 ACL の作成（CLI）

番号付き拡張 ACL を作成するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**access-list** *access-list-number* {**deny** | **permit**} *protocol source source-wildcard destination destination-wildcard* [**precedence** *precedence*] [**tos** tos] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `Device(config)# access-list 101 permit ip host 10.1.1.2 any precedence 0 tos 0 log`	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 *access-list-number* には、100 ～ 199 または 2000 ～ 2699 の 10 進数を指定します。 条件が一致した場合にパケットを拒否する場合は **deny** を指定し、許可する場合は **permit** を指定します。 *protocol* には、インターネット プロトコルの名前または番号を入力します。**ahp**、**eigrp**、**esp**、**gre**、**icmp**、**igmp**、**igrp**、**ip**、**ipinip**、**nos**、**ospf**、**pcp**、**pim**、**tcp**、**udp**、または IP プロトコル番号を表す 0 ～ 255 の整数を使用できます。一致条件としてインターネット プロトコル（ICMP、TCP、UDP など）を指定するには、キーワード **ip** を使用します。 （注） この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加の特定パラメータについては、次のステップを参照してください。 *source* には、パラメータの送信元であるネットワークまたはホストの番号を指定します。 *source-wildcard* は、ワイルドカード ビットを送信元アドレスに適用します。 *destination* には、パラメータの宛先であるネットワークまたはホストの番号を指定します。

	コマンドまたはアクション	目的
		destination-wildcard は、ワイルドカードビットを宛先アドレスに適用します。 source、source-wildcard、destination、および destination-wildcard の値は、次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • 0.0.0.0 255.255.255.255（任意のホスト）を表すキーワード **any**。 • 単一のホスト 0.0.0.0 を表すキーワード **host**。 その他のキーワードはオプションであり、次の意味を持ちます。 • **precedence**：パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、**routine**（0）、**priority**（1）、**immediate**（2）、**flash**（3）、**flash-override**（4）、**critical**（5）、**internet**（6）、**network**（7）です。 • **fragments**：2 つ目以降のフラグメントをチェックする場合に入力します。 • **tos**：パケットを 0 ～ 15 の番号または名前で指定するサービス タイプ レベルと一致させる場合に入力します。指定できる値は、**normal**（0）、**max-reliability**（2）、**max-throughput**（4）、**min-delay**（8）です。 • **time-range**：時間範囲の名前を指定します。 • **dscp**：パケットを 0 ～ 63 の番号で指定する DSCP 値と一致させる場合に入力します。または、指定できる値のリストを表示するには、疑問符（?）を使用します。

	コマンドまたはアクション	目的
		（注） コントローラは次の機能をサポートしている必要があります。 • DCSP のマーク • UP のマーク • DSCP と UP のマッピング 「DSCP から UP へのマッピング」の詳細については、次を参照してください。 https://tools.ietf.org/html/draft-ietf-tsvwg-ieee-802-11-01 （注） **dscp** 値を入力する場合は、**tos** または **precedence** を入力できません。**dscp** を入力せずに **tos** と **precedence** の両方の値を入力できます。
ステップ 3	**access-list** *access-list-number* {**deny** | **permit**} **tcp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] [*flag*] 例： `Device(config)# access-list 101 permit tcp any any eq 500`	拡張 TCP アクセス リストおよびアクセス条件を定義します。 次に示す例外を除き、拡張 IPv4 ACL に対して説明するパラメータと同じパラメータを使用します。 （任意）*operator* および *port* を入力すると、送信元ポート（*source source-wildcard* の後に入力した場合）または宛先ポート（*destination destination-wildcard* の後に入力した場合）が比較されます。演算子の候補には、**eq**（次の値に等しい）、**gt**（次の値より大きい）、**lt**（次の値より小さい）、**neq**（次の値に等しくない）、および **range**（次の範囲）があります。演算子にはポート番号を指定する必要があります（range の場合は 2 つのポート番号をスペースで区切って指定する必要があります）。

	コマンドまたはアクション	目的
		port には、10 進数（0 ～ 65535）のポート番号または TCP ポート名を入力します。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。 他のオプションのキーワードの意味は次のとおりです。 • *flag*：指定された TCP ヘッダー ビットを基準にして照合します。入力できるフラグは、**ack**（確認応答）、**fin**（終了）、**psh**（プッシュ）、**rst**（リセット）、**syn**（同期）、または **urg**（緊急）です。
ステップ 4	**access-list** *access-list-number* {**deny** | **permit**} **udp** *source source-wildcard* [*operator port*] *destination destination-wildcard* [*operator port*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `Device(config)# access-list 101 permit udp any any eq 100`	（任意）拡張 UDP アクセス リストおよびアクセス条件を定義します。 UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[operator [port]] ポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。また、UDP では、**flag**は無効です。
ステップ 5	**access-list** *access-list-number* {**deny** | **permit**} **icmp** *source source-wildcard destination destination-wildcard* [*icmp-type* | [[*icmp-type icmp-code*] | [*icmp-message*]] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `Device(config)# access-list 101 permit icmp any any 200`	拡張 ICMP アクセス リストおよびアクセス条件を定義します。 ICMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコード パラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • *icmp-type*：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • *icmp-code*：ICMP パケットを ICMP メッセージ コード タイプでフィルタリングする場合に入力します。指

	コマンドまたはアクション	目的
		定できる値の範囲は、0 ～ 255 です。 • *icmp-message*：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。
ステップ 6	**access-list** *access-list-number* {**deny** | **permit**} **igmp** *source source-wildcard destination destination-wildcard* [*igmp-type*] [**precedence** *precedence*] [**tos** *tos*] [**fragments**] [**time-range** *time-range-name*] [**dscp** *dscp*] 例： `Device(config)# access-list 101 permit igmp any any 14`	（任意）拡張 IGMP アクセス リストおよびアクセス条件を定義します。 IGMP パラメータは拡張 IPv4 ACL の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。 *igmp-type*IGMP メッセージタイプと比較するには、0～15 の番号またはメッセージ名（**dvmrp**、**host-query**、**host-report**、**pim**、または **trace**）を入力します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

名前付き標準 ACL の作成（GUI）

手順

	コマンドまたはアクション	目的
ステップ 1	**[Configuration]** > **[Security]** > **[ACL]** の順にクリックします。	
ステップ 2	[Add] をクリックして、新しい ACL 設定を作成します。	
ステップ 3	[Add ACL Setup] ウィンドウで、次のパラメータを入力します。	• [ACL Name]：ACL の名前を入力します。 • [ACL Type]：[IPv4 Standard]。 • [Sequence]：有効な範囲は 1 ～ 99 または 1300 ～ 1999 です。

	コマンドまたはアクション	目的
		• [Action]：ドロップダウン リストからアクセスの [Permit] または [Deny] を選択します。 • [Source Type]：[any]、[Host]、または [Network] を選択します。 • [Log]：ロギングを有効または無効にします。これは、レイヤ 3 インターフェイスに関連付けられている ACL のみに限定されます。
ステップ 4	[追加（Add）] をクリックしてルールを追加します。	
ステップ 5	[Save & Apply to Device] をクリックします。	

名前付き標準 ACL の作成

名前を使用して標準 ACL を作成するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip access-list standard** *name* 例： `Device(config)# ip access-list standard 20`	名前を使用して標準 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、1 ～ 99 の番号を使用できます。

	コマンドまたはアクション	目的
ステップ 4	次のいずれかを使用します。 • **deny** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**] • **permit** {*source* [*source-wildcard*] | **host** *source* | **any**} [**log**] 例： `Device(config-std-nacl)# deny 192.168.0.0 0.0.255.255 255.255.0.0 0.0.255.255` または `Device(config-std-nacl)# permit 10.108.0.0 0.0.0.0 255.255.255.0 0.0.0.0`	アクセス リスト コンフィギュレーション モードで、パケットを転送するのかドロップするのかを決定する 1 つ以上の拒否条件または許可条件を指定します。 • **host** *source*：送信元および送信元ワイルドカードの値である *source* 0.0.0.0。 • **any**：送信元および送信元ワイルドカードの値である 0.0.0.0 255.255.255.255
ステップ 5	**end** 例： `Device(config-std-nacl)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 7	**copy running-config startup-config** 例： `Device# 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。

名前付き拡張 ACL の作成

名前を使用して拡張 ACL を作成するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip access-list extended** *name* 例： `Device(config)# ip access-list extended 150`	名前を使用して拡張 IPv4 アクセス リストを定義し、アクセス リスト コンフィギュレーション モードを開始します。 名前には、100 ～ 199 の番号を使用できます。
ステップ 4	{**deny** | **permit**} *protocol* {*source* [*source-wildcard*] | **host** *source* | **any**} {*destination* [*destination-wildcard*] | host *destination* | **any**} [**precedence** *precedence*] [**tos** *tos*] [**log**] [**time-range** *time-range-name*] 例： `Device(config-ext-nacl)# permit 0 any any`	アクセス リスト コンフィギュレーション モードで、許可条件または拒否条件を指定します。**log** キーワードを使用すると、違反を含むアクセス リストのログ メッセージを取得できます。 • **host** *source*：送信元および送信元ワイルドカードの値である *source* 0.0.0.0。 • **host** *destination*：接続先および接続先ワイルドカードの値である *destination* 0.0.0.0。 • **any**：source および source wildcard の値または destination および destination wildcard の値である 0.0.0.0 255.255.255.255
ステップ 5	**end** 例： `Device(config-ext-nacl)# end`	特権 EXEC モードに戻ります。
ステップ 6	**show running-config** 例：	入力を確認します。

	コマンドまたはアクション	目的
	`Device# show running-config`	
ステップ 7	**copy running-config startup-config** 例： `Device# 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。

拡張 ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホスト アドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセスリスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

次のタスク

作成した名前付き ACL は、インターフェイスまたは VLAN に適用できます。

インターフェイスへの IPv4 ACL の適用（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[ACL]** の順に選択します。

ステップ 2 [Associating Interfaces] をクリックします。

ステップ 3 [Available Interfaces] リストからインターフェイスを選択して、右側に ACL の詳細を表示します。必要に応じて、ACL の詳細を変更できます。

ステップ 4 [Save & Apply to Device] をクリックします。

インターフェイスへの IPv4 ACL の適用（CLI）

ここでは、IPv4 ACL をネットワーク インターフェイスへ適用する方法について説明します。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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* 例： `Device(config)#`	設定するインターフェイスを指定し、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。 インターフェイスには、レイヤ 2 インターフェイス（ポート ACL）またはレイヤ3インターフェイス（ルータ ACL）を指定できます。
ステップ 3	**ip access-group** {*access-list-number* | *name*} {**in** | **out**} 例： `Device(config-if)# ip access-group 2 in`	指定されたインターフェイスへのアクセスを制御します。
ステップ 4	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	アクセス リストの設定を表示します。
ステップ 6	**copy running-config startup-config** 例： `Device# 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。

IPv4 ACL のモニタリング

スイッチに設定されている ACL、およびインターフェイスと VLAN に適用された ACL を表示して IPv4 ACL をモニタできます。

ip access-group インターフェイス コンフィギュレーション コマンドを使用して、レイヤ 2 またはレイヤ 3 インターフェイスに ACL を適用した場合は、そのインターフェイスのアクセス グループを表示できます。また、レイヤ 2 インターフェイスに適用された MAC ACL も表示できます。この情報を表示するには、次の表に記載された特権 EXEC コマンドを使用します。

表 *15:* アクセス リストおよびアクセス グループを表示するコマンド

コマンド	目的
show access-lists [*number* | *name*]	最新の IP および MAC アドレス アクセス リストの全体やその一部、または特定のアクセス リスト（番号付きまたは名前付き）の内容を表示します。
show ip access-lists [*number* | *name*]	最新の IP アクセス リスト全体、または特定の IP アクセス リスト（番号付きまたは名前付き）を表示します。
show ip interface *interface-id*	インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、**ip access-group** インターフェイス コンフィギュレーション コマンドを使用して ACL を適用した場合は、アクセス グループも表示に含まれます。
show running-config [**interface** *interface-id*]	スイッチまたは指定されたインターフェイスのコンフィギュレーションファイルの内容（設定されたすべての MAC および IP アクセス リストや、どのアクセス グループがインターフェイスに適用されたかなど）を表示します。
show mac access-group [**interface** *interface-id*]	すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リスト を表示します。

ACL の設定例

例：ACL へのコメントの挿入

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント（注釈）を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、permit ステートメントまたは deny ステートメントの前後どちらにでも配置できます。コメントがどの permit ステートメントまたは deny ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する permit または deny ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list** *access-list number* **remark** *remark* グローバル コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
Device(config)# access-list 1 remark Permit only Jones workstation through
Device(config)# access-list 1 permit 171.69.2.88
Device(config)# access-list 1 remark Do not allow Smith through
Device(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリには、**remark** アクセスリスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
Device(config)# ip access-list extended telnetting
Device(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Device(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

例：ワイヤレス環境でのポリシー プロファイルへの IPv4 ACL の適用

次に、ワイヤレス環境でポリシー プロファイルに IPv4 ACL を適用する例を示します。

（注） すべての IPv4 ACL をポリシー プロファイルに関連付ける必要があります。

この例では、拡張 ACL を使用して TCP トラフィックを許可しています。

1. IPv4 ACL を作成します。

```
Device(config)# ip access-list extended <acl-name>
Device(config-ext-nacl)# 10 permit ip any 10.193.48.224 0.0.0.31
Device (config-ext-nacl)# 20 permit ip any any
```

2. ポリシー プロファイルに IPv4 ACL を適用します。

```
Device(config)# wireless profile policy <policy-profile-name>
Device(config-wireless-policy)# shutdown
Device(config-wireless-policy)# ipv4 acl <acl-name>
Device(config-wireless-policy)# no shutdown
```

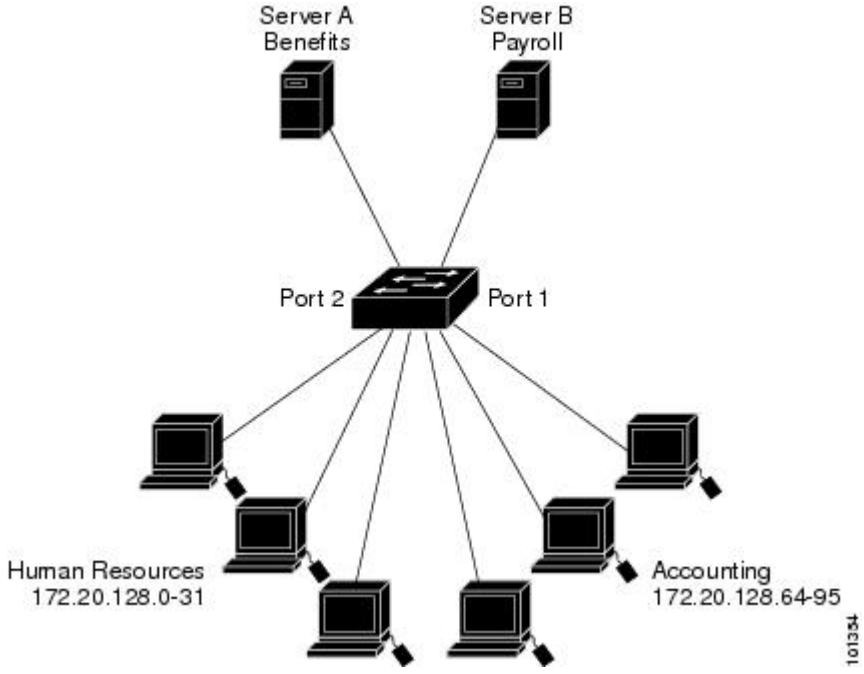
IPv4 ACL の設定例

ここでは、IPv4 ACL を設定および適用する例を示します。ACL のコンパイルに関する詳細については、『*Cisco IOS Security Configuration Guide, Release 12.4*』および『*Cisco IOS IP Configuration Guide, Release 12.4*』の「IP Adderssing and Services」の章にある「Configuring IP Services」の項を参照してください。

小規模ネットワークが構築されたオフィス用の ACL

図 *8 : ルータ ACL* によるトラフィックの制御

次に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッド ポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユーザは制限されています。



ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバに着信するトラフィックをフィルタリングします。

- 拡張 ACL を作成し、サーバからポート 1 に着信するトラフィックをフィルタリングします。

例：小規模ネットワークが構築されたオフィスの ACL

次に、標準ACLを使用してポートからサーバBに着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ～ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッド ポート 1 から送信されるトラフィックに適用されます。

```
Device(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Device(config)# end
Device# how access-lists
Standard IP access list 6
    10 permit 172.20.128.64, wildcard bits 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 6 out
```

次に、拡張ACLを使用してサーバBからポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバ B）から経理部の宛先アドレス 172.20.128.64 ～ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。このACLは、ルーテッドポート1に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル（IP）を入力する必要があります。

```
Device(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Device(config)# end
Device# show access-lists
Extended IP access list 106
    10 permit ip any 172.20.128.64 0.0.0.31
Device(config)# interface gigabitethernet1/0/1
Device(config-if)# ip access-group 106 in
```

例：番号付き ACL

次の例のネットワーク 10.0.0.0 は、2 番目のオクテットがサブネットを指定するクラス A ネットワークです。つまり、サブネットマスクは255.255.0.0 です。ネットワーク 10.0.0.0 アドレスの 3 番目および 4 番目のオクテットで特定のホストを指定します。アクセス リスト 2 を使用して、サブネット 48 のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセス リストの最終行は、ネットワーク 10.0.0.0 の他のすべてのサブネット上のアドレスが許可されることを示します。この ACL は、ポートに着信するパケットに適用されます。

```
Device(config)# access-list 2 permit 10.48.0.3
Device(config)# access-list 2 deny 10.48.0.0 0.0.255.255
Device(config)# access-list 2 permit 10.0.0.0 0.255.255.255
Device(config)#
Device(config-if)# ip access-group 2 in
```

例：拡張 ACL

次の例の先頭行は、1023 よりも大きい宛先ポートへの着信 TCP 接続を許可します。2 番めの行は、ホスト 128.88.1.2 の SMTP ポートへの着信 TCP 接続を許可します。3 番めの行は、エラー フィードバック用の着信 ICMP メッセージを許可します。

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Device(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Device(config)# access-list 102 permit icmp any any
Device(config)#
Device(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと TCP 接続を確立できるようにする場合を想定しています。ただし、IP ホストからは、専用メール ホストのメール（SMTP）ポートを除き、ネットワーク上のホストと TCP 接続を確立できないようにします。

SMTP は、接続の一端では TCP ポート 25、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは 25 です。安全なネットワーク システムでは常にポート 25 でのメール接続が使用されているため、着信サービスとを個別に制御できます。

```
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 23
Device(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 eq 25
Device(config)#
Device(config-if)# ip access-group 102 in
```

例：名前付き ACL

名前付き標準 ACL および名前付き拡張 ACL の作成

次に、*Internet_filter* という名前の標準 ACL および *marketing_group* という名前の拡張 ACL を作成する例を示します。*Internet_filter* ACL は、送信元アドレス 1.2.3.4 から送信されるすべてのトラフィックを許可します。

```
Device(config)# ip access-list standard Internet_filter
Device(config-ext-nacl)# permit 1.2.3.4
Device(config-ext-nacl)# exit
```

marketing_group ACL は、宛先アドレスとワイルドカードの値 171.69.0.0 0.0.255.255 への任意の TCP Telnet トラフィックを許可し、その他の TCP トラフィックを拒否します。ICMP トラフィックを許可し、任意の送信元から、宛先ポートが 1024 より小さい 171.69.0.0 ～ 179.69.255.255 の宛先アドレスへ送信される UDP トラフィックを拒否します。それ以外のすべての IP トラフィックを拒否して、結果を示すログが表示されます。

```
Device(config)# ip access-list extended marketing_group
Device(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Device(config-ext-nacl)# deny tcp any any
Device(config-ext-nacl)# permit icmp any any
```

```
Device(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Device(config-ext-nacl)# deny ip any any log
Device(config-ext-nacl)# exit
```

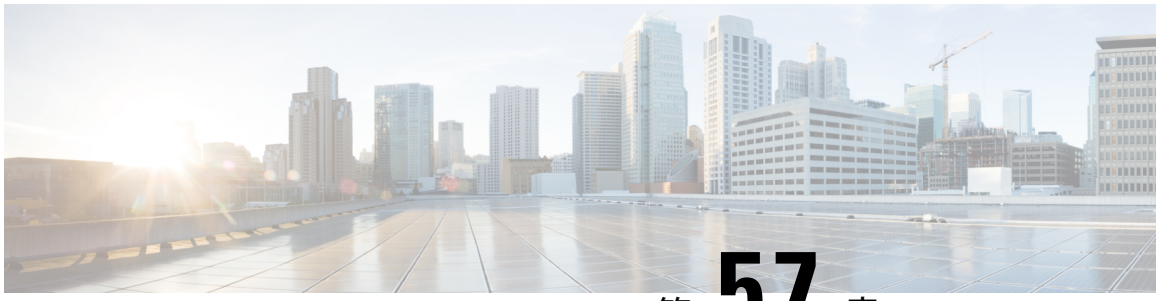
Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
Device(config)# interface gigabitethernet3/0/1

Device(config-if)# ip address 2.0.5.1 255.255.255.0
Device(config-if)# ip access-group Internet_filter out
Device(config-if)# ip access-group marketing_group in
```

名前付き ACL からの個別 ACE の削除

次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
Device(config)# ip access-list extended border-list
Device(config-ext-nacl)# no permit ip host 10.1.1.3 any
```



第 57 章

DNS ベースのアクセス コントロール リスト

DNS ベースのアクセス コントロール リストについて

DNS ベースの ACL は、Apple および Android デバイスなどのクライアント デバイスに使用されます。これらのデバイスを使用する場合、デバイスがアクセス権を持つ範囲を特定するために Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに認証前 ACL を設定できます。

コントローラで DNS ベースの ACL を有効にするには、ACL の許可された URL を設定する必要があります。URL は、ACL で事前設定しておく必要があります。

DNS ベースの ACL によって、登録フェーズ中のクライアントは、設定された URL への接続を許可されます。コントローラは ACL 名で設定され、認証前 ACL が適用されるように AAA サーバによって返されます。ACL 名が AAA サーバによって返されると、ACL は Web リダイレクト用にクライアントに適用されます。

クライアント認証フェーズでは、ISE サーバが事前認証 ACL （url-redirect acl）を返します。DNS スヌーピングは、登録が完了してクライアントが SUPPLICANT PROVISIONING 状態になるまで、各クライアントの AP で実行されます。URL で設定された ACL がコントローラで受信されると、CAPWAP ペイロードは AP に送信され、クライアントの DNS スヌーピングが有効になり URL がスヌーピングされます。

適切な URL スヌーピングにより、AP は DNS 応答の解決済みドメイン名の IP アドレスを学習します。ドメイン名が設定された URL に一致すると、DNS 応答が IP アドレスについて解析され、IP アドレスは CAPWAP ペイロードとしてコントローラに送信されます。コントローラに

よって IP アドレスの許可リストに IP アドレスが追加されるため、クライアントは設定された URL にアクセスできます。

DNS ベースのアクセス コントロール リストの制約事項

DNS ベースの ACL には次の制約があります。

- 認証前フィルタと認証後フィルタはローカルモードでサポートされています。Flex（ファブリック）モードでは認証前フィルタのみがサポートされています。
- ISE からプッシュされる ACL オーバーライドはサポートされていません。

Flex Mode

URL フィルタ リストの定義

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**urlfilter list** *list-name* 例： `Device(config)# urlfilter list urllist_flex_preauth`	URL フィルタ リストを設定します。 ここで、*list-name* は URL フィルタ リスト名を指します。リスト名は 32 文字以内の英数字にする必要があります。
ステップ 3	**action permit** 例： `Device(config-urlfilter-params)# action permit`	アクションとして、permit（ホワイトリスト）または deny（ブラックリスト）を設定します。
ステップ 4	**redirect-server-ip4** *IPv4-address* 例： `Device(config-urlfilter-params)# redirect-server-ipv4 8.8.8.8`	URL リストの IPv4 リダイレクト サーバを設定します。 ここで、*IPv4-address* は IPv4 アドレスを指します。
ステップ 5	**redirect-server-ip6** *IPv6-address* 例：	URL リストの IPv6 リダイレクト サーバを設定します。

	コマンドまたはアクション	目的
	`Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::81`	ここで、*IPv6-address* は IPv6 アドレスを指します。
ステップ 6	**url** *url* 例： `Device(config-urlfilter-params)# url url1.dns.com`	URL を設定します。 ここで、*url*は URL の名前を指します。
ステップ 7	**end** 例： `Device(config-urlfilter-params)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Flex プロファイルへの URL フィルタ リストの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *default-flex-profile* 例： `Device(config)# wireless profile flex default-flex-profile`	新しい flex ポリシーを作成します。 デフォルトの flex プロファイル名は *default-flex-profile* です。
ステップ 3	**acl-policy** *acl policy name* 例： `Device(config-wireless-flex-profile)# acl-policy acl_name`	ACL ポリシーを設定します。
ステップ 4	**urlfilter list** *name* 例： `Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth`	Flex プロファイルに URL リストを適用します。
ステップ 5	**end** 例： `Device(config-wireless-flex-profile-acl)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

中央 Web 認証用の ISE の設定（GUI）

中央 Web 認証用に ISE を設定するには、次の手順に従います。

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 [Policy] をクリックし、[Policy Elements] をクリックします。

ステップ 3 [Results] をクリックします。

ステップ 4 [Authorization] を展開し、[Authorization Profiles] をクリックします。

ステップ 5 [Add] をクリックして、URL フィルタ用の新しい許可プロファイルを作成します。

ステップ 6 [Name] フィールドにプロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

ステップ 7 [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] オプションを選択します。

ステップ 8 [Advanced Attributes Setting] セクションで、ドロップダウン リストから [Cisco:cisco-av-pair] を選択します。

ステップ 9 それぞれのペアの後にある（[+]）アイコンをクリックして 1 つずつ入力します。

- url-redirect-acl=<sample_name>
- url-redirect=<sample_redirect_URL>

次に例を示します。

```
Cisco:cisco-av-pair = priv-lvl=15
Cisco:cisco-av-pair = url-redirect-acl=ACL-REDIRECTTTTTTTTTTTTTTTTTTT2
Cisco:cisco-av-pair = url-redirect=
https://9.10.8.247:port/portal/gateway?sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-00505daf2f0a&daysToExpiry=value&action=cwa
```

ステップ 10 [Attributes Details] セクションの内容を確認し、[Save] をクリックします。

中央 Web 認証用の ISE の設定

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 [Policy] をクリックし、[Policy Elements] をクリックします。

ステップ 3 [Results] をクリックします。

ステップ 4 [Authorization] を展開し、[Authorization Profiles] をクリックします。

ステップ 5 [Add] をクリックして、URL フィルタ用の新しい許可プロファイルを作成します。

ステップ 6 [Name] フィールドに、プロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

ステップ 7 [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。

ステップ 8 [Advanced Attributes Setting] セクションで、ドロップダウン リストから [Cisco:cisco-av-pair] を選択します。

ステップ 9 それぞれのペアの後にある（[+]）アイコンをクリックして 1 つずつ入力します。

- url-redirect-acl=<sample_name>
- url-redirect=<sample_redirect_URL>

次に例を示します。

```
Cisco:cisco-av-pair = priv-lvl=15
Cisco:cisco-av-pair = url-redirect-acl=ACL-REDIRECTTTTTTTTTTTTTTTTTTT2
Cisco:cisco-av-pair = url-redirect=
https://9.10.8.247:port/portal/gateway?sessionId=SessionIdValue&portal=0ce17ad0-6d90-11e5-978e-00505bf2f0a&daysToExpiry=value&action=cwa
```

ステップ 10 [Attributes Details] セクションの内容を確認し、[Save] をクリックします。

ローカル モード

URL フィルタ リストの定義

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**urlfilter list** *list-name* 例： `Device(config)# urlfilter list urllist_local_preauth`	URL フィルタ リストを設定します。 ここで、*list-name* は URL フィルタ リスト名を指します。リスト名は 32 文字以内の英数字にする必要があります。
ステップ 3	**action permit** 例： `Device(config-urlfilter-params)# action permit`	アクションとして、permit（ホワイトリスト）または deny（ブラックリスト）を設定します。
ステップ 4	**filter-type post-authentication** 例：	（注） このステップは、認証後 URL フィルタを設定するときにのみ適用されます。

	コマンドまたはアクション	目的
	`Device(config-urlfilter-params)# filter-type post-authentication`	URL リストを認証後フィルタとして設定します。
ステップ 5	**redirect-server-ip4** *IPv4-address* 例： `Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101`	URL リストの IPv4 リダイレクト サーバを設定します。 ここで、*IPv4-address* は IPv4 アドレスを指します。
ステップ 6	**redirect-server-ip6** *IPv6-address* 例： `Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82`	URL リストの IPv6 リダイレクト サーバを設定します。 ここで、*IPv6-address* は IPv6 アドレスを指します。
ステップ 7	**url** *url* 例： `Device(config-urlfilter-params)# url url1.dns.com`	URL を設定します。 ここで、*url*は URL の名前を指します。
ステップ 8	**end** 例： `Device(config-urlfilter-params)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー プロファイルへの URL フィルタ リストの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	ワイヤレス ポリシー プロファイルを設定します。 ここで、*profile-policy* は WLAN ポリシー プロファイルの名前を指します。
ステップ 3	**urlfilter list** {**pre-auth-filter** *name* | **post-auth-filter** *name*} 例：	ポリシー プロファイルに URL リストを適用します。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# urlfilter list pre-auth-filter urllist_local_preauth` `Device(config-wireless-policy)# urlfilter list post-auth-filter urllist_local_postauth`	ここで、*name* は、以前に設定された認証前または認証後 URL フィルタ リストの名前を指します。 （注） クライアントの join 中に、ポリシーで設定された URL フィルタが適用されます。
ステップ 4	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

中央 Web 認証用の ISE の設定

許可プロファイルの作成

手順

ステップ 1 Cisco Identity Services Engine（ISE）にログインします。

ステップ 2 [Policy] をクリックし、[Policy Elements] をクリックします。

ステップ 3 [Results] をクリックします。

ステップ 4 [Authorization] を展開し、[Authorization Profiles] をクリックします。

ステップ 5 [Add] をクリックして、URL フィルタ用の新しい許可プロファイルを作成します。

ステップ 6 [Name] フィールドに、プロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

ステップ 7 [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。

ステップ 8 [Advanced Attributes Setting] セクションで、ドロップダウン リストから [Cisco:cisco-av-pair] を選択します。

ステップ 9 それぞれのペアの後にある（[+]）アイコンをクリックして 1 つずつ入力します。

- url-filter-preauth=<preauth_filter_name>
- url-filter-postauth=<postauth_filter_name>

次に例を示します。

```
Cisco:cisco-av-pair = url-filter-preauth=urllist_pre_cwa
Cisco:cisco-av-pair = url-filter-postauth=urllist_post_cwa
```

ステップ 10 [Attributes Details] セクションの内容を確認し、[Save] をクリックします。

認証ルールへの許可プロファイルのマッピング

手順

ステップ 1 [Policy] > [Authentication] ページで、[Authentication] をクリックします。

ステップ 2 認証ルールの名前を入力します。

たとえば、「MAB」と入力します。

ステップ 3 [If] 条件フィールドで、プラス（[+]）アイコンをクリックします。

ステップ 4 [Compound condition] を選択し、[WLC_Web_Authentication] を選択します。

ステップ 5 [and ...] の横にある矢印をクリックして、ルールをさらに展開します。

ステップ 6 [Identity Source] フィールドの [+] アイコンをクリックし、[Internal endpoints] を選択します。

ステップ 7 [If user not found] ドロップダウン リストから [Continue] を選択します。

このオプションを使用すると、MAC アドレスが不明な場合でもデバイスを認証できます。

ステップ 8 **[保存（Save）]** をクリックします。

許可ルールへの許可プロファイルのマッピング

手順

ステップ 1 [Policy] > [Authorization] をクリックします。

ステップ 2 [Rule Name] フィールドに、名前を入力します。

たとえば、「CWA Post Auth」などと入力します。

ステップ 3 [Conditions] フィールドで、プラス（[+]）アイコンを選択します。

ステップ 4 ドロップダウン リストをクリックして、[Identity Groups] 領域を表示します。

ステップ 5 [User Identity Groups] > [user_group] を選択します。

ステップ 6 [and ...] の横にあるプラス記号（[+]）をクリックして、ルールをさらに展開します。

ステップ 7 [Conditions] フィールドで、プラス（[+]）アイコンを選択します。

ステップ 8 [Compound Conditions] を選択し、新しい条件の作成を選択します。

ステップ 9 設定アイコンで、オプションから [Add Attribute/Value] を選択します。

ステップ 10 [Description] フィールドで、ドロップダウン リストから属性として [Network Access] > [UseCase] を選択します。

ステップ 11 [Equals] 演算子を選択します。

ステップ 12 右側のフィールドから、[GuestFlow] を選択します。

ステップ 13 [Permissions] フィールドで、プラス（[+]）アイコンを選択してルールの結果を選択します。

[Standard] > [PermitAccess] オプションを選択するか、または必要な属性を返すカスタム プロファイルを作成できます。

DNS ベースのアクセス コントロール リストの表示

指定されたワイヤレス URL フィルタの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless urlfilter details <urllist_flex_preauth>
```

すべてのワイヤレス URL フィルタのサマリーを表示するには、次のコマンドを使用します。

```
Device# show wireless urlfilter summary
```

結果のポリシー セクションでクライアントに適用された URL フィルタを表示するには、次のコマンドを使用します。

```
Device# show wireless client mac-address <MAC_addr> detail
```

DNS ベースのアクセス コントロール リストの設定例

Flex Mode

例：*URL* フィルタ リストの定義

次に、Flex モードで URL リストを定義する例を示します。

```
Device# configure terminal
Device(config)# urlfilter list urllist_flex_pre
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4 8.8.8.8
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::81
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

例：*Flex* プロファイルへの *URL* フィルタ リストの適用

次に、Flex モードで Flex プロファイルに URL リストを適用する例を示します。

```
Device# configure terminal
Device(config)# wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy acl_name
Device(config-wireless-flex-profile-acl)# urlfilter list urllist_flex_preauth
Device(config-wireless-flex-profile-acl)# end
```

ローカル モード

例：認証前 *URL* フィルタ リストの定義

次に、URL フィルタ リスト（認証前）を定義する例を示します。

```
Device# configure terminal
Device(config)# urlfilter list urllist_local_preauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

例*:*：認証後 *URL* フィルタ リストの定義

次に、URL フィルタ リスト（認証後）を定義する例を示します。

```
Device# configure terminal
Device(config)# urlfilter list urllist_local_postauth
Device(config-urlfilter-params)# action permit
Device(config-urlfilter-params)# filter-type post-authentication
Device(config-urlfilter-params)# redirect-server-ipv4 9.1.0.101
Device(config-urlfilter-params)# redirect-server-ipv6 2001:300:8::82
Device(config-urlfilter-params)# url url1.dns.com
Device(config-urlfilter-params)# end
```

例：ポリシー プロファイルへの *URL* フィルタ リストの適用

次に、ローカル モードでポリシー プロファイルに URL リストを適用する例を示します。

```
Device# configure terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# urlfilter list pre-auth-filter urllist_local_preauth
Device(config-wireless-policy)# urlfilter list post-auth-filter urllist_local_postauth
Device(config-wireless-policy)# end
```

DNS スヌーピング エージェント（DSA）の確認

DNS スヌーピング エージェント クライアントの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
```

DSA が有効になっているインターフェイスの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
enabled-intf
```

uCode メモリ内のパターン リストを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list
```

パターン リストの OpenDNS 文字列を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
hw-pattern-list odns_string
```

パターン リストの FQDN フィルタを表示するには、次のコマンドを使用します。

```
Device#
show platform hardware chassis active qfp feature dns-snoop-agent client hw-pattern-list
 fqdn-filter <fqdn_filter_ID>
```

（注） *fqdn_filter_ID* の有効な範囲は 1 ～ 16 です。

DSA クライアントの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client info
```

CPP クライアントのパターン リストを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
pattern-list
```

パターン リストの OpenDNS 文字列を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
pattern-list odns_string
```

パターン リストの FQDN フィルタを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent client
pattern-list fqdn-filter <fqdn_filter_ID>
```

（注） *fqdn_filter_ID* の有効な範囲は 1 ～ 16 です。

DSA データパスの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
```

DSA IP キャッシュ テーブルの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache
```

DSA アドレス エントリの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache address {ipv4 <IPv4_addr> | ipv6 <IPv6_addr>}
```

すべての DSA IP キャッシュ アドレスの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache all
```

DSA IP キャッシュ パターンの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
ip-cache pattern <pattern>
```

DSA データパス メモリの詳細を表示するには、次のコマンドを使用します。

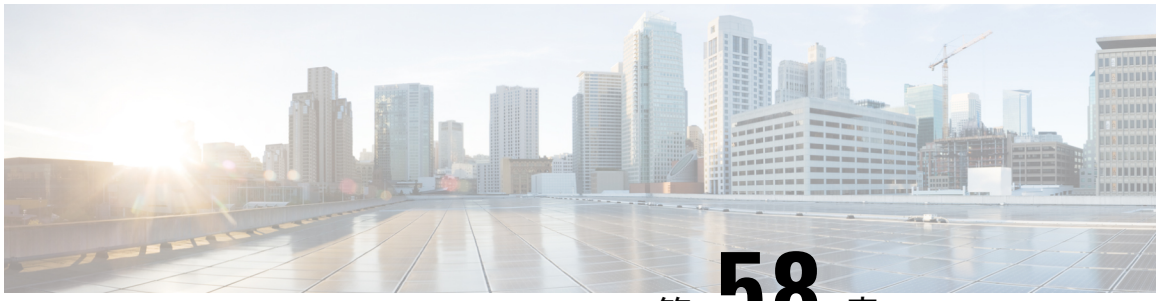
```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath memory
```

DSA 正規表現テーブルを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath
regexp-table
```

DSA の統計情報を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature dns-snoop-agent datapath stats
```



第 58 章

特定の URL のホワイトリスト登録

特定の URL のホワイトリスト登録

この機能は、コントローラまたは AP で特定の URL をホワイトリストに登録するのに便利です。これにより、インターネットに接続していなくてもそれらの特定の URL を使用できるようになります。キャプティブ ポータルとウォールド ガーデンの Web 認証用の URL をホワイトリストに登録できます。ホワイトリストに登録された URL にアクセスする際に認証は必要ありません。ホワイトリストに登録されていないサイトにアクセスしようとすると、ログインページにリダイレクトされます。

URL ホワイトリスト登録の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**urlfilter list** *<urlfilter-name>* 例： `Device(config)# urlfilter list url-whitelist-nbn`	URLfilter プロファイルを設定します。
ステップ 3	**action**［**deny** | **permit**］ 例：	リストをホワイトリストとして設定します。**Permit** コマンドではリストをホワイトリストとして設定し、**deny** コマン

	コマンドまたはアクション	目的
	`Device(config-urlfilter-params)#action permit`	ドではリストをブラックリストとして設定します。
ステップ 4	{**redirect-server-ipv4** | **redirect-server-ipv6**} 例： `Device(config-urlfilter-params)#redirect-server-ipv4 X.X.X.X`	IPv4 または IPv6 サーバにリストを設定します。
ステップ 5	**url** *url-to-be-whitelisted* 例： `Device(config-urlfilter-params)#url www.cisco.com`	URL をホワイトリストに登録します。

ホワイトリストに登録された URL フィルタは、flex プロファイルで ACL ポリシーに関連付ける必要があります。

（注） **acl-policy** の名前を *preauth_v4* と指定する必要があります。そうしないと AP に適用されません。

例

flexプロファイルでのホワイトリストに登録されたURLとACLポリシーの関連付け：

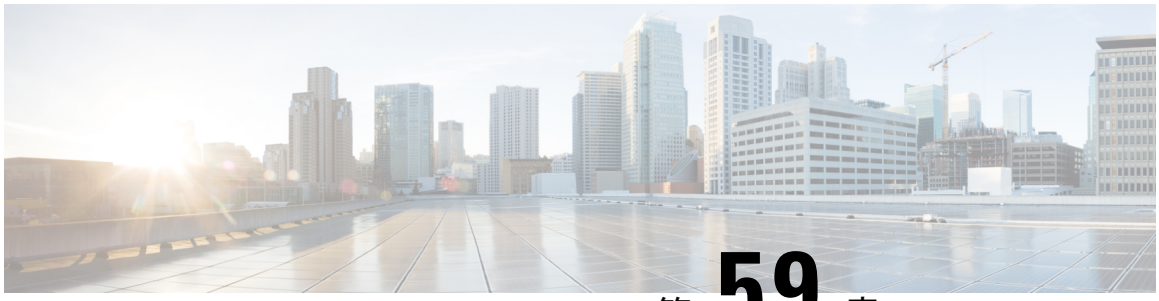
```
Device(config)#wireless profile flex default-flex-profile
Device(config-wireless-flex-profile)# acl-policy preauth_v4
Device(config-wireless-flex-profile-acl)# urlfilter list url_whitelist_nbn
Device(config-wireless-flex-profile-acl)# exit
Device(config-wireless-flex-profile)# description "default flex profile"
```

コントローラでの URL ホワイトリスト登録の確認

コントローラでのURLホワイトリストのサマリーと詳細を確認するには、次の **show** コマンドを使用します。

```
Device#show wireless urlfilter summary
Black-list    - DENY
White-list    - PERMIT
Filter-Type   - Specific to Local Mode

URL-List                          ID  Filter-Type  Action   Redirect-ipv4  Redirect-ipv6
-------------------------------------------------------------------------------------------
url-whitelist                     1    PRE-AUTH     PERMIT   1.1.1.1

Device#

Device#show wireless urlfilter details url-whitelist
```

```
List Name.................. : url-whitelist
Filter ID.............. : : 1
Filter Type................ : PRE-AUTH
Action..................... : PERMIT
Redirect server ipv4...... : 1.1.1.1
Redirect server ipv6...... :
Configured List of URLs
   URL..................... : www.cisco.com
```



第 59 章

Web ベース認証

この章では、デバイスで Web ベース認証を設定する方法について説明します。この章の内容は、次のとおりです。

ローカル Web 認証の概要

IEEE 802.1x サプリカントが実行されていないホスト システムでエンド ユーザを認証するには、Web 認証プロキシとして知られているローカル Web 認証機能を使用します。

（注） Web ベース認証は、レイヤ 2 およびレイヤ 3 インターフェイス上に設定できます。

HTTP セッションを開始すると、ローカル Web 認証は、ホストからの入力 HTTP パケットを代行受信し、ユーザに HTML ログイン ページを送信します。ユーザはクレデンシャルを入力します。このクレデンシャルは、ローカル Web 認証機能により、認証のために認証、許可、アカウンティング（AAA）サーバに送信されます。

認証に成功した場合、ローカル Web 認証は、ログインの成功を示す HTML ページをホストに送信し、AAA サーバから返されたアクセス ポリシーを適用します。

認証に失敗した場合、ローカル Web 認証は、ログインの失敗を示す HTML ページをユーザに転送し、ログインを再試行するように、ユーザにプロンプトを表示します。最大試行回数を超過した場合、ローカル Web 認証は、ログインの期限切れを示す HTML ページをホストに転送し、このユーザは Web 認証の失敗という除外理由で除外されます。

（注） WLAN のグローバルまたはパラメータ マップ（method-type、custom、redirect）は、同じ Web 認証方式（consent、web consent、webauth など）を使用するときにのみ使用する必要があります。WLAN にパラメータマップを設定していない場合は、グローバル パラメータマップがデフォルトで適用されます。

（注） Webauth クライアントの認証試行時に受信する traceback には、パフォーマンスや行動への影響はありません。これは、ACL アプリケーションの EPM に FFM が返信したコンテキストがすでにキュー解除済み（タイマーの有効期限切れの可能性あり）で、セッションが「未承認」になった場合にまれに発生します。

Web ページがホストされている場所に基づいて、ローカル Web 認証は次のように分類できます。

- 内部：ローカル Web 認証時に、コントローラの内部デフォルト HTML ページ（ログイン、成功、失敗、および期限切れ）が使用されます。
- カスタマイズ：ローカル Web 認証時に、カスタマイズされた Web ページ（ログイン、成功、失敗、および期限切れ）がコントローラにダウンロードされ、使用されます。
- 外部：組み込みまたはカスタム Web ページを使用する代わりに、外部 Web サーバ上でカスタマイズされた Web ページがホストされます。

さまざまな Web 認証ページに基づき、Web 認証のタイプは次のように分類できます。

- *Webauth*：これが基本的な Web 認証です。この場合、コントローラはユーザ名とパスワードの入力が必要なポリシーページを提示します。ネットワークにアクセスするには、ユーザは正しいクレデンシャルを入力する必要があります。
- *Consent* または *web-passthrough*：この場合、コントローラは [Accept] ボタンまたは [Deny] ボタンが表示されたポリシー ページを提示します。ネットワークにアクセスするには、ユーザは [Accept] ボタンをクリックする必要があります。
- *Webconsent*：これは webauth と consent の Web 認証タイプの組み合わせです。この場合、コントローラは [Accept] ボタンまたは [Deny] ボタンがあり、ユーザ名とパスワードの入力が必要なポリシーページを提示します。ネットワークにアクセスするには、ユーザは正しいクレデンシャルを入力して [Accept] ボタンをクリックする必要があります。

（注）
- webauth パラメータマップ情報は、**show running-config** コマンドの出力を使用して表示できます。
- ワイヤレス Web 認証機能は、バイパス タイプをサポートしていません。

関連トピック

無線ゲスト アクセス （1119 ページ）

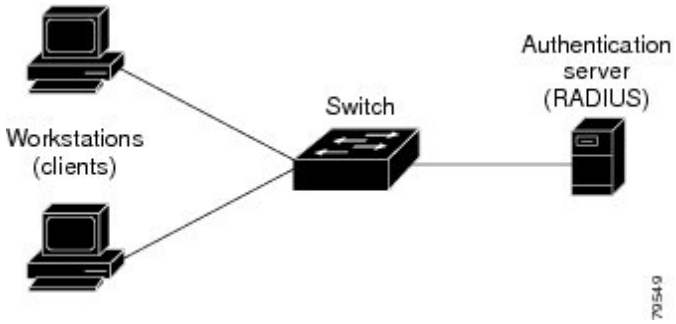
デバイスのロール

ローカル Web 認証では、ネットワーク上のデバイスに次のような固有の役割があります。

- クライアント：LAN およびサービスへのアクセスを要求し、スイッチからの要求に応答するデバイス（ワークステーション）。このワークステーションでは、JavaScript がイネーブルに設定された HTML ブラウザが実行されている必要があります。
- 認証サーバ：クライアントを認証します。認証サーバはクライアントの識別情報を確認し、そのクライアントが LAN およびスイッチのサービスへのアクセスを許可されたか、あるいはクライアントが拒否されたのかをスイッチに通知します。
- スイッチ：クライアントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。スイッチはクライアントと認証サーバとの仲介デバイス（プロキシ）として動作し、クライアントに識別情報を要求し、その情報を認証サーバで確認し、クライアントに応答をリレーします。

図 *9*：ローカル *Web* 認証のデバイスの役割

次の図は、ネットワーク上でのこれらのデバイスの役割を示します。



認証プロセス

ローカル Web 認証を有効にすると、次のイベントが発生します。

- ユーザが HTTP セッションを開始します。
- HTTP トラフィックが代行受信され、認証が開始されます。スイッチは、ユーザにログインページを送信します。ユーザはユーザ名とパスワードを入力します。スイッチはこのエントリを認証サーバに送信します。
- 認証に成功した場合、スイッチは認証サーバからこのユーザのアクセスポリシーをダウンロードし、アクティブ化します。ログインの成功ページがユーザに送信されます
- 認証に失敗した場合は、スイッチはログインの失敗ページを送信します。ユーザはログインを再試行します。失敗の回数が試行回数の最大値に達した場合、スイッチはログイン期

限切れページを送信します。このホストはウォッチ リストに入れられます。ウォッチ リストのタイム アウト後、ユーザは認証プロセスを再試行することができます。

- 認証サーバがスイッチに応答せず、AAA 失敗ポリシーが設定されている場合、スイッチはホストに失敗アクセス ポリシーを適用します。ログインの成功ページがユーザに送信されます
- ホストがレイヤ 2 インターフェイス上の ARP プローブに応答しなかった場合、またはホストがレイヤ 3 インターフェイスでアイドル タイムアウト内にトラフィックを送信しなかった場合、スイッチはクライアントを再認証します。
- この機能は、ダウンロードされたタイムアウト、またはローカルに設定されたセッション タイムアウトを適用します。

（注） Cisco IOS XE Denali 16.1.1 以降では、WLC でのローカル Web 認証のデフォルトのセッション タイムアウト値は1800秒です。Cisco IOS XE Denali 16.1.1 より前は、デフォルトのセッション タイムアウト値は無限の秒数でした。

- Termination-Action が RADIUS である場合、この機能は、サーバに NRH 要求を送信します。Termination-Action は、サーバからの応答に含まれます。
- Termination-Action がデフォルトである場合、セッションは廃棄され、適用されたポリシーは削除されます。

ローカル Web 認証バナー

Web 認証を使用して、デフォルトのカスタマイズ済み Web ブラウザ バナーを作成して、スイッチにログインしたときに表示するようにできます。

このバナーは、ログインページと認証結果ポップアップページの両方に表示されます。デフォルトのバナー メッセージは次のとおりです。

- 認証成功
- 認証失敗
- 認証期限切れ

ローカル Web 認証バナーは、新スタイル（セッション認識型）の CLI モードで次のように設定できます。

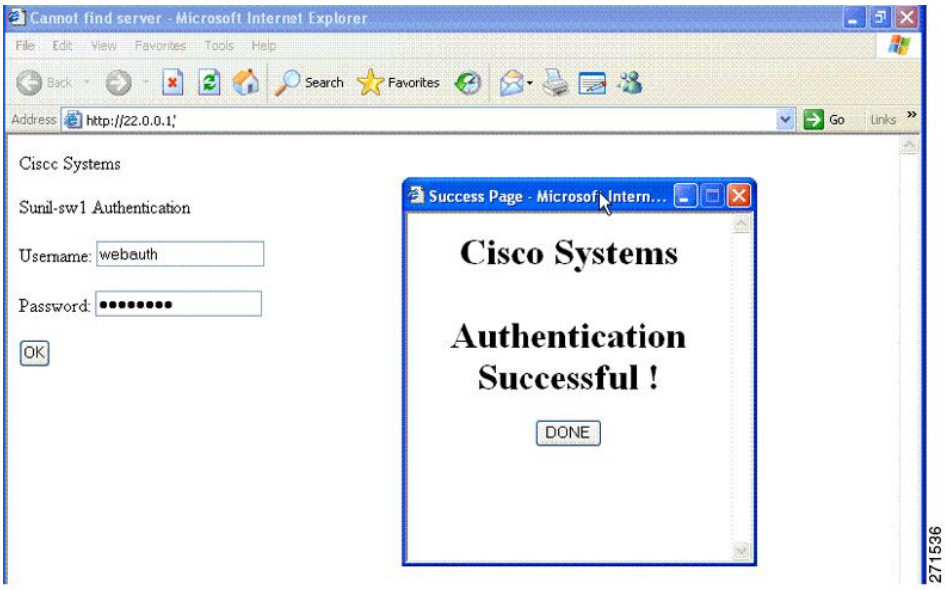
- 新スタイル モード：次のグローバル コンフィギュレーション コマンドを使用します。

  parameter-map type webauth global

  banner text <text>

ログイン ページには、デフォルトのバナー、*Cisco Systems*、および *Switch host-name Authentication* が表示されます。*Cisco Systems* は認証結果ポップアップ ページに表示されます。

図 *10* : 認証成功バナー



バナーは次のようにカスタマイズ可能です。

- スイッチ名、ルータ名、または会社名などのメッセージをバナーに追加する。
  - 新スタイルモード：次のグローバルコンフィギュレーション コマンドを使用します。

    parameter-map type webauth global

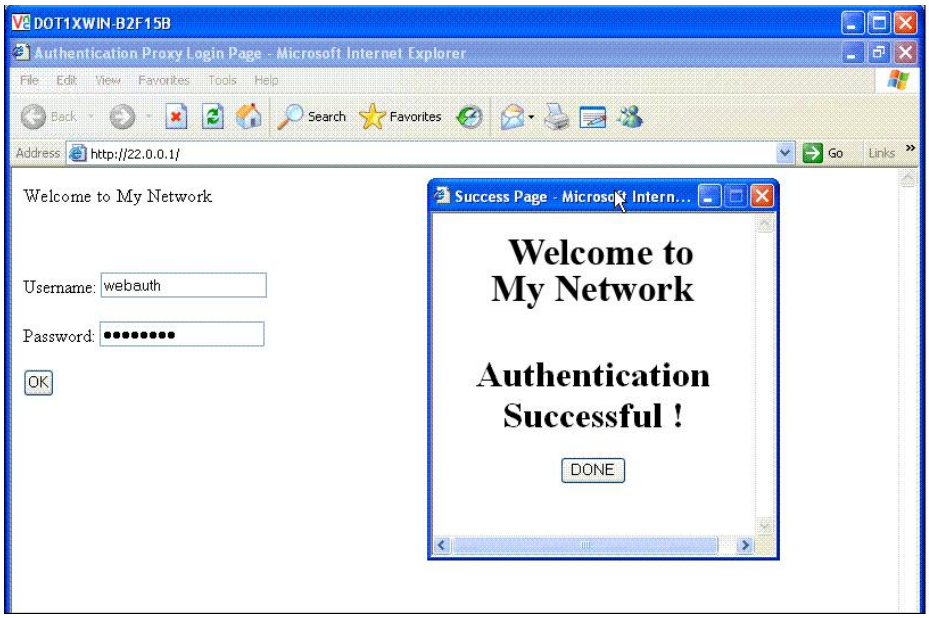
    banner text <text>

- ロゴまたはテキスト ファイルをバナーに追加する。
  - 新スタイルモード：次のグローバルコンフィギュレーション コマンドを使用します。

    parameter-map type webauth global

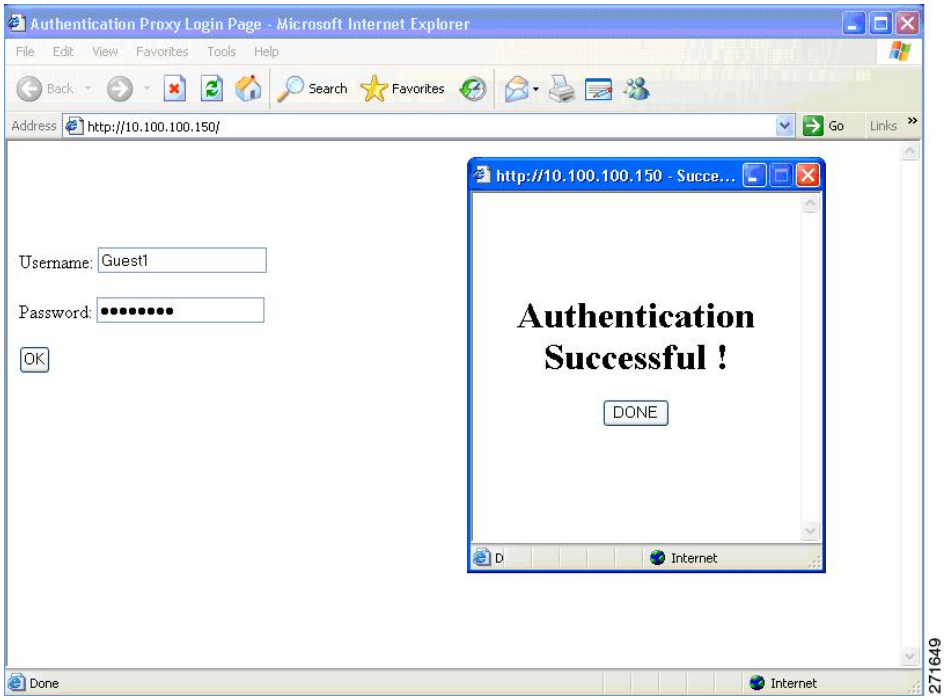
    banner file <filepath>

図 *11* : カスタマイズされた *Web* バナー



バナーがイネーブルにされていない場合、Web認証ログイン画面にはユーザ名とパスワードのダイアログボックスだけが表示され、スイッチにログインしたときにはバナーは表示されません。

図 *12* : バナーが表示されていないログイン画面



カスタマイズされたローカル Web 認証

ローカル Web 認証プロセスでは、スイッチ内部の HTTP サーバは、認証中のクライアントに配信される4種類のHTMLページをホストします。サーバはこれらのページを使用して、ユーザに次の 4 種類の認証プロセス ステートを通知します。

- ログイン：資格情報が要求されています。
- 成功：ログインに成功しました。
- 失敗：ログインに失敗しました。
- 期限切れ：ログインの失敗回数が多すぎて、ログイン セッションが期限切れになりました。

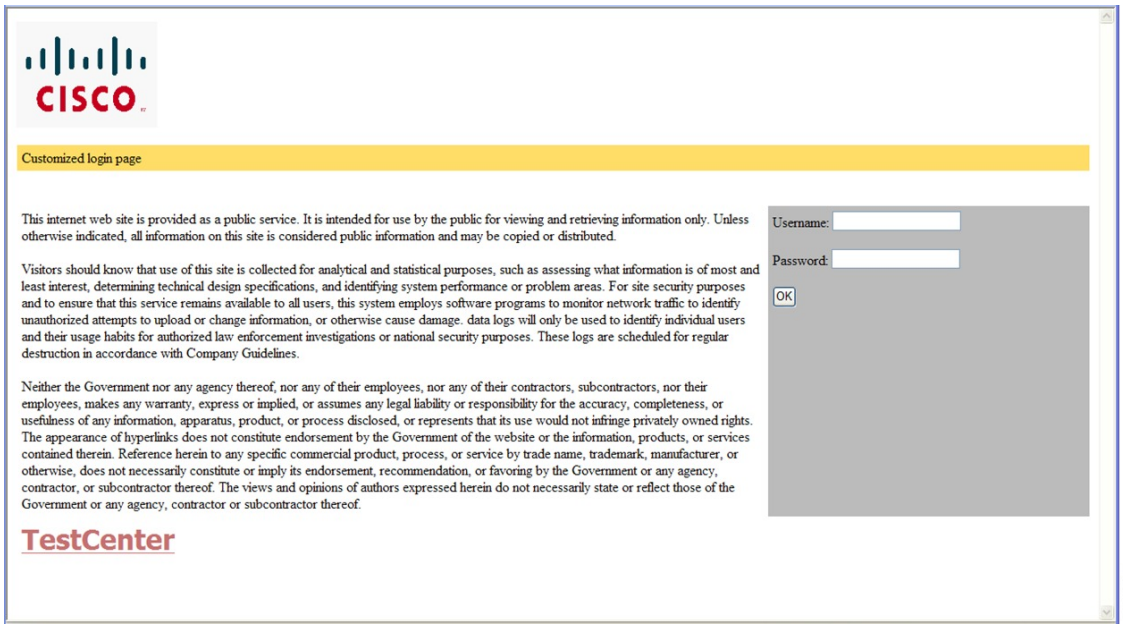
ガイドライン

- デフォルトの内部 HTML ページの代わりに、独自の HTML ページを使用することができます。
- ロゴを使用することもできますし、ログイン、成功、失敗、および期限切れ Web ページでテキストを指定することもできます。
- バナー ページで、ログイン ページのテキストを指定できます。
- これらのページは、HTML で記述されています。
- 成功ページには、特定の URL にアクセスするための HTML リダイレクト コマンドを記入する必要があります。
- この URL 文字列は有効な URL（例：http://www.cisco.com）でなければなりません。不完全なURLは、Webブラウザで、「ページが見つかりません」またはこれに類似するエラーの原因となる可能性があります。
- HTTP 認証で使用される Web ページを設定する場合、これらのページには適切な HTML コマンド（例：ページのタイムアウトを設定、暗号化されたパスワードの設定、同じページが 2 回送信されていないことの確認など）を記入する必要があります.
- 設定されたログイン フォームがイネーブルにされている場合、特定の URL にユーザをリダイレクトするCLIコマンドは使用できません。管理者は、Webページにリダイレクトが設定されていることを保証する必要があります。
- 認証後、特定のURLにユーザをリダイレクトするCLIコマンドを入力してから、Webページを設定するコマンドを入力した場合、特定の URL にユーザをリダイレクトする CLI コマンドは効力を持ちません。
- 設定された Web ページは、スイッチのブート フラッシュ、またはフラッシュにコピーできます。
- ログインページを1つのフラッシュ上に、成功ページと失敗ページを別のフラッシュ（たとえば、スタック マスター、またはメンバのフラッシュ）にすることができます。

- 4 ページすべてを設定する必要があります。
- Web ページを使ってバナー ページを設定した場合、このバナー ページには効果はありません。
- システムディレクトリ（たとえば、flash、disk0、disk）に保存されていて、ログイン ページに表示する必要のあるロゴ ファイル（イメージ、フラッシュ、オーディオ、ビデオなど）すべてには、必ず、*web_auth_<filename>* の形式で名前をつけてください。
- 設定された認証プロキシ機能は、HTTP と SSL の両方をサポートしています。

デフォルトの内部 HTML ページの代わりに、自分の HTML ページを使用することができます。認証後のユーザのリダイレクト先で、内部成功ページの代わりとなる URL を指定することもできます。

図 *13* : カスタマイズ可能な認証ページ



成功ログインに対するリダイレクト URL の注意事項

成功ログインに対するリダイレクション URL を設定する場合、次の注意事項に従ってください。

- カスタム認証プロキシ Web ページ機能がイネーブルに設定されている場合、リダイレクション URL 機能はディセーブルにされ、CLI では使用できません。リダイレクションは、カスタム ログイン成功ページで実行できます。
- リダイレクション URL 機能が有効に設定されている場合、設定された auth-proxy-banner は使用されません。
- リダイレクション URL の指定を解除するには、このコマンドの **no** 形式を使用します。

- Web ベースの認証クライアントが正常に認証された後にリダイレクション URL が必要な場合、URL 文字列は有効な URL（たとえば http://）で開始し、その後に URL 情報が続く必要があります。http:// を含まないURL が指定されると、正常に認証が行われても、そのリダイレクション URL によって Web ブラウザでページが見つからないまたは同様のエラーが生じる場合があります。

ローカル Web 認証の設定方法

デフォルトのローカル Web 認証の設定

次の表に、デフォルトのローカル Web 認証の設定を示します。

表 *16 :* デフォルトのローカル *Web* 認証の設定

機能	デフォルト設定
AAA	無効
RADIUS サーバ • IP アドレス • UDP 認証ポート • Key	• 指定なし • 指定なし
無活動タイムアウトのデフォルト値	3600 秒
無活動タイムアウト	イネーブル

AAA 認証の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。

ステップ 2 [Authentication] セクションで [Add] をクリックします。

ステップ 3 表示される [Quick Setup: AAA Authentication] ウィンドウに、メソッド リストの名前を入力します。

ステップ 4 ネットワークへのアクセスを許可する前に実行する認証のタイプを [Type] ドロップダウン リストから選択します。

ステップ 5 [Group Type] ドロップダウン リストから、サーバのグループをアクセス サーバとして割り当てるか、またはローカル サーバを使用してアクセスを認証するかを選択します。

ステップ 6 グループ内のサーバが使用できない場合にフォールバック方式として機能するようにローカルサーバを設定するには、[Fallback to local] チェックボックスをオンにします。

ステップ 7 [Available Server Groups] リストで、ネットワークへのアクセスの認証に使用するサーバ グループを選択し、[>] アイコンをクリックして [Assigned Server Groups] リストに移動します。

ステップ 8 [Save & Apply to Device] をクリックします。

AAA 認証の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA 機能をイネーブルにします。
ステップ 2	**aaa authentication login** {**default** | *named_authentication_list*} **group** *AAA_group_name* 例： `Device(config)# aaa authentication login default group group1`	ログイン時の認証方法のリストを定義します。 **named_authentication_list** は、31 文字未満の名前を示します。 **AAA_group_name** はサーバ グループ名を示します。サーバグループ **server_name** をその先頭で定義する必要があります。
ステップ 3	**aaa authorization network** {**default** | **named**} **group** *AAA_group_name* 例： `Device(config)# aaa authorization network default group group1`	Web ベース許可の許可方式リストを作成します。
ステップ 4	**tacacs server** *server-name* 例： `Device(config)# tacacs server yourserver`	AAA サーバを指定します。
ステップ 5	**address** {**ipv4** | **ipv6**}*ip_address* 例：	TACACS サーバの IP アドレスを設定します。

	コマンドまたはアクション	目的
	`Device(config-server-tacacs)# address ipv4 10.0.1.12`	
ステップ 6	**tacacs-server host** {*hostname* | *ip_address*} 例： `Device(config)# tacacs-server host 10.1.1.1`	AAA サーバを指定します。

HTTP/HTTPS サーバの設定（GUI）

手順

ステップ 1 **[Administration]** > **[Management]** > **[HTTP/HTTPS/Netconf]** の順に選択します。

ステップ 2 [HTTP/HTTPS Access Configuration] セクションで、[HTTP Access] を有効にして、HTTP 要求をリッスンするポートを入力します。デフォルトのポートは 80 です。有効な値は、80 または 1025 ～ 65535 の値です。

ステップ 3 デバイスで [HTTPS Access] を有効にし、HTTPS 要求をリッスンする指定ポートを入力します。デフォルトのポートは 1025 です。有効な値は、443 または 1025 ～ 65535 の値です。セキュア HTTP 接続の場合、HTTP サーバが送受信するデータは暗号化されてインターネットに送信されます。SSL 暗号化を伴う HTTP は、Web ブラウザからスイッチを設定するような機能に、セキュアな接続を提供します。

ステップ 4 [Personal Identity Verification] について [enabled] または [disabled] を選択します。

ステップ 5 [HTTP Trust Point Configuration] セクションで、[Enable Trust Point] を有効にして、認証局サーバをトラストポイントとして使用します。

ステップ 6 [Trust Points] ドロップダウン リストから、トラスト ポイントを選択します。

ステップ 7 [Timeout Policy Configuration] セクションで、HTTP タイムアウト ポリシーを秒単位で入力します。有効な値の範囲は、10 ～ 600 秒です。

ステップ 8 セッションがタイムアウトするまでに許容される非アクティブな時間（分数）を入力します。有効な値の範囲は、180 ～ 1200 秒です。

ステップ 9 サーバの有効期間を秒単位で入力します。有効値の範囲は、1 ～ 86400 秒です。

ステップ 10 デバイスが受け取ることのできる要求の最大数を入力します。有効値の範囲は、1 ～ 86400 件です。

ステップ 11 設定を保存します。

HTTP サーバの設定（CLI）

ローカル Web 認証を使用するには、Device内で HTTP サーバをイネーブルにする必要があります。このサーバは HTTP または HTTPS のいずれかについてイネーブルにできます。

（注） Apple の疑似ブラウザは、**ip http secure-server** コマンドを設定するだけでは開きません。**ip http server** コマンドも設定する必要があります。

HTTP または HTTPS のいずれかについてサーバをイネーブルにするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip http server** 例： `Device(config)# ip http server`	HTTP サーバをイネーブルにします。ローカル Web 認証機能は、HTTP サーバを使用してホストと通信し、ユーザ認証を行います。
ステップ 4	**ip http secure-server** 例： `Device(config)# ip http secure-server`	HTTPS をイネーブルにします。 カスタム認証プロキシ Web ページを設定するか、成功ログインのリダイレクション URL を指定します。 （注） **ip http secure-server** コマンドを入力したときに、セキュア認証が確実に行われるようにするには、ユーザが HTTP 要求を送信した場合でも、ログイン ページは必ずHTTPS（セキュアHTTP）形式になるようにします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

パラメータ マップの作成

ローカル Web 認証の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Web Auth] ページで、[Add] をクリックします。

ステップ 3 表示される [Create Web Auth Parameter] ウィンドウで、パラメータ マップの名前を入力します。

ステップ 4 [Maximum HTTP Connections] フィールドに、許可する HTTP 接続の最大数を入力します。

ステップ 5 [Init-State Timeout] フィールドに、ユーザがログイン ページで有効なログイン情報を入力できなかったために初期状態タイマーを期限切れにするまでの時間を入力します。

ステップ 6 Web 認証パラメータのタイプを選択します。

ステップ 7 [Apply to Device] をクリックします。

ステップ 8 [Web Auth] ページで、パラメータ マップの名前をクリックします。

ステップ 9 表示される [Edit WebAuth Parameter] ウィンドウで、必要な [Banner Type] を選択します。

- [Banner Text] を選択した場合は、表示するバナー テキストを入力します。
- [File Name] を選択した場合は、バナー テキストを取得する取得元のファイルのパスを指定します。

ステップ 10 必要に応じて、仮想 IP アドレスを入力します。

ステップ 11 [WebAuth Intercept HTTPS]、[Captive Bypass Portal]、および [Watch List Enable] の適切なステータスを設定します。

ステップ 12 [Watch List Expiry Timeout] フィールドに、ウォッチリストをタイムアウトにするまでの時間を秒単位で入力します。

ステップ 13 [Disable Success Window]、[Disable Logout Window]、および [Login Auth Bypass for FQDN] の適切なステータスを設定します。

ステップ 14 スリープ状態のクライアントの認証を有効にするには、[Sleeping Client Status] チェックボックスをオンにし、[Sleeping Client Timeout] を分単位で指定します。有効な範囲は 10 ～ 43200 分です。

ステップ 15 [Advanced] タブをクリックします。

ステップ 16 [Redirect for log-in] フィールドに、ログイン要求を送信する外部サーバの名前を入力します。

ステップ 17 [Redirect On-Success] フィールドに、ログインが成功した後にリダイレクトする外部サーバの名前を入力します。

ステップ 18 [Redirect On-Failure] フィールドに、ログインが失敗した後にリダイレクトする外部サーバの名前を入力します。

ステップ 19 外部ローカル Web 認証を設定するには、次のタスクを実行します。

a) [Redirect to External Server] の [edirect Append for AP MAC Address] フィールドに、AP の MAC アドレスを入力します。

b) [Redirect Append for Client MAC Address] フィールドに、クライアントの MAC アドレスを入力します。

c) [Redirect Append for WLAN SSID] フィールドに、WLAN SSID を入力します。

d) [Portal IPV4 Address] フィールドに、リダイレクトを送信するポータルの IPv4 アドレスを入力します。

e) IPv6 アドレスを使用する場合は、[Portal IPV6 Address] フィールドに、リダイレクトを送信するポータルの IPv6 アドレスを入力します。

ステップ 20 カスタマイズされたローカル Web 認証を設定するには、次のタスクを実行します。

a) [Customized Page] で、次のページを指定します。

- **[Login Failed Page]**
- **[Login Page]**
- **[Logout Page]**
- **[Login Successful Page]**

ステップ 21 [Update & Apply] をクリックします。

内部ローカル Web 認証の設定（CLI）

内部ローカル Web 認証を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**parameter-map type webauth** {*parameter-map-name* | **global**} 例： `Device(config)# parameter-map type webauth sample`	パラメータ マップを作成します。 **parameter-map-name** は 99 文字を超えないようにする必要があります。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

カスタマイズされたローカル Web 認証の設定（CLI）

カスタマイズされたローカル Web 認証を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)# parameter-map type webauth sample`	webauth タイプ パラメータを設定します。
ステップ 4	**type** {**authbypass** | **consent** | **webauth** | **webconsent**} 例： `Device(config-params-parameter-map)# type webauth`	WebAuth のサブタイプとして、passthru、consent、webauth、webconsent などを設定します。

	コマンドまたはアクション	目的
ステップ 5	**custom-page login device** *html-filename* 例： `Device(config-params-parameter-map)# custom-page login device bootflash:login.html`	カスタマイズされたログイン ページを設定します。
ステップ 6	**custom-page login expired device** *html-filename* 例： `Device(config-params-parameter-map)# custom-page login expired device bootflash:loginexpired.html`	カスタマイズされたログイン期限切れページを設定します。
ステップ 7	**custom-page success device** *html-filename* 例： `Device(config-params-parameter-map)# custom-page success device bootflash:loginsuccess.html`	カスタマイズされたログイン成功ページを設定します。
ステップ 8	**custom-page failure device** *html-filename* 例： `Device(config-params-parameter-map)# custom-page failure device bootflash:loginfail.html`	カスタマイズされたログイン失敗ページを設定します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

外部ローカル Web 認証の設定（CLI）

外部ローカル Web 認証を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# 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 3	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)# parameter-map type webauth sample`	webauth タイプ パラメータを設定します。
ステップ 4	**type** {**authbypass** | **consent** | **webauth** | **webconsent**} 例： `Device(config-params-parameter-map)# type webauth`	WebAuth のサブタイプとして、consent、passthru、webauth、webconsent などを設定します。
ステップ 5	**redirect** [**for-login** | **on-failure** | **on-success**] *URL* 例： `Device(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html`	ログイン ページ、失敗ページ、および成功ページのリダイレクト URL を設定します。 （注） リダイレクト url では、Ctrl+v キーを押し、「?」を入力して ?文字を設定する必要があります。 ?文字は、ISE が外部ポータルとして設定されている場合に、URL で一般的に使用されます。
ステップ 6	**redirect portal** {**ipv4** | **ipv6**} *ip-address* 例： `Device(config-params-parameter-map)# redirect portal ipv4 23.0.0.1`	外部ポータルの IPv4 アドレスを設定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

Web 認証 WLAN の設定

Web 認証セキュリティを使用して WLAN を設定し、認証リストとパラメータ マップをマッピングするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wlan** *profile-name wlan-id ssid-name* 例： `Device(config)# wlan mywlan 34 mywlan-ssid`	WLAN の名前と ID を指定します。 *profile-name* は、最大 32 文字の英数字からなる WLAN 名です。 *wlan-id* はワイヤレス LAN の ID です。有効な範囲は 1 ～ 512 です。 *ssid-name* は、最大 32 文字の英数字からなる SSID です。
ステップ 4	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 5	**security web-auth** { **authentication-list** *authentication-list-name* | **parameter-map** *parameter-map-name*} 例： `Device(config-wlan)# security web-auth authentication-list webauthlistlocal` `Device(config-wlan)# security web-auth parameter-map sample`	WLAN の Web 認証を有効にします。 ここで、各変数は次のように定義されます。 • **authentication-list** *authentication-list-name*：IEEE 802.1x の認証リストを指定します。 • **parameter-map** *parameter-map-name*：パラメータ マップを設定します。

	コマンドまたはアクション	目的
		（注） **security web-auth** が有効になっている場合、デフォルトの **authentication-list** とグローバルの **parameter-map** がマッピングされます。これは、明示的に記述されていない認証リストとパラメータマップに適用されます。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

認証前 Web 認証 ACL の設定（GUI）

始める前に

アクセス コントロール リスト（ACL）と WLAN の設定を完了していることを確認します。

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 WLAN の名前をクリックします。
ステップ 3 [Edit WLAN] ウィンドウで、[Security] タブをクリックし、[Layer3] タブをクリックします。
ステップ 4 [Show Advanced Settings] をクリックします。
ステップ 5 [Preauthenticaion ACL] セクションで、WLAN にマッピングする適切な ACL を選択します。
ステップ 6 [Update & Apply to Device] をクリックします。

認証前 Web 認証 ACL の設定（CLI）

事前認証 Web 認証 ACL を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例：	特権 EXEC モードをイネーブルにします。

	コマンドまたはアクション	目的
	`Device> enable`	• パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**access-list** *access-list-number* {**deny** | **permit**} *source source-wildcard-bits* 例： `Device(config)# access-list 2 deny your_host`	ACL リストを作成します。 *access-list-number* には、1 ～ 99、100 ～ 199、300 ～ 399、600 ～ 699、1300 ～ 1999、2000 ～ 2699、または 2700 ～ 2799 の 10 進数を指定します。 条件が一致した場合に拒否する場合は **deny**、許可する場合は **permit** を指定します。 *source* には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 • ドット付き 10 進表記による 32 ビット長の値。 • キーワード **any** は 0.0.0.0 255.255.255.255 という *source* および *source-wildcard* の省略形です。source-wildcard を入力する必要はありません。 • キーワード **host** は source 0.0.0.0 という *source* および *source-wildcard* の省略形です。 （任意）*source-wildcard* は、ワイルド カード ビットを送信元アドレスに適用します。
ステップ 4	**wlan** *profile-name wlan-id ssid-name* 例： `Device(config)# wlan mywlan 34 mywlan-ssid`	WLAN を作成します。 *profile-name* は、最大 32 文字の英数字からなる WLAN 名です。 *wlan-id* はワイヤレス LAN の ID です。有効な範囲は 1 ～ 512 です。

	コマンドまたはアクション	目的
		ssid-name は、最大 32 文字の英数字からなる SSID です。
ステップ 5	**ip access-group web** *access-list-name* 例： `Device(config-wlan)# ip access-group web name`	ACL を Web 認証 WLAN にマッピングします。 *access-list-name* は IPv4 ACL 名または ID です。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

Web 認証要求の最大再試行回数の設定

最大 Web 認証要求再試行回数を設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wireless security web-auth retries** *number* 例： `Device(config)# wireless security web-auth retries 2`	*number* は Web 認証要求の最大試行回数です。有効な範囲は 0 ～ 20 です。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。

Web 認証ページ内のローカル バナーの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

ステップ 3 [General] タブで、必要なバナー タイプを選択します。

- [Banner Text] を選択した場合は、表示するバナー テキストを入力します。
- [File Name] を選択した場合は、バナー テキストを取得する取得元のファイルのパスを指定します。

ステップ 4 [Update & Apply] をクリックします。

Web 認証ページ内のローカル バナーの設定（CLI）

Web 認証ページ内のローカル バナーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip admission auth-proxy-banner http** [*banner-text* | *file-path*] 例： `Device(config)# ip admission auth-proxy-banner http C My Switch C`	ローカルバナーをイネーブルにします。 （任意）*C banner-text C*（*C* は区切り文字）、またはバナーに表示されるファイル（たとえば、ロゴまたはテキストファイル）のファイル パスを入力して、カスタム バナーを作成します。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# 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。

Webpassthrough の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device # 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	**parameter-map type webauth** *parameter-map name* 例： `Device (config) # parameter-map type webauth webparalocal`	webauth タイプ パラメータを設定します。
ステップ 3	**type consent** 例： `Device (config-params-parameter-map) # type consent`	WebAuth タイプを同意として設定します。
ステップ 4	**end** 例： `Device (config-params-parameter-map) # end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show running-config | section parameter-map type webauth** *parameter-map* 例： `Device (config) # show running-config | section parameter-map type webauth test`	設定の詳細を表示します。

例

事前認証 ACL の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *wlan-name* 例： `Device (config)# wlan ramban`	*wlan-name* にはプロファイル名を入力します。
ステップ 3	**shutdown** 例： `Device (config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 4	**ip access-group web** *preauthrule* 例： `Device (config-wlan)# ip access-group web preauthrule`	認証前に適用する必要のある ACL を設定します。
ステップ 5	**no shutdown** 例： `Device (config)# no shutdown`	WLAN をイネーブルにします。
ステップ 6	**end** 例： `Device (config-wlan)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 7	**show wlan name** *wlan-name* 例： `Device# show wlan name ramban`	設定の詳細を表示します。

無線による管理機能について

無線による管理機能を使用すると、ワイヤレス クライアントを使用してローカル コントローラを監視および設定できます。コントローラとの間のアップロードおよびダウンロード（転送）を除くすべての管理タスクを実行できます。

無線による管理機能の制限

- 無線による管理機能は、クライアントが中央スイッチングの場合にのみ無効にできます。

無線による管理機能の設定（GUI）

手順

ステップ 1 **[Administration]** > **[Device]** > **[Wireless]** を選択します。
ステップ 2 [Management Via Wireless] チェックボックスをオンにして機能を有効にします。
ステップ 3 設定を保存します。

無線による管理機能の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**[no] wireless mgmt-via-wireless** 例： `Device(config)# wireless mgmt-via-wireless`	ワイヤレス クライアント経由の管理アクセスを有効にします。

	コマンドまたはアクション	目的
ステップ 3	**end**	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 4	**show running-config | include mgmt-via-wireless** 例： `Device# show running-config | include mgmt-via-wireless`	ワイヤレス クライアント経由の管理アクセスのステータスを確認します。

ローカル Web 認証の設定例

例：Web 認証証明書の入手

次の例は、Web 認証証明書を取得する方法を示しています。

```
Device# configure terminal
Device(config)# crypto pki import cert pkcs12 tftp://9.1.0.100/ldapserver-cert.p12 cisco
Device(config)# end
Device# show crypto pki trustpoints cert
 Trustpoint cert:
    Subject Name:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
          Serial Number (hex): 00
    Certificate configured.
Device# show  crypto pki certificates cert
Certificate
  Status: Available
  Certificate Serial Number (hex): 04
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    Name: ldapserver
    e=rkannajr@cisco.com
    cn=ldapserver
    ou=WNBU
    o=Cisco
    st=California
    c=US
```

```
  Validity Date:
    start date: 07:35:23 UTC Jan 31 2012
    end   date: 07:35:23 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12
  Storage: nvram:rkannajrcisc#4.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 00
  Certificate Usage: General Purpose
  Issuer:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Subject:
    e=rkannajr@cisco.com
    cn=sthaliya-lnx
    ou=WNBU
    o=Cisco
    l=SanJose
    st=California
    c=US
  Validity Date:
    start date: 07:27:56 UTC Jan 31 2012
    end   date: 07:27:56 UTC Jan 28 2022
  Associated Trustpoints: cert ldap12 ldap
  Storage: nvram:rkannajrcisc#0CA.cer
```

例：Web 認証証明書の表示

次の例は、Web 認証証明書を表示する方法を示しています。

```
Device# show crypto ca certificate verb
     Certificate
     Status: Available
     Version: 3
     Certificate Serial Number (hex): 2A9636AC00000000858B
     Certificate Usage: General Purpose
     Issuer:
    cn=Cisco Manufacturing CA
    o=Cisco Systems
    Subject:
    Name: WS-C3780-6DS-S-2037064C0E80
    Serial Number: PID:WS-C3780-6DS-S SN:FOC1534X12Q
    cn=WS-C3780-6DS-S-2037064C0E80
    serialNumber=PID:WS-C3780-6DS-S SN:FOC1534X12Q
    CRL Distribution Points:
    http://www.cisco.com/security/pki/crl/cmca.crl
    Validity Date:
    start date: 15:43:22 UTC Aug 21 2011
    end   date: 15:53:22 UTC Aug 21 2021
    Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Signature Algorithm: SHA1 with RSA Encryption
    Fingerprint MD5: A310B856 A41565F1 1D9410B5 7284CB21
```

```
Fingerprint SHA1: 04F180F6 CA1A67AF 9D7F561A 2BB397A1 0F5EB3C9
X509v3 extensions:
X509v3 Key Usage: F0000000
  Digital Signature
  Non Repudiation
  Key Encipherment
  Data Encipherment
X509v3 Subject Key ID: B9EEB123 5A3764B4 5E9C54A7 46E6EECA 02D283F7
X509v3 Authority Key ID: D0C52226 AB4F4660 ECAE0591 C7DC5AD1 B047F76C
Authority Info Access:
Associated Trustpoints: CISCO_IDEVID_SUDI
Key Label: CISCO_IDEVID_SUDI
```

例：デフォルトの Web 認証ログイン ページの選択

次の例は、デフォルトの Web 認証ログイン ページを選択する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth test
This operation will permanently convert all relevant authentication commands to their
CPL control-policy equivalents. As this conversion is irreversible and will
disable the conversion CLI 'authentication display [legacy|new-style]', you are strongly
 advised to back up your current configuration before proceeding.
Do you wish to continue? [yes]: yes
Device(config)# wlan wlan50
Device(config-wlan)# shutdown
Device(config-wlan)# security web-auth authentication-list test
Device(config-wlan)# security web-auth parameter-map test
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show running-config | section wlan50
wlan wlan50 50 wlan50
 security wpa akm cckm
 security wpa wpa1
 security wpa wpa1 ciphers aes
 security wpa wpa1 ciphers tkip
 security web-auth authentication-list test
 security web-auth parameter-map test
 session-timeout 1800
 no shutdown

Device# show running-config | section parameter-map type webauth test
parameter-map type webauth test
 type webauth
```

例：IPv4 外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択

次の例は、IPv4 外部 Web サーバからカスタマイズされた Web 認証ログイン ページを選択する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv4 1.1.1.1
Device(config-params-parameter-map)# parameter-map type webauth test
```

```
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9.1.0.100/login.html
Device(config-params-parameter-map)# redirect portal ipv4 9.1.0.100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test
type webauth
redirect for-login http://9.1.0.100/login.html
redirect portal ipv4 9.1.0.100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

例：IPv6 外部 Web サーバでのカスタマイズされた Web 認証ログイン ページの選択

次の例は、IPv6 外部 Web サーバからカスタマイズされた Web 認証ログイン ページを選択する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth global
Device(config-params-parameter-map)# virtual-ip ipv6 1:1:1::1
Device(config-params-parameter-map)# parameter-map type webauth test
Device(config-params-parameter-map)# type webauth
Device(config-params-parameter-map)# redirect for-login http://9:1:1::100/login.html
Device(config-params-parameter-map)# redirect portal ipv6 9:1:1::100
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map
parameter-map type webauth global
virtual-ip ipv6 1:1:1::1
parameter-map type webauth test
type webauth
redirect for-login http://9:1:1::100/login.html
redirect portal ipv6 9:1:1::100
security web-auth parameter-map rasagna-auth-map
security web-auth parameter-map test
```

例：WLAN ごとのログイン ページ、ログイン失敗ページ、およびログアウト ページの割り当て

次の例は、WLAN ごとのログイン割り当て、ログイン失敗、およびログアウト ページを割り当てる方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth test
Device(config-params-parameter-map)# custom-page login device flash:loginsantosh.html
Device(config-params-parameter-map)# custom-page login expired device
flash:loginexpire.html
Device(config-params-parameter-map)# custom-page failure device flash:loginfail.html
Device(config-params-parameter-map)# custom-page success device flash:loginsucess.html
Device(config-params-parameter-map)# end
```

```
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
 custom-page login device flash:loginsantosh.html
 custom-page success device flash:loginsucess.html
 custom-page failure device flash:loginfail.html
 custom-page login expired device flash:loginexpire.html
```

例：事前認証 ACL の設定

次の例は、事前認証 ACL を設定する方法を示しています。

```
Device# configure terminal
Device(config)# wlan fff
Device(config-wlan)# shutdown
Device(config-wlan)# ip access-group web preauthrule
Device(config-wlan)# no shutdown
Device(config-wlan)# end
Device# show wlan name fff
```

例：Webpassthrough の設定

次の例は、Webpassthrough を設定する方法を示しています。

```
Device# configure terminal
Device(config)# parameter-map type webauth webparalocal
Device(config-params-parameter-map)# type consent
Device(config-params-parameter-map)# end
Device# show running-config | section parameter-map type webauth test
 parameter-map type webauth test
 type webauth
 redirect for-login http://9.1.0.100/login.html
 redirect portal ipv4 9.1.0.100
```

第 60 章

中央 Web 認証

中央 Web 認証について

中央 Web 認証では、Web ポータルとして機能する中央デバイス（この例では ISE）を配置することができます。通常のローカル Web 認証と比較した場合の主な相違点は、MAC フィルタリングまたは dot1x 認証に伴ってレイヤ 2 にシフトされることです。また、RADIUS サーバ（この例では ISE）が、スイッチに対して Web リダイレクションの必要性を指示する特別な属性を返す点も異なります。このソリューションにより、Web 認証を開始する際の遅延が解消されます。

クライアント ステーションの MAC アドレスがグローバルに RADIUS サーバに知られていない場合（ただし他の基準を使用することも可能）、サーバはリダイレクション属性を返し、コントローラは（MAC フィルタリングを使用して）ステーションを認可しますが、Web トラフィックをポータルへリダイレクトするためのアクセス リストを配置します。

ユーザがゲスト ポータルへログインすると、クライアントの再認証が可能になり、認可変更（CoA）を使用する新しいレイヤ 2 MAC フィルタリングが行われます。これにより、ISE が Web 認証ユーザだったことが ISE により記憶され、ISE は、ネットワークにアクセスするために必要な許可属性をコントローラにプッシュします。

関連トピック

無線ゲスト アクセス （1119 ページ）

中央 Web 認証の前提条件

次のことに注意してください。

- Cisco Identity Services Engine（ISE）
- クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ

ISE の設定方法

ISE を設定するには、次の手順に従います。

1. 認可プロファイルを作成します。
2. 認証ルールを作成します。
3. 認可ルールを作成します。

認可プロファイルの作成

手順

ステップ 1 [Policy] をクリックし、[Policy Elements] をクリックします。

ステップ 2 [Results] をクリックします。

ステップ 3 [Authorization] を展開し、[Authorization Profiles] をクリックします。

ステップ 4 [Add] をクリックして、中央 Web 認証用の新しい認可プロファイルを作成します。

ステップ 5 [Name] フィールドに、プロファイルの名前を入力します。たとえば、CentralWebauth と入力します。

ステップ 6 [Access Type] ドロップダウン リストから [ACCESS_ACCEPT] を選択します。

ステップ 7 [Web Redirection (CWA, MDM, NSP, CPP)] チェックボックスをオンにし、ドロップダウン リストから [Centralized Web Auth] を選択します。

ステップ 8 [ACL] フィールドに、リダイレクトするトラフィックを定義する ACL の名前を入力します。たとえば、「redirect」などと入力します。

ステップ 9 [Value] フィールドで、デフォルト値またはカスタマイズされた値を選択します。

[Value] 属性は、ISE がデフォルトの Web ポータルを参照するか、または ISE 管理者が作成したカスタム Web ポータルを参照するかを定義します。

ステップ 10 **[保存（Save）]** をクリックします。

認証ルールの作成

認証プロファイルを使用して認証ルールを作成するには、次の手順に従います。

手順

ステップ 1 **[Policy]** > **[Authentication]** ページで、[Authentication] をクリックします。

ステップ 2 認証ルールの名前を入力します。たとえば、「MAB」と入力します。

ステップ 3 [If] 条件フィールドで、プラス（[+]）アイコンをクリックします。

ステップ 4 [Compound condition] を選択し、[Wireless_MAB] を選択します

ステップ 5 [and ...] の横にある矢印をクリックして、ルールをさらに展開します。

ステップ 6 [Identity Source] フィールドの [+] アイコンをクリックし、[Internal endpoints] を選択します。

ステップ 7 [If user not found] ドロップダウン リストから [Continue] を選択します。

このオプションを使用すると、MAC アドレスが不明な場合でもデバイスを認証できます。

ステップ 8 **[保存（Save）]** をクリックします。

認可ルールの作成

認可ポリシーでは多数のルールを設定できます。このセクションでは [MAC not known] ルールが設定されています。

手順

ステップ 1 [Policy] > [Authorization] をクリックします。

ステップ 2 [Rule Name] フィールドに、名前を入力します。たとえば、「Mac not known」などと入力します。

ステップ 3 [Conditions] フィールドで、プラス（[+]）アイコンをクリックします。

ステップ 4 [Compound Conditions] を選択し、[Wireless_MAB] を選択します

ステップ 5 設定アイコンで、オプションから [Add Attribute/Value] を選択します。

ステップ 6 [Description] フィールドで、ドロップダウン リストから属性として [Network Access] > [AuthenticationStatus] を選択します。

ステップ 7 [Equals] 演算子を選択します。

ステップ 8 右側のフィールドから、[UnknownUser] を選択します。

ステップ 9 [Permissions] フィールドで、以前に作成した認可プロファイル名を選択します。

ISE は、ユーザ（または MAC）が不明の場合でも続行されます。

これで、不明なユーザにログインページが表示されるようになりました。ただし、ユーザが自分のログイン情報を入力すると、再びISE の認証要求が表示されます。そのため、ユーザがゲストユーザである場合に満たされる条件で別のルールを設定する必要があります。たとえば、「UseridentityGroup Equals Guest」を使用している場合に、すべてのゲストがこのグループに属すると仮定します。

ステップ 10 [Conditions] フィールドで、プラス（[+]）アイコンをクリックします。

ステップ 11 [Compound Conditions] を選択し、新しい条件の作成を選択します。

新しいルールは「MAC not known」ルールの前に置く必要があります。

ステップ 12 設定アイコンで、オプションから [Add Attribute/Value] を選択します。

ステップ 13 [Description] フィールドで、ドロップダウン リストから属性として [Network Access] > [UseCase] を選択します。

ステップ 14 [Equals] 演算子を選択します。

ステップ 15 右側のフィールドから、[GuestFlow] を選択します。

ステップ 16 [Permissions] フィールドで、プラス（[+]）アイコンを選択してルールの結果を選択します。

[Standard] > [PermitAccess] オプションを選択するか、または必要な属性を返すカスタム プロファイルを作成できます。

ユーザがログイン ページで承認されると、レイヤ 2 認証の再起動の結果として、ISE により COA がトリガーされます。ユーザがゲスト ユーザとして識別されると、ユーザが承認されます。

ネットワーク デバイスで中央 Web 認証を設定する方法

ネットワーク デバイスで中央 web 認証を設定するには、次の手順に従います。

1. WLAN を設定します。
2. ポリシー プロファイルを設定します。
3. リダイレクト ACL を設定します。
4. 中央 Web 認証用の AAA を設定します。
5. Flex プロファイルでリダイレクト ACL を設定します。

WLAN の設定（GUI）

（注） リダイレクト URL と ACL をダウンロードするには、レイヤ 2 認証の MAC フィルタリングを有効にする必要があります。

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [WLANs] ページで、 WLAN の名前をクリックするか、[Add] をクリックして新規に作成します。

ステップ 3 表示される [Add/Edit WLAN] ウィンドウで、[General] タブをクリックして次のパラメータを設定します。

- [Profile Name] フィールドに、プロファイルの名前を入力します。
- [SSID] フィールドに、SSID 名を入力します。

  SSID 名には、長さが最大 32 文字の英数字を使用できます。
- [WLAN ID] フィールドに、ID 番号を入力します。

  有効な範囲は 1 ～ 512 です。
- [Radio Policy] ドロップダウン リストから、802.11 無線帯域を選択します。
- [Broadcast SSID] フィールドを設定し、[Enabled] または [Disabled] のステータスを切り替えます。
- [Status] フィールドを設定し、[Enabled] または [Disabled] のステータスを切り替えます。

ステップ 4 [Security] タブをクリックし、[Layer 2] タブをクリックして、次のパラメータを設定します。

- [ayer 2 Security Mode]：ドロップダウンリストから、[None] を選択します。この設定により、レイヤ 2 セキュリティが無効になります。
- [MAC Filtering]：WLAN で MAC フィルタリングを有効にするには、このチェックボックスをオンにします。

ステップ 5 [Save & Apply to Device] をクリックします。

WLAN の設定（CLI）

（注） リダイレクト URL と ACL をダウンロードするには、レイヤ 2 認証の MAC フィルタリングを有効にする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan wlan-name wlan-id SSID-name** 例： `Device(config)# wlan wlanProfileName 1 ngwcSSID`	WLAN コンフィギュレーション サブモードを開始します。 **wlan-name** は、設定されている WLAN の名前です。

	コマンドまたはアクション	目的
		wlan-id はワイヤレス LAN の ID です。指定できる範囲は 1 ～ 512 です。 **SSID-name** は、最大 32 文字の英数字からなる SSID 名です。 （注） すでにこのコマンドを設定している場合は、**wlan** **wlan-name** コマンドを入力します。
ステップ 3	**mac-filtering** [*name*] 例： `Device(config-wlan)# mac-filtering name`	デフォルトで WLAN での MAC フィルタリングを有効にします。 （注） 認証リストを事前に設定していない場合は、MAC フィルタリングの設定時にデフォルトの認証リストが仮定されます。
ステップ 4	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 5	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN を停止します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

```
Device# config terminal
Device(config)# wlan wlanProfileName 1 ngwcSSID
Device(config-wlan)# mac-filtering default
Device(config-wlan)# no security wpa
Device(config-wlan)# no shutdown
Device(config-wlan)# end
```

ポリシー プロファイルの設定（CLI）

（注） AAA または ISE サーバからのポリシーを適用するには、AAA オーバーライドが必要です。リダイレクト URL とリダイレクト ACL を ISE サーバから受信すると、NAC を使用して中央 Web 認証（CWA）がトリガーされます。

クライアントが関連付けられるポリシー プロファイルで、NAC と AAA オーバーライドの両方が使用可能である必要があります。

アクセス ポイント（AP）が他のどのポリシー プロファイルにも関連付けられていない場合は、デフォルト ポリシー プロファイルが AP に関連付けられます。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless profile policy default-policy-profile** 例： `Device(config)# wireless profile policy default-policy-profile`	デフォルト ポリシー プロファイルを設定します。
ステップ 2	**vlan vlan-id** 例： `Device(config-wireless-policy)# vlan 41`	特定のポリシー プロファイルに VLAN をマッピングします。vlan-id を指定しない場合は、デフォルトのネイティブの vlan 1 が適用されます。vlan-id の有効な範囲は 1 ～ 4096 です。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA サーバまたは ISE サーバから受信したポリシーを適用するように AAA オーバーライドを設定します。
ステップ 4	**nac** 例： `Device(config-wireless-policy)# nac`	ポリシープロファイルに NAC を設定します。
ステップ 5	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	WLAN を停止します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

例

```
Device# config terminal
Device(config)# wireless profile policy default-policy-profile
Device(config-wireless-policy)# vlan 41
Device(config-wireless-policy)# aaa-override
Device(config-wireless-policy)# nac
Device(config-wireless-policy)# no shutdown
Device(config-wireless-policy)# end
```

ポリシー プロファイルの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞を選択します。

ステップ 2 [Policy Profile] ページで、[Add] をクリックします。

ステップ 3 [Add Policy Profile] ウィンドウの [General] タブで、ポリシー プロファイルの名前と説明を入力します。

ステップ 4 ポリシー プロファイルを有効にするには、[Status] を [Enabled] に設定します。

ステップ 5 スライダを使用して、[Passive Client] と [Encrypted Traffic Analytics] を有効または無効にします。

ステップ 6 [CTS Policy] セクションで、次について適切なステータスを選択します。

- [Inline Tagging]：コントローラまたはアクセス ポイントが送信元 SGT を認識するために使用するトランスポート メカニズム。
- [SGACL Enforcement]

ステップ 7 デフォルトの **SGT** を指定します。有効な範囲は 2 ～ 65519 です。

ステップ 8 [WLAN Switching Policy] セクションで、必要に応じて次を選択します。

- [Central Switching]
- [Central Authentication]
- [Central DHCP]
- [Central Association Enable]
- [Flex NAT/PAT]

ステップ 9 [Save & Apply to Device] をクリックします。

リダイレクト ACL の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ip access-list extended redirect** 例： `Device(config)# ip access-list extended redirect`	ISE がリダイレクト ACL（**redirect** という名前）を使用するように設定されているため、HTTP および HTTPS ブラウジングは（他の ACL ごとの）認証なしでは機能しません。
ステップ 3	**deny ip any host ISE-IP-add** 例： `Device(config)# deny ip any host 123.123.134.112`	ISE へのトラフィックを許可し、その他のすべてのトラフィックをブロックします。
ステップ 4	**deny ip host ISE-IP-add any** 例： `Device(config)# deny ip host 123.123.134.112 any`	ISE へのトラフィックを許可し、その他のすべてのトラフィックをブロックします。 （注） このACLは、ローカルモードと flex モードの両方に適用できます。
ステップ 5	**permit TCP any any eq web address/port-number** 例： HTTP の場合： `Device(config)# permit TCP any any eq www` `Device(config)# permit TCP any any eq 80` 例： HTTPS の場合： `Device(config)# permit TCP any any eq 443`	ISE ログイン ページへのすべての HTTP または HTTPS アクセスをリダイレクトします。HTTP ではポート番号 80 が使用され、HTTPS では ポート番号 443 が使用されます。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

中央 Web 認証用の AAA の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	コントローラの認可変更（CoA）を設定します。
ステップ 2	**client ISE-IP-add server-key radius shared secret** 例： `Device(config-locsvr-da-radius)# client 123.123.134.112 4 SECRET`	**ISE-IP-add** は RADIUS クライアントの IP アドレスです。 **server-key** は RADIUS クライアントのサーバキーです。 **radius shared secret** は次を対象とします。 • **0**：暗号化されていないキーを指定します。 • **6**：暗号化されたキーを指定します。 • **7**：「隠し」キーを指定します。 • **Word**：暗号化されていない（クリアテキスト）サーバ キー。 （注） これらのステップはすべて、AAA が設定されている場合にのみ機能します。詳細については、「AAA 認証の設定」を参照してください。

例

```
Device# config terminal
Device(config)# aaa server radius dynamic-author
Device(config-locsvr-da-radius)# client 123.123.134.112 4 SECRET
Device(config)# end
```

Flex プロファイルでのリダイレクト ACL の設定（GUI）

リダイレクト ACL の定義を FlexConnect プロファイル内のアクセス ポイントに送信する必要があります。それには、AP に関連付けられているリダイレクト ACL を、クライアントがホス

トされている FlexConnect プロファイルに設定する必要があります。アクセス ポイントがどの FlexConnect プロファイルでも設定されていない場合は、デフォルトの FlexConnect プロファイルが関連付けられます。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Flex] > > を選択します。

ステップ 2 [Flex Profile] ページで、 FlexConnect プロファイルの名前をクリックするか、[Add] をクリックして新しい FlexConnect プロファイルを作成します。

ステップ 3 表示される [Add/Edit Flex Profile] ウィンドウで、[Policy ACL] タブをクリックします。

ステップ 4 [Add] をクリックして、ACL を FlexConnect プロファイルにマッピングします。

ステップ 5 ACL 名を選択し、中央 Web 認証を有効にして、認証 URL フィルタを指定します。

ステップ 6 [Save] をクリックします。

ステップ 7 [Update & Apply to Device] をクリックします。

Flex プロファイルでのリダイレクト ACL の設定（CLI）

リダイレクト ACL の定義を Flex プロファイル内のアクセス ポイントに送信する必要があります。それには、AP に関連付けられているリダイレクト ACL を、クライアントがホストされている Flex プロファイルに設定する必要があります。アクセス ポイントがどの Flex プロファイルでも設定されていない場合は、デフォルトの Flex プロファイルが関連付けられます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex default-flex-profile** 例： `Device(config)# wireless profile flex default-flex-profile`	新しい flex ポリシーを作成します。デフォルトの flex プロファイル名は **default-flex-profile** です。
ステップ 3	**acl-policy** *acl policy name* 例： `Device(config-wireless-flex-profile)# acl-policy acl1`	ACL ポリシーを設定します。
ステップ 4	**central-webauth** 例：	中央 Web 認証を設定します。

	コマンドまたはアクション	目的
	`Device(config-wireless-flex-profile-acl)# central-webauth`	
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

スリープ状態にあるクライアントの認証

スリープ状態にあるクライアントの認証について

Web 認証に成功したゲスト アクセスを持つクライアントは、ログイン ページから別の認証プロセスを実行せずにスリープおよび復帰することを許可されています。再認証が必要になるまでスリープ状態にあるクライアントが記録される期間を設定できます。有効範囲は 10 ～ 43200 分、デフォルトは 720 分です。この期間は、WLAN にマッピングされている WebAuth パラメータ マップで設定できます。スリープ状態のクライアント タイマーは、アイドル タイムアウト、セッション タイムアウト、WLAN の無効化、AP の非稼働状態などを契機として有効になります。

この機能は FlexConnect のローカル スイッチング、中央認証のシナリオでサポートされています。

⚠

注意 スリープ モードに切り替わったクライアント MAC アドレスがスプーフィングされた場合、ラップトップなどの偽のデバイスを認証することができます。

モビリティのシナリオ

次に、モビリティ シナリオでの注意事項を示します。

- 同じサブネットの L2 ローミングがサポートされています。
- アンカー スリープ タイマーを適用できます。
- スリープ状態にあるクライアントの情報は、クライアントがアンカー間を移動する場合に、複数の自動アンカー間で共有されます。

スリープ状態にあるクライアントは、次のシナリオでは再認証が必要ありません。

- モビリティ グループに 2 台のコントローラがあるとします。1 台のコントローラに関連付けられているクライアントがスリープ状態になり、その後復帰して他方のコントローラに関連付けられます。

- モビリティ グループに 3 台のコントローラがあるとします。1 台目のコントローラにアンカーされた 2 台目のコントローラに関連付けられたクライアントは、スリープ状態から復帰して、3 台目のコントローラに関連付けられます。
- クライアントはスリープ状態から復帰して、エクスポート アンカーにアンカーされた同じまたは別のエクスポート外部コントローラに関連付けられます。

関連トピック

無線ゲスト アクセス （1119 ページ）

スリープ状態にあるクライアントの認証に関する制約事項

- スリープ クライアント機能は、WebAuth セキュリティが設定された WLAN に対してのみ動作します。
- スリープ状態にあるクライアントは WLAN ごとにのみ設定できます。
- スリープ状態にあるクライアントの認証機能は、レイヤ 3 セキュリティが有効な WLAN でのみサポートされています。
- レイヤ 3 セキュリティでは、認証、パススルー、および On MAC Filter 失敗 Web ポリシーがサポートされています。条件付き Web リダイレクトとスプラッシュ ページ Web リダイレクト Web ポリシーはサポートされていません。
- スリープ状態にあるクライアントの中央 Web 認証はサポートされていません。
- スリープ状態にあるクライアントの認証機能は、ゲスト LAN およびリモート LAN ではサポートされていません。
- ローカル ユーザ ポリシーを持つスリープ状態のゲスト アクセス クライアントはサポートされません。この場合、WLAN 固有のタイマーが適用されます。

スリープ状態のクライアントの認証の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

ステップ 3 [Sleeping Client Status] チェックボックスをオンにします。

ステップ 4 [Update & Apply to Device] をクリックします。

スリープ状態のクライアントの認証の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**[no] parameter-map type webauth** {*parameter-map-name* | **global**} 例： `Device(config)# parameter-map type webauth global`	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。
ステップ 3	**sleeping-client** [**timeout** *time*] 例： `Device(config-params-parameter-map)# sleeping-client timeout 100`	スリープ状態のクライアントのタイムアウトを100分に設定します。有効な範囲は 10 ～ 43200 分です。 （注） タイムアウト キーワードを使用しない場合、スリープ状態のクライアントにはデフォルトのタイムアウト値である720分が設定されます。
ステップ 4	**end**	parameter-map webauth コンフィギュレーション モードを終了し、特権EXECモードに戻ります。
ステップ 5	**show wireless client sleeping-client** 例： `Device# show wireless client sleeping-client`	クライアントのMACアドレスと、それぞれのセッションの残り時間を表示します。
ステップ 6	**clear wireless client sleeping-client** [**mac-address** *mac-addr*] 例： `Device# clear wireless client sleeping-client mac-address 00e1.e1e1.0001`	• **clear wireless client sleeping-client**：スリープ状態のクライアントキャッシュからスリープ状態のクライアント エントリをすべて削除します。 • **clear wireless client sleeping-client mac-address** *mac-addr*：スリープ状態のクライアント キャッシュから特定の MAC エントリを削除します。

第 61 章

ISE の簡素化と拡張

セキュリティ設定用のユーティリティ

この章では、次のコマンドを使用してすべてのRADIUS サーバ側設定を行う方法について説明します。

wireless-default radius server *IP* **key** *secret*

この簡易設定オプションは次の機能を提供します。

- RADIUS サーバの設定時に、デフォルト ケースのすべての AAA 設定を行います。
- WLAN では、メソッドリストの設定がデフォルトで仮定されます。
- デフォルトで RADIUS アカウンティングを有効にします。
- デフォルトで RADIUS アグレッシブ フェールオーバーを無効にします。
- RADIUS 要求のタイムアウトをデフォルトで 5 秒に設定します。
- キャプティブ バイパス ポータルを有効にします。

このコマンドは、次の設定をバックグラウンドで行います。

```
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting identity default start-stop group radius
!
aaa server radius dynamic-author
 client <IP> server-key cisco123
!
radius server RAD_SRV_DEF_<IP>
 description Configured by wireless-default
 address ipv4 <IP> auth-port 1812 acct-port 1813
 key <key>
!
aaa local authentication default authorization default
aaa session-id common
```

```
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host <IP>
permit tcp any any eq www
!
parameter-map type webauth global
  captive-portal-bypass
  virtual-ip ipv4 1.1.1.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

このため、設定ガイドの内容をすべて調べなくても、簡易な設定要件を満たすようにワイヤレス コントローラを設定することができます。

複数の RADIUS サーバの設定

このユーティリティを使用すると、最大 10 台の RADIUS サーバを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless-default radius server** *IP* **key** *secret* 例： `Device(config)# wireless-default radius server 9.2.58.90 key cisco123`	複数の RADIUS サーバを設定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AAA および RADIUS サーバの設定の確認

AAA サーバの詳細を表示するには、次のコマンドを使用します。

```
Device# show run aaa
Device# show run
```

```
!
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting Identity default start-stop group radius
!
aaa server radius dynamic-author
 client 9.2.58.90 server-key cisco123
!
radius server RAD_SRV_DEF_9.2.58.90
 description Configured by wireless-default
 address ipv4 9.2.58.90 auth-port 1812 acct-port 1813
 key cisco123
!
aaa local authentication default authorization default
aaa session-id common
!
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host 9.2.58.90
permit tcp any any eq www
!
parameter-map type webauth global
  captive-portal-bypass
  virtual-ip ipv4 1.1.1.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

（注） このユーティリティに新しいコマンドを追加すると **show run aaa** の出力が変わる場合があります。

ローカルおよび中央 Web 認証のキャプティブ ポータル バイパスの設定

キャプティブ バイパスについて

WISPr は、ユーザが異なるワイヤレス サービス プロバイダー間をローミングできるようにするドラフト プロトコルです。一部のデバイス（Apple iOS デバイスなど）には、指定の URL に対する HTTP WISPr 要求に基づいて、デバイスがインターネットに接続するかどうかを決定するときに使用するメカニズムが搭載されています。このメカニズムは、インターネットへの直接接続が不可能なときにデバイスが自動的に Web ブラウザを開くために使用されます。これ

により、ユーザがインターネットにアクセスするために、自身の認証情報を提供することが可能となります。実際の認証は、デバイスが新しい SSID に接続するたびにバックグラウンドで実行されます。

クライアント デバイス（Apple IOS デバイス）は、WISPr 要求をコントローラに送信します。コントローラはユーザ エージェントの詳細をチェックし、コントローラでの Web 認証代行受信により HTTP 要求をトリガーします。ユーザエージェントによって提供される IOS バージョンおよびブラウザの詳細の確認後に、コントローラによってクライアントはキャプティブ ポータル設定のバイパスを許可され、インターネットにアクセスできます。

この HTTP 要求は、他のページ要求がワイヤレス クライアントによって実行されると、コントローラでの Web 認証代行受信をトリガーします。この代行受信によって Web 認証プロセスが発生し、プロセスは正常に完了します。Web認証がいずれかのコントローラ スプラッシュ ページ機能で使用されていると（設定された RADIUS サーバが URL を指定）、WISPr 要求が非常に短い間隔で発信されるので、スプラッシュ ページが表示されることはなく、いずれかのクエリーが指定のサーバに到達できるとただちに、バックグラウンドで実行されている Web リダイレクションまたはスプラッシュ ページ表示プロセスが中断されます。そして、デバイスによってページ要求が処理され、スプラッシュ ページ機能は中断されます。

たとえば、Apple は iOS 機能を導入して、キャプティブ ポータルがある場合のネットワーク アクセスを容易にしました。この機能では、ワイヤレス ネットワークへの接続に関する Web 要求を送信することにより、キャプティブ ポータルの存在を検出します。この要求は、Apple IOS バージョン 6 以前の場合は http://www.apple.com/library/test/success.html に、Apple IOS バージョン 7 以降の場合は複数の該当するターゲット URL に送られます。応答が受信されると、インターネット アクセスが使用可能であると見なされ、それ以上の操作は必要ありません。応答が受信されない場合、インターネット アクセスはキャプティブ ポータルによってブロックされたと見なされ、Apple の Captive Network Assistant（CNA）が疑似ブラウザを自動起動して管理ウィンドウでポータル ログインを要求します。ISE キャプティブ ポータルへのリダイレクト中に、CNA が切断される場合があります。コントローラは、この疑似ブラウザがポップアップ表示されないようにします。

現在、WISPr 検出プロセスをバイパスするようにコントローラを設定できるようになりました。それによって、ユーザが、ユーザ コンテキストでスプラッシュ ページ ロードを引き起こす Web ページを要求したときに、バックグラウンドで WISPr 検出を実行せずに、Web 認証代行受信だけが行われるようにすることができます。

LWA および CWA における WLAN のキャプティブ バイパスの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

ステップ 3 [Captive Bypass Portal] チェックボックスをオンにします。

ステップ 4 [Update & Apply to Device] をクリックします。

LWA および CWA内の WLAN におけるキャプティブ バイパスの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)# parameter-map type webauth WLAN1_MAP`	パラメータ マップを作成します。 *parameter-map-name* は 99 文字を超えないようにする必要があります。
ステップ 3	**captive-portal-bypass** 例： `Device(config)# captive-portal-bypass`	キャプティブ バイパスを設定します。
ステップ 4	**wlan** *profile-name wlan-id ssid-name* 例： `Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME`	WLAN の名前と ID を指定します。 • *profile-name* は、最大 32 文字の英数字からなる WLAN 名です。 • *wlan-id* はワイヤレス LAN の ID です。有効な範囲は 1 ～ 512 です。 • *ssid-name* は、最大 32 文字の英数字からなる SSID です。
ステップ 5	**security web-auth** 例： `Device(config-wlan)# security web-auth`	WLAN の Web 認証を有効にします。
ステップ 6	**security web-auth parameter-map** *parameter-map-name* 例： `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	パラメータ マップをマッピングします。 （注） パラメータ マップが WLAN に関連付けられていない場合は、グローバル パラメータ マップの設定と見なされます。

	コマンドまたはアクション	目的
ステップ 7	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

DHCP オプション 55 および 77 の ISE への送信

DHCP オプション 55 および 77 について

DHCP センサーは、ネイティブおよびリモート プロファイリングのために、ISE で次の DHCP オプションを使用します。

- **オプション 12**：ホスト名
- **オプション 6**：クラス ID

これと一緒に、次のオプションをプロファイリングのために ISE に送信する必要があります。

- **オプション 55**：パラメータ要求リスト
- **オプション 77**：ユーザ クラス

DHCP オプション 55 および 77 を ISE に送信するための設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[Policy]** を選択します。

ステップ 2 [Policy Profile] ページで、[Add] をクリックして [Add Policy Profile] ウィンドウを表示します。

ステップ 3 [Access Policies] タブをクリックし、[RADIUS Profiling] チェックボックスと [DHCP TLV Caching] チェックボックスをオンにして、WLANで RADIUS プロファイリングと DHCP TLV キャッシングを設定します。

ステップ 4 [Save & Apply to Device] をクリックします。

DHCP オプション 55 および 77 を ISE に送信するための設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy rr-xyz-policy-1`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**dhcp-tlv-caching** 例： `Device(config-wireless-policy)# dhcp-tlv-caching`	WLAN で DHCP TLV キャッシングを設定します。
ステップ 4	**radius-profiling** 例： `Device(config-wireless-policy)# radius-profiling`	WLAN でクライアント RADIUS プロファイリングを設定します。
ステップ 5	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

EAP 要求のタイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps client-exclusion dot1x-timeout** 例： `Device(config)# wireless wps client-exclusion dot1x-timeout`	タイムアウト時および応答がない場合の除外を有効にします。 デフォルトでは、この機能は有効です。 無効にするには、コマンドの先頭に **no** を付けます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

キャプティブ ポータル

キャプティブ ポータル設定

この機能を使用すると、AP に基づき同じ SSID に対して、複数の Web 認証 URL（外部のキャプティブ URL を含む）を設定できます。デフォルトの設定では、グローバル URL が認証に使用されます。オーバーライド オプションは、WLAN および AP レベルで使用できます。

優先順位は次のとおりです。

- AP
- WLAN
- グローバル コンフィギュレーション

キャプティブ ポータルの設定の制約事項

- この設定は、スタンドアロン コントローラでのみサポートされています。
- エクスポート アンカー設定はサポートされていません。

キャプティブ ポータルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**Configure Terminal** 例： `Device# 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	**wlan** {*<profile-name>* | **shutdown**} **<1-4096>** *<network-name>* 例： `Device(config)#wlan edc6 6 edc`	WLANプロファイルを設定します。すべてのWLANを有効または無効にし、WLANIDを作成します。プロファイル名と SSID ネットワーク名には、最大 32 文字の英数字を使用できます。
ステップ 3	**ip** {**access-group** | **verify**} web *<IPvL-ACL-Name>* 例： `Device(config-wlan)#ip access-group web CPWebauth`	WLAN の Web ACL を設定します。 （注） この操作を実行する前に、WLANを無効にしておく必要があります。
ステップ 4	**no security wpa** 例： `Device(config-wlan)#no security wpa`	WPA セキュリティを無効にします。

	コマンドまたはアクション	目的
ステップ 5	**no security wpa akm dot1x** 例： `Device(config-wlan)#no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 6	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)#no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化を無効にします。
ステップ 7	**security web-auth** {**authentication-list** *authentication-list-name* | **authorization-list** *authorization-list-name* | **on-macfilter-failure** | **parameter-map** *parameter-map-name*} 例： `Device(config-wlan)#security web-auth authentication-list cp-webauth` `Device(config-wlan)#security web-auth parameter-map parMap6`	WLAN の Web 認証を有効にします。ここで、各変数は次のように定義されます。 • **authentication-list** *authentication-list-name*：IEEE 802.1x の認証リストを指定します。 • **authorization-list** *authorization-list-name*：IEEE 802.1x のオーバーライド認可リストを指定します。 • **on-macfilter-failure**：MAC フィルタの失敗における Web 認証を有効にします。 • **parameter-map** *parameter-map-name*：パラメータマップを設定します。 （注） **security web-auth** を有効にすると、デフォルトの **authentication-list** とグローバル **parameter-map** がマッピングされます。これは、明示的に記述されていない認証リストとパラメータマップに適用されます。
ステップ 8	**no shutdown** 例： `Device(config-wlan)#no shutdown`	WLAN をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 9	**exit** 例： `Device(config-wlan)#exit`	WLAN 設定を終了します。
ステップ 10	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)#parameter-map type webauth parMap6`	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。
ステップ 11	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)#parameter-map type webauth parMap6`	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。
ステップ 12	**type webauth** 例： `Device(config-params-parameter-map)# type webauth`	webauth タイプ パラメータを設定します。
ステップ 13	**timeout init-state sec** <*timeout-seconds*> 例： `Device(config-params-parameter-map)# timeout inti-state sec 3600`	WEBAUTHのタイムアウトを秒単位で設定します。タイムアウト（秒単位）パラメータの有効な範囲は 60 ～ 3932100 秒です。
ステップ 14	**redirect for-login** <*URL-String*> 例： `Device(config-params-parameter-map)# redirect for-login https://172.16.100.157/portal/login.html`	ログイン時のリダイレクト用のURL文字列を設定します。
ステップ 15	**exit** 例： `Device(config-params-parameter-map)# exit`	パラメータ設定を終了します。
ステップ 16	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy policy_tag_edc6`	ポリシータグを設定し、ポリシータグコンフィギュレーションモードを開始します。
ステップ 17	**wlan** *wlan-profile-name* **policy** *policy-profile-name* 例：	WLAN プロファイルにポリシー プロファイルをアタッチします。

	コマンドまたはアクション	目的
	`Device(config)# wlan edc6 policy policy_profile_flex`	
ステップ 18	**end** 例： `Device(config-policy-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

キャプティブ ポータル設定：例

次に、複数の AP を異なるロケーションに配置して同じ SSID をブロードキャストするものの、クライアントを異なるリダイレクト ポータルにリダイレクトする例を示します。

異なるリダイレクト ポータルを指す複数のパラメータ マップを設定するには、次のようにします。

```
parameter-map type webauth parMap1
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.3:8080/portal/PortalSetup.action?portal=cfdbce00-2ce2-11e8-b83c-005056a06b27
redirect portal ipv4 172.16.12.3
!
!
parameter-map type webauth parMap11
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.4:8443/portal/PortalSetup.action?portal=094e7270-3808-11e8-9797-02421e4cae0c
redirect portal ipv4 172.16.12.4
!
```

これらのパラメータ マップを異なる WLAN に関連付けます。

```
wlan edc1 1 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap11
no shutdown
wlan edc2 2 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap1
no shutdown
```

（注） すべての WLAN に同じ SSID があります。

WLAN を異なるポリシー タグに関連付けます。

```
wireless tag policy policy_tag_edc1
wlan edc1 policy policy_profile_flex
wireless tag policy policy_tag_edc2
wlan edc2 policy policy_profile_flex
```

これらのポリシー タグを目的の AP に割り当てます。

```
ap E4AA.5D13.14DC
policy-tag policy_tag_edc1
site-tag site_tag_flex
ap E4AA.5D2C.3CAC
policy-tag policy_tag_edc2
site-tag site_tag_flex
```

第 62 章

複数の RADIUS サーバ間での認証および認可

複数の RADIUS サーバ間での認証および認可について

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ は、認証と認可の両方を組み合わせた単一の RADIUS サーバと要求および応答トランザクションを行うアプローチを使用します。コントローラでの認証と認可は、複数の RADIUS サーバに分割することができます。

RADIUS サーバは、認証サーバ、認可サーバ、またはその両方の役割を担うことができます。認証と認可を異なる RADIUS サーバで行う場合は、コントローラ上の Session Aware Network（SANet）コンポーネントによって、クライアントがコントローラに参加するときに一方のサーバで認証を行い、別のサーバで認可を行うことが可能になりました。

認証は、Cisco ISE、Cisco DNAC、Free Radius、または任意のサードパーティ製 RADIUS サーバを使用して実行できます。認証サーバで認証が成功すると、コントローラは、認証サーバから受信した属性を、認可サーバとして指定された別の RADIUS サーバに中継します。

その後、認可サーバは次の処理を実行します。

- サーバで定義されている他のポリシーやルールを使用して、受信した属性を処理する。
- 認証応答の一部として属性を導出し、コントローラに返す。

（注） 認証と認可の分割設定では、両方のサーバを使用可能にする必要があります。また、コントローラがセッションを受け入れられるように、両方のサーバで ACCESS-ACCEPT を使用して認証と認可を正常に行う必要があります。

認証および認可サーバの分割による WLAN の 802.1X セキュリティの設定

明示的な認証および認可サーバ リストの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[AAA]** の順に選択します。

ステップ 2 [Authentication Authorization and Accounting] ページで、[Servers/Groups] タブをクリックします。

ステップ 3 次のオプションから、設定する AAA サーバのタイプをクリックします。

- RADIUS
- TACACS+
- LDAP

この手順では、RADIUS サーバの設定について説明します。

ステップ 4 [RADIUS] オプションを選択した状態で、[Add] をクリックします。

ステップ 5 RADIUS サーバの名前と、サーバの IPv4 または IPV6 アドレスを入力します。

ステップ 6 デバイスと、RADIUS サーバ上で動作するキー文字列 RADIUS デーモンとの間で使用される認証および暗号キーを入力します。PAC キーまたは非 PAC キーのどちらを使用するかを選択できます。

ステップ 7 サーバのタイムアウト値を入力します。有効な範囲は 1 ～ 1000 秒です。

ステップ 8 再試行回数を入力します。有効な範囲は 0 ～ 100 です。

ステップ 9 [Support for CoA] フィールドは [Enabled] 状態のままにしておきます。

ステップ 10 [Save & Apply to Device] をクリックします。

ステップ 11 [Authentication Authorization and Accounting] ページで、[RADIUS] オプションを選択した状態で、[Server Groups] タブをクリックします。

ステップ 12 [Add] をクリックします。

ステップ 13 表示される [Create AAA RADIUS Server Group] ウィンドウで、RADIUS サーバ グループの名前を入力します。

ステップ 14 [MAC-Delimiter] ドロップダウン リストから、RADIUS サーバに送信される MAC アドレスで使用される区切り文字を選択します。

ステップ 15 [MAC Filtering] ドロップダウン リストから、MAC アドレスをフィルタリングするための基準値を選択します。

ステップ 16 サーバ グループのデッド タイムを設定し、稼働特性が異なる別のサーバ グループに AAA トラフィックを転送するには、[Dead-Time] フィールドに、サーバが停止していると見なされる時間を分単位で入力します。

ステップ 17 [Available Servers] リストから、サーバ グループに含めるサーバを選択し、それらを [Assigned Servers] リストに移動します。

ステップ 18 [Save & Apply to Device] をクリックします。

明示的な認証サーバリストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *server-name* 例： `Device(config)# radius server free-radius-authc-server`	RADIUS サーバ名を指定します。
ステップ 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* 例： `Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813`	RADIUS サーバのパラメータを指定します。
ステップ 5	[**pac**] **key** *key* 例： `Device(config-radius-server)# key cisco`	デバイスと、RADIUS サーバ上で動作するキー文字列 RADIUS デーモンとの間で使用される認証および暗号キーを指定します。
ステップ 6	**exit** 例： `Device(config-radius-server)# exit`	コンフィギュレーション モードに戻ります。
ステップ 7	**aaa group server radius** *server-group* 例：	RADIUS サーバ グループの ID を作成します。

	コマンドまたはアクション	目的
	`Device(config)# aaa group server radius authc-server-group`	
ステップ 8	**server name** *server-name* 例： `Device(config)# server name free-radius-authc-server`	
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。 詳細については、「外部認証用の AAA の設定」を参照してください。

明示的な認可サーバリストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *server-name* 例： `Device(config)# radius server cisco-dnac-authz-server`	RADIUS サーバ名を指定します。
ステップ 4	**address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number* 例： `Device(config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813`	RADIUS サーバのパラメータを指定します。

	コマンドまたはアクション	目的
ステップ 5	[**pac**] **key** *key* 例： `Device(config-radius-server)# pac key cisco`	デバイスと、RADIUS サーバ上で動作するキー文字列 RADIUS デーモンとの間で使用される認可および暗号キーを指定します。
ステップ 6	**exit** 例： `Device(config-radius-server)# exit`	コンフィギュレーション モードに戻ります。
ステップ 7	**aaa group server radius** *server-group* 例： `Device(config)# aaa group server radius authz-server-group`	RADIUS サーバ グループの ID を作成します。
ステップ 8	**server name** *server-name* 例： `Device(config)# server name cisco-dnac-authz-server`	
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.1X セキュリティ用の認証および認可リストの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan wlan-foo 222 foo-ssid`	WLAN コンフィギュレーション サブモードを開始します。 • *wlan-name*：設定されている WLAN の名前です。

	コマンドまたはアクション	目的
		• *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID-name*：最大 32 文字の英数字からなる SSID 名です。 （注） すでにこのコマンドを設定している場合は、**wlan** *wlan-name* コマンドを入力します。
ステップ 4	**security dot1x authentication-list** *authenticate-list-name* 例： `Device(config-wlan)# security dot1x authentication-list authc-server-group`	dot1x セキュリティ用の認証リストを有効にします。
ステップ 5	**security dot1x authorization-list** *authorize-list-name* 例： `Device(config-wlan)# security dot1x authorization-list authz-server-group`	dot1x セキュリティ用の認可リストを指定します。 **Cisco Digital Network Architecture Center**（**DNAC**）の詳細については、DNAC のマニュアルを参照してください。
ステップ 6	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

認証および認可サーバの分割による WLAN の Web 認証の設定

- #unique_699
- #unique_700
- Web 認証用の認証および認可リストの設定 （623 ページ）

Web 認証用の認証および認可リストの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**wlan** *wlan-name wlan-id SSID-name* 例： `Device(config)# wlan wlan-bar 333 bar-ssid`	WLAN コンフィギュレーション サブモードを開始します。 • *wlan-name*：設定されている WLAN の名前です。 • *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID-name*：最大 32 文字の英数字からなる SSID 名です。 （注） すでにこのコマンドを設定している場合は、**wlan** *wlan-name* コマンドを入力します。
ステップ 4	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 5	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 6	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。

	コマンドまたはアクション	目的
ステップ 7	**security web-auth** {**authentication-list** *authenticate-list-name* | **authorization-list** *authorize-list-name*} 例： `Device(config-wlan)# security web-auth authentication-list authc-server-group`	dot1x セキュリティ用の認証または認可リストを有効にします。 （注） WPA セキュリティ、dot1x の AKM、および WPA2 セキュリティを無効にしていない場合は、次のエラーが表示されます。 *% switch-1:dbm:wireless:web-auth cannot be enabled. Invalid WPA/WPA2 settings.*
ステップ 8	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

認証と認可の分割設定の確認

WLAN の詳細を表示するには、次のコマンドを使用します。

```
Device# show run wlan
wlan wlan-foo 222 foo-ssid
security dot1x authentication-list authc-server-group
security dot1x authorization-list authz-server-group

wlan wlan-bar 333 bar-ssid
security web-auth authentication-list authc-server-group
security web-auth authorization-list authz-server-group
```

AAA 認証およびサーバの詳細を表示するには、次のコマンドを使用します。

```
Device# show run aaa
!
aaa authentication dot1x default group radius
username cisco privilege 15 password 0 cisco
!
!
radius server free-radius-authc-server
 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
 key cisco
!
radius server cisco-dnac-authz-server
 address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
 pac key cisco
!
!
aaa new-model
aaa session-id common
!
```

802.1Xセキュリティ用の認証および認可リストを表示するには、次のコマンドを使用します。

```
Device# show wlan name wlan-foo | sec 802.1x
802.1x authentication list name               : authc-server-group
802.1x authorization list name                : authz-server-group
            802.1x                            : Enabled
```

Web 認証用の認証および認可リストを表示するには、次のコマンドを使用します。

```
Device# show wlan name wlan-bar | sec Webauth
    Webauth On-mac-filter Failure             : Disabled
    Webauth Authentication List Name          : authc-server-group
    Webauth Authorization List Name           : authz-server-group
    Webauth Parameter Map                     : Disabled
```

設定例

サードパーティの RADIUS サーバを使用した認証のための Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定：例

次に、サードパーティの RADIUS サーバを使用した認証のための Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定例を示します。

```
Device(config)# radius server free-radius-authc-server
Device(config-radius-server)# address ipv4 9.2.62.56 auth-port 1812 acct-port 1813
Device(config-radius-server)# key cisco
Device(config-radius-server)# exit
Device(config)# aaa group server radius authc-server-group
Device(config)# server name free-radius-authc-server
Device(config)# end
```

Cisco ISE または DNAC を使用した認証のための Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定：例

次に、Cisco ISE または DNAC を使用した認証のための Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定例を示します。

```
Device(config)# radius server cisco-dnac-authz-server
Device (config-radius-server)# address ipv4 9.4.62.32 auth-port 1812 acct-port 1813
Device (config-radius-server)# pac key cisco
Device (config-radius-server)# exit
Device(config)# aaa group server radius authz-server-group
Device(config)# server name cisco-dnac-authz-server
Device(config)# end
```

第 63 章

セキュア LDAP（SLDAP）

SLDAP について

Transport Layer Security（TLS）

Transport Layer Security（TLS）は、プライバシー、認証、およびデータ整合性によるデータのセキュア トランザクションを可能にするアプリケーションレベル プロトコルです。TLS は、証明書、公開キーおよび秘密キーに基づいて、クライアントの ID を証明します。

証明書は認証局（CA）によって発行されます。

各証明書には次のものが含まれています。

- 発行された権限の名前。
- 証明書の発行先エンティティの名前。
- エンティティの公開キー。
- 証明書の有効期限を示すエンティティのタイムスタンプ。

TLS による LDAP のサポートについては、LDAP プロトコルの拡張である RFC 2830 を参照してください。

LDAP 操作

バインド

バインド操作は、サーバに対してユーザを認証するために使用されます。LDAP サーバとの接続を開始するために使用されます。LDAP はコネクション型プロトコルです。クライアントはプロトコル バージョンと認証情報を指定します。

LDAP は次のバインドをサポートします。

- 認証済みバインド：認証済みバインドは、ルートの認定者名（DN）とパスワードが使用できる場合に実行されます。
- 匿名バインド：ルート DN とパスワードがない場合は、匿名バインドが実行されます。

LDAP 環境では、検索操作が実行されてから、バインド操作が実行されます。これは、パスワード属性が検索操作の一部として返される場合、パスワードの確認を LDAP クライアントのローカルで実行できるためです。したがって、余計なバインド操作を実行する必要がなくなります。パスワード属性が返されない場合、バインド操作を後で実行できます。検索操作を先に実行してバインド操作を後で実行するもう 1 つの利点は、ユーザ名（cn 属性）の前にベース DN を付けることで DN を構成するのではなく、検索結果で受信した DN をユーザ DN として使用できることです。LDAP サーバに保存されているすべてのエントリには、固有の DN があります。

DN は 2 つの部分で構成されます。

- 相対識別名（RDN）
- レコードが存在する LDAP サーバ内の場所。

LDAP サーバに保存されているエントリのほとんどには名前があり、多くの場合、名前は Common Name（cn）属性で保存されます。すべてのオブジェクトには名前があるため、LDAP に保存されているほとんどのオブジェクトは RDN のベースとして cn 値を使用します。

検索

検索操作は、LDAP サーバを検索するために使用されます。クライアントは検索の開始点（ベース DN）、検索範囲（オブジェクト、その子、またはそのオブジェクトをルートとするサブツリー）、およびサーチ フィルタを指定します。

認可要求の場合、検索操作はバインド操作なしで直接実行されます。検索操作を正常に実行するには、LDAP サーバを特定の特権で設定します。この特権レベルは、バインド操作で設定します。

LDAP 検索操作は、特定のユーザについて複数のユーザ エントリを返す可能性があります。このような場合、LDAP クライアントは適切なエラー コードを AAA に返します。このようなエラーを回避するために、単一のエントリに一致させるための適切なサーチ フィルタを設定する必要があります。

比較

認証のために、比較操作を使用して、バインド要求を比較要求で置換します。比較操作によって、接続のための最初のバインド パラメータを維持できます。

LDAP ダイナミック属性マッピング

Lightweight Directory Access Protocol（LDAP）は、AAA サーバとの通信に適した強力で柔軟性の高いプロトコルです。LDAP 属性マップには、サーバから取得した属性を、セキュリティアプライアンスによってサポートされるシスコ属性にクロスリファレンスする方式が備わっています。

ユーザがセキュリティアプライアンスを認証すると、次にセキュリティアプライアンスはサーバを認証し、LDAP プロトコルを使用してそのユーザのレコードを取得します。このレコードは、サーバにユーザ インターフェイスに表示されるフィールドに関連付けられた LDAP 属性で構成されます。取得される各属性には、ユーザ レコードを更新する管理者が入力した値が含まれます。

SLDAP の設定の前提条件

セキュア Transport Layer Security（TLS）のセキュア接続を使用している場合、 X.509 証明書を設定する必要があります。

SLDAP の設定の制約事項

- LDAP 照会はサポートされていません
- LDAP サーバからの割り込みメッセージまたは通知は処理されません。
- LDAP 認証は、インタラクティブ（端末）セッションではサポートされていません。

SLDAP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ldap server** *name* 例：	Lightweight Directory Access Protocol（LDAP）サーバを定義し、LDAP サー

	コマンドまたはアクション	目的
	`Device(config)# ldap server server1`	バ コンフィギュレーション モードを開始します。
ステップ 4	**ipv4** *ipv4-address* 例： `Device(config-ldap-server)# ipv4 9.4.109.20`	IPv4 を使用して LDAP サーバの IP アドレスを指定します。
ステップ 5	**timeout retransmit** *seconds* 例： `Device(config-ldap-server)# timeout retransmit 20`	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが LDAP 要求を再送信する前に応答を待機する秒数を指定します。
ステップ 6	**bind authenticate root-dn password** [**0** *string* | **7** *string*] *string* 例： `Device(config-ldap-server)# bind authenticate root-dn CN=ldapipv6user,CN=Users,DC=ca,DC=ssh2,DC=com password Cisco12345`	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと LDAP サーバ間で使用される共有秘密テキスト ストリングを指定します。 暗号化されていない共有秘密を設定するには、**0** 回線オプションを使用します。 暗号化された共有秘密を設定するには、**7** 回線オプションを使用します。
ステップ 7	**base-dn** *string* 例： `Device(config-ldap-server)# base-dn CN=Users,DC=ca,DC=ssh2,DC=com`	検索のベース識別名（DN）を指定します。
ステップ 8	**mode secure** [**no- negotiation**] 例： `Device(config-ldap-server)# mode secure no- negotiation`	TLS 接続を開始するよう LDAP を設定し、セキュア モードを指定します。
ステップ 9	**end** 例： `Device(config-ldap-server)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AAA サーバ グループの設定（GUI）

AAA サーバ グループを使用するようにデバイスを設定すると、既存のサーバ ホストをグループ化し、設定済みのサーバ ホストのサブセットを選択して、それらのサーバを特定のサービスに使用することが簡単にできます。サーバ グループは、グローバル サーバ ホストの一覧と一

緒に使用されます。サーバ グループには、選択したサーバ ホストの IP アドレスが一覧表示されます。

次のサーバ グループを作成できます。

手順

ステップ 1 RADIUS

a) [Services] > [Security] > [AAA] > [Server Groups] > [RADIUS] を選択します。
b) [Add] ボタンをクリックします。[Create AAA Radius Server Group] ダイアログボックスが表示されます。
c) [Name] フィールドに、RADIUS サーバ グループの名前を入力します。
d) [MAC-Delimiter] ドロップダウン リストから目的の区切り文字を選択します。コロン、ハイフン、およびシングルハイフンから選択できます。
e) [MAC-Filtering] ドロップダウン リストから目的のフィルタを選択します。[mac] および [Key] を選択できます。
f) サーバを非稼働にするには、[Dead-Time (mins)] フィールドに値を入力します。値は 1 ～ 1440 の範囲で指定する必要があります。
g) [Available Servers] リストから使用可能なサーバを選択し、[>] ボタンをクリックして [Assigned Servers] リストに移動します。
h) [Save & Apply to Device] ボタンをクリックします。

ステップ 2 TACACS+

a) [Services] > [Security] > [AAA] > [Server Groups] > [TACACS+] を選択します。
b) [Add] ボタンをクリックします。[Create AAA Tacacs Server Group] ダイアログボックスが表示されます。
c) [Name] フィールドに、TACACS サーバ グループの名前を入力します。
d) [Available Servers] リストから使用可能なサーバを選択し、[>] ボタンをクリックして [Assigned Servers] リストに移動します。
e) [Save & Apply to Device] ボタンをクリックします。

ステップ 3 LDAP

a) [Services] > [Security] > [AAA] > [Server Groups] > [LDAP] を選択します。
b) [Add] ボタンをクリックします。[Create AAA Ldap Server Group] ダイアログボックスが表示されます。
c) [Name] フィールドに、LDAP サーバ グループの名前を入力します。
d) [Available Servers] リストから使用可能なサーバを選択し、[>] ボタンをクリックして [Assigned Servers] リストに移動します。
e) [Save & Apply to Device] ボタンをクリックします。

AAA サーバ グループの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**aaa group server ldap** *group-name* 例： `Device(config)# aaa group server ldap name1`	グループ名を使用して AAA サーバ グループを定義し、LDAP サーバ グループ コンフィギュレーション モードを開始します。 グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS、LDAP、または TACACS+ です。
ステップ 5	**server** *name* 例： `Device(config-ldap-sg)# server server1`	特定の LDAP サーバを定義済みのサーバ グループと関連付けます。 セキュリティ サーバは、IP アドレスと UDP ポート番号で識別されます。
ステップ 6	**exit** 例： `Device(config-ldap-sg)# exit`	LDAP サーバ グループ コンフィギュレーション モードを終了します。

認証要求のための検索操作とバインド操作の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA をイネーブルにします。
ステップ 4	**ldap server** *name* 例： `Device(config)# ldap server server1`	Lightweight Directory Access Protocol（LDAP）サーバを定義し、LDAP サーバ コンフィギュレーション モードを開始します。
ステップ 5	**authentication bind-first** 例： `Device(config-ldap-server)# authentication bind-first`	認証要求のために一連の検索操作とバインド操作を設定します。
ステップ 6	**authentication compare** 例： `Device(config-ldap-server)# authentication compare`	バインド要求を認証の比較要求に置き換えます。
ステップ 7	**exit** 例： `Device(config-ldap-server)# exit`	LDAP サーバ グループ コンフィギュレーション モードを終了します。

SLDAP サーバでのダイナミック属性マップの設定

既存のユーザ定義属性名と値を、セキュリティ アプライアンスと互換性があるシスコ属性名と値にマッピングする、LDAP 属性マップを作成する必要があります。作成した属性マップは、必要に応じて LDAP サーバにバインドしたり削除したりできます。

（注） 属性マッピング機能を適切に使用するには、シスコ LDAP 属性の名前と値、およびユーザ定義属性の名前と値を理解する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ldap attribute-map** *map-name* 例： `Device(config)# ldap attribute-map map1`	ダイナミック LDAP 属性マップを設定し、属性マップ コンフィギュレーション モードを開始します。
ステップ 4	**map type** *ldap-attr-type aaa-attr-type* 例： `Device(config-attr-map)# map type department supplicant-group`	属性マップを定義します。
ステップ 5	**exit** 例： `Device(config-attr-map)# exit`	属性マップ コンフィギュレーション モードを終了します。

SLDAP の設定の確認

デフォルトの LDAP 属性マッピングの詳細を表示するには、次のコマンドを使用します。

```
Device# show ldap attributes
```

LDAP サーバの状態情報や、それ以外のサーバの各種カウンタを表示するには、次のコマンドを使用します。

```
Device# show ldap server
```

第 64 章

RADIUS DTLS

RADIUS DTLS について

Remote Authentication Dial-In User Service（RADIUS）は、ネットワークへの管理アクセス権を取得しようとするユーザに対して中央管理されたセキュリティ機能を提供する、クライアントまたはサーバプロトコルです。RADIUS プロトコルは広く導入されている認証および認可プロトコルであり、完全な認証、認可、およびアカウンティング（AAA）ソリューションを実現します。

RADIUS DTLS のポート

RADIUS のポート（DTLS サーバ）は認証とアカウンティングに使用されます。デフォルトの DTLS サーバ ポートは 2083 です。

RADIUS DTLS ポート番号は **dtls port** *port_number* を使用して変更できます。詳細については、「RADIUS DTLS ポート番号の設定」を参照してください。

共有秘密

すでに特定のサーバに対して DTLS を有効にしている場合は、共有秘密として **radius/dtls** を使用できます。

CTS 通信のための PAC の処理

CTS 通信のために ISE から PAC をダウンロードできます。PAC をダウンロードしたら、共有秘密の代わりに PAC キーを使用してすべての CTS 属性を暗号化する必要があります。

その後、ISE は PAC を使用してそれらの属性を復号化します。

セッション管理

RADIUS クライアントは、DTLS サーバからの応答にのみ依存します。セッションが理想的なタイムアウトに最も適している場合は、セッションを閉じる必要があります。

応答が無効の場合は、セッションを削除する必要があります。

DTLS 経由で RADIUS パケットを送信する必要がある場合は、特定のサーバで DTLS セッションを再確立する必要があります。

ロード バランシング

複数の DTLS サーバとロード バランシング方式が設定されています。

要求を必要とする送信先の AAA サーバを選択する必要があります。その後、特定のサーバの DTLS コンテキストを使用し、RADIUS パケットを暗号化して送り返します。

接続タイムアウト

暗号化された RADIUS パケットを送信した後、再送信タイマーを開始する必要があります。再送信タイマーが期限切れになる前に応答がなかった場合は、パケットが再暗号化され再送信されます。

この試行回数は、**dtls retries** の設定に従って、またはデフォルト値まで継続できます。試行回数が制限を超えると、サーバは使用不可となり、応答は AAA クライアントに戻されます。

（注） デフォルトの接続タイムアウトは 5 秒です。

接続の再試行回数

RADIUS DTLS は UDP ベースであるため、特定の再試行回数において特定のタイムアウト間隔後に接続を再試行する必要があります。

すべての再試行を終えると、DTLS 接続では次のことが実行されます。

- 失敗としてマークされます。
- RADIUS 要求を処理するために次に使用可能なサーバを検索します。

（注） デフォルトの接続再試行回数は 5 回です。

アイドル タイムアウト

アイドル タイマーが期限切れになり、最後のアイドル タイムアウト以降にトランザクションが存在しない場合、DTLS セッションは閉じたままになります。

DTLS セッションを確立した後、アイドル タイマーを開始できます。アイドル タイマーを 30 秒間にわたって開始し、RADIUS DTLS パケットの 1 つが送信されると、30 秒後にアイドル タイマーが期限切れになり、RADIUS DTLS トランザクションの数がチェックされます。

アイドル タイマーの値がゼロを超えると、アイドル タイマーはトランザクション カウンタをリセットし、タイマーを再開します。

（注） デフォルトのアイドル タイムアウトは 60 秒です。

サーバおよびサーバ グループのフェールオーバーの処理

RADIUS サーバは DTLS ありおよび DTLS なしで設定できます。DTLS 対応サーバと非 DTLS サーバを使用して AAA サーバ グループを作成することをお勧めします。ただし、AAA サーバ グループの設定時にはこのような制限は受けません。

DTLS サーバを選択し、DTLS サーバが接続を確立し、RADIUS 要求パケットが DTLS サーバに送信されるとします。すべての RADIUS の再試行後も DTLS サーバが応答しない場合は、同じサーバ グループ内で次に設定されているサーバに引き継がれます。次のサーバが DTLS サーバの場合、RADIUS 要求パケットの処理は次のサーバで続行されます。次のサーバが非 DTLS サーバの場合、RADIUS 要求パケットの処理はそのサーバ グループでは行われません。その後、サーバ グループのフェールオーバーが発生し、次のサーバ グループが使用可能であれば、同じシーケンスが次のサーバ グループで続行されます。

（注） サーバ グループ内では、DTLS サーバか非 DTLS サーバのいずれかのみを使用する必要があります。

前提条件

IOS および BINOS AAA のサポート

AAA サーバは、IOS および BINOS プラットフォームで動作します。IOS で RADIUS DTLS のサポートを完了したら、同じサポートを BINOS にも移植する必要があります。

RADIUS DTLS サーバの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *server-name* 例： `Device(config)# radius server R1`	RADIUS サーバ名を指定します。
ステップ 4	**dtls** 例： `Device(config-radius-server)# dtls`	DTLS パラメータを設定します。
ステップ 5	**end** 例： `Device(config-radius-server)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RADIUS DTLS 接続タイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *server-name* 例：	RADIUS サーバ名を指定します。

	コマンドまたはアクション	目的
	`Device(config)# radius server R1`	
ステップ 4	**dtls connectiontimeout** *timeout* 例： `Device(config-radius-server)# dtls connectiontimeout 1`	RADIUS DTLS 接続タイムアウトを設定します。 ここで、各変数は次のように定義されます。 *timeout* は、DTLS 接続タイムアウト値を指します。有効な範囲は 1 ～ 65535 です。
ステップ 5	**end** 例： `Device(config-radius-server)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RADIUS DTLS アイドル タイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *server-name* 例： `Device(config)# radius server R1`	RADIUS サーバ名を指定します。
ステップ 4	**dtls idletimeout** *idle_timeout* 例： `Device(config-radius-server)# dtls idletimeout 2`	RADIUS DTLS アイドル タイムアウトを設定します。 ここで、各変数は次のように定義されます。 *idle_timeout* は、DTLS アイドル タイムアウト値を指します。有効な範囲は 1 ～ 65535 です。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-radius-server)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RADIUS DTLS サーバの送信元インターフェイスと VRF の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *server-name* 例： `Device(config)# radius server R1`	RADIUS サーバ名を指定します。
ステップ 4	**dtls ip** {**radius source-interface Ethernet-Internal** *interface_number* | **vrf forwarding** *table_name*} 例： `Device(config-radius-server)# dtls ip radius source-interface Ethernet-Internal 0` `Device(config-radius-server)# dtls ip vrf forwarding table1`	RADIUS DTLS サーバの送信元インターフェイスと VRF を設定します。 ここで、各変数は次のように定義されます。 • *interface_number* は、イーサネット内部インターフェイス番号を指します。デフォルト値は 0 です。 • *table_name* は、転送テーブルの名前を指します。
ステップ 5	**end** 例： `Device(config-radius-server)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RADIUS DTLS ポート番号の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *server-name* 例： `Device(config)# radius server R1`	RADIUS サーバ名を指定します。
ステップ 4	**dtls port** *port_number* 例： `Device(config-radius-server)# dtls port 2`	RADIUS DTLS ポート番号を設定します。 ここで、各変数は次のように定義されます。 *port_number* は、DTLS ポート番号を指します。有効な範囲は 1 ～ 65535 です。
ステップ 5	**end** 例： `Device(config-radius-server)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RADIUS DTLS 接続再試行回数の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**radius server** *server-name* 例： `Device(config)# radius server R1`	RADIUS サーバ名を指定します。
ステップ 4	**dtls retries** *retry_number* 例： `Device(config-radius-server)# dtls retries 3`	RADIUS 接続の再試行回数を設定します。 ここで、各変数は次のように定義されます。 *retry_number* は、DTLS 接続の再試行回数を指します。有効な範囲は 1 ～ 65535 です。
ステップ 5	**end** 例： `Device(config-radius-server)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RADIUS DTLS トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**radius server** *server-name* 例： `Device(config)# radius server R1`	RADIUS サーバ名を指定します。
ステップ 4	**dtls trustpoint** {**client** *LINE* **dtls** | **server** *LINE* **dtls**} 例： `Device(config-radius-server)# dtls trustpoint client client1 dtls` `Device(config-radius-server)# dtls trustpoint server server1 dtls`	クライアントとサーバにトラストポイントを設定します。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-radius-server)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

DTLS ダイナミック認証の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	RFC 3576 サポート用のローカル サーバ プロファイルを設定します。
ステップ 4	**dtls** 例： `Device(config-locsvr-da-radius)# dtls`	DTLS 送信元パラメータを設定します。
ステップ 5	**end** 例： `Device(config-locsvr-da-radius)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

クライアントの DTLS の有効化

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	RFC 3576 サポート用のローカル サーバ プロファイルを設定します。
ステップ 4	**client** *IP_addr* **dtls** 例： `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls`	クライアントの DTLS を有効にします。
ステップ 5	**end** 例： `Device(config-locsvr-da-radius)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

DTLS のクライアント トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	RFC 3576 サポート用のローカル サーバ プロファイルを設定します。
ステップ 4	**client** *IP_addr* **dtls** {**client-tp** *client-tp-name* | **server-tp** *server-tp-name*} 例： `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls client-tp client_tp_name`	DTLS のクライアント トラストポイントを設定します。
ステップ 5	**end** 例： `Device(config-locsvr-da-radius)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

DTLS アイドル タイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	RFC 3576 サポート用のローカル サーバ プロファイルを設定します。
ステップ 4	**client** *IP_addr* **dtls idletimeout** *timeout-interval* {**client-tp** *client_tp_name* | **server-tp** *server_tp_name*} 例： `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls idletimeout 62 client-tp dtls_ise`	DTLS のアイドル時間を設定します。 ここで、各変数は次のように定義されます。 *timeout-interval* は、アイドル タイムアウト間隔を指します。有効な範囲は 60 ～ 600 です。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-locsvr-da-radius)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

DTLS のサーバ トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを開始します。
ステップ 2	**configure terminal** 例： `Device# 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 3	**aaa server radius dynamic-author** 例： `Device(config)# aaa server radius dynamic-author`	RFC 3576 サポート用のローカル サーバ プロファイルを設定します。
ステップ 4	**client** *IP_addr* **dtls server-tp** *server_tp_name* 例： `Device(config-locsvr-da-radius)# client 10.104.49.14 dtls server-tp dtls_client`	サーバ トラストポイントを設定します。
ステップ 5	**end** 例： `Device(config-locsvr-da-radius)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RADIUS DTLS サーバの設定の確認

DTLS 対応サーバに関する情報を表示するには、次のコマンドを使用します。

```
Device# show aaa servers
DTLS: Packet count since last idletimeout 1,
Send handshake count 3,
Handshake Success 1,
```

```
Total Packets Transmitted 1,
Total Packets Received 1,
Total Connection Resets 2,
Connection Reset due to idle timeout 0,
Connection Reset due to No Response 2,
Connection Reset due to Malformed packet 0,
```

RADIUS DTLS 固有の統計情報のクリア

Radius DTLS 固有の統計情報をクリアするには、次のコマンドを使用します。

```
Device# clear aaa counters servers radius {<server-id> | all}
```

（注） *server-id* は、**show aaa servers** によって表示されるサーバ ID を指します。0 ～ 2147483647 の範囲の値を指定できます。

第 65 章

MAC 認証バイパス

MAC 認証バイパス

MAC 認証バイパス（MAB）機能を使用し、クライアント MAC アドレスに基づいてクライアントを許可するようにコントローラを設定できます。

MAB を有効にすると、コントローラはクライアント ID として MAC アドレスを使用します。認証サーバには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。クライアントの検出後、コントローラはクライアントからのパケットを待機します。コントローラは、MAC アドレスに基づくユーザ名とパスワードを含む RADIUS アクセス/要求フレームを認証サーバに送信します。認証が成功すると、コントローラはクライアントにネットワークへのアクセス権を付与します。認証が失敗した場合、ゲスト WLAN が設定されていれば、コントローラはゲスト WLAN にポートを割り当てます。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、認証されたクライアントの場合と同じです。再認証の間、ポートは前に割り当てられた WLAN のままです。再認証が成功すると、コントローラは同じ WLAN でポートを保持します。再認証が失敗した場合、ゲスト WLAN が設定されていれば、コントローラはゲスト WLAN にポートを割り当てます。

MAB の設定に関する注意事項

- MAB の設定に関する注意事項は、802.1x 認証の注意事項と同じです。

- MAC アドレスで認可された後にポートで MAB を無効にしても、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバ データベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAB によって接続されているにもかかわらず非アクティブなホストのタイムアウト時間を設定できます。有効な範囲は 1 ～ 65535 秒です。

WLAN の 802.11 セキュリティの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

ステップ 3 [Security] タブで次の設定を行えます。

- レイヤ 2
- Layer3
- AAA

ステップ 4 [Layer2] タブで次の設定を行えます。

a) [Layer2 Security Mode] を次のオプションから選択します。

- [None]：レイヤ 2 セキュリティなし。
- [WPA + WPA2]：Wi-Fi Protected Access。
- Static WEP：静的 WEP 暗号化パラメータ。

b) 必要に応じて、[MAC Filtering] を有効にしますMAC フィルタリングは、MAC 認証バイパス（MAB）とも呼ばれます。

c) [Protected Management Frame] セクションの [PMF] で、[Disabled]、[Optional]、または [Required] を選択します。デフォルトでは、PMF は無効になっています。

d) [WPA Parameters] セクションで、必要に応じて次のオプションを選択します。

- WPA Policy

- WPA2 Policy
- WPA2 Encryption

e) [Auth Key Mgmt] のオプションを選択します。
f) AP 間の [Fast Transition] の適切なステータスを選択します。
g) 分散システム経由の高速移行を有効にするには、[Over the DS] チェック ボックスをオンにします。
h) [Reassociation Timeout] の値（秒単位）を入力します。これは、高速移行の再アソシエーションがタイムアウトするまでの時間です。
i) [Save & Apply to Device] をクリックします。

ステップ 5 [Layer3] タブで次の設定を行えます。

a) Web ポリシーを使用するには、[Web Policy] チェック ボックスをオンにします。
b) 必要な [Webauth Parameter Map] 値をドロップダウンリストから選択します。
c) 必要な [Authentication List] 値をドロップダウンリストから選択します。
d) [Show Advanced Settings] セクションで、[On Mac Filter Failure] チェック ボックスをオンにします。
e) [Conditional Web Redirect] と [Splash Web Redirect] を有効にします。
f) ドロップダウンリストから適切な IPv4 および IPv6 ACL を選択します。
g) [Save & Apply to Device] をクリックします。

ステップ 6 [AAA] タブで次の設定を行えます。

a) ドロップダウンから認証リストを選択します。
b) WLAN でローカル EAP 認証を有効にするには、[Local EAP Authentication] チェック ボックスをオンにします。また、必要な [EAP Profile Name] をドロップダウンリストから選択します。
c) [Save & Apply to Device] をクリックします。

WLAN の 802.11 セキュリティの設定（CLI）

WLAN の 802.11 セキュリティを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *profile-name wlan-id ssid* **例：** `Device(config)# wlan ha-wlan-dot1x-test 3 ha-wlan-dot1x-test`	WLAN プロファイルを設定します。

	コマンドまたはアクション	目的
ステップ 2	**security dot1x authentication-list** *auth-list-name* 例： `Device(config-wlan)# security dot1x authentication-list default`	dot1x セキュリティ用のセキュリティ認証リストを有効にします。
ステップ 3	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

外部認証用の AAA の設定

外部認証用に AAA を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**radius server** *server-name* 例： `Device(config)# radius server ISE`	Radius サーバを設定します。
ステップ 2	**address** {**ipv4** | **ipv6**}*radius-server-ip-address* **auth-port** *auth-port-no* **acct-port** *acct-port-no* 例： `Device(config-radius-server)# address ipv4 9.2.58.90 auth-port 1812 acct-port 1813`	Radius サーバのアドレスを指定します。
ステップ 3	**key** *key* 例： `Device(config-radius-server)# key any123`	サーバごとの暗号キーを設定します。
ステップ 4	**exit** 例： `Device(config-locsvr-da-radius)# exit`	コンフィギュレーションモードに戻ります。
ステップ 5	**aaa local authentication default authorization default** 例：	デフォルトのローカル認証および許可を選択します。

	コマンドまたはアクション	目的
	`Device(config)# aaa local authentication default authorization default`	
ステップ 6	**aaa new-model** 例： `Device(config)# aaa new-model`	AAA認証モデルを作成します。新しいアクセス制御コマンドと機能を有効にします。
ステップ 7	**aaa session-id common** 例： `Device(config)# aaa session-id common`	コモン セッション ID を作成します。
ステップ 8	**aaa authentication dot1x default group radius** 例： `Device(config)# aaa authentication dot1x default group radius`	デフォルトの dot1x 方式の認証を設定します。 .
ステップ 9	**aaa authorization network default group radius** 例： `Device(config)# aaa authorization network default group radius`	ネットワーク サービスの認証を設定します。
ステップ 10	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	SysAuthControl を有効にします。

ローカル認証用の AAA の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Wireless Networks] ページで [Add] をクリックします。

ステップ 3 表示される [Add WLAN] ウィンドウで、**[Security]** > **[AAA]** を選択します。

ステップ 4 [Authentication List] ドロップダウンから値を選択します。

ステップ 5 WLAN でローカル EAP 認証を有効にするには、[Local EAP Authentication] チェック ボックスをオンにします。

ステップ 6 [EAP Profile Name] ドロップダウンから値を選択します。

ステップ 7 [Save & Apply to Device] をクリックします。

ローカル認証用の AAA の設定（CLI）

ローカル認証用に AAA を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**aaa authentication dot1x default local** **例：** `Device(config)# aaa authentication dot1x default local`	デフォルトのローカル RADIUS サーバを使用するように設定します。
ステップ 2	**aaa authorization network default local** **例：** `Device(config)# aaa authorization network default local`	認証方式をローカルに設定します。
ステップ 3	**aaa authorization credential-download default local** **例：** `Device(config)# aaa authorization credential-download default local`	ローカル サーバからログイン情報をダウンロードするようにデフォルト データベースを設定します。
ステップ 4	**username** *mac-address***mac** **例：** `Device(config)# username 6038e0dc2d3f mac`	ユーザ名を使用したMACフィルタリング向け。
ステップ 5	**aaa local authentication default authorization default** **例：** `Device(config)# aaa local authentication default authorization default`	ローカル認証方式リストを設定します。
ステップ 6	**aaa new-model** **例：** `Device(config)# aaa new-model`	AAA 認証モデルを作成します。新しいアクセス制御コマンドと機能を有効にします。
ステップ 7	**aaa session-id common** **例：** `Device(config)# aaa session-id common`	コモン セッション ID を作成します。

ローカル認証用の MAB の設定

ローカル認証用に MAB を設定するには、次の手順に従います。

始める前に

AAA ローカル認証を設定します。

username *mac-address* **mac** コマンドを使用して、WLAN 設定（ローカル認証）のユーザ名を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *profile-name wlan-id* 例： `wlan CR1_SSID_mab-local-default 1 CR1_SSID_mab-local-default`	WLAN の名前と ID を指定します。
ステップ 2	**mac-filtering default** 例： `Device(config-wlan)# mac-filtering default`	WLAN の MAC フィルタリング サポートを設定します。
ステップ 3	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 4	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 6	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 7	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

外部認証用の MAB の設定（GUI）

始める前に

AAA 外部認証を設定します。

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[WLANs]** の順に選択します。
ステップ 2 [Wireless Networks] ページで WLAN の名前をクリックします。
ステップ 3 [Edit WLAN] ウィンドウで [Security] タブをクリックします。
ステップ 4 [Layer2] タブで、[MAC Filtering] チェック ボックスをオンにして機能を有効にします。
ステップ 5 MAC フィルタリングを有効にした状態で、ドロップダウンリストから [Authorization List] を選択します。
ステップ 6 設定を保存します。

外部認証用の MAB の設定（CLI）

外部認証用に MAB を設定するには、次の手順に従います。

始める前に

AAA 外部認証を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *wlan-name wlan-id ssid-name* **例：** `wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radius`	WLAN の名前と ID を指定します。
ステップ 2	**mac-filtering** *list-name* **例：** `Device(config-wlan)# mac-filtering ewlc-radius`	MAC フィルタリング パラメータを設定します。
ステップ 3	**no security wpa** **例：** `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。

	コマンドまたはアクション	目的
ステップ 4	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 6	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 7	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

第 66 章

IP ソース ガード

IP ソース ガードの概要

IP ソースガード（IPSG）は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのレイヤ 2 セキュリティ機能です。IPv4 と IPv6 の両方のワイヤレス クライアントをサポートします。

IPSG 機能は、ワイヤレス コントローラで認識されていない送信元 IP アドレスを使用したパケットの転送を阻止します。このセキュリティ機能はデフォルトでは有効になっていないため、明示的に設定する必要があります。WLAN ごとに有効化され、その WLAN に接続しているすべてのワイヤレス クライアントがこの機能を継承します。

ワイヤレス コントローラは、IPSG 機能の IP/MAC ペア バインディング テーブルを維持します。ワイヤレス コントローラはこのテーブルを使用して、すべてのワイヤレス クライアントの IP アドレスと MAC アドレスの組み合わせ（バインディング）情報を追跡します。このバインディング情報は、IP 学習プロセスの一環としてキャプチャされます。この機能が WLAN で有効になっている場合、ワイヤレス コントローラがワイヤレス クライアントからの着信パケットを転送するのは、パケットの送信元 IP アドレスと MAC アドレスの組み合わせに一致するバインディング テーブル エントリが検出された場合のみです。エントリが検出されない場合、パケットはドロップされます。

IP ソース ガードの設定

IPSG を設定するには、次の手順に従います。

始める前に

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、クライアントごとに 1 つの IPv4 アドレスと、最大 8 つの IPv6 アドレス（リンク ローカル アドレスを含む）をサポートします。

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *profile-name wlan-id ssid* 例： `Device(config)# wlan mywlan 34 mywlan-ssid`	使用する WLAN の名前と ID を指定します。 （注） WLAN がまだ設定されていない場合は、この手順によって WLAN が作成されます。
ステップ 2	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 3	**ip verify source mac-check** 例： `Device(config-wlan)# ip verify source mac-check`	IP ソース ガード機能を有効にします。
ステップ 4	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

第 67 章

Dynamic Frequency Selection（動的周波数選択）

動的周波数選択について

動的周波数選択（DFS）は、レーダー信号による干渉を回避するために、レーダー信号を検出して DFS 対応 5.0 GHz（802.11a/h）無線の周波数を自動的に設定するプロセスです。規制ドメインで使用するように設定された無線が、レーダー システムに干渉しないようにする必要があります。

通常の DFS では、40 または 80 MHz 帯域幅のいずれかのチャネルでレーダー信号が検出されると、チャネル全体がブロックされます。Flex DFS を使用すると、セカンダリ チャネルでレーダー信号が検出されていない場合は AP がセカンダリ チャネルに移動され、帯域幅が（通常は半分に）削減されます。

動的周波数選択の設定

DFS を設定するには、次の手順に従います。

始める前に

- 対応する AP が、いずれかの DFS チャネル上に存在する必要があります。
- 設定変更を適用する前に、無線をシャットダウンします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**no ap dot11 5ghz dtpc** 例： `Device(config)# no ap dot11 5ghz dtpc`	802.11a ダイナミック伝送パワーコントロール（DTPC）設定を無効にします。
ステップ 3	**ap dot11 5ghz channelswitch mode** *mode-num* 例： `Device(config)# ap dot11 5ghz channelswitch mode 1`	802.11h チャネル スイッチ モードを設定します。
ステップ 4	**ap dot11 5ghz power-constraint** *value* 例： `Device(config)# ap dot11 5ghz power-constraint 12`	802.11h 電力制限値を設定します。
ステップ 5	**ap dot11 5ghz smart-dfs** 例： `Device(config)# ap dot11 5ghz smart-dfs`	レーダー干渉チャネルの非占有時間を設定します。

DFS の確認

DFS 設定を確認するには、次のコマンドを使用します。

802.11h 設定を表示するには、次のコマンドを使用します。

```
Device# show wireless dot11h
```

802.11h 設定の自動 RF 情報を表示するには、次のコマンドを使用します。

```
Device# show ap auto-rf dot11 5ghz
```

Cisco AP の自動 RF 情報を表示するには、次のコマンドを使用します。

```
Device# show ap name ap1 auto-rf dot11 5gh
```

第 68 章

不正なデバイスの管理

不正なデバイスについて

不正なアクセス ポイントは、正規のクライアントをハイジャックし、プレーンテキストまたは他の DoS 攻撃や man-in-the-middle 攻撃を使用して無線 LAN の運用を妨害する可能性があります。つまり、ハッカーは、不正なアクセス ポイントを使用することで、ユーザ名やパスワードなどの機密情報を入手することができます。すると、ハッカーは一連のクリア ツー センド（CTS）フレームを送信できるようになります。アクセス ポイントになりすまして、特定のクライアントには送信を許可し、他のすべてのクライアントには待機するように指示が送られると、正規のクライアントは、ネットワーク リソースに接続できなくなってしまいます。無線 LAN サービス プロバイダーは、空間からの不正なアクセス ポイントの締め出しに強い関心を持っています。

不正なアクセス ポイントは安価で簡単に利用できることから、企業の従業員は、IT 部門に報告して同意を得ることなく、認可されていない不正なアクセス ポイントを既存の LAN に接続し、アドホック無線ネットワークを確立することがあります。これらの不正アクセス ポイントは、企業のファイアウォールの内側にあるネットワーク ポートに接続可能であるため、重大なネットワーク セキュリティ侵犯となることがあります。通常、従業員は不正なアクセス ポイントのセキュリティ設定を有効にしないので、権限のないユーザがこのアクセス ポイントを使って、ネットワーク トラフィックを傍受し、クライアント セッションをハイジャックすることは簡単です。ワイヤレス ユーザがエンタープライズ ネットワーク内のアクセス ポイントに接続する場合、エンタープライズ セキュリティ違反が発生する可能性が高くなります。

次に、不正なデバイスの管理に関する注意事項を示します。

- アクセス ポイントは、関連付けられたクライアントに対応するように設計されています。これらのアクセス ポイントは比較的短時間でオフチャネル スキャンを実行します（各チャネル約 50 ミリ秒）。大量の不正 AP とクライアントを高感度で検出する場合、モニタ モー

ド アクセス ポイントを使用する必要があります。あるいは、スキャン間隔を 180 秒から 120 秒や 60 秒などに短縮して、無線がオフチャネルになる頻度を増やします。これにより、不正が検出される可能性は増加します。ただしこの場合も、アクセス ポイントは引き続き各チャネル上で約 50 ミリ秒を費やします。

- 家庭環境で展開されるアクセス ポイントは多数の不正デバイスを検出する可能性が高いため、OfficeExtend アクセス ポイントでは不正検出がデフォルトで無効になっています。
- クライアント カードの実装により、アドホックの抑制の効果が低下することがあります。
- 不正の状態と、状態の自動的な移行を可能にするユーザ定義の分類規則を使って、不正なアクセス ポイントを分類および報告できます。
- 各コントローラの不正封じ込めの数は、モニタ モードのアクセス ポイントの場合は無線ごとに 3 および 6 に制限されています。
- Rogue Location Discovery Protocol（RLDP）は、オープン認証に設定されている不正なアクセス ポイントを検出します。
- RLDP はブロードキャスト Basic Service Set Identifier（BSSID）を使用する不正なアクセス ポイント（つまり Service Set Identifier をビーコンでブロードキャストするアクセス ポイント）を検出します。
- RLDP は、同じネットワークにある不正なアクセス ポイントのみを検出します。ネットワークのアクセス リストによって不正なアクセス ポイントからコントローラへの RLDP のトラフィックの送信が阻止されている場合は、RLDP は機能しません。
- RLDP は 5 GHz の動的周波数選択（DFS）チャネルでは機能しません。
- メッシュ AP で RLDP が有効にされていて、その AP が RLDP タスクを実行すると、そのメッシュ AP のアソシエーションはコントローラから解除されます。回避策は、メッシュ AP で RLDP を無効にすることです。
- RLDP がモニタ モードではない AP で有効になっている場合、RLDP の処理中にクライアント接続の中断が発生します。
- 設定を使用して手動の阻止を実行すると、不正エントリは有効期限が切れた後でも保持されます。
- 不正エントリの有効期限が切れると、管理対象のアクセス ポイントはすべてのアクティブな封じ込めを停止するように指示されます。
- 不正を自動、ルールなどのその他の方法で阻止すると、不正エントリは期限切れになると削除されます。
- コントローラは、不正なクライアントの検証を AAA サーバに一度だけ要求します。その結果、不正なクライアント検証が最初の試行で失敗すると、不正なクライアントは今後脅威として検出されなくなります。これを回避するには、[**Validate Rogue Clients Against AAA**] を有効にする前に、認証サーバに有効なクライアント エントリを追加します。

不正検出の制約事項

- DFS チャネルでの不正封じ込めはサポートされていません。

Rogue Location Discovery Protocol

Rogue Location Discovery Protocol（RLDP）は、不正 AP で認証が設定されていない（オープン認証）場合に使用される積極的なアプローチです。このモードは、デフォルトで無効になっており、不正チャネルに移動して、クライアントとして不正に接続するようにアクティブ AP に指示します。この間に、アクティブ AP は、接続されたすべてのクライアントに認証解除メッセージを送信してから、無線インターフェイスをシャットダウンします。次に、クライアントとして不正 AP にアソシエートします。その後で、AP は、不正 AP から IP アドレスの取得を試み、ローカル AP と不正接続情報を含む User Datagram Protocol（UDP）パケット（ポート 6352）を不正 AP を介してコントローラに転送します。コントローラがこのパケットを受信すると、不正 AP が RLDP 機能を使用して有線ネットワークで検出されたことをネットワーク管理者に通知するためのアラームが設定されます。

ここで、Lightweight AP から送信される UDP （宛先ポート 6352）パケットのサンプルを示します。0020 0a 01 01 0d 0a 01 .....(.*..... 0030 01 1e 00 07 85 92 78 01 00 00 00 00 00 00 00 00 ......x..... 0040 00 00 00 00 00 00 00 00 00 00 00 00

最初の 5 バイトのデータには、不正 AP によってローカル モード AP に割り当てられた DHCP アドレスが含まれています。次の 5 バイトはコントローラの IP アドレスで、その後に不正 AP MAC アドレスを表す 6 バイトが続きます。その後に、18 バイトの 0 が続きます。

次の手順では、RLDP の機能について説明します。

1. 信号強度値を使用して不正に最も近い統合 AP を特定します。
2. その後で、この AP が WLAN クライアントとして不正に接続します。3 回のアソシエーションを試みて、成功しない場合はタイムアウトします。
3. アソシエーションが成功すると、AP が DHCP を使用して IP アドレスを取得します。
4. IP アドレスが取得されたら、AP（WLAN クライアントとして機能している）は、コントローラの IP アドレスのそれぞれに UDP パケットを送信します。
5. コントローラがクライアントから RLDP パケットの 1 つでも受信すると、その不正が on-wire としてマークされます。

（注） コントローラのネットワークと不正デバイスが設置されたネットワークの間にフィルタリングルールが設定されている場合は、RLDP パケットがコントローラに到達できません。

RLDP の注意事項：

- RLDP は、認証と暗号化が無効になっている SSID をブロードキャストするオープン不正 AP でのみ動作します。

- RLDP では、クライアントとして機能しているマネージド AP が不正ネットワーク上で DHCP を介して IP アドレスを取得できる必要があります。
- 手動 RLDP を使用して、不正上で RLDP トレースを複数回試すことができます。
- RLDP プロセス中は、AP がクライアントにサービスを提供できません。これがローカル モード AP のパフォーマンスと接続に悪影響を及ぼします。この問題を回避するために、RLDP はモニタ モード AP に対してのみ選択的に有効にできます。
- RLDP は、5GHz DFS チャネルで動作する不正 AP への接続は試行しません。

（注） RLDPは、シスコのAtonomous不正アクセスポイントではサポートされていません。これらのアクセスポイントは、RLDPクライアントによって送信されたDHCP検出要求をドロップします。また不正なアクセスポイントチャネルが動的周波数選択（DFS）を必要とする場合、RLDPはサポートされません。

不正なデバイスの検出

コントローラは、近くにあるすべてのアクセス ポイントを継続的に監視し、不正なアクセス ポイントとクライアントに関する情報を自動的に検出および収集します。コントローラは不正アクセス ポイントを検出すると、Rogue Location Discovery Protocol（RLDP）不正アクセス ポイントがネットワークに接続されているかどうかを確認します。

コントローラは、オープン認証不正デバイスで RLDP を開始します。RLDP が FlexConnect またはローカル モードのアクセス ポイントを使用すると、クライアントはその時点で接続を解除されます。RLDPのサイクルが終了すると、クライアントはアクセスポイントに再接続します。不正アクセス ポイントが検出された時点で（auto-configured）、RLDP プロセスが開始されます。

すべてのアクセス ポイント、または監視（リッスン専用）モードに設定されたアクセス ポイントでのみRLDPを使用するようにコントローラを設定できます。後者のオプションでは、混雑した無線周波数（RF）空間での自動不正アクセス ポイント検出が実現され、不要な干渉を生じさせたり、正規のデータ アクセス ポイント機能に影響を与えずにモニタリングを実行できます。すべてのアクセスポイントでRLDPを使用するようにコントローラを設定した場合、モニタ アクセス ポイントとローカル（データ）アクセス ポイントの両方が近くにあると、コントローラは常に RLDP 動作に対してモニタ アクセス ポイントを選択します。ネットワーク上に不正があるとRLDPが判断した場合、検出された不正を手動または自動で阻止することを選択できます。

RLDPは、オープン認証に設定されている不正なアクセスポイントの存在をネットワーク上で一度だけ（デフォルト設定の再試行回数）検出します。再試行回数は、**wireless wps rogue ap rldp retries** 設定 CLI を使用して設定できます。

3 種類の方法でコントローラから RLDP を開始またはトリガーできます。

1. コントローラの CLI から RLDP 開始コマンドを手動で入力します。

   wireless wps rogue ap mac-address *mac-address* **rldp initiate**

2. コントローラの設定 CLI から RLDP をスケジュールします。

   wireless wps rogue ap rldp schedule

3. 自動 RLDP。コントローラの CLI または GUI から自動 RLDP を設定できますが、次の注意事項を考慮してください。

   - 不正検出のセキュリティ レベルが custom に設定されている場合にのみ、自動 RLDP オプションを設定できます。
   - 自動 RLDP および RLDP のスケジュールを同時に有効にすることはできません。

不正なアクセス ポイントは、自動または手動で Contained 状態に変更されます。コントローラは、不正の阻止に最も効果的なアクセス ポイントを選択し、そのアクセス ポイントに情報を提供します。アクセスポイントは、無線あたりの不正阻止数のリストを保存します。自動阻止の場合は、監視モードのアクセス ポイントだけを使用するようにコントローラを設定できます。阻止動作は次の 2 つの方法で開始されます。

- コンテナ アクセス ポイントが定期的に不正阻止のリストを確認し、ユニキャスト阻止フレームを送信します。不正なアクセスポイントの阻止の場合、フレームは不正なクライアントがアソシエートされている場合にのみ送信されます。
- 阻止された不正アクティビティが検出されると、阻止フレームが送信されます。

個々の不正阻止には、一連のユニキャスト アソシエーション解除フレームおよび認証解除フレームの送信が含まれます。

Cisco Prime Infrastructure のインタラクションと不正検出

Cisco Prime Infrastructure ではルール ベースの分類がサポートされ、コントローラで設定された分類ルールが使用されます。コントローラは、次のイベント後に Cisco Prime Infrastructure にトラップを送信します。

- 不明なアクセス ポイントが Friendly 状態に初めて移行すると、コントローラは、不正の状態が Alert の場合にのみ Cisco Prime Infrastructure にトラップを送信します。不正の状態が Internal または External であると、トラップは送信されません。
- タイムアウトの経過後に不正エントリが削除されると、Malicious（Alert、Threat）または Unclassified（Alert）に分類された不正アクセス ポイントに関して、コントローラから Cisco Prime Infrastructure にトラップが送信されます。コントローラでは、不正の状態が Contained、Contained Pending、Internal、および External である不正なエントリは削除されません。

Rogue Location Discovery Protocol（RLDP）の設定方法

アラームを生成する RLDP の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [Rogue Policies] タブで、[Rogue Detection Security Level] ドロップダウンを使用してセキュリティ レベルを選択します。

ステップ 3 [Expiration timeout for Rogue APs (seconds)] フィールドに、タイムアウト値を入力します。

ステップ 4 [Validate Rogue Clients against AAA] チェック ボックスをオンにして、AAA サーバに対して不正クライアントを検証します。

ステップ 5 [Validate Rogue APs against AAA] チェック ボックスをオンにして、AAA サーバに対して不正アクセス ポイントを検証します。

ステップ 6 [Rogue Polling Interval (seconds)] フィールドに、不正のポーリング間隔を入力します。

ステップ 7 [Detect and Report Adhoc Networks] チェック ボックスをオンにして、AAA サーバに対して不正クライアントを検証します。

ステップ 8 [Rogue Detection Client Number Threshold] フィールドに、不正クライアント検出のしきい値を入力します。

ステップ 9 [Auto Contain] セクションで、次の詳細情報を入力します。

ステップ 10 [Auto Containment Level] ドロップダウンを使用してレベルを選択します。

ステップ 11 自動封じ込めをモニタ モードの AP のみに制限するには、[Auto Containment only for Monitor Mode APs] チェック ボックスをオンにします。

ステップ 12 自動封じ込めを有線の不正 AP のみに制限するには、[Rogue on Wire] チェック ボックスをオンにします。

ステップ 13 自動封じ込めを特定の SSID を使用する不正 AP のみに制限するには、[Using our SSID] チェック ボックスをオンにします。

ステップ 14 自動封じ込めをアドホック不正 AP のみに制限するには、[Adhoc Rogue AP] チェック ボックスをオンにします。

ステップ 15 [Apply] をクリックします。

アラームを生成する RLDP の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps rogue ap rldp alarm-only <monitor-ap-only>** 例： `Device(config)# wireless wps rogue ap rldp alarm-only` `Device(config)# wireless wps rogue ap rldp alarm-only monitor-ap-only`	RLDP でアラームを生成できるようにします。この方法では、RLDP は常に有効になります。 **monitor-ap-only** キーワードはオプションです。 **alarm-only** キーワードのみを指定してコマンドを実行すると、AP モードの制限なしで RLDP が有効になります。 **alarm-only <monitor-ap-only>** キーワードを指定してコマンドを実行すると、モニタ モードのアクセス ポイントでのみ RLDP が有効になります。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

自動封じ込め用の RLDP の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [RLDP] タブで、[Rogue Location Discovery Protocol] ドロップダウンを使用してすべての AP を選択します。

ステップ 3 [Retry Count] フィールドに再試行回数を入力します。

ステップ 4 [Schedule RLDP] チェック ボックスをオンにしてスケジュールを設定し、曜日と開始時刻および終了時刻を入力します。

ステップ 5 [Apply] をクリックします。

自動封じ込め用の RLDP の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps rogue ap rldp auto-contain** [**monitor-ap-only**] 例： `Device(config)# wireless wps rogue ap rldp auto-contain` `Device(config)# wireless wps rogue ap rldp auto-contain monitor-ap-only`	RLDP で自動封じ込めを実行できるようにします。この方法では、RLDP は常に有効になります。 **monitor-ap-only** キーワードはオプションです。 **auto-contain** キーワードのみを指定してコマンドを実行すると、AP モードの制限なしで RLDP が有効になります。 **auto-contain <monitor-ap-only>** キーワードを指定してコマンドを実行すると、モニタ モードのアクセス ポイントでのみ RLDP が有効になります。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RLDP のスケジュールの設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Wireless Protection Policies] の順に選択します。

ステップ 2 [RLDP] タブで、[Rogue Location Discovery Protocol] ドロップダウンリストから次のオプションのいずれかを選択します。

- [Disable]（デフォルト）：すべてのアクセス ポイントで RLDP を無効にします。
- [All APs]：すべての AP で RLDP を有効にします。
- [Monitor Mode APs]：モニタ モードの AP でのみ RLDP を有効にします。

ステップ 3 再試行の回数を入力します。

ステップ 4 不正ロケーション検出プロセスをスケジュール設定する場合は、[Schedule RLDP] チェック ボックスをオンにしてから、プロセスを実行する曜日、開始時刻、終了時刻を指定します。

ステップ 5 [Apply] をクリックします。

RLDP のスケジュールの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps rogue ap rldp schedule day** *day* **start** *start-time* **end** *end-time* 例： `Device(config)# wireless wps rogue ap rldp schedule day Monday start 10:10:01 end 12:00:00`	スケジュール設定された曜日、開始時刻、終了時刻に基づいて RLDP を有効にします。 ここで、各変数は次のように定義されます。 *day* は、RLDP のスケジューリングを実行できる曜日です。値は Monday、Tuesday、Wednesday、Thursday、Friday、Saturday、および Sunday です。 *start-time* は、RLDP のスケジューリングの開始時刻です。開始時刻は **HH:MM:SS** 形式で入力する必要があります。 *end time* は、RLDP のスケジューリングの終了時刻です。終了時刻は **HH:MM:SS** 形式で入力する必要があります。
ステップ 3	**wireless wps rogue ap rldp schedule** 例： `Device(config)# wireless wps rogue ap rldp schedule`	スケジュールを有効にします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

不正アクセス ポイントでの RLDP 再試行回数の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Wireless Protection Policies]** を選択します。

ステップ 2 [Wireless Protection Policies] ページで [RLDP] タブをクリックします。

ステップ 3 [Retry Count] フィールドに、不正アクセス ポイントの RLDP 再試行の値を入力します。

有効な範囲は 1 ～ 5 です。

ステップ 4 設定を保存します。

不正アクセス ポイントでの RLDP 再試行回数の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps rogue ap rldp retries** *num-entries* 例： `Device(config)# wireless wps rogue ap rldp retries 2`	不正アクセス ポイントでの RLDP 再試行回数を有効にします。 *num-entries* は、不正アクセス ポイントごとの RLDP 再試行回数です。 有効な範囲は 1 ～ 5 です。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

不正検出の設定方法

不正検出の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *profile-name* **rogue detection min-rssi** *rssi in dBm* 例： `Device(config)# ap profile profile1` `Device(config)# rogue detection min-rssi -100`	不正に必要な最小 RSSI 値を指定します。これは、APが不正を検出し、deviceで不正エントリが作成されるために必要な値です。 rssi in dBmパラメータの有効範囲は–128 ～ –70 dBm で、デフォルト値は –128 dBm です。 （注） この機能は、すべてのAPモードに適用できます。RSSI値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、APが不正を検出する最小RSSI値を指定することで、このオプションを使用して不正をフィルタリングすることができます。
ステップ 3	**ap profile** *profile-name* **rogue detection min-transient-time** *time in seconds* 例： `Device(config)# ap profile profile1` `Device(config)# rogue detection min-transient-time 120`	不正が初めてスキャンされた後、AP で不正スキャンを連続的に実行する間隔を入力します。 time in sec パラメータの有効範囲は 120 ～ 1800 秒で、デフォルト値は 0 です。

	コマンドまたはアクション	目的
		（注） この機能は、モニタ モードの AP のみに適用されます。 一時的な間隔値を使用して、APが不正をスキャンする間隔を制御できます。APでは、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。 この機能には次の利点があります。 • APからコントローラへの不正レポートが短くなる • 一時的な不正エントリをコントローラで回避できる • 一時的な不正への不要なメモリ割り当てを回避できる
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

不正検出の検証

この項では、不正検出の新しいコマンドについて説明します。

次のコマンドは、上で不正検出を検証するために使用できます。

表 *17*：アドホック不正情報の確認

コマンド	目的
show wireless wps rogue adhoc detailed *mac_address*	アドホック不正の詳細情報を表示します。
show wireless wps rogue adhoc summary	すべてのアドホック不正のリストを表示します。

表 *18* : 不正 *AP* 情報の確認

コマンド	目的
show wireless wps rogue ap clients *mac_address*	不正に関連付けられているすべての不正クライアントのリストを表示します。
show wireless wps rogue ap custom summary	カスタム不正 AP の情報を表示します。
show wireless wps rogue ap detailed *mac_address*	不正 AP の詳細情報を表示します。
show wireless wps rogue ap friendly summary	危険性のない不正 AP の情報を表示します。
show wireless wps rogue ap list *mac_address*	特定の AP によって検出された不正 AP のリストを表示します。
show wireless wps rogue ap malicious summary	悪意のある不正 AP の情報を表示します。
show wireless wps rogue ap rldp detailed *mac_address*	不正 AP の RLDP の詳細を表示します。
show wireless wps rogue ap rldp in progress	進行中の RLDP のリストを表示します。
show wireless wps rogue ap rldp summary	RLDP スケジューリング情報の要約を表示します。
show wireless wps rogue ap summary	すべての不正 AP のリストを表示します。
show wireless wps rogue ap unclassified summary	未分類の不正 AP の情報を表示します。

表 *19* : 不正の自動封じ込めに関する情報の確認

コマンド	目的
show wireless wps rogue auto-contain	不正の自動封じ込めに関する情報を表示します。

表 *20* : 分類ルールの情報の確認

コマンド	目的
show wireless wps rogue rule detailed *rule_name*	分類ルールの詳細情報を表示します。
show wireless wps rogue rule summary	すべての不正ルールのリストを表示します。

表 *21* : 不正統計情報の確認

コマンド	目的
show wireless wps rogue stats	不正統計情報を表示します。

表 *22 :* 不正クライアントの情報の確認

コマンド	目的
show wireless wps rogue client detailed *mac_address*	不正クライアントの詳細情報を表示します。
show wireless wps rogue client summary	すべての不正クライアントのリストを表示します。

表 *23 :* 不正無視リストの確認

コマンド	目的
show wireless wps rogue ignore-list	不正無視リストを表示します。

例：不正検出の設定

この例は、検出された不正 AP が存在する必要がある最小 RSSI を、で作成されたエントリを持つように設定する方法を示しています。

```
Device# configure terminal
Device(config)# ap profile profile1
Device(config)# rogue detection min-rssi -100
Device(config)# end
Device# show wireless wps rogue client summary/show wireless wps rogue ap summary
```

次に、分類インターバルを設定する例を示します。

```
Device# configure terminal
Device(config)# ap profile profile1
Device(config)# rogue detection min-transient-time 500
Device(config)# end
Device# show wireless wps rogue client summary/show wireless wps rogue ap summary
```

第 69 章

不正なアクセス ポイントの分類

不正なアクセス ポイントの分類について

コントローラ ソフトウェアでは、不正アクセス ポイントを Friendly、Malicious、Custom、または Unclassified に分類して表示するルールを作成できます。

デフォルトでは、いずれの分類ルールも使用されません。ルールを有効にする必要があります。したがって、すべての未知（管理対象外）のアクセス ポイントは Unclassified に分類されます。ルールを作成または変更し、条件を設定して有効にすると、すべての不正アクセス ポイントが再分類されます。ルールを変更するたびに、すべてのアクセス ポイント（Friendly、Malicious、および Unclassified）にルールが適用されます。

（注）

- ルールベースの分類は、アドホック不正クライアントおよび不正クライアントには適用されません。
- 1 台のコントローラにつき最大 64 の不正分類ルールを設定できます。

コントローラは、管理対象のアクセス ポイントの 1 つから不正レポートを受信すると、次のように応答します。

- 不明なアクセス ポイントが危険性のない MAC アドレスのリストに含まれている場合、コントローラはそのアクセス ポイントを Friendly に分類します。
- 不明なアクセス ポイントが危険性のない MAC アドレスのリストに含まれていない場合、コントローラはそのアクセス ポイントに対して不正分類ルールの適用を開始します。
- 不正アクセス ポイントを手動で分類する場合は、不正ルールが適用されません。

- 設定されているルールの条件に不正アクセスポイントが一致すると、コントローラはそのルールに設定された分類タイプに基づいて不正を分類します。
- 設定されたルールのいずれにも不正アクセスポイントが一致しない場合、不正はUnclassifiedのままになります。

  コントローラは、すべての不正アクセス ポイントに対して上記の手順を繰り返します。
- 不正アクセスポイントが同じ有線ネットワーク上で検出されると、ルールが設定されていなくても、コントローラは不正の状態を Threat とマークし、そのアクセス ポイントを自動的にMaliciousに分類します。その後は、不正を手動で封じ込めて不正の状態をContainedに変更できます。不正アクセス ポイントがネットワーク上で使用不可能な場合、コントローラは不正の状態を Alert としてマークします。その後は、不正を手動で封じ込めることができます。
- 必要に応じて、各アクセスポイントを本来とは異なる分類タイプや不正の状態に手動で変更することも可能です。
- 分類を実行する前に、不正アクセス ポイントは一時的に Pending としてマークされます。

表 *24*：分類マッピング

ルール ベースの分類タイプ	不正の状態
Custom	• Alert：管理ステーションへの通知以外の操作は実行されません。コントローラの管理ステーションは、コントローラと有線ネットワークを管理します。 • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。どの管理対象アクセスポイントも封じ込めに使用できない場合、不正は Contained Pending 状態になります。
[Delete]	不正アクセス ポイントを削除します。
Friendly	• Internal：不明なアクセス ポイントが WLAN のセキュリティに脅威を与えない場合は、手動で Friendly、Internal に設定できます。たとえば、ラボ ネットワーク内のアクセス ポイントがこれに該当します。 • External：ネットワーク内に存在する不明なアクセスポイントがWLANのセキュリティに脅威を与えない場合は、手動でFriendly、Externalに設定できます。たとえば、隣接するコーヒー ショップのアクセス ポイントがこれに該当します。 • Alert：管理ステーションへの通知以外の操作は実行されません。管理ステーションは、コントローラと有線ネットワークを管理します。

ルール ベースの分類タイプ	不正の状態
Malicious	• Alert：管理ステーションへの通知以外の操作は実行されません。管理ステーションは、コントローラと有線ネットワークを管理します。 • Threat：未知（管理対象外）のアクセス ポイントがネットワーク上に発見され、WLAN のセキュリティに脅威を与えています。 • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。どの管理対象アクセスポイントも封じ込めに使用できない場合、不正は Contained Pending 状態になります。
Unclassified	• Alert：管理ステーションへの通知以外の操作は実行されません。管理ステーションは、コントローラと有線ネットワークを管理します。 • Contained：未知（管理対象外）のアクセス ポイントが封じ込められています。どの管理対象アクセスポイントも封じ込めに使用できない場合、不正は Contained Pending 状態になります。

前述したように、ユーザ定義のルールに基づいて、未知のアクセスポイントの分類タイプと不正の状態をコントローラで自動的に変更できます。または、手動で未知のアクセスポイントを別の分類タイプや不正の状態に移行させることも可能です。

不正なアクセス ポイントの分類の制限

- カスタム タイプの不正の分類は、不正ルールに関連付けられています。このため、不正を手動で Custom として分類することはできません。カスタム クラスの変更は、不正ルールが使用されている場合にのみ行われます。
- 一部の SNMP トラップは、不正分類の変更に対して、ルールによって 30 分ごとに封じ込めのために送信されます。
- 不正ルールは、優先順位に従って、コントローラ内の新しい着信不正レポートごとに適用されます。
- 不正がのルールを満たし、分類されると、同じレポートの優先順位リスト内で下位に下がることはありません。
- 不正分類ルールは、管理対象アクセスポイントで受信するすべてのレポートで再評価されます。したがって、不正アクセスポイントは、別のルールが最後のレポートと一致している場合、1 つの状態から別の状態に移行することがあります。
- 不正 AP が Friendly に分類されるか、または無視された場合、その不正 AP に関連付けられている不正クライアントはすべて追跡されません。

不正なアクセス ポイントの分類方法

不正アクセス ポイントおよびクライアントの手動による分類（GUI）

手順

ステップ 1 [Monitoring] > [Wireless] > [Rogues] の順に選択します。
ステップ 2 [Unclassified] タブで AP を選択し、下部のペインに詳細を表示します。
ステップ 3 [Class Type] ドロップダウンを使用して、ステータスを設定します。
ステップ 4 [Apply] をクリックします。

不正アクセス ポイントおよびクライアントの手動による分類（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps rogue adhoc** { **alert** *mac-addr* | **auto-contain** | **contain** *mac-addr containment-level* | **internal** *mac-addr* | **external** *mac-addr*} 例： `Device(config)# wireless wps rogue adhoc alert 74a0.2f45.c520`	アドホック不正を検出して報告します。 **adhoc** キーワードの後に、次のいずれかのオプションを入力します。 • **alert**：アドホック不正アクセス ポイントをアラート モードに設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。 • **auto-contain**：アドホック不正の自動的な封じ込めを自動封じ込めモードに設定します。 • **contain**：アドホック不正アクセス ポイントの封じ込めを封じ込めモードに設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力し、

	コマンドまたはアクション	目的
		containment-level パラメータに封じ込めレベルを入力します。*containment-level* の有効な範囲は 1 ～ 4 です。 • **external**：アドホック不正アクセス ポイントを **external** に設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。 • **internal**：アドホック不正アクセス ポイントを **internal** に設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。
ステップ 3	**wireless wps rogue ap** { **friendly** *mac-addr* **state** [**external** | **internal**] | **malicious** *mac-addr* **state** [**alert** | **contain** *containment-level*]} 例： `Device(config)# wireless wps rogue ap malicious 74a0.2f45.c520 state contain 3`	不正アクセス ポイントを設定します。 **ap** キーワードの後に、次のいずれかのオプションを入力します。 • **friendly**：危険性のない不正アクセス ポイントを設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。その後、**state** キーワードに続けて **internal** または **external** のいずれかのオプションを入力します。**internal** オプションを選択した場合は、外部アクセス ポイントを信頼していることを示します。**external** オプションを選択した場合は、不正アクセス ポイントの存在を認識していることを示します。 • **malicious**：悪意のある不正アクセス ポイントを設定します。このオプションを選択した場合は、*mac-addr* パラメータに MAC アドレスを入力します。その後、**state** キーワードに続けて **alert** または **contain** のいずれかのオプションを入力します。

	コマンドまたはアクション	目的
		• **alert**：悪意のある不正アクセス ポイントを**アラート** モードに設定します。 • **contain**：悪意のある不正アクセス ポイントを**封じ込め**モードに設定します。このオプションを選択した場合は、*containment-level* パラメータに封じ込めレベルを入力します。有効な範囲は 1 ～ 4 です。
ステップ 4	**wireless wps rogue client** { **contain** *mac-addr containment-level*} 例： `Device(config)# wireless wps rogue client contain 74a0.2f45.c520 2`	不正クライアントを設定します。 **client** キーワードの後に次のオプションを入力します。 **contain**：不正クライアントを封じ込めます。このオプションを選択した後は、*mac-addr* パラメータに MAC アドレスを入力し、*containment-level* パラメータに封じ込めレベルを入力します。*containment-level* の有効な範囲は 1 ～ 4 です。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

不正分類ルールの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Wireless Protection Policies]** を選択します。

ステップ 2 [Wireless Protection Policies] ページで [Rogue AP Rules] タブを選択します。

ステップ 3 [Rogue AP Rules] ページで、**ルール**の名前をクリックするか、[Add] をクリックして新しいルールを作成します。

ステップ 4 表示される [Add/Edit Rogue AP Rule] ウィンドウで、[Rule Name] フィールドにルールの名前を入力します。

ステップ 5 次の [Rule Type] ドロップダウンリストのオプションからルール タイプを選択します。

- Friendly

- Malicious
- Unclassified
- Custom

不正分類ルールの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wps rogue rule** *rule-name* **priority** *priority* 例： `Device(config)# wireless wps rogue rule rule_3 priority 3`	ルールを作成またはイネーブルにします。ルールの作成時にルールのプライオリティを入力する必要があります。 （注） ルールの作成後に編集およびプライオリティの変更が可能なのは、無効になっている不正ルールのみです。有効になっている不正ルールのプライオリティは変更できません。編集時の不正ルールのプライオリティ変更は任意です。
ステップ 3	**classify** {**friendly** | **malicious**} 例： `Device(config)# wireless wps rogue rule rule_3 priority 3` `Device(config-rule)# classify friendly`	このルールに一致する不正アクセス ポイントに適用する必要がある分類を指定します。
ステップ 4	**condition** {**client-count** *value* | **duration** *duration_value* | **encryption** | **infrastructure** | **rssi** | **ssid** *ssid_name* | **wildcard-ssid**} 例： `Device(config)# wireless wps rogue rule rule_3 priority 3` `Device(config-rule)# condition client-count 5`	不正アクセス ポイントが満たす必要がある次の条件をルールに追加します。 • **client-count**：不正アクセス ポイントに最小数のクライアントがアソシエートされている必要があります。たとえば、不正アクセス ポイントに関連付けられているクライアントの数が設定値以上の場合、

	コマンドまたはアクション	目的
		アクセス ポイントは Malicious に分類されます。このオプションを選択する場合は、不正アクセスポイントに関連付けられるクライアントの最小数を *value* パラメータに入力します。有効な範囲は 1 ～ 10（両端の値を含む）で、デフォルト値は 0 です。 • **duration**：不正アクセス ポイントが最小期間で検出される必要があります。このオプションを選択する場合は、*duration_value* パラメータに最小検出期間の値を入力します。有効な範囲は 0 ～ 3600 秒（両端の値を含む）で、デフォルト値は 0 秒です。 • **encryption**：アドバタイズされた WLAN で暗号化が無効になっている必要があります。 • **infrastructure**：SSID がコントローラで認識される必要があります。 • **rssi**：最小 RSSI 値の不正アクセスポイントが検出される必要があります。分類が Friendly の場合、この条件では、最大 RSSI 値の不正アクセス ポイントが検出される必要があります。有効な範囲は -95 ～ -50 dBm（両端の値を含む）です。 • **ssid**：不正アクセスポイントには、特定の SSID が必要です。コントローラによって管理されていない SSID が必要です。このオプションを選択する場合は、*ssid_name* パラメータに SSID を入力します。SSID は事前に作成した設定済みの SSID リストに追加されます。 • **wildcard-ssid**：不正アクセス ポイントによってアドバタイズされた SSID の部分文字列（一部）が、指

	コマンドまたはアクション	目的
		定した入力値と一致する必要があります。
ステップ 5	**match** {**all** | **any**} 例： `Device(config)# wireless wps rogue rule rule_3 priority 3` `Device(config-rule)# match all`	検出された不正アクセス ポイントがルールに一致していると見なされ、そのルールの分類タイプが適用されるには、ルールで定義されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。
ステップ 6	**default** 例： `Device(config)# wireless wps rogue rule rule_3 priority 3` `Device(config-rule)# default`	コマンドをデフォルトに設定します。
ステップ 7	**exit** 例： `Device(config)# wireless wps rogue rule rule_3 priority 3` `Device(config-rule)# exit` `Device(config)#`	サブモードを終了します。
ステップ 8	**shutdown** 例： `Device(config)# wireless wps rogue rule rule_3 priority 3` `Device(config-rule)# shutdown`	特定の不正ルールを無効にします。この例では、ルール **rule_3** が無効になります。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 10	**configure terminal** 例： `Device# 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 11	**wireless wps rogue rule shutdown** 例： `Device(config)# wireless wps rogue rule shutdown`	すべての不正ルールを無効にします。

	コマンドまたはアクション	目的
ステップ 12	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

不正分類ルールのモニタリング

次のコマンドを使用して、不正分類ルールをモニタリングできます。

表 *25*：不正分類ルールのモニタリング用コマンド

コマンド	目的
show wireless wps rogue rule detailed	分類ルールの詳細情報を表示します。
show wireless wps rogue rule summary	分類ルールの概要を表示します。

例：不正なアクセス ポイントの分類

次に、不正アクセス ポイントを Friendly として分類および表示できるルールの作成例を示します。

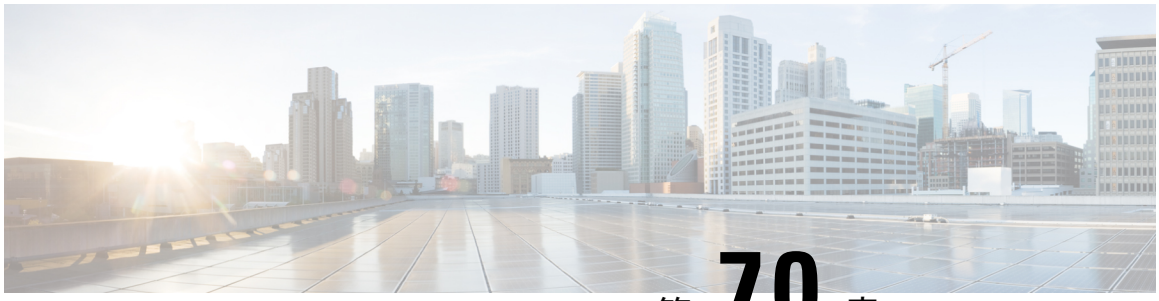
```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# classify friendly state internal
Device(config-rule)# end
```

この例は、不正アクセス ポイントが満たす必要がある条件を適用する方法を示しています。

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# condition client-count 5
Device(config-rule)# condition duration 1000
Device(config-rule)# end
```

次の例では、ルールを有効にする方法を示します。

```
Device# configure terminal
Device(config)# wireless wps rogue rule ap1 priority 1
Device(config-rule)# no shutdown
```



第 70 章

セキュア シェルの設定

セキュア シェルの設定について

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

SSH およびスイッチ アクセス

セキュア シェル（SSH）は、デバイスに対する安全なリモート接続を可能にするプロトコルです。SSH は、デバイスの認証時に強力な暗号化を行うことで、リモート接続について Telnet 以上のセキュリティを実現します。このソフトウェア リリースは、SSH バージョン 1（SSHv1）および SSH バージョン 2（SSHv2）をサポートしています。

IPv6 の SSH 機能は IPv4 における機能と同じです。IPv6 の場合、SSH は IPv6 アドレスをサポートし、IPv6 トランスポート上において、リモート IPv6 ノードとのセキュリティ保護および暗号化された接続を有効化します。

SSH サーバ、統合クライアント、およびサポートされているバージョン

セキュア シェル（SSH）統合クライアント機能は、SSH プロトコル上で動作し、デバイスの認証および暗号化を実現するアプリケーションです。SSH クライアントによって、シスコ デバイスは別のシスコ デバイスなど SSH サーバを実行するデバイスに対して、セキュアで暗号化

された接続を実行できます。この接続は、接続が暗号化される点を除いてTelnetのアウトバウンド接続と同様の機能を提供します。SSHクライアントは、認証および暗号化により、保護されていないネットワーク上でもセキュアな通信ができます。

SSHサーバおよびSSH統合クライアントは、スイッチ上で実行されるアプリケーションです。SSH サーバは、このリリースでサポートされている SSH クライアントおよび、他社製の SSH クライアントと使用します。SSHクライアントは、市販の一般的なSSHサーバと連動します。SSH クライアントは、Data Encryption Standard（DES）、3DES、およびパスワード認証の暗号をサポートします。

スイッチは、SSHv1 または SSHv2 サーバをサポートします。

スイッチは、SSHv1 クライアントをサポートしています。

（注） SSH クライアント機能を使用できるのは、SSH サーバがイネーブルの場合だけです。

ユーザ認証は、デバイスに対するTelnetセッションの認証と同様に実行されます。SSHは、次のユーザ認証方式もサポートします。

- TACACS+
- RADIUS
- ローカル認証および許可

SSH 設定時の注意事項

スイッチを SSH サーバまたは SSH クライアントとして設定する場合は、次の注意事項に従ってください。

- SSHv2 サーバは、SSHv1 サーバで生成される RSA キーのペアを使用できます（逆の場合も同様です）。
- スタック マスターで SSH サーバが実行されている場合で、スタック マスターに障害が発生した場合、新しいスタック マスターでは、前のスタック マスターによって生成された RSA キー ペアが使用されます。
- **crypto key generate rsa**グローバル コンフィギュレーション コマンドを入力した後、CLI エラー メッセージが表示される場合、RSA キーペアは生成されていません。ホスト名およびドメインを再設定してから、**crypto key generate rsa** コマンドを入力してください。
- RSA キーのペアを生成する場合に、メッセージ「No host name specified」が表示されることがあります。このメッセージが表示された場合は、**hostname** 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ホスト名を設定する必要があります。
- RSA キーのペアを生成する場合に、メッセージ「No domain specified」が表示されることがあります。このメッセージが表示された場合は、**ip domain-name** 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 IP ドメイン名を設定する必要があります。

- ローカル認証および許可の方法を設定する場合に、コンソール上で AAA がディセーブルにされていることを確認してください。

セキュア コピー プロトコルの概要

Secure Copy Protocol（SCP）機能は、スイッチの設定やイメージ ファイルのコピーにセキュアな認証方式を提供します。SCP にはセキュア シェル（SSH）が必要です（Berkeley の r-tool に代わるセキュリティの高いアプリケーションおよびプロトコルです）。

SSH を動作させるには、スイッチに RSA の公開キーと秘密キーのペアが必要です。これは SSH が必要な SCP も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。

また、SSH には AAA 認証が必要のため、適切に設定するには、SCP にも AAA 認証が必要になります。

- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。

（注） SCP を使用する場合、copy コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。

セキュア コピー プロトコル

セキュア コピー プロトコル（SCP）機能は、deviceの設定やスイッチ イメージ ファイルのコピーにセキュアな認証方式を提供します。SCP は一連の Berkeley の r-tools に基づいて設計されているため、その動作内容は、SCP が SSH のセキュリティに対応している点を除けば、Remote Copy Protocol（RCP）と類似しています。また、SCP では認証、許可、およびアカウンティング（AAA）の設定が必要なため、deviceはユーザが正しい権限レベルを保有しているかどうかを特定できます。セキュア コピー機能を設定するには、SCP の概念を理解する必要があります。

SFTP のサポート

SFTP クライアントのサポートは、Cisco IOS XE Gibraltar 16.10.1 リリース以降で導入されています。SFTP クライアントはデフォルトで有効になっており、個別の設定は必要ありません。

SFTP プロシージャは、**scp** および **tftp** コマンドの場合と同様に、**copy** コマンドを使用して呼び出すことができます。**sftp** コマンドを使用した一般的なファイル ダウンロード手順は、次のように実行できます。

copy sftp://*user* :*password* @*server-ip*/*file-name* **flash0://** *file-name*

copy コマンドの詳細については、次の URL を参照してください。
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/fund/copy.html

セキュア シェルを設定するための前提条件

セキュア シェル（SSH）用にスイッチを設定するための前提条件は、次のとおりです。

- SSH を動作させるには、スイッチに Rivest、Shamir、および Adleman（RSA）の公開キーと秘密キーのペアが必要です。これは SSH が必要なセキュア コピー プロトコル（SCP）も同様で、セキュアな転送を実現させるには、これらのキーのペアが必要です。
- SCP をイネーブルにする前に、スイッチの SSH、認証、許可、およびアカウンティングを適切に設定してください。
- SCP は SSH を使用してセキュアな転送を実行するため、ルータには RSA キーのペアが必要です。
- SCP はセキュリティについて SSH に依存します。
- SCP の設定には認証、許可、アカウンティング（AAA）の許可も必要なため、ルータはユーザが正しい権限レベルを保有しているか確認する必要があります。
- ユーザが SCP を使用するには適切な許可が必要です。
- 適切な許可を得ているユーザは、SCP を使用して Cisco IOS File System（IFS）のファイルをスイッチに（またはスイッチから）自由にコピーできます。コピーには **copy** コマンドを使用します。また、許可されている管理者もこの作業をワークステーションから実行できます。
- セキュア シェル（SSH）サーバは、IPsec（データ暗号規格（DES）または 3DES）の暗号化ソフトウェア イメージを必要とします。SSH クライアントは、IPsec（DES または 3DES）の暗号化ソフトウェア イメージが必要です。
- グローバル コンフィギュレーション モードで **hostname** および **ip domain-name** コマンドを使用して、デバイスのホスト名とホスト ドメインを設定します。

セキュア シェルの設定に関する制約事項

セキュア シェル用に device を設定するための制約事項は、次のとおりです。

- スイッチは、Rivest, Shamir, and Adelman（RSA）認証をサポートします。
- SSH は、実行シェル アプリケーションだけをサポートします。
- SSH サーバおよび SSH クライアントは、データ暗号規格（DES）（56 ビット）および 3DES（168 ビット）データ暗号化ソフトウェアでのみサポートされます。DES ソフトウェア イメージの場合、使用できる暗号化アルゴリズムは DES だけです。3DES ソフトウェア イメージの場合、DES と 3DES の両方の暗号化アルゴリズムを使用できます。

- device は、128 ビット キー、192 ビット キー、または 256 ビット キーの Advanced Encryption Standard（AES）暗号化アルゴリズムをサポートします。ただし、キーを暗号化する対称暗号化 AES はサポートされません。
- SCP を使用する場合、**copy** コマンドにパスワードを入力することはできません。プロンプトが表示されたときに、入力する必要があります。
- ログイン バナーはセキュア シェル バージョン 1 ではサポートされません。セキュア シェル バージョン 2 ではサポートされています。
- リバース SSH の代替手段をコンソール アクセス用に設定する場合、-l キーワード、userid :{number} {ip-address} デリミタ、および引数が必須です。
- FreeRADIUS over RADSEC でクライアントを認証するには、1024 ビットよりも長い RSA キーを生成する必要があります。その場合は、**crypto key generate rsa general-keys exportable label** *label-name* コマンドを使用します。

SSH の設定方法

SSH を実行するためのDeviceのセットアップ

SSH を実行するようにDeviceをセットアップするには、次の手順を実行します。

始める前に

ローカル アクセスまたはリモート アクセス用にユーザ認証を設定します。この手順は必須です。詳細については、次の関連項目を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**hostname** *hostname* 例：	Deviceのホスト名および IP ドメイン名を設定します。

	コマンドまたはアクション	目的
	`Device(config)# hostname your_hostname`	（注） この手順を実行するのは、Deviceを SSH サーバとして設定する場合だけです。
ステップ 4	**ip domain-name** *domain_name* 例： `Device(config)# ip domain-name your_domain`	Deviceのホストドメインを設定します。
ステップ 5	**crypto key generate rsa** 例： `Device(config)# crypto key generate rsa`	Device上でローカルおよびリモート認証用に SSH サーバを有効にし、RSA キーペアを生成します。Deviceの RSA キーペアを生成すると、SSH が自動的に有効になります。 最小モジュラス サイズは、1024 ビットにすることを推奨します。 RSA キーのペアを生成する場合に、モジュラスの長さの入力を求められます。モジュラスが長くなるほど安全ですが、生成と使用に時間がかかります。 （注） この手順を実行するのは、Deviceを SSH サーバとして設定する場合だけです。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# 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。

SSH サーバの設定

SSH サーバを設定するには、次の手順を実行します。

（注） Deviceを SSH サーバとして設定する場合にのみ、この手順が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ip ssh version** [**1** | **2**] 例： `Device(config)# ip ssh version 1`	（任意）SSH バージョン 1 または SSH バージョン 2 を実行するようにDeviceを設定します。 • **1**：SSH バージョン 1 を実行するようにDeviceを設定します。 • **2**：SSH バージョン 2 を実行するようにDeviceを設定します。 このコマンドを入力しない場合、またはキーワードを指定しない場合、SSH サーバは、SSH クライアントでサポートされている最新バージョンの SSH を選択します。たとえば、SSH クライアントが SSHv1 および SSHv2 をサポートする場合、SSH サーバは SSHv2 を選択します。
ステップ 4	**ip ssh window-size** 例： Device(config)# **ip ssh window-size**	SSH ウィンドウ サイズを指定します。推奨されるウィンドウ サイズは 32K 以下です。デフォルトのウィンドウ サイズは 8912 です。

	コマンドまたはアクション	目的
		32K を超える**ウィンドウサイズ**を選択すると、次の場合を除き、CPU に何らかの影響がある可能性があります。 • ネットワーク帯域幅が十分にある。 • クライアントがこのサイズに対応できる。 • ネットワークの遅延がない。 （注） この CLI は SCP 操作に対してのみ推奨され、コピーが完了したら無効にすることができます。
ステップ 5	**ip ssh** {**timeout** *seconds* | **authentication-retries** *number*} 例： `Device(config)# ip ssh timeout 90 authentication-retries 2`	SSH 制御パラメータを設定します。 • タイムアウト値は秒単位で指定します（デフォルト値は 120 秒）。指定できる範囲は 0 ～ 120 秒です。このパラメータは、SSH ネゴシエーション フェーズに適用されます。接続が確立されると、Device は CLI ベース セッションのデフォルトのタイムアウト値を使用します。 デフォルトでは、ネットワーク上の複数の CLI ベース セッション（セッション 0 ～ 4）に対して、最大 5 つの暗号化同時 SSH 接続を使用できます。実行シェルが起動すると、CLI ベース セッションのタイムアウト値はデフォルトの 10 分に戻ります。 • クライアントをサーバへ再認証できる回数を指定します。デフォルトは 3 です。指定できる範囲は 0 ～ 5 です。 両方のパラメータを設定する場合はこの手順を繰り返します。
ステップ 6	次のいずれかまたは両方を使用します。 • `line vty` *line_number*[*ending_line_number*]	（任意）仮想端末回線設定を設定します。

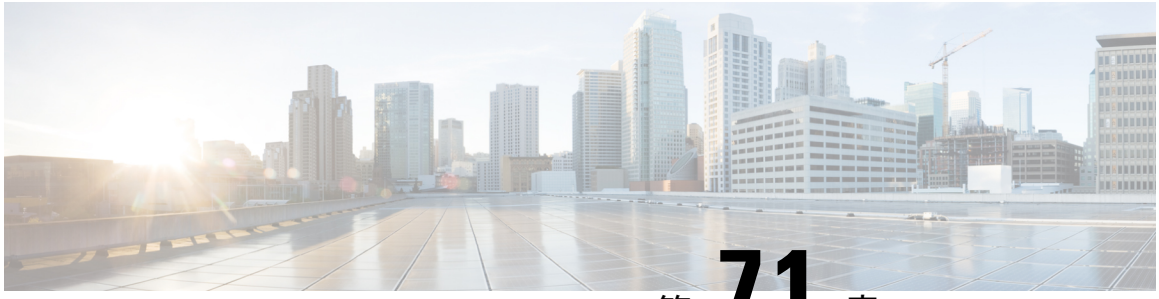
	コマンドまたはアクション	目的
	• **transport input ssh** 例： `Device(config)# line vty 1 10` または `Device(config-line)# transport input ssh`	• ライン コンフィギュレーション モードを開始して、仮想端末回線設定を設定します。*line_number* および *ending_line_number* には、回線のペアを指定します。指定できる範囲は 0 ～ 15 です。 • Deviceが非 SSH Telnet 接続を阻止するように指定します。これにより、ルータはSSH接続に限定されます。
ステップ 7	**end** 例： `Device(config-line)# end`	特権 EXEC モードに戻ります。
ステップ 8	**show running-config** 例： `Device# show running-config`	入力を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# 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。

SSH の設定およびステータスのモニタリング

次の表に、SSH サーバの設定およびステータスを示します。

表 *26 : SSH* サーバの設定およびステータスを表示するコマンド

コマンド	目的
show ip ssh	SSH サーバのバージョンおよび設定情報を表示します。
show ssh	SSH サーバのステータスを表示します。



第 71 章

秘密 PSK

秘密事前共有キーについて

Internet of Things（IoT）の出現により、インターネットに接続されるデバイスの数は著しく増加しています。これらのデバイスがすべて 802.1x サプリカントをサポートしているわけではないため、インターネットに接続するための代替メカニズムが必要です。セキュリティメカニズムの 1 つである WPA-PSK が代替手段として考えられます。現在の設定では、PSK は同じ WLAN に接続するすべてのクライアントで同じです。教育機関などの一部の設置環境では、これによりキーが不正ユーザに共有され、セキュリティ違反が生じます。このため、大規模な範囲でクライアントごとに一意の PSK をプロビジョニングすることが必要になります。

Identity PSK は、同じ SSID の個人またはユーザ グループのために作成される一意の PSK です。クライアントに複雑な設定は必要ありません。PSK と同じシンプルさで、IoT、BYOD（Bring Your Own Device）、およびゲスト展開に適しています。

Identity PSK は 802.1x 未対応のほとんどのデバイスでサポートされるため、より強力な IoT セキュリティを実現します。他に影響を与えずに 1 つのデバイスまたは個人に対するアクセスを簡単に取り消せます。何千ものキーを簡単に管理でき、AAA サーバを介して配布することができます。

IPSK ソリューション

クライアントの認証時に、AAA サーバはクライアントの MAC アドレスを認証し、Cisco-AV ペア リストの一部としてパスフレーズ（設定されている場合）を送信します。シスコ ワイヤレス コントローラ（WLC）は RADIUS 応答の一部としてこれを受信し、追加処理を行って PSK を計算します。

対応するアクセス ポイントによる SSID ブロードキャストに対してクライアントがアソシエーション要求を送信すると、ワイヤレス LAN コントローラはクライアントの特定の MAC アドレスを含む RADIUS 要求パケットを形成し、RADIUS サーバに中継します。

RADIUS サーバは認証を実行し、クライアントが許可されているかどうか、および WLC への応答として ACCESS-ACCEPT または ACCESS-REJECT のいずれかを送信するかどうかをチェックします。

Identity PSK をサポートするために、認証サーバは認証応答を送信するだけでなく、この特定のクライアントに AV ペア パスフレーズを提供します。これは、PMK の計算に使用されます。

RADIUS サーバは、ユーザ名、VLAN、Quality of Service（QoS）など、このクライアントに固有の追加パラメータも応答に含めることがあります。1 人のユーザが複数のデバイスを所有している場合は、すべてのデバイスで同じパスフレーズを使用できます。

WLAN での PSK の設定（CLI）

WLAN で PSK を設定するには、次の手順に従います。

始める前に

- WLAN で事前共有キー（PSK）のセキュリティを設定する必要があります。
- AAA サーバからのオーバーライドがない場合は、対応する WLAN 上の値が認証用と見なされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *wlan-name wlan-id ssid* 例： `Device(config)# wlan test-profile 4 abc`	WLAN と SSID を設定します。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	**security wpa akm psk** 例：	セキュリティ タイプ PSK を設定します。

	コマンドまたはアクション	目的
	`Device(config-wlan)# security wpa akm psk`	
ステップ 5	**security wpa akm psk set-key** *ascii/hex key* 例： `Device(config-wlan)# security wpa akm psk set-key asci 0`	PSK 認証キー管理（AKM）の共有キーを設定します。
ステップ 6	**security wpa akm psk** 例： `Device(config-wlan)# security wpa akm psk`	PSK サポートを設定します。
ステップ 7	**mac-filtering** *auth-list-name* 例： `Device(config-wlan)# mac-filtering test1`	WLAN で MAC フィルタリングを指定します。

WLAN での PSK の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 [Wireless Networks] ページで [Security] タブをクリックします。
ステップ 3 表示される [Layer 2] ウィンドウで、[WPA Parameters] セクションに移動します。
ステップ 4 [Auth Key Mgmt] ドロップダウンから [PSK] を選択します。
ステップ 5 [Save & Apply to Device] をクリックします。

WLAN へのポリシー プロファイルの適用（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。
ステップ 2 [Manage Tags] ページで、[Policy] タブをクリックします。
ステップ 3 [Add] をクリックして、[Add Policy Tag] ウィンドウを表示します。
ステップ 4 ポリシー タグの名前と説明を入力します。

ステップ 5 [Add] をクリックして、WLAN とポリシーをマッピングします。

ステップ 6 適切なポリシープロファイルを使用してマッピングするWLANプロファイルを選択し、チェック アイコンをクリックします。

ステップ 7 [Save & Apply to Device] をクリックします。

WLAN へのポリシー プロファイルの適用（CLI）

WLAN にポリシー プロファイルを適用するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-iot`	デフォルト ポリシー プロファイルを設定します。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA サーバまたは Cisco Identify Services Engine（ISE）サーバから受信したポリシーを適用するように AAA オーバーライドを設定します。

秘密 PSK の確認

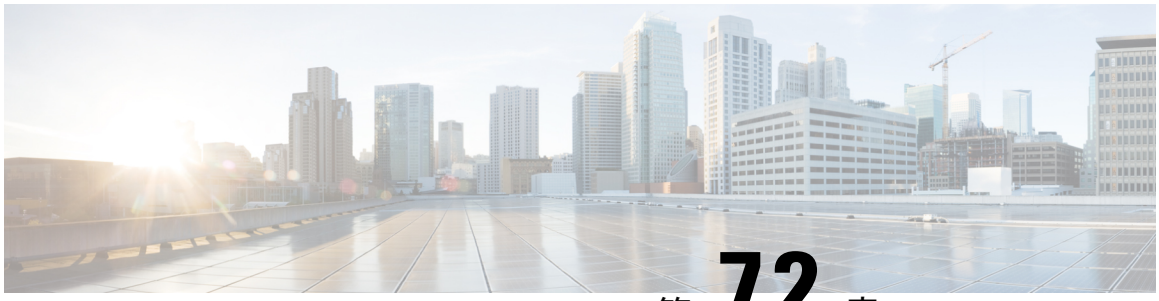
WLAN とクライアントの設定を確認するには、次の **show** コマンドを使用します。

```
Device# show wlan id 2


WLAN Profile Name     : test_ppsk
=================================================
Identifier                                       : 2
Network Name (SSID)                              : test_ppsk
Status                                           : Enabled
Broadcast SSID                                   : Enabled
Universal AP Admin                               : Disabled
Max Associated Clients per WLAN                  : 0
Max Associated Clients per AP per WLAN           : 0
Max Associated Clients per AP Radio per WLAN     : 0
Number of Active Clients                         : 0
Exclusionlist Timeout                            : 60
CHD per WLAN                                     : Enabled
```

```
Interface                                       : default
Multicast Interface                             : Unconfigured
WMM                                             : Allowed
WifiDirect                                      : Invalid
Channel Scan Defer Priority:
  Priority (default)                            : 4
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Diagnostics Channel Capability            : Disabled
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : test1
Accounting list name                            : Disabled
802.1x authentication list name                 : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2)           : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            TKIP Cipher                         : Disabled
            AES Cipher                          : Enabled
        Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Enabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            PMF dot1x                           : Disabled
            PMF PSK                             : Disabled
    CCKM TSF Tolerance                          : 1000
    FT Support                                  : Disabled
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
    PMF Support                                 : Disabled
        PMF Association Comeback Timeout        : 1
        PMF SA Query Time                       : 200
    Web Based Authentication                    : Disabled
    Conditional Web Redirect                    : Disabled
    Splash-Page Web Redirect                    : Disabled
    Webauth On-mac-filter Failure               : Disabled
    Webauth Authentication List Name            : Disabled
    Webauth Parameter Map                       : Disabled
    Tkip MIC Countermeasure Hold-down Timer     : 60
Call Snooping                                   : Disabled
Passive Client                                  : Disabled
Non Cisco WGB                                   : Disabled
Band Select                                     : Disabled
Load Balancing                                  : Disabled
Multicast Buffer                                : Disabled
Multicast Buffer Size                           : 0
IP Source Guard                                 : Disabled
Assisted-Roaming
    Neighbor List                               : Disabled
    Prediction List                             : Disabled
    Dual Band Support                           : Disabled
IEEE 802.11v parameters
```

```
    Directed Multicast Service                : Disabled
    BSS Max Idle                              : Disabled
        Protected Mode                        : Disabled
    Traffic Filtering Service                 : Disabled
    BSS Transition                            : Enabled
        Disassociation Imminent               : Disabled
            Optimised Roaming Timer           : 40
            Timer                             : 200
    WNM Sleep Mode                            : Disabled
802.11ac MU-MIMO                              : Disabled

Device# show wireless client mac-address a886.adb2.05f9 detail


Client MAC Address : a886.adb2.05f9
Client IPv4 Address : 9.9.58.246
Client Username : A8-86-AD-B2-05-F9
AP MAC Address : c025.5c55.e400
AP Name: saurabh-3600
AP slot : 1
Client State : Associated
Policy Profile : default-policy-profile
Flex Profile : default-flex-profile
Wireless LAN Id : 6
Wireless LAN Name: SSS_PPSK
BSSID : c025.5c55.e40f
Connected For : 280 seconds
Protocol : 802.11n - 5 GHz
Channel : 60
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 320 sec (Remaining time: 40 sec)
Input Policy Name  :
Input Policy State : None
Input Policy Source : None
Output Policy Name  :
Output Policy State : None
Output Policy Source : None
WMM Support : Enabled
U-APSD Support : Enabled
  U-APSD value : 0
  APSD ACs    : BK, BE, VI, VO
Fastlane Support : Disabled
Power Save : OFF
Current Rate : m22
Supported Rates : 9.0,18.0,36.0,48.0,54.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 09/27/2017 16:32:25 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 280 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : PSK
AAA override passphrase: Yes
Management Frame Protection : No
Protected Management Frame - 802.11w : No
```

```
EAP Type : Not Applicable
VLAN : 58
Access VLAN : 58
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_90000005
  IIF ID           : 0x90000005
  Device Type      : Apple-Device
  Protocol Map     : 0x000001
  Authorized       : TRUE
  Session timeout  : 320
  Common Session ID: 1F3809090000005DC30088EA
  Acct Session ID  : 0x00000000
  Auth Method Status List
        Method : MAB
                SM State         : TERMINATE
                Authen Status    : Success
  Local Policies:
        Service Template : wlan_svc_default-policy-profile (priority 254)
                Absolute-Timer   : 320
                VLAN             : 58
  Server Policies:
  Resultant Policies:
                VLAN             : 58
                Absolute-Timer   : 320
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Local
FlexConnect Dhcp Status : Local
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 59795
  Number of Bytes Sent : 21404
  Number of Packets Received : 518
  Number of Packets Sent : 274
  Number of EAP Id Request Msg Timeouts :
  Number of EAP Request Msg Timeouts :
  Number of EAP Key Msg Timeouts :
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : -32 dBm
  Signal to Noise Ratio : 58 dB
Fabric status : Disabled
```



第 72 章

マルチ事前共有キー

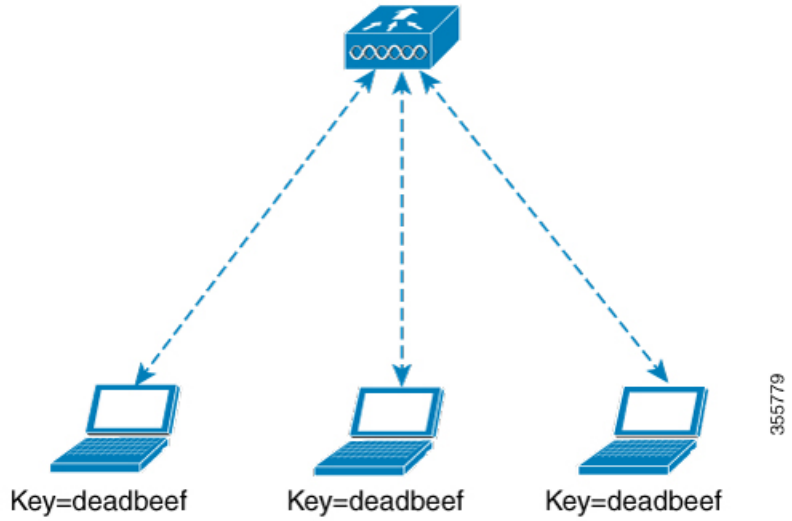
マルチ事前共有キーについて

マルチ PSK 機能は、1 つの SSID で同時に複数の PSK をサポートします。設定された PSK のいずれかを使用してネットワークに接続できます。これは Identity PSK（iPSK）とは異なり、同じ SSID 上の個人またはユーザ グループに対して一意の PSK が作成されます。

16.10 以降では、SSID ごとに 5 つの PSK がサポートされます（拡張可能）。

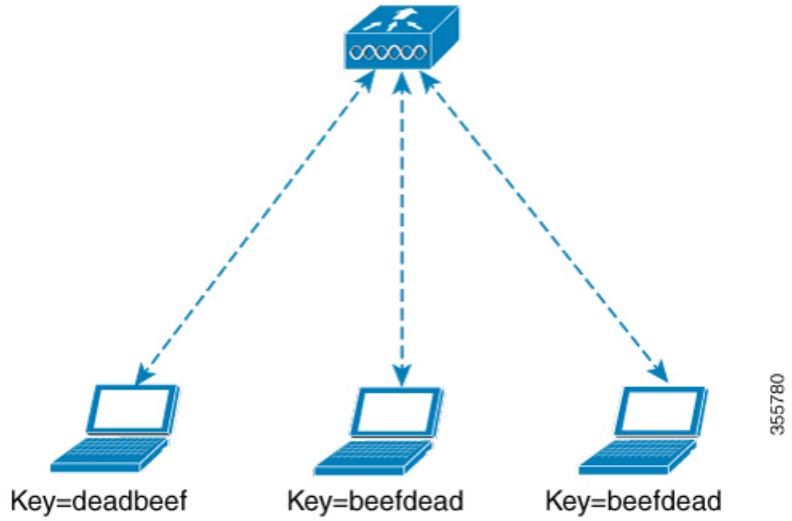
従来の PSK では、次の図に示すように、ネットワークに接続しているすべてのクライアントが同じパスワードを使用します。

図 *14* : 従来の *PSK*



ところがマルチ PSK を使用すると、クライアントは次の図に示すように設定済みの事前共有キーのいずれかを使用してネットワークに接続できます。

図 *15* : マルチ *PSK*



マルチ PSK では、同じ SSID に 2 つのパスワード（deadbeef と beefdead）が設定されます。このシナリオでは、クライアントはいずれかのパスワードを使用してネットワークに接続できます。

マルチ PSK の制約事項

- 中央認証は、ローカル、フレックス、およびファブリック モードでのみサポートされています。
- 中央認証フレックス モードの場合、スタンドアロン AP は、最もプライオリティの高い PSK（*priority 0* キー）を使用するクライアントの接続を許可します。最もプライオリティの高い PSK を使用しない新しいクライアントは、スタンドアロン モードでは拒否されます。
- マルチ PSK はローカル認証をサポートしません。

マルチ事前共有キーの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Wireless Networks] ページで WLAN の名前をクリックします。

ステップ 3 [Edit WLAN] ウィンドウで [Security] タブをクリックします。

ステップ 4 [Layer2] タブで、[Layer2 Security Mode] を次のオプションから選択します。

- [None]：レイヤ 2 セキュリティなし
- [802.1X]：WEP 802.1X データ暗号化タイプ
- [WPA + WPA2]：Wi-Fi Protected Access
- [Static WEP]：静的 WEP 暗号化パラメータ
- [Static WEP+802.1X]：静的 WEP と 802.1X の両方のパラメータ。

パラメータ	説明
802.1X	
WEP Key Size	キーサイズを選択します。使用可能な値は、[None]、[40 bits]、および [104 bits] です。
WPA + WPA2	
Protected Management Frame（保護された管理フレーム）	次のオプションから選択します。 • ディセーブル • 任意 • 必須

パラメータ	説明
WPA Policy	WPA ポリシーを有効にするには、このチェック ボックスをオンにします。
WPA Encryption	WPA 暗号化規格を選択します。WPA ポリシーを有効にしている場合は、WPA 暗号化規格を指定する必要があります。
WPA2 Policy	WPA2 ポリシーを有効にするには、このチェック ボックスをオンにします。
WPA2 Encryption	WPA2 暗号化規格を選択します。WPA ポリシーを有効にしている場合は、WPA 暗号化規格を指定する必要があります。
Auth Key Mgmt	次のオプションからキー再生成メカニズムを選択します。 • 802.1X • [FT + 802.1X] • [PSK]：PSK 形式と事前共有キーを指定する必要があります • [CCKM]：CCKM タイムスタンプの許容値を指定する必要があります • [802.1X + CCKM]：CCKM タイムスタンプの許容値を指定する必要があります • [FT + 802.1X + CCKM]：CCKM タイムスタンプの許容値を指定する必要があります
Static WEP	
[Key Size]	次のオプションからキーサイズを選択します。 • 40 ビット • 104 ビット
Key Index	1 ～ 4 の範囲でキー インデックスを選択します。各 WLAN に 1 つの一意な WEP キー インデックスを適用できます。WEP キーインデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化に設定できる WLAN は 4 つのみです。

パラメータ	説明
Key Format	暗号キーの形式として、ASCII または HEX のいずれかを選択します。
Encryption Key	長さが 13 文字の暗号キーを入力します。
Static WEP + 802.1X	
[Key Size]	次のオプションからキーサイズを選択します。 • 40 ビット • 104 ビット
Key Index	1 ～ 4 の範囲でキー インデックスを選択します。各 WLAN に 1 つの一意な WEP キー インデックスを適用できます。WEP キーインデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化に設定できる WLAN は 4 つのみです。
Key Format	暗号キーの形式として、ASCII または HEX のいずれかを選択します。
Encryption Key	長さが 13 文字の暗号キーを入力します。
WEP Key Size	次のオプションから選択します。 • なし • 40 ビット • 104 ビット

ステップ 5 [Save & Apply to Device] をクリックします。

マルチ事前共有キーの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *wlan-name wlan-id ssid* 例： `Device(config)# wlan mywlan 1 SSID_name`	WLAN と SSID を設定します。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	**security wpa akm psk** 例： `Device(config-wlan)# security wpa akm psk`	PSK を設定します。
ステップ 5	**security wpa wpa2 mpsk** 例： `Device(config-wlan)# security wpa wpa2 mpsk`	マルチ PSK を設定します。
ステップ 6	**priority** *priority_value* **set-key** {**ascii** [**0** | **8**] *pre-shared-key* | **hex** [**0** | **8**] *pre-shared-key*} 例： `Device(config-mpsk)# priority 0 set-key ascii 0 deadbeef`	PSK のプライオリティおよび関連するすべてのパスワードを設定します。 *priority_value* の範囲は 0 ～ 4 です。 （注） マルチ PSK には **priority 0** キーを設定する必要があります。
ステップ 7	**no shutdown** 例： `Device(config-mpsk)# no shutdown`	WLAN を有効にします。
ステップ 8	**exit** 例： `Device(config-wlan)# exit`	WLAN コンフィギュレーション モードを終了して、コンフィギュレーション モードに戻ります。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

マルチ PSK 設定の確認

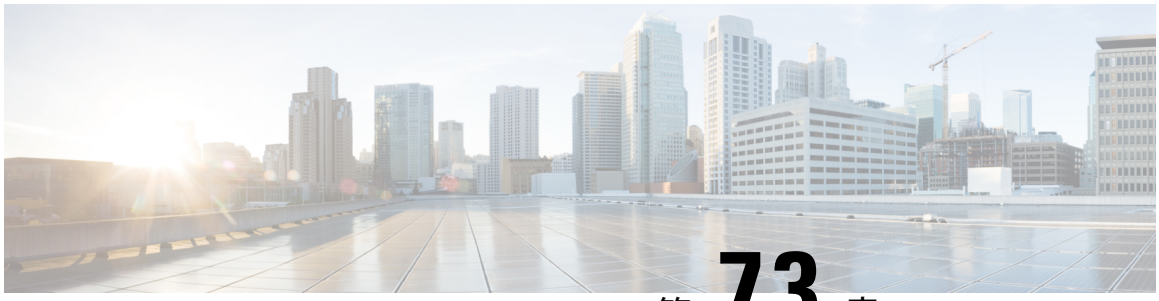
WLAN とクライアントの設定を確認するには、次のコマンドを使用します。

```
Device# show wlan id 8
WLAN Profile Name     : wlan_8
================================================
Identifier                                      : 8
Network Name (SSID)                             : ssid_8
Status                                          : Enabled
Broadcast SSID                                  : Enabled
Universal AP Admin                              : Disabled
Max Associated Clients per WLAN                 : 0
Max Associated Clients per AP per WLAN          : 0
Max Associated Clients per AP Radio per WLAN    : 200
Number of Active Clients                        : 0
CHD per WLAN                                    : Enabled
Multicast Interface                             : Unconfigured
WMM                                             : Allowed
WifiDirect                                      : Invalid
Channel Scan Defer Priority:
  Priority (default)                            : 5
  Priority (default)                            : 6
Scan Defer Time (msecs)                         : 100
Media Stream Multicast-direct                   : Disabled
CCX - AironetIe Support                         : Enabled
CCX - Diagnostics Channel Capability            : Disabled
Peer-to-Peer Blocking Action                    : Disabled
Radio Policy                                    : All
DTIM period for 802.11a radio                   : 1
DTIM period for 802.11b radio                   : 1
Local EAP Authentication                        : Disabled
Mac Filter Authorization list name              : Disabled
Mac Filter Override Authorization list name     : Disabled
Accounting list name                            :
802.1x authentication list name                 : Disabled
802.1x authorization list name                  : Disabled
Security
    802.11 Authentication                       : Open System
    Static WEP Keys                             : Disabled
    802.1X                                      : Disabled
    Wi-Fi Protected Access (WPA/WPA2/WPA3)      : Enabled
        WPA (SSN IE)                            : Disabled
        WPA2 (RSN IE)                           : Enabled
            MPSK                                : Enabled
            AES Cipher                          : Enabled
            CCMP256 Cipher                      : Disabled
            GCMP128 Cipher                      : Disabled
            GCMP256 Cipher                      : Disabled
        WPA3 (WPA3 IE)                          : Disabled
        Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Enabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            FT SAE                              : Disabled
            PMF dot1x                           : Disabled
            PMF PSK                             : Disabled
            SAE                                 : Disabled
            OWE                                 : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Disabled
    CCKM TSF Tolerance                          : 1000
    FT Support                                  : Adaptive
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
    PMF Support                                 : Disabled
```

```
        PMF Association Comeback Timeout       : 1
        PMF SA Query Time                      : 200
    Web Based Authentication                   : Disabled
    Conditional Web Redirect                   : Disabled
    Splash-Page Web Redirect                   : Disabled
    Webauth On-mac-filter Failure              : Disabled
    Webauth Authentication List Name           : Disabled
    Webauth Authorization List Name            : Disabled
    Webauth Parameter Map                      : Disabled
    Tkip MIC Countermeasure Hold-down Timer    : 60
Non Cisco WGB                                  : Disabled
Band Select                                    : Enabled
Load Balancing                                 : Disabled
Multicast Buffer                               : Disabled
Multicast Buffer Size                          : 0
IP Source Guard                                : Disabled
Assisted-Roaming
    Neighbor List                              : Disabled
    Prediction List                            : Disabled
    Dual Band Support                          : Disabled
IEEE 802.11v parameters
    Directed Multicast Service                 : Disabled
    BSS Max Idle                               : Disabled
        Protected Mode                         : Disabled
    Traffic Filtering Service                  : Disabled
    BSS Transition                             : Enabled
        Disassociation Imminent                : Disabled
            Optimised Roaming Timer            : 40
            Timer                              : 200
    WNM Sleep Mode                             : Disabled
802.11ac MU-MIMO                               : Disabled
802.11ax paramters
    OFDMA Downlink                             : unknown
    OFDMA Uplink                               : unknown
    MU-MIMO Downlink                           : unknown
    MU-MIMO Uplink                             : unknown
    BSS Color                                  : unknown
    Partial BSS Color                          : unknown
    BSS Color Code                             :
```

WLAN の詳細を表示するには、次のコマンドを使用します。

```
Device# show run wlan
wlan wlan_8 8 ssid_8
 security wpa psk set-key ascii 0 deadbeef
 no security wpa akm dot1x
 security wpa akm psk
 security wpa wpa2 mpsk
  priority 0 set-key ascii 0 deadbeef
  priority 1 set-key ascii 0 deaddead
  priority 2 set-key ascii 0 d123d123
  priority 3 set-key hex 0 023456789012345678901234567890123456789012345678901234567890123456789012345678901234

  priority 4 set-key hex 0 123456789012345678901234567890123456789012345678901234567890123456789012345678901234

 no shutdown
```



第 73 章

クライアントの複数認証

クライアントの複数認証について

複数認証機能は、クライアント接続でサポートされるレイヤ2およびレイヤ3セキュリティ タイプの拡張機能です。

（注） 特定の SSID に対して L2 認証と L3 認証の両方を有効にすることができます。

特定のクライアントに対する認証の組み合わせのサポートについて

複数認証機能は、WLANプロファイルで設定された特定のクライアントに対する複数の認証の組み合わせをサポートします。

次の表に、サポートされる認証の組み合わせの概要を示します。

レイヤ 2	レイヤ 3	サポートあり
MAB	CWA	はい
MAB	LWA	はい
MAB + PSK	-	対応
MAB + 802.1X	-	対応

MAB のエラー	LWA	はい
802.1X	CWA	はい
802.1X	LWA	はい
PSK	LWA	はい
PSK	CWA	はい
iPSK + MAB	CWA	はい

16.10.1 以降では、WLAN の 802.1X 設定で、WPA または WPA2 設定を使用した Web 認証設定がサポートされます。

この機能は、次の AP モードもサポートしています。

- Local
- FlexConnect
- ファブリック

クライアントの複数認証の設定

802.1X およびローカル Web 認証用の WLAN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name wlan-id SSID_Name* 例： `Device(config)# wlan wlan-test 3 ssid-test`	WLAN コンフィギュレーション サブモードを開始します。 • *profile-name*：設定する WLAN のプロファイル名です。 • *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID_Name*：最大 32 文字の英数字からなる SSID です。

	コマンドまたはアクション	目的
		（注） すでにこのコマンドを設定している場合は、**wlan** *profile-name* コマンドを入力します。
ステップ 3	**security dot1x authentication-list** *auth-list-name* 例： `Device(config-wlan)# security dot1x authentication-list default`	dot1x セキュリティ用のセキュリティ認証リストを有効にします。 この設定は、すべての dot1x セキュリティ WLAN で類似しています。
ステップ 4	**security web-auth authentication-list** *authenticate-list-name* 例： `Device(config-wlan)# security web-auth authentication-list default`	dot1x セキュリティ用の認証リストを有効にします。
ステップ 5	**security web-auth parameter-map** *parameter-map-name* 例： `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	パラメータ マップをマッピングします。 （注） パラメータ マップが WLAN に関連付けられていない場合は、グローバル パラメータ マップの設定と見なされます。
ステップ 6	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

事前共有キー（PSK）およびローカル Web 認証用の WLAN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name wlan-id SSID_Name* 例： `Device(config)# wlan wlan-test 3 ssid-test`	WLAN コンフィギュレーション サブモードを開始します。 • *profile-name*：設定する WLAN のプロファイル名です。

	コマンドまたはアクション	目的
		• *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID_Name*：最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *profile-name* コマンドを入力します。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	**security wpa akm psk set-key** *ascii/hex key* 例： `Device(config-wlan)# security wpa akm psk set-key asci 0`	PSK AKM の共有キーを設定します。
ステップ 5	**security web-auth authentication-list** *authenticate-list-name* 例： `Device(config-wlan)# security web-auth authentication-list default`	WLAN の認証リストを有効にします。
ステップ 6	**security web-auth parameter-map** *parameter-map-name* 例： `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	パラメータ マップをマッピングします。 （注） パラメータ マップが WLAN に関連付けられていない場合は、グローバル パラメータ マップの設定と見なされます。

PSK または iPSK（ID 事前共有キー）および中央 Web 認証用の WLAN の設定

WLAN の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name wlan-id SSID_Name* 例： `Device(config)# wlan wlan-test 3 ssid-test`	WLAN コンフィギュレーション サブモードを開始します。 • *profile-name*：設定する WLAN のプロファイル名です。 • *wlan-id*：ワイヤレス LAN の ID です。範囲は 1 ～ 512 です。 • *SSID_Name*：最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *profile-name* コマンドを入力します。
ステップ 3	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 4	**security wpa akm psk set-key** *ascii/hex key* 例： `Device(config-wlan)# security wpa akm psk set-key asci 0`	PSK AKM の共有キーを設定します。
ステップ 5	**mac-filtering** *list-name* 例： `Device(config-wlan)# mac-filtering ewlc-radius`	MAC フィルタリング パラメータを設定します。

WLAN へのポリシー プロファイルの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-profile-name* 例： `Device(config)# wireless profile policy policy-iot`	デフォルト ポリシー プロファイルを設定します。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa override`	AAA サーバまたは ISE サーバから受信したポリシーを適用するように AAA オーバーライドを設定します。
ステップ 4	**nac** 例： `Device(config-wireless-policy)# nac`	ポリシープロファイルに NAC を設定します。
ステップ 5	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	WLAN を停止します。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

複数の認証設定の確認

レイヤ 2 認証

L2 認証（Dot1x）が完了すると、クライアントは Webauth Pending 状態に移行します。

L2 認証後のクライアントの状態を確認するには、次のコマンドを使用します。

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
-------------------------------------------------------------------------------------------------
```

```
58ef.68b6.aa60 ewlc1_ap_1   3  Webauth Pending    11n(5)        Dot1x  Local
Number of Excluded Clients: 0
```

```
Device# show wireless client mac-address <mac_address> detail
Auth Method Status List

   Method : Dot1x

    Webauth State    : Init

    Webauth Method   : Webauth

  Local Policies:

   Service Template : IP-Adm-V6-Int-ACL-global (priority 100)

    URL Redirect ACL : IP-Adm-V6-Int-ACL-global

   Service Template : IP-Adm-V4-Int-ACL-global (priority 100)

    URL Redirect ACL : IP-Adm-V4-Int-ACL-global

   Service Template : wlan_svc_default-policy-profile_local (priority 254)

    Absolute-Timer   : 1800

    VLAN             : 50
```

```
Device# show platform software wireless-client chassis active R0
        ID  MAC Address      WLAN  Client     State
------------------------------------------------------------------------------------------

  0xa0000003      58ef.68b6.aa60    3             L3          Authentication
```

```
Device# show platform software wireless-client chassis active F0
    ID     MAC Address   WLAN  Client     State  AOM ID    Status
------------------------------------------------------------------------------------------
0xa0000003    58ef.68b6.aa60    3           L3          Authentication.         730.
   Done
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary
Client Type Abbreviations:
RG - REGULAR   BLE - BLE
 HL - HALO    LI - LWFL INT
 Auth State Abbrevations:
 UK - UNKNOWN    IP - LEARN    IP IV - INVALID
 L3 - L3 AUTH RN - RUN
 Mobility State Abbreviations:
 UK - UNKNOWN       IN - INIT
 LC - LOCAL               AN - ANCHOR
 FR - FOREIGN          MT - MTE
 IV - INVALID
 EoGRE Abbreviations:
 N - NON EOGRE Y - EOGRE

CPP IF_H   DP IDX       MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
------------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
summary
Vlan   DP IDX         MAC Address      VLAN   CT   MCVL AS MS E   WLAN      POA
------------------------------------------------------------------------------------
0X49   0xa0000003    58ef.68b6.aa60     50    RG     0  L3 LC N wlan-test 0x90000003
```

レイヤ 3 認証

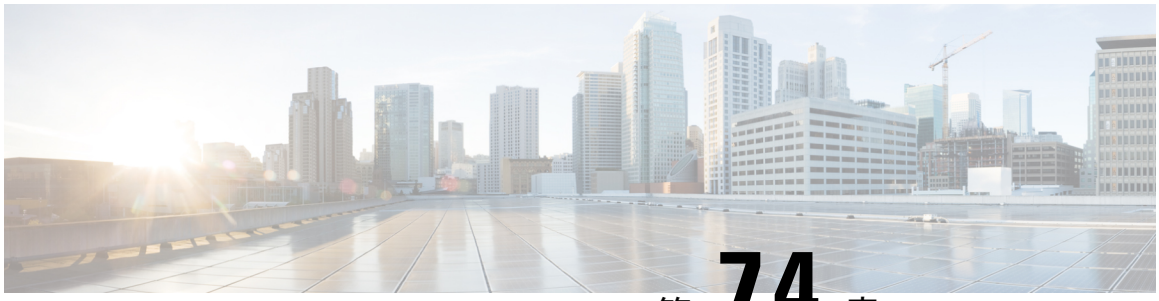
L3 認証が成功すると、クライアントは Run 状態に移行します。

L3 認証後のクライアントの状態を確認するには、次のコマンドを使用します。

```
Device# show wireless client summary
Number of Local Clients: 1
MAC Address  AP Name  WLAN  State  Protocol  Method  Role
---------------------------------------------------------------------------------------------------------

58ef.68b6.aa60   ewlc1_ap_1  3     Run    11n(5)   Web Auth      Local
Number of Excluded Clients: 0

Device# show wireless client mac-address 58ef.68b6.aa60 detail
Auth Method Status List

    Method : Web Auth

     Webauth State    : Authz

     Webauth Method   : Webauth

   Local Policies:

    Service Template : wlan_svc_default-policy-profile_local (priority 254)

     Absolute-Timer   : 1800

     VLAN             : 50

   Server Policies:

  Resultant Policies:

     VLAN             : 50

     Absolute-Timer   : 1800

Device# show platform software wireless-client chassis active R0
ID          MAC Address     WLAN    Client State
-----------------------------------------------
0xa0000001 58ef.68b6.aa60    3          Run

Device# show platform software wireless-client chassis active f0
    ID       MAC Address    WLAN    Client State   AOM ID.  Status
-------------------------------------------------------------------
0xa0000001 58ef.68b6.aa60.   3          Run         11633    Done

Device# show platform hardware chassis active qfp feature wireless wlclient cpp-client
summary
Client Type Abbreviations:
RG - REGULAR   BLE - BLE
 HL - HALO    LI - LWFL INT
 Auth State Abbrevations:
 UK - UNKNOWN    IP - LEARN    IP IV - INVALID
 L3 - L3 AUTH RN - RUN
 Mobility State Abbreviations:
 UK - UNKNOWN       IN - INIT
 LC - LOCAL                AN - ANCHOR
 FR - FOREIGN          MT - MTE
 IV - INVALID
 EoGRE Abbreviations:
 N - NON EOGRE Y - EOGRE
```

```
CPP IF_H   DP IDX       MAC Address   VLAN  CT  MCVL AS MS E   WLAN     POA
------------------------------------------------------------------------------
0X49     0XA0000003    58ef.68b6.aa60  50   RG   0   RN LC N wlan-test 0x90000003
```

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
summary
Vlan   pal_if_hd1        mac           Input Uidb     Output Uidb
-----------------------------------------------------------------
50     0xa0000003    58ef.68b6.aa60     95929            95927
```



第 74 章

Cisco TrustSec の設定

Cisco TrustSec の概要

Cisco TrustSec は、ネットワーク内のユーザ、ホスト、およびネットワーク デバイスを強力に識別する機能に基づいた、シスコ ネットワーク デバイスのセキュリティを改善します。TrustSec は、特定の役割についてデータ トラフィックを一意に分類することで、トポロジに依存しない、スケーラブルなアクセス コントロールを実現します。TrustSec は、認証されたピアおよびこれらのピアとの暗号化リンク間で信頼を確立することで、データの機密保持および整合性を保証します。

Cisco TrustSec の主要コンポーネントは、Cisco Identity Services Engine（ISE）です。スイッチ上で手動で設定することもできますが、Cisco ISE は TrustSec ID およびセキュリティ グループ ACL（SGACL）でスイッチをプロビジョニングできます。

（注） CTS サーバを新しいサーバに変更する前に、**clear cts environment-data** コマンドを使用して CTS 環境データを手動でクリアする必要があります。これにより、**show cts environment-data** コマンドの実行時に、更新されたデータを取得できるようになります。

MTU の注意事項

1518 バイトを超える CTS タグ付きパケットは、Cisco vWLC コントローラでドロップされることがあります。これは、vWLC インスタンスをホストしている UCS サーバで着信パケットのサイズが制限されているためです。UCS サーバのデフォルト MTU は 1500 であるため、1518 バイトのパケットのみが許可されます。この超過分の 18 バイトには、802.1Q の 4 バイトとイーサネット ヘッダーの 14 バイトが含まれています。

CTS タグ用に設定されたイーサネット リンクにより、Cisco メタデータと呼ばれる 8 バイトのカプセル化が課されます。その結果、イーサネットパケットの合計サイズは、8 バイト増えて 1526 バイト（1518 + 8 = 1526）になります。したがって、イーサネットの追加の 8 バイトに対応するために、受信インターフェイスの MTU を 8 バイト増やす必要があります。

ルータおよびスイッチ（たとえば、Cisco ASR 1000 シリーズ ルータ、Cisco 4000 シリーズ サービス統合型ルータ、Cisco Catalyst 3000 シリーズ スイッチ、Cisco Catalyst 9000 シリーズ スイッチ）上の CTS インターフェイスは、MTU を 1508 バイトに自動調整して追加の 8 バイトに対応します。ただし、UCS サーバなどの他のデバイスでは、MTU を 1508 に増やすために手動更新が必要です。UCS でジャンボ MTU を設定する方法については、次のリンクを参照してください。

https://www.cisco.com/c/en/us/support/docs/servers-unified-computing/ucs-b-series-blade-servers/117601-configure-UCS-00.html

Cisco TrustSec の機能

次の表に、TrustSec がイネーブルになった Cisco スイッチで実装される TrustSec 機能を示します。継続的な TrustSec の General Availability リリースによって、サポートされるスイッチの数および各スイッチでサポートされる TrustSec 機能の数は増加しています。

Cisco TrustSec の機能	説明
802.1AE タギング（MACSec）	IEEE 802.1AE に基づくワイヤレート ホップ単位レイヤ 2 暗号化のプロトコル。 MACSec 対応デバイス間において、パケットは送信デバイスからの出力で暗号化され、受信デバイスへの入力で復号化されます。デバイス内では平文です。 この機能は、TrustSec ハードウェア対応デバイス間だけで利用できます。 （注） この機能は、Catalyst 3850 および Catalyst 3650 スイッチではサポートされていません。

Cisco TrustSec の機能	説明
エンドポイントアドミッションコントロール（EAC）	EAC は、TrustSec ドメインに接続しているエンドポイント ユーザまたはデバイスの認証プロセスです。通常、EAC はアクセス レベル スイッチで実行されます。EAC プロセスの認証および許可に成功すると、ユーザまたはデバイスに対してセキュリティ グループ タグが割り当てられます。現在、EAC は 802.1X、MAC 認証バイパス（MAB）、および Web 認証プロキシ（WebAuth）とすることができます。
ネットワーク デバイス アドミッション コントロール（NDAC）	NDAC は、TrustSec ドメイン内の各ネットワーク デバイスがピア デバイスのクレデンシャルおよび信頼性を確認できる認証プロセスです。NDAC は、IEEE 802.1X ポート ベースの認証に基づく認証フレームワークを利用し、EAP 方式として EAP-FAST を使用します。NDAC プロセスの認証および許可に成功すると、IEEE 802.1AE暗号化のセキュリティ アソシエーション プロトコル ネゴシエーションとなります。
セキュリティ グループ アクセス コントロール リスト（SGACL）	セキュリティ グループ アクセス コントロール リスト（SGACL）は、セキュリティ グループ タグをポリシーと関連付けます。ポリシーは、TrustSec ドメインから出力される SGT タグ付きトラフィックに対して適用されます。
Cisco TrustSec SGACL のハイ アベイラビリティ	Cisco TrustSec セキュリティ グループ アクセス コントロール リスト（SGACL）は、Cisco StackWise 技術をサポートしているスイッチでのハイ アベイラビリティ機能をサポートしています。Cisco StackWise 技術によってステートフルな冗長性が提供され、スイッチ スタックはアクセス制御エントリを強制し、処理できます。 この機能を有効にする Cisco TrustSec 固有の設定はありません。

Cisco TrustSec の機能	説明
セキュリティ アソシエーション プロトコル（SAP）	NDAC 認証のあと、セキュリティ アソシエーション プロトコル（SAP）は、その後の TrustSec ピア間の MACSec リンク暗号化のキーおよび暗号スイートについて、自動的にネゴシエーションを行います。SAP は IEEE 802.11i で定義されます。 （注） この機能は、Catalyst 3850 および Catalyst 3650 スイッチではサポートされていません。
セキュリティ グループ タグ（SGT）	SGT は、TrustSec ドメイン内の送信元のセキュリティ分類を示す 16 ビットの単一ラベルです。イーサネット フレームまたは IP パケットに追加されます。
SGT Exchange Protocol（SXP）	Security Group Tag Exchange Protocol（SXP）。SXP を使用すると、TrustSec にハードウェアで対応していないデバイスが Cisco Identity Services Engine（ISE）または Cisco Secure アクセス コントロール システム（ACS）から認証されたユーザとデバイスの SGT 属性を受信できます。デバイスは、次にセキュリティ グループ アクセス コントロール リスト（SGACL）強制のために、送信元トラフィックをタグ付けする TrustSec にハードウェアで対応しているデバイスに、sourceIP-to-SGT バインディングを転送できます。

リンクの両端で 802.1AE MACsec をサポートしている場合、SAP ネゴシエーションが実行されます。サプリカントとオーセンティケータの間で EAPOL-Key が交換され、暗号スイートのネゴシエーション、セキュリティ パラメータの交換、およびキーの管理が実行されます。これらの作業が正常に完了すると、セキュリティ アソシエーション（SA）が確立します。

ソフトウェア バージョンとライセンスおよびリンク ハードウェア サポートに応じて、SAP ネゴシエーションは次の動作モードの 1 つを使用できます。

- Galois Counter Mode（GCM）：認証と暗号化
- GCM authentication（GMAC）：GCM 認証、暗号化なし
- No Encapsulation：カプセル化なし（クリア テキスト）
- null：カプセル化、認証または暗号化なし

セキュリティ グループ アクセス コントロール リスト

セキュリティ グループは、アクセス コントロール ポリシーを共有するユーザ、エンドポイント デバイス、およびリソースのグループです。セキュリティ グループは、管理者が Cisco Identity Services Engine（ISE）で定義します。新しいユーザやデバイスが Cisco TrustSec ドメインに追加されると、認証サーバは、それらの新しいエンティティを適切なセキュリティ グループに割り当てます。Cisco TrustSec は各セキュリティ グループに一意の 16 ビットの番号を割り当てます。番号の範囲は Cisco TrustSec ドメイン内でグローバルです。ワイヤレス デバイス内のセキュリティ グループの数は、認証されたネットワーク エンティティの数までに限定されます。セキュリティ グループの番号を手動で設定する必要はありません。

デバイスが認証されると、Cisco TrustSec はそのデバイスから発信されるすべてのパケットに、デバイスのセキュリティ グループ番号を含む SGT をタグ付けします。パケットは、Cisco TrustSec ヘッダーにこの SGT を含めて、ネットワーク内のあるゆる場所に運びます。

SGT には送信元のセキュリティ グループが含まれているため、タグは送信元 SGT（S-SGT）と呼ばれることがあります。接続先デバイスもセキュリティ グループ（宛先 SG）に割り当てられます。このグループは、 Cisco TrustSec パケットに接続先デバイスのセキュリティ グループ番号が含まれていない場合でも、宛先 SGT（D-SGT）として参照できます。

セキュリティ グループ アクセス コントロール リスト（SGACL）を使用すると、ユーザと宛先リソースのセキュリティ グループの割り当てに基づいて、ユーザが実行できる操作を制御できます。Cisco TrustSec ドメインでのポリシーの適用は、軸の 1 つが送信元セキュリティ グループ番号でもう 1 つが宛先セキュリティ グループ番号の権限マトリックスで表されます。マトリックス本体の各セルには、送信元セキュリティ グループから宛先セキュリティ グループに送信されるパケットに適用される必要がある権限を指定した SGACL の順序付きリストが含まれています。ワイヤレス クライアントが認証されると、マトリックス セルにすべての SGACL がダウンロードされます。

ワイヤレス クライアントは、ネットワークに接続するときにすべての ACL をコントローラにプッシュします。

Cisco TrustSec は、ネットワーク内のユーザとデバイスをセキュリティ グループに割り当て、セキュリティ グループ間でアクセス コントロールを適用することにより、ネットワーク内でロールベースのトポロジに依存しないアクセス コントロールを実現します。SGACL は、デバイス ID に基づいてアクセス コントロール ポリシーを定義します。ロールと権限が同じであれば、ネットワーク トポロジが変更されてもセキュリティ ポリシーは変更されません。ユーザがワイヤレス グループに追加されたら、適切なセキュリティ グループにユーザを割り当てるだけで、そのユーザはただちにそのグループの権限を受け取ります。

ロールベースの権限を使用することで、ACL のサイズが縮小され、ACL のメンテナンスが簡易化されています。Cisco TrustSec では、設定されるアクセス コントロール エントリ（ACE）の数は、指定されている権限の数によって決まるため、ACE の数がかなり少なくなります。

SGACL をサポートする AP のリストは次のとおりです。

- Cisco Aironet 1700 シリーズ アクセス ポイント
- Cisco Aironet 1800 シリーズ アクセス ポイント

- Cisco Aironet 2700 シリーズ アクセス ポイント
- Cisco Aironet 2800 シリーズ アクセス ポイント
- Cisco Aironet 3700 シリーズ アクセス ポイント
- Cisco Aironet 4800 シリーズ アクセス ポイント

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ上の SGACL でサポートされているシナリオは次のとおりです。

- ワイヤレスからワイヤレス（エンタープライズ ネットワーク内）：
  - ローカル スイッチングを使用したフレックス モード：送信元ワイヤレス ネットワークから宛先ワイヤレス ネットワークにパケットが送信されたときに、出力 AP で SGACL の適用が行われます。
  - 中央スイッチングを使用したフレックス モード：SGACL の適用は出力 AP で実行されます。これを実行するために、コントローラはSGT交換プロトコル（SXP）を介してセキュリティ グループ タグ（IP-SGT）バインディングに IP アドレスをエクスポートする必要があります。
- 有線からワイヤレス（DC から エンタープライズ ネットワーク）：パケットが宛先 AP に到達すると、適用が行われます。
- ワイヤレスから有線（エンタープライズ ネットワークから DC）：パケットが有線ネットワークの入力に到達すると、アップリンク スイッチで適用が行われます。

注意事項および制約事項

- SGACL の適用は、ローカル モードのコントローラで実行されます。
- SGACL の適用は、ローカル スイッチングを実行しているフレックス モード AP で実行されます。
- ブランチから DC のシナリオでは、ワイヤレス クライアントの SGACL の適用が、上流に位置するスイッチまたはボーダー ゲートウェイのいずれかで実行されます。
- SGACL の適用は、非 IP または IP ブロードキャスト トラフィック、マルチキャスト トラフィックではサポートされません。
- WLAN ごとの SGT 割り当てはサポートされていません。
- SGACL の適用は、AP とワイヤレス コントローラの間（アップストリームまたはアップストリーム トラフィックから）のコントロールプレーン トラフィックに対しては実行されません。
- 非スタティック SGACL 設定は、ISE から受信したダイナミック SGACL ポリシーでのみサポートされます。
- AP でのスタティック SGACL 設定はサポートされていません。

インライン タギング

インライン タギングは、コントローラまたは AP が送信元 SGT を認識するために使用するトランスポート メカニズムです。

トランスポート メカニズムには次の 2 つのタイプがあります。

- 中央スイッチング：中央でスイッチングされるパケットの場合、コントローラは Cisco メタデータ（CMD）タグを付けることによって、コントローラと関連付けられているワイヤレス クライアントから送信されるすべてのパケットのインライン タギングを実行します。分散システムから着信するパケットの場合、インライン タギングでは、S-SGT タグを学習するために、コントローラによってパケットからの CMD ヘッダーの取り外しも行われます。その後、コントローラは SGACL を適用するために S-SGT を含むパケットを転送します。
- ローカル スイッチング：ローカルでスイッチングされたトラフィックを送信するために、AP はクライアントから送信された、自身と関連付けられているパケットのインライン タギングを実行します。トラフィックを受信するために、AP はローカルでスイッチングされたパケットと中央でスイッチングされたパケットの両方を処理し、パケットの S-SGT タグを使用して、SGACL ポリシーを適用します。

コントローラでワイヤレス Cisco TrustSec が有効になっている場合、スイッチとタグ交換するように SXP を有効化して設定することもできます。ワイヤレス Cisco TrustSec モードと SXP モードの両方がサポートされていますが、ワイヤレス Cisco TrustSec（AP 上）と SXP の両方を同時に有効な状態にする使用例はありません。

ポリシーの実施

Cisco TrustSec アクセス コントロールは、入力タギングと出力の適用を使用して実装されます。Cisco TrustSec ドメインの入力点では、送信元からのトラフィックは、送信元エンティティのセキュリティ グループ番号を含む SGT でタグ付けされます。SGT は、そのトラフィックでドメイン全体に伝達されます。Cisco TrustSec ドメインの出力ポイントでは、出力デバイスは送信元 SGT（S-SGT）および宛先エンティティ（D-SGT）のセキュリティ グループを使用して、SGACL ポリシー マトリックスから適用するアクセス ポリシーを決定します。

ポリシーの適用は、AP の中央およびローカルの両方でスイッチド トラフィックに適用できます。有線クライアントがワイヤレス クライアントと通信する場合、AP はダウンストリーム トラフィックを適用します。ワイヤレス クライアントが有線クライアントと通信する場合、AP はアップストリーム トラフィックを適用します。AP はこの方法により、ダウンストリーム トラフィックとワイヤレス間トラフィックの両方でトラフィックを適用します。適用が機能するためには、S-SGT、D-SGT、および ACL が必要です。AP は、Cisco ISE サーバで利用可能な情報からすべてのワイヤレス クライアントの SGT 情報を取得します。

（注） トラフィックを適用するためには、Cisco AP はリスナー モードまたはリスナーとスピーカーの両方のモードである必要があります。これは、リスナー モードで IP-SGT バインディングの完全なセットが保持されるためです。AP で適用を有効にすると、対応するポリシーがダウンロードされて AP にプッシュされます。

AP での SGACL の有効化

（注） 設定を無効にするには、以下のコマンドの **no** 形式を使用します。たとえば、**cts role-based enforcement** は AP のロールベース アクセス コントロールの適用を無効にします。

始める前に

- AP 上のセキュリティ グループ アクセス コントロール リスト（SGACL）は、ワイヤレス コントローラが FlexConnect モードの場合にのみ有効化できます。
- タグ付きパケットを送信または受信するように、アップリンク ポートで **cts manual** コマンドを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex xyz-flex-profile`	RFプロファイルを設定し、RFプロファイル コンフィギュレーション モードを開始します。
ステップ 3	**cts role-based enforcement** 例： `Device(config-wireless-flex-profile)# cts role-based enforcement`	AP のロールベース アクセス コントロールの適用を有効にします。
ステップ 4	**cts inline-tagging** 例： `Device(config-wireless-flex-profile)# cts inline-tagging`	AP でインライン タギングを有効にします。

	コマンドまたはアクション	目的
ステップ 5	**cts profile** *profile-name* 例： `Device(config-wireless-flex-profile)# cts profile xyz-profile`	CTS プロファイル名を有効にします。
ステップ 6	**exit** 例： `Device(config-wireless-flex-profile)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site xyz-site`	サイト タグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 8	**flex-profile** *flex-profile-name* 例： `Device(config-site-tag)# flex-profile xyz-flex-profile`	flex プロファイルを設定します。
ステップ 9	**exit** 例： `Device(config-site-tag)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 10	**ap** *mac-address* 例： `Device(config)# ap F866.F267.7DFB`	AP を設定し、AP プロファイル コンフィギュレーション モードを開始します。
ステップ 11	**site-tag** *site-tag-name* 例： `Device(config-ap-tag)# site-tag xyz-site`	サイト タグを AP にマッピングします。

次のタスク

show cts ap sgt-info *ap-name* コマンドを使用して、AP の SGACL 設定を確認します。

ローカルモードでのSGACL、インラインタギング、および SGT の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy xyz-policy-profile`	WLAN のポリシー プロファイルを作成します。
ステップ 3	**cts inline-tagging** 例： `Device(config-wireless-policy)# cts inline-tagging`	CTS インライン タギングを有効にします。
ステップ 4	**cts role-based enforcement** 例： `Device(config-wireless-policy)# cts role-based enforcement`	CTS SGACL の適用を有効にします。
ステップ 5	**cts sgt** *sgt-value* 例： `Device(config-wireless-policy)# cts sgt 100`	（任意）デフォルトのセキュリティ グループ タグ（SGT）を設定します。 （注） SGT は、クライアントが ISE サーバではなくオープン認証を使用する場合にのみ、ユーザ セッションに必要です。

TrustSec 用の ISE の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**radius server** *server-name* 例： `Device(config)# radius server Test-SERVER1`	RADIUS サーバ名を指定します。
ステップ 3	**address ipv4** *ip address* 例： `Device(config-radius-server)# address ipv4 124.3.50.62`	RADIUS サーバのプライマリ パラメータを指定します。
ステップ 4	**pac key** *key* 例： `Device(config-radius-server)# pac key cisco`	デバイスと、RADIUS サーバ上で動作するキー文字列 RADIUS デーモンとの間で使用される認証および暗号キーを指定します。
ステップ 5	**exit** 例： `Device(config-radius-server)# exit`	コンフィギュレーション モードに戻ります。
ステップ 6	**aaa group server radius** *server-group* 例： `Device(config)# aaa group server radius authc-server-group`	RADIUS サーバ グループの ID を作成します。
ステップ 7	**cts authorization list** *mlist-name* 例： `Device(config)# cts authorization list authc-list`	CTS 認証リストを作成します。
ステップ 8	**aaa authorization network** *mlist-name* **group** *name* 例： `Device(config)# aaa authorization network default group group1`	Web ベース許可の許可方式リストを作成します。 （注） コントローラに設定されている ISE IP アドレスが、ISE に設定されている IP アドレス（**[Work Center]** > **[TrustSec]** > **[Components]** > **[Trustsec AAA Servers]**）と同じであることを確認します。

Cisco TrustSec 設定の確認

ワイヤレス CTS SGACL 設定の概要を表示するには、次のコマンドを使用します。

```
Device# show wireless cts summary

Local Mode CTS Configuration

Policy Profile Name               SGACL Enforcement     Inline-Tagging   Default-Sgt

-------------------------------------------------------------------------------------
xyz-policy                        DISABLED              ENABLED          0

wireless-policy1                  DISABLED              DISABLED         0

w-policy-profile1                 DISABLED              DISABLED         0

default-policy-profile            DISABLED              DISABLED         0


Flex Mode CTS Configuration

Flex Profile Name                 SGACL Enforcement     Inline-Tagging
------------------------------------------------------------------------
xyz-flex                          DISABLED              ENABLED
demo-flex                         DISABLED              DISABLED
flex-demo                         DISABLED              DISABLED
xyz-flex-profile                  DISABLED              DISABLED
default-flex-profile              DISABLED              DISABLED
```

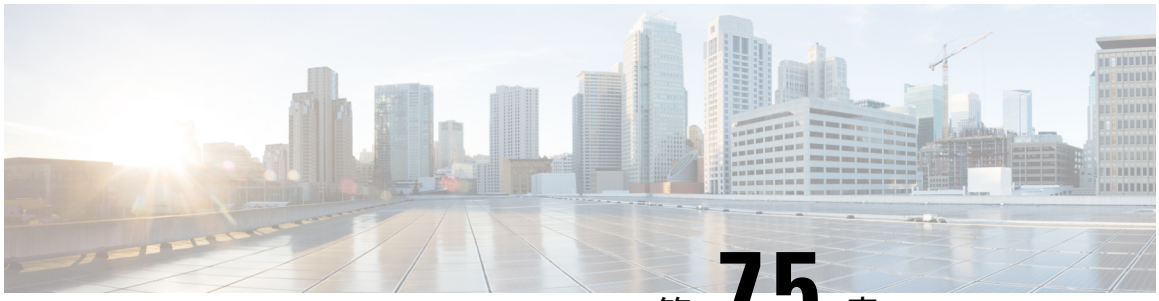
さまざまなワイヤレス プロファイルの CTS 固有の設定ステータスを表示するには、次のコマンドを使用します。

```
Device# show cts wireless profile policy xyz-policy

Policy Profile Name           : xyz-policy
CTS
  Role-based enforcement         : ENABLED
  Inline-tagging                 : ENABLED
   Default SGT   : 100

Policy Profile Name            : foo2
CTS
  Role-based enforcement         : DISABLED
  Inline-tagging                 : ENABLED
  Default SGT           : NOT-DEFINED

Policy Profile Name                    : foo3
CTS
  Role-based enforcement         : DISABLED
  Inline-tagging                 : DISABLED
  Default SGT    : 65001
```

特定のワイヤレス プロファイルの CTS 設定を表示するには、次のコマンドを使用します。

```
Device# show wireless profile policy detailed xyz-policy

Policy Profile Name           : xyz-policy
```

```
Description                   :
Status                        : DISABLED
VLAN                          : 1
Client count                  : 0
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
!
.
.
.WGB Policy Params
  Broadcast Tagging           : DISABLED
  Client VLAN                 : DISABLED
Mobility Anchor List
  IP Address                                 Priority
CTS
  Role-based enforcement         : ENABLED
  Inline-tagging                 : ENABLED
  Default SGT                  : NOT-DEFINED
```



第 75 章

SGT インライン タギングと SXPv4

AP および SXPv4 での SGT インライン タギングの概要

Cisco TrustSec（CTS）は、信頼できるネットワーク デバイスのドメインを確立することによってセキュア ネットワークを構築します。ドメイン内の各デバイスは、そのピアによって認証されます。ドメイン内のデバイス間リンクでの通信は、暗号化、メッセージ整合性検査、データパス リプレイ防止メカニズムを組み合わせたセキュリティで保護されます。

スケーラブル グループ タグ（SGT）交換プロトコル（SXP）は、CTS をサポートする複数のプロトコルの 1 つです。CTS SXP バージョン 4（SXPv4）は、ネットワークの古いバインディングを防ぐため、ループ検出メカニズムを追加することで、SXP の機能を強化しました。さらに、Cisco TrustSec は SGT インライン タギングをサポートしているため、クリア テキスト（暗号化されていない）イーサネット パケットに組み込まれた SGT の伝達が可能になります。

ワイヤレス クライアントが接続され、ISE によって認証されると、コントローラ上で IP-SGT バインディングが生成されます。同じ SGT が他のクライアントの詳細とともに AP にプッシュされます。

AP および SXPv4 での SGT インライン タギングの詳細については、https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_usr_cts/configuration/xe-3s/sec-usr-cts-xe-3s-book/sec-cts-sxpv4.html にある『**Cisco TrustSec Configuration Guide**』を参照してください。

SXP プロファイルの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless cts-sxp profile** *profile-name* 例： `Device(config)# wireless cts-sxp profile rr-profile`	ワイヤレスCTSプロファイルを設定し、cts-sxp プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**cts sxp enable** 例： `Device(config-cts-sxp-profile)# cts sxp enable`	Cisco TrustSec の SXP をイネーブルにします。

アクセス ポイントでの SGT インライン タギングの設定

AP で SGT インライン タギングを設定するには、次の手順に従います。

始める前に

- インライン タギングのために AP にプッシュされる SGT は、ISE 認証によるダイナミック SGT 割り当てによるものだけです。コントローラで設定されているスタティック バインディングではサポートされていません。
- SGT は、AP がフレックス モードで動作している場合にのみプッシュされます。

SGT インライン タギングは、次の AP でのみサポートされています。

- Cisco Aironet 1700I
- Cisco Aironet 1800 シリーズ
- Cisco Aironet 2700 シリーズ
- Cisco Aironet 3700 シリーズ
- Cisco Aironet 3800 シリーズ
- Cisco Aironet 4800 シリーズ

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile flex** *flex-profile* 例： `Device(config)# wireless profile flex rr-xyz-flex-profile`	ワイヤレス flex プロファイルを設定し、ワイヤレス flex プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**cts inline-tagging** 例： `Device(config-wireless-flex-profile)# cts inline-tagging`	AP でインライン タギングを有効にします。

SXP 接続の設定（GUI）

SXP グローバル コンフィギュレーションを設定するには、次の手順を実行します。

手順

ステップ 1 [Global] セクションで、[SXP Enabled] チェック ボックスをオンにして SXP を有効にします。

ステップ 2 [Default Source IP] フィールドに IP アドレスを入力します。

ステップ 3 [Reconciliation Period (sec)] フィールドに値を入力します。

ステップ 4 [Retry Period (sec)] フィールドに値を入力します。

ステップ 5 [Set New Default Password] チェック ボックスをオンにします。このチェック ボックスをオンにすると、[Password Type] および [Enter Password] フィールドが表示されます。

ステップ 6 [Password Type] ドロップダウンリストから、使用可能なタイプのいずれかを選択します。

ステップ 7 [Enter Password] フィールドに値を入力します。

ステップ 8 [Apply] ボタンをクリックします。

ステップ 9 [Peer] セクションで [Add] ボタンをクリックします。

ステップ 10 [Peer IP] フィールドに IP アドレスを入力します。

ステップ 11 [Source IP] フィールドに IP アドレスを入力します。

ステップ 12 [Password] ドロップダウンリストから、使用可能なタイプのいずれかを選択します。

ステップ 13 [Mode of Local Device] ドロップダウンリストから、使用可能なタイプのいずれかを選択します。

ステップ 14 [Save & Apply to Device] ボタンをクリックします。

ステップ 15 [AP] タブで [Add] ボタンをクリックします。[Add SXP AP] ダイアログボックスが表示されます。

ステップ 16 プロファイルの名前を [Name] フィールドに入力します。

ステップ 17 [Status] フィールドを [Enabled] に設定して AP を有効にします。

ステップ 18 [Default Password] フィールドに値を入力します。

ステップ 19 [CTS Speaker Seconds]、[CTS Recon Period]、[CTS Retry Period]、[CTS Listener Maximum]、および [CTS Listener Minimum] の値（秒単位）を入力します。

ステップ 20 [CTS SXP Profile Connections] セクションで [Add] をクリックします。

ステップ 21 [Peer IP] フィールドに IP アドレスを入力します。

ステップ 22 [Connection Mode] ドロップダウンリストからいずれかのモードを選択します。使用可能なモードは、[Both]、[Listener]、および [Speaker] です。

ステップ 23 [Password Type] ドロップダウンリストから、[None] または [Default] を選択します。

ステップ 24 [Add] ボタンをクリックします。

ステップ 25 [Save & Apply to Device] ボタンをクリックします。

SXP 接続の設定

SXP 接続を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**cts sxp enable** 例： `Device(config)# cts sxp enable`	CTS SXP サポートを有効にします。
ステップ 3	**cts sxp connection peer** *ipv4-address***password none mode local speaker** 例： `Device(config)# cts sxp connection peer 1.1.1.1 password none mode local speaker`	CTS-SXP ピア アドレス接続を設定します。 （注） パスワードは必ずしも *none* にする必要はありません。モードはスピーカーかリスナーまたはその両方を使用できます。

次のタスク

設定を確認するには、次のコマンドを使用します。

```
Device# show running-config | inc sxp
```

アクセス ポイントへの SGT プッシュの確認

ワイヤレス クライアントが接続されて ISE によって認証されると、コントローラ上で IP-SGT バインディングが生成されます。これは、次のコマンドを使用して確認できます。

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
1.1.1.1                 100     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1
```

SXP 接続ステータスを確認するには、次のコマンドを使用します。

```
Device# show cts sxp connections

 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
----------------------------------------------
Peer IP          : 40.1.1.1
Source IP        : 40.1.1.2
Conn status      : On
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: none
Hold timer is running
Duration since last state change: 0:00:00:06 (dd:hr:mm:sec)


Total num of SXP Connections = 1
```

SXP 接続を介して学習されたバインディングを表示するには、次のコマンドを使用します。

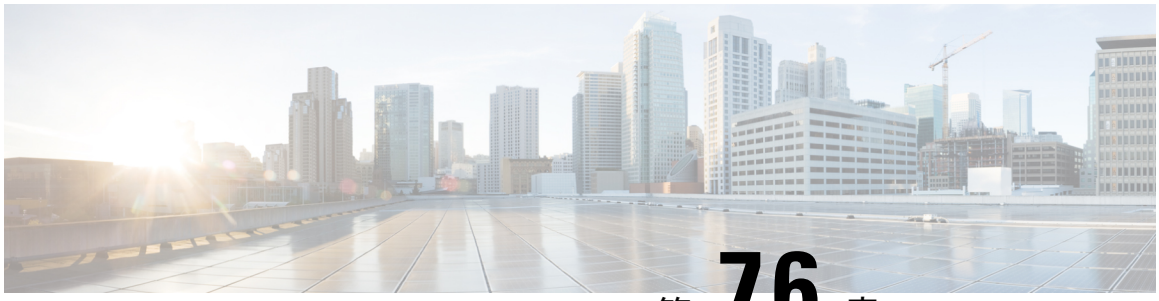
```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information
```

```
IP Address              SGT     Source
============================================
1.1.1.1                 100     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1
```

AP のインライン タギングのステータスとその IP-SGT バインディングを確認するには、AP で次のコマンドを使用します。

```
AP# show capwap client rcb

AdminState                          : ADMIN_ENABLED
OperationState                      : UP
Name                                : AP2C33.1185.C4D0
SwVer                               : 16.6.230.41
HwVer                               : 1.0.0.0
MwarApMgrIp                         : 9.3.72.38
MwarName                            : mohit-ewlc
MwarHwVer                           : 0.0.0.0
Location                            : default location
ApMode                              : FlexConnect
ApSubMode                           : Not Configured
CAPWAP Path MTU                     : 1485
CAPWAP UDP-Lite                     : Enabled
IP Prefer-mode                      : IPv4
AP Link DTLS Encryption             : OFF
AP TCP MSS Adjust                   : Disabled
LinkAuditing                        : disabled
Efficient Upgrade State             : Disabled
Flex Group Name                     : anrt-flex
AP Group Name                       : default-group
Cisco Trustsec Config
   AP Inline Tagging Mode                : Enabled
! The status can be Enabled or Disabled and is based on the tag that is pushed to the
AP.
      AP Sgacl Enforcement                  : Disabled
      AP Override Status                    : Disabled


AP# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information
        IP SGT SOURCE
9.3.74.101  17  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
Total number of active   bindings = 1

Active IPv6-SGT Bindings Information
                       IP SGT SOURCE
fe80::c1d5:3da2:dc96:757d  17  LOCAL

IP-SGT Active Bindings Summary
============================================
Total number of LOCAL    bindings = 1
```

```
Total number of active   bindings = 1
```



第 76 章

ローカルで有効な証明書

ローカルで有効な証明書 （LSC）について

このモジュールでは、ローカルで有効な証明書（LSC）を使用するように Cisco Catalyst 9800 シリーズ ワイヤレス コントローラおよび Lightweight アクセス ポイント（LAP）を設定する方法について説明します。LSC を使用する Public Key Infrastructure（PKI）を選択した場合は、AP とコントローラで LSC を生成できます。その後、証明書を使用してコントローラと AP を相互認証することができます。

シスコ コントローラは、LSC を使用するように設定できます。独自の PKI でセキュリティを強化して認証局（CA）を管理し、生成された証明書でポリシー、制約事項、および使用方法を定義する場合は、LSC を使用できます。

コントローラで新しい LSC 証明書をプロビジョニングし、次に認証局（CA）サーバから Lightweight アクセス ポイント（LAP）をプロビジョニングする必要があります。

LAP は、CAPWAP プロトコルを使用してコントローラと通信します。証明書への署名と、LAP およびコントローラ自体の CA 証明書の発行については、コントローラから要求を開始する必要があります。LAP は CA サーバと直接通信しません。CA サーバの詳細がコントローラに設定され、アクセス可能である必要があります。

コントローラは、デバイス上で生成された certReqs を CA に転送するために Simple Certificate Enrollment Protocol（SCEP）を使用し、CA から署名済み証明書を取得するために SCEP を再度使用します。

SCEP は、PKI クライアントと認証局サーバが証明書の登録と失効をサポートするために使用する証明書管理プロトコルです。これはシスコで広く使用され、多くの CA サーバでサポートされています。SCEP プロトコルでは、HTTP は PKI メッセージのトランスポート プロトコルとして使用されます。SCEP の主な目的は、ネットワーク デバイスに証明書を安全に発行する

ことです。SCEP は多くの操作に対応していますが、このリリースでは次の操作に使用されています。

- CA および RA 公開キーの配布
- 認証登録

コントローラでの証明書プロビジョニング

新しい LSC 証明書（CA 証明書とデバイス証明書の両方）をコントローラにインストールする必要があります。

SCEP プロトコルを使用する場合、CA 証明書は CA サーバから受け取ります。この時点ではコントローラに証明書が存在しないため、これは純粋な **Get** 操作です。これらの証明書はコントローラ上にインストールされます。AP が LSC でプロビジョニングされるときに、同じ CA 証明書が AP にもプッシュされます。

デバイスの証明書の登録操作

CA 署名付き証明書を要求する LAP とコントローラの両方に対して、certRequest が PKCS#10 メッセージとして送信されます。certRequest には、X.509 証明書に組み込まれ、要求者の秘密キーでデジタル署名される件名、公開キー、およびその他の属性が含まれています。これらは CA に送信され、そこで certRequest が X.509 証明書に変換されます。

PKCS#10 certRequest を受け取る CA が要求者の ID を認証し、要求が変更されていないことを確認するためには、追加情報が必要です。証明書の要求または応答を送受信するために、PKCS#10 は PKCS#7 などの他のアプローチと何度も組み合わされます。

ここで、PKCS#10 は PKCS#7 SignedData メッセージ タイプでラップされます。これは SCEP クライアント機能の一部としてサポートされ、PKCSReq メッセージがコントローラに送信されます。登録操作が成功すると、CA 証明書とデバイス証明書の両方がコントローラ上で使用可能になります。

Lightweight アクセス ポイントでの証明書プロビジョニング

LAP で新しい証明書をプロビジョニングするには、CAPWAP モードで LAP が新しい署名付き X.509 証明書を取得できる必要があります。これを実現するために、LAP はコントローラに certRequest を送信します。このコントローラは CA プロキシとして機能し、CA により署名された LAP 用の certRequest の取得に対応します。

certReq および certResponse は LWAPP ペイロードを使用して LAP に送信されます。

LSC CA 証明書と LAP デバイス証明書の両方が LAP にインストールされ、システムが自動リブートします。システムが次に起動するときには、LSC を使用するように設定されているため、AP は接続要求の一部として LSC デバイス証明書をコントローラに送信します。接続応答の一部として、コントローラは新しいデバイス証明書を送信すると同時に、新しい CA ルート証明書を使用して受信 LAP 証明書を検証します。

（注） LSC は、コントローラとすべての Cisco Aironet アクセス ポイントでサポートされています。

また、LSC はコントローラで有効になっています（GUI および CLI）。

次の作業

コントローラおよび AP の既存の PKI インフラストラクチャを使用して証明書の登録を設定、許可、および管理するには、LSC プロビジョニングを使用する必要があります。

ローカルで有効な証明書のプロビジョニング

PKI トラストポイントの RSA キーの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**crypto key generate rsa exportable general-keys modulus** *key_size* **label** *RSA_key* 例： `Device(config)# crypto key generate rsa exportable general-keys modulus 2048 label ewlc-tp1`	PKI トラストポイントの RSA キーを設定します。 • **key_size** には、キー係数のサイズを入力します。有効な範囲は 360 ～ 4096 です。 • **RSA_key** には、RSA キー ペアのラベルを入力します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

PKI トラストポイント パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**crypto pki trustpoint** *trustpoint_name* 例： `Device(config)# crypto pki trustpoint microsoft-ca`	外部 CA サーバの新しいトラスト ポイントを作成します。*trustpoint_name* はトラストポイント名を指します。
ステップ 3	**enrollment url** *HTTP_URL* 例： `Device(ca-trustpoint)# enrollment url http://CA_server/certsrv/mscep/mscep.dll`	トラストポイント登録パラメータを使用してトラストポイントを登録します。
ステップ 4	**subject-name** *subject_name* 例： `Device(ca-trustpoint)# subject-name C=IN, ST=KA, L=Bengaluru, O=Cisco, CN=eagle-eye/emailAddress=support@abc.com`	トラストポイントの件名パラメータを作成します。
ステップ 5	**rsakeypair** *RSA_key key_size* 例： `Device(ca-trustpoint)# rsakeypair ewlc-tp1`	RSA キーをトラストポイントの RSA キーにマッピングします。 • *RSA_key*：RSA キー ペアのラベルを指します。 • *key_size*：署名キーの長さを指します。範囲は 360 ～ 4096 です。
ステップ 6	**revocation** {**crl** | **none** | **ocsp**} 例： `Device(ca-trustpoint)# revocation none`	失効を確認します。
ステップ 7	**end** 例： `Device(ca-trustpoint)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

CA サーバを使用した PKI トラストポイントの認証と登録（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[PKI Management]** を選択します。

ステップ 2 [Trustpoint] セクションで [Add] をクリックします。

ステップ 3 トラストポイントのラベルと登録 URL を入力します。

ステップ 4 [Authenticate] チェック ボックスをオンにして、トラストポイントのラベルを認証します。

ステップ 5 [Subject Name] セクションに、国コード、都道府県、場所、組織、ドメイン名、および電子メール アドレスを入力します。

ステップ 6 [Key Generated] チェック ボックスをオンにして、使用可能な RSA キー ペアを表示します。[Available RSA Keypairs] ドロップダウンリストから選択できます。

ステップ 7 [Enroll Trustpoint] チェック ボックスをオンにしてパスワードを入力し、確認します。

ステップ 8 [Save & Apply to Device] をクリックします。

CA サーバを使用した PKI トラストポイントの認証と登録（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**crypto pki authenticate** *trustpoint_name* 例： `Device(config)# crypto pki authenticate microsoft-ca`	CA 証明書を取得します。
ステップ 3	**yes** 例： `Device(config)# % Do you accept this certificate? [yes/no]: yes` `Trustpoint CA certificate accepted.`	
ステップ 4	**crypto pki enroll** *trustpoint_name* 例： `Device(config)# crypto pki enroll microsoft-ca` `%` `% Start certificate enrollment ..`	クライアント証明書を登録します。

	コマンドまたはアクション	目的
	% Create a challenge password. You will need to verbally provide this password to the CA Administrator in order to revoke your certificate. For security reasons your password will not be saved in the configuration. Please make a note of it.	
ステップ 5	**password** 例： `Device(config)# abcd123`	パスワードを入力します。
ステップ 6	**password** 例： `Device(config)# abcd123`	パスワードを再入力します。
ステップ 7	**yes** 例： `Device(config)# % Include the router serial number in the subject name? [yes/no]: yes`	
ステップ 8	**no** 例： `Device(config)# % Include an IP address in the subject name? [no]: no`	
ステップ 9	**yes** 例： `Device(config)#` **Request certificate from CA? [yes/no]: yes** **% Certificate request sent to Certificate Authority** **% The 'show crypto pki certificate verbose client' commandwill show the fingerprint.**	
ステップ 10	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

LSC 証明書による AP の接続試行回数の設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。
ステップ 2 [All Access Points] ページで LSC プロビジョンの名前をクリックします。
ステップ 3 [Status] ドロップダウンを使用して LSC を有効にします。
ステップ 4 [Trustpoint Name] ドロップダウンを使用して、トラストポイントを検索または選択します。
ステップ 5 [Number of Join Attempts] フィールドに再試行回数を入力します。
ステップ 6 [Apply] をクリックします。

LSC 証明書による AP の接続試行回数の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap lsc-provision join-attempt** *number_of_attempts* 例： `Device(config)# ap lsc-provision join-attempt 10`	新しくプロビジョニングされた LSC 証明書を使用した AP の接続試行回数を指定します。 AP の接続回数が指定の制限を超えると、AP は MIC 証明書を使用して再接続します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

LSC 証明書の件名パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap lsc-provision subject-name-parameter country** *country-str* **state** *state-str* **city** *city-str* **domain** *domain-str* **org** *org-str* **email-address** *email-addr-str* 例： `Device(config)# ap lsc-provision subject-name-parameter country India state Karnataka city Bangalore domain domain1 org Right email-address adc@gfe.com`	AP によって生成された証明書要求の件名に含める属性を指定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

LSC 証明書のキー サイズの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap lsc-provision key-size**{**1024** | **2048**} 例： `Device(config)# ap lsc-provision key-size 1024`	AP 上の LSC 証明書に対して生成されるキーのサイズを指定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

アクセス ポイントでの LSC プロビジョニング用トラストポイントの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap lsc-provision trustpoint** *tp-name* 例： `Device(config)# ap lsc-provision trustpoint microsoft-ca`	LCS を AP にプロビジョニングする際に使用するトラストポイントを指定します。 *tp-name* はトラストポイント名を指します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AP の LSC プロビジョン リストの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [All Access Points] ページで LSC プロビジョンの名前をクリックします。

ステップ 3 [Status] ドロップダウンを使用して LSC を有効にします。

ステップ 4 [Trustpoint Name] ドロップダウンを使用して、トラストポイントを検索または選択します。

ステップ 5 [Number of Join Attempts] フィールドに再試行回数を入力します。

ステップ 6 [Key Size] ドロップダウンを使用してキーを選択します。

ステップ 7

ステップ 8 [Edit AP Join Profile] ウィンドウで [CAPWAP] タブをクリックします。

ステップ 9 [Add APs to LSC Provision List] セクションで、[Select File] オプションを使用して AP の詳細を含む CSV ファイルをアップロードします。ファイルを選択したら [Upload File] をクリックします。

ステップ 10 [AP MAC Address] フィールドを使用して、MAC アドレスで AP を検索し、追加することもできます。プロビジョン リストに追加された AP は、[APs in provision List] リストボックスに表示されます。

ステップ 11 [Subject Name Parameters] セクションに、次の詳細情報を入力します。

- Country
- 都道府県（State）
- 市区町村郡（City）
- Organisation
- department
- 電子メール アドレス

ステップ 12 [Apply] をクリックします。

AP の LSC プロビジョン リストの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**[no] ap lsc-provision mac-address** *mac-addr* 例： `Device(config)# no ap lsc-provision mac-address 001b.3400.02f0`	LSC プロビジョン リストにアクセス ポイントを追加します。 （注） **ap lsc-provision provision-list** コマンドを使用して AP のリストをプロビジョニングできます。 （または） **ap lsc-provision** コマンドを使用してすべての AP をプロビジョニングできます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

すべてのアクセス ポイントに対する LSC プロビジョニングの設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > > の順に選択します。

ステップ 2 [Access Points] ページで [LSC Provision] セクションを展開します。

ステップ 3 [Status] を [Enabled] 状態に設定します。

[Status] を [Provision List] に設定すると、そのプロビジョン リストに含まれている AP に対してのみ LSC プロビジョニングが設定されます。

ステップ 4 [Trustpoint Name] ドロップダウンリストから、すべての AP に対して適切なトラストポイントを選択します。

ステップ 5 [Number Of Join Attempts] フィールドに、AP がコントローラへの接続を再試行できる回数を入力します。

ステップ 6 [Key Size] ドロップダウンリストを使用して、次のオプションから証明書の適切なキー サイズを選択します。

- 2048
- 3072
- 4096

ステップ 7 [Add APs to LSC Provision List] セクションで [Select File] オプションをクリックして、AP の詳細を含む CSV ファイルをアップロードします。ファイルを選択したら [Upload File] をクリックします。

ステップ 8 [AP MAC Address] フィールドに AP の MAC アドレスを入力して AP を検索し、追加することもできます。プロビジョン リストに追加された AP は、[APs in Provision List] セクションに表示されます。

ステップ 9 [Subject Name Parameters] セクションに、次の詳細情報を入力します。

1. Country
2. 都道府県（State）
3. 市区町村郡（City）
4. マニュアルの構成
5. 部門
6. 電子メール アドレス

ステップ 10 [Apply] をクリックします。

すべてのアクセス ポイントに対する LSC プロビジョニングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**[no] ap lsc-provision** 例： `Device(config)# no ap lsc-provision`	すべてのアクセスポイントに対してLSC プロビジョニングを有効にします。 デフォルトでは、LSC プロビジョニングはすべての AP に対して無効になっています。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

プロビジョン リストに含まれるアクセス ポイントに対する LSC プロビジョニングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap lsc-provision provision-list** 例： `Device(config)# ap lsc-provision provision-list`	プロビジョン リストに設定されている一連のアクセス ポイントに対して LSC プロビジョニングを有効にします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

LSC 設定の確認

ワイヤレス管理トラストポイントの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless management trustpoint

Trustpoint  Name : microsoft-ca
Certificate Info : Available
Certificate Type : LSC
Certificate Hash : 9e5623adba5307facf778e6ea2f5082877ea4beb
 Private key Info : Available
```

AP の LSC プロビジョンに関連する設定の詳細を表示するには、次のコマンドを使用します。

```
Device# show ap lsc-provision summary

AP LSC-provisioning : Disabled
Trustpoint used for LSC-provisioning : microsoft-ca
LSC Revert Count in AP reboots : 10

AP LSC Parameters :
Country : IN
State : KA
City : BLR
Orgn : ABC
Dept : ABC
Email : support@abc.com
Key Size : 2048

AP LSC-provision List : Enabled
Total number of APs in provision list: 3

Mac Address
-----------
0038.df24.5fd0
2c5a.0f22.d4ca
e4c7.22cd.b74f
```

LSC の管理トラストポイントの設定（GUI）

手順

ステップ 1 **[Administration]** > **[Management]** > **[HTTP/HTTPS]** の順に選択します。

ステップ 2 [HTTP Trust Point Configuration] セクションで、[Enable Trust Point] フィールドを [Enabled] 状態に設定します。

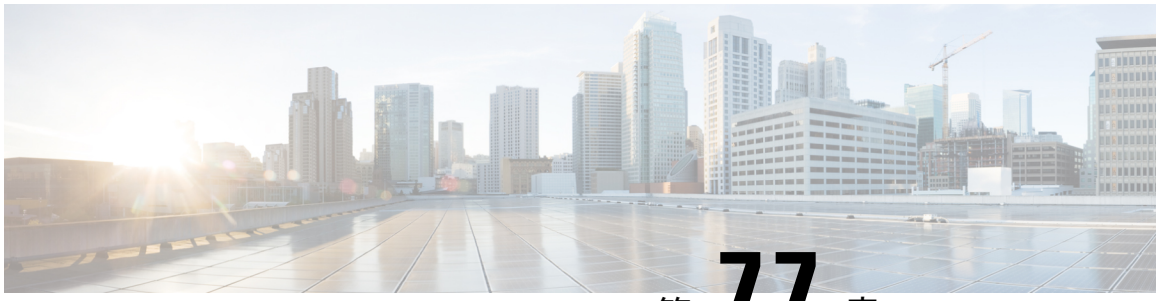
ステップ 3 [Trust Points] ドロップダウンリストから、適切なトラストポイントを選択します。

ステップ 4 設定を保存します。

LSC の管理トラストポイントの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless management trustpoint** *trustpoint_name* 例： `Device(config)# wireless management trustpoint microsoft-ca`	LSC の管理トラストポイントを設定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。



第 77 章

Cisco Umbrella WLAN

Cisco Umbrella WLAN について

Cisco Umbrella WLAN は、既知と緊急の両方の脅威を自動検出する、クラウド提供のネットワーク セキュリティ サービスをドメイン ネーム システム（DNS） レベルで提供します。

この機能により、マルウェア、ボットネットワーク、およびフィッシングが実際に悪意のある脅威になる前に、それらをホストしているサイトをブロックできます。

Cisco Umbrella WLAN を使用すると、次のことが可能です。

- シングル ポイントでのユーザ グループごとのポリシーの設定。
- ネットワーク、グループ、ユーザ、デバイス、またはIPアドレスごとのポリシーの設定。

  ポリシーの優先順位は次のとおりです。

  1. ローカル ポリシー
  2. AP グループ
  3. WLAN

- リアルタイムのビジュアルセキュリティアクティビティダッシュボードと集約レポート。
- スケジュール設定と電子メールによるレポートの送信。
- 最大 60 のコンテンツ カテゴリのサポートとカスタム ホワイトリスト エントリとブラックリスト エントリを追加するためのプロビジョニング。

この機能は、次のシナリオでは機能しません。

- アプリケーションまたはホストが、DNS を使用する代わりに IP アドレスを直接使用してドメイン名をクエリしている場合。
- クライアントが Web プロキシに接続されていて、サーバ アドレスを解決するための DNS クエリを送信しない場合。

Cisco Umbrella アカウントへのコントローラの登録

はじめる前に

- Cisco Umbrella のアカウントが必要です。
- Cisco Umbrella からの API トークンが必要です。

ここでは、Cisco Umbrella アカウントにコントローラを登録するプロセスについて説明します。

コントローラは、Umbrella パラメータ マップを使用して Cisco Umbrella サーバに登録します。Umbrella パラメータ マップごとに API トークンが必要です。Cisco Umbrella は、コントローラのデバイス ID を使用して応答します。デバイス ID は、Umbrella パラメータ マップ名と 1 対 1 でマッピングされています。

Cisco Umbrella ダッシュボードを使用したコントローラの API トークンの取得

Cisco Umbrella ダッシュボードで、[Device Name] にコントローラとその ID が表示されていることを確認します。

コントローラでの API トークンの適用

ネットワークに Cisco Umbrella の API トークンを登録します。

DNS クエリと応答

WLAN にデバイスを登録して Umbrella パラメータ マップを設定すると、WLAN に接続しているクライアントからの DNS クエリが Umbrella DNS リゾルバにリダイレクトされるようになります。

（注） これは、ローカル ドメインの正規表現パラメータ マップに設定されていないすべてのドメインに適用されます。

クエリと応答は、Umbrella パラメータ マップの DNScrypt オプションに基づいて暗号化されます。

Cisco Umbrella の設定の詳細については、『Integration for ISR 4K and ISR 1100 – Security Configuration Guide』を参照してください。

制限事項と考慮事項

この機能の制限事項と考慮事項は次のとおりです。

- デバイス登録が成功すると、ワイヤレス Cisco Umbrella プロファイルを WLAN や AP グループなどのワイヤレス エンティティに適用できます。
- L3 モビリティの場合、Cisco Umbrella は常にアンカー コントローラで適用する必要があります。

Cisco Umbrella WLAN の設定

コントローラで Cisco Umbrella を設定するには、次の作業を行います。

- Cisco Umbrella ダッシュボードから API トークンを取得する必要があります。
- Cisco Umbrella 登録サーバとの HTTPS 接続を確立するために、ルート証明書が必要です。**crypto pki trustpool import terminal** コマンドを使用して、**digicert.com** からコントローラにルート証明書をインポートする必要があります。

トラスト プールへの CA 証明書のインポート

始める前に

ここでは、ルート証明書を取得して Cisco Umbrella 登録サーバとの HTTPS 接続を確立する方法について詳しく説明します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**crypto pki trustpool import url** *http://www.cisco.com/security/pki/trs/ios.p7b* 例： `Device(config)# crypto pki trustpool import url http://www.cisco.com/security/pki/trs/ios.p7b`	シスコの Web サイトからルート証明書を直接インポートします。 （または）**ステップ 3、4、5** を実行します。
ステップ 3	**crypto pki trustpool import terminal** 例： `Device(config)# crypto pki trustpool import terminal`	import terminal コマンドを実行して、ルート証明書をインポートします。

	コマンドまたはアクション	目的
ステップ 4	次の場所で入手できる PEM 形式の CA 証明書を入力します。「関連情報」の項を参照して、CA 証明書をダウンロードしてください。 例： `----BEGIN CERTIFICATE----` `MIIElDCCA3ygAwIBAgIQAf2j627KdciIQ4tyS8+8kT` `!` `.` `.` `.` `j6tJLp07kzQoH3jOlOrHvdPJbRzeXDLz` `----END CERTIFICATE----`	**digicert.com** から CA 証明書を貼り付けて、ルート証明書をインポートします。
ステップ 5	**quit** 例： `Device(config)# quit`	**quit** コマンドを入力して、ルート証明書をインポートします。 （注） 証明書のインポートが完了すると、メッセージが届きます。

ローカル ドメインの正規表現パラメータ マップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**parameter-map type regex** *parameter-map-name* 例： `Device(config)# parameter-map type regex dns_wl`	正規表現パラメータ マップを作成します。
ステップ 3	**pattern** *regex-pattern* 例： `Device(config-profile)# pattern www.google.com`	照合する正規表現パターンを設定します。
ステップ 4	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config-profile)# end`	ンフィギュレーション モードを終了できます。

WLAN でのパラメータ マップ名の設定（GUI）

手順

ステップ 1 [Configuration] > [Security] > [Web Auth] を選択します。

ステップ 2 [Add] ボタンをクリックします。[Create WebAuth Parameter] ダイアログボックスが表示されます。

ステップ 3 [Parameter-map name] フィールドにパラメータ マップの名前を入力します。

ステップ 4 [Maximum HTTP connections] フィールドに値を入力します。1 ～ 200 の範囲で値を入力する必要があります。

ステップ 5 [Init-State Timeout(secs)] フィールドに値を入力します。60 ～ 3932100 の範囲で値を入力する必要があります。

ステップ 6 [Type] ドロップダウンリストから必要なオプションを選択します。

ステップ 7 [Apply to Device] ボタンをクリックします。

Umbrella パラメータ マップの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**parameter-map type umbrella global** 例： `Device(config)# parameter-map type umbrella global`	Umbrella グローバル パラメータ マップを作成します。
ステップ 3	**token** *token-value* 例： `Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166`	Umbrella トークンを設定します。

	コマンドまたはアクション	目的
ステップ 4	**local-domain** *regex-parameter-map-name* 例： `Device(config-profile)# local-domain dns_wl`	ローカル ドメインの正規表現パラメータ マップを設定します。
ステップ 5	**end** 例： `Device(config-profile)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

DNScrypt の有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**parameter-map type umbrella global** 例： `Device(config)# parameter-map type umbrella global`	Umbrella グローバル パラメータ マップを作成します。
ステップ 3	**token** *token-value* 例： `Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166`	Umbrella トークンを設定します。
ステップ 4	**local-domain** *regex-parameter-map-name* 例： `Device(config-profile)# local-domain dns_wl`	ローカル ドメインの正規表現パラメータ マップを設定します。
ステップ 5	[**no**] **dnscrypt** 例： `Device(config-profile)# no dnscrypt`	DNScrypt を有効または無効にします。 デフォルトでは、DNScrypt オプションは有効です。
ステップ 6	**end** 例： `Device(config-profile)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

UDP セッションのタイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**parameter-map type umbrella global** 例： `Device(config)# parameter-map type umbrella global`	Umbrella グローバル パラメータ マップを作成します。
ステップ 3	**token** *token-value* 例： `Device(config-profile)# token 57CC80106C087FB1B2A7BAB4F2F4373C00247166`	Umbrella トークンを設定します。
ステップ 4	**local-domain** *regex-parameter-map-name* 例： `Device(config-profile)# local-domain dns_wl`	ローカル ドメインの正規表現パラメータ マップを設定します。
ステップ 5	**udp-timeout** *timeout_value* 例： `Device(config-profile)# udp-timeout 2`	UDP セッションのタイムアウト値を設定します。 *timeout_value* の範囲は 1 ～ 30 秒です。 （注） **public-key** および **resolver** パラメータマップ オプションには、デフォルト値が自動的に入力されます。したがって、変更する必要はありません。
ステップ 6	**end** 例： `Device(config-profile)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN でのパラメータ マップ名の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**umbrella-param-map** *umbrella-name* 例： `Device(config-wireless-policy)# umbrella-param-map global`	WLAN の Umbrella OpenDNS 機能を設定します。
ステップ 4	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Cisco Umbrella 設定の確認

Umbrella 設定の詳細を表示するには、次のコマンドを使用します。

```
Device# show umbrella config
```

デバイス登録の詳細を表示するには、次のコマンドを使用します。

```
Device# show umbrella <deviceid>
```

Umbrella デバイス ID の詳細な説明を表示するには、次のコマンドを使用します。

```
Device# show umbrella <deviceid> detailed
```

Umbrella DNSCrypt の詳細を表示するには、次のコマンドを使用します。

```
Device# show umbrella dnscrypt
```

Umbrella グローバル パラメータ マップの詳細を表示するには、次のコマンドを使用します。

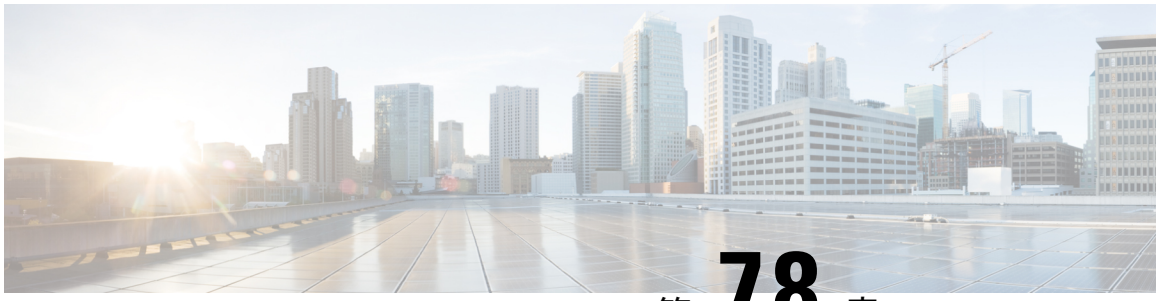
```
Device# show parameter-map type umbrella global
```

正規表現パラメータ マップの詳細を表示するには、次のコマンドを使用します。

```
Device# show parameter-map type regex <parameter-map-name>
```

Umbrella の統計情報を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature umbrella datapath stats
```



第 78 章

FIPS

FIPS の概要

連邦情報処理標準（FIPS）140-2 は、暗号化モジュールの検証に使用されるセキュリティ規格です。暗号化モジュールは、米国政府機関およびその他の規制産業（金融機関や医療機関など）が取扱注意ではあるが機密ではない（SBU）情報の収集、保存、転送、共有、および配布に使用するために民間企業によって製造されます。

FIPS の詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html。

FIPS が有効な状態の場合、一部のパスワードと事前共有キーに次の最小長を指定する必要があります。

- コントローラとマップ サーバ間の SD-Access ワイヤレスの場合、両者間のすべての TCP メッセージの認証に事前共有キー（LISP 認証キーなど）が使用されます。この事前共有キーの長さは 14 文字以上にする必要があります。
- ISAKMP キー（Crypto ISAKMP キーなど）の長さは、14 文字以上にする必要があります。

FIPS の注意事項および制約事項

- コントローラ スイッチでは、レガシー AP をサポートするためにレガシー キーが使用されます。ただし FIPS モードの場合は、暗号化エンジンがレガシー キーを脆弱なキーとし

て検出し、エラー メッセージ「% Error in generating keys: could not generate test signature」を表示して拒否します。コントローラのブートアップ時に表示されるこのようなエラーメッセージは、無視することをお勧めします（FIPS モードで動作している場合）。

FIPS のセルフテスト

暗号モジュールは、適正に動作していることを確認するために、電源投入時のセルフテストと条件付きセルフテストを実行しなければなりません。

電源投入時セルフテストは、デバイスの電源が投入された後に自動的に実行されます。デバイスが FIPS モードになるのは、すべてのセルフテストが正常に完了した後だけです。いずれかのセルフテストが失敗すると、デバイスはシステム メッセージをログに記録し、エラー状態に移行します。また、電源投入時自己診断テストが失敗した場合、デバイスは起動できません。

既知解テスト（KAT）を利用すると、暗号アルゴリズムは正しい出力があらかじめわかってるデータに対して実行され、その計算出力は前回生成された出力と比較されます。計算出力が既知解と等しくない場合は、既知解テストに失敗したことになります。

電源投入時セルフテストでは次を含むテストが行われます。

- ソフトウェアの整合性
- アルゴリズム テスト

何かに対応してセキュリティ機能または操作が始動された場合は、条件付きセルフテストが実行されなければなりません。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

デバイスは、既知解テスト（KAT）という暗号化アルゴリズムを使用して、デバイス上に実装されている FIPS 140-2 で承認された暗号機能（暗号化、復号化、認証、および乱数生成）ごとに FIPS モードをテストします。デバイスは、このアルゴリズムを、すでに正しい出力がわかっているデータに対して適用します。次に、計算された出力を、以前に生成された出力と比較します。計算された出力が既知解に等しくない場合は、KAT が失敗します。

適用可能なセキュリティ機能または操作が呼び出された場合は、条件付きセルフテストが自動的に実行されます。電源投入時セルフテストとは異なって、条件付きセルフテストはそれぞれに関連する機能がアクセスされるたびに実行されます。

条件付きセルフテストでは次を含むテストが行われます。

- ペア整合性テスト：このテストは公開キー/秘密キー ペアが生成されたときに実行されます。
- 乱数連続生成テスト：このテストは乱数が生成されたときに実行されます。
- バイパス
- ソフトウェア ロード

FIPS の設定

アクティブ コントローラとスタンバイ コントローラの両方に同じ FIPS 認証キーが設定されていることを確認します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**fips authorization-key** *key* 例： `Device(config)# fips authorization-key 12345678901234567890123456789012`	キーは 32 桁の 16 進数文字である必要があります。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

次のタスク

次にコントローラを再起動して FIPS モードを有効にする必要があります。コントローラの再起動後、AP もコントローラに再接続してすぐに再起動します。

FIPS のモニタリング

FIPS に関する情報を表示するには、次のコマンドを使用します。

コマンド	目的
show fips authorization-key	インストール済みの認証キーを表示します。
show fips status	デバイスの FIPS のステータスを表示します。

CC

コモン クライテリアについて

コモン クライテリア（CC）は、製品開発者が要求するセキュリティ機能をデバイスが備えているかどうかを検証するテスト基準です。CC 認定は、24 か国で正式に認められています。

CC は一連の要件、テスト、評価方法で構成され、評価対象（ToE）が特定の保護プロファイルに準拠していることを保証します。この場合、ToEは次の保護プロファイルに準拠している必要があります。

- ネットワーク デバイス（NDcPP）v2 のコラボレーション保護プロファイル（2017 年 5 月 5 日現在）
- ワイヤレス ローカル エリア ネットワーク（WLAN）アクセス システム拡張パッケージ バージョン 1（2015 年 5 月 29 日現在）

CC の詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/common-criteria.html

コモン クライテリアの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless wlancc** 例： `Device(config)# wireless wlancc`	コントローラのコモン クライテリア モードを設定します。 （注） コモン クライテリア モードを有効にした後、コントローラを再起動します。
ステップ 3	**ap dtls-cipher** *ciphersuite* 例： `Device(config)# ap dtls-cipher DHE-RSA-AES256-SHA256`	DTLS でサポートされている暗号スイートを設定します。 （注） コントローラを再起動して、選択した暗号スイートをアクティブにします。

	コマンドまたはアクション	目的
ステップ 4	**ap dtls-version** {**dtls_1_0** | **dtls_1_2**} 例： `Device(config)# ap dtls-version dtls_1_2`	DTLS バージョン 1.0 または 1.2 を設定します。 （注） 変更を有効にするには、設定を保存してコントローラをリロードします。
ステップ 5	**end** 例： `Device(config)# end`	コンフィギュレーション モードを終了して、特権EXECモードを開始します。

CC 設定の確認

ワイヤレス認定の設定を表示するには、次の **show** コマンドを使用します。

```
Device# show wireless certification config
Wireless Certification Configurations

WLANCC                                    : Configured
AP DTLS Cipher Suite                      : DHE-RSA-AES128-SHA
                                            DHE-RSA-AES256-SHA
                                            DHE-RSA-AES256-SHA256
                                            ECDHE-ECDSA-AES128-GCM-SHA256
                                            ECDHE-ECDSA-AES256-GCM-SHA384
AP DTLS Version                           : DTLS v1.2
```

CC モードの動作のチェック ポイント

CC モードの動作については、次の点に注意する必要があります。

表 *27 : CC* モードの動作のチェック ポイント

機能	説明
リンク暗号化	データ リンクの暗号化は、C91xx Wireless Mobility Express プラットフォームではサポートされていません。
リンク暗号化	C91xx Wireless Mobility Express プラットフォーム以外では、データ リンクの暗号化（ECDHE キーペアを使用）を有効にすると、APが継続的にフラッピングします。
LDAP	セキュア LDAP は強力な暗号をサポートしていないため、CC 認定に含まれていません。

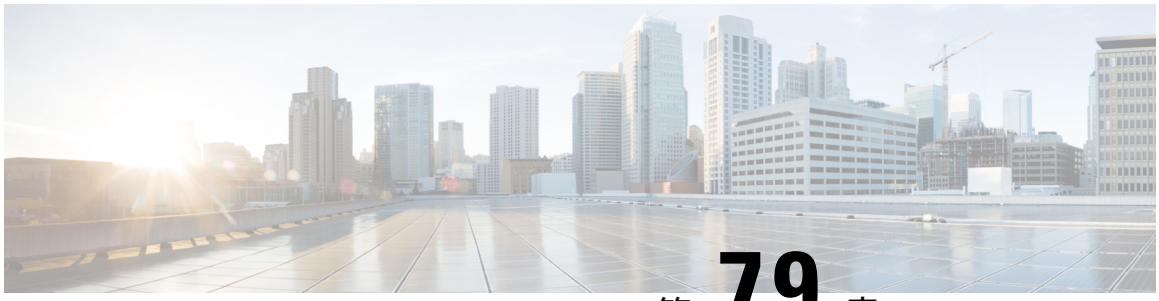
機能	説明
モビリティ	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ間のモビリティは、RSAベースのキーを持つワイヤレス管理トラストポイントとして LSC を使用して実現できます。
モビリティ	AireOS WLC と Cisco Catalyst 9800 シリーズ ワイヤレスコントローラ間のモビリティがサポートされています（ワイヤレス管理トラストポイントのSUDI証明書とMIC証明書を使用）。
モビリティ	AireOS WLC と Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ間のモビリティは、ワイヤレス管理トラストポイントの LSC 証明書を使用した場合はサポートされません。
CC モード	**show wireless certification config** コマンドは、WLANCC、AP-dtls-ciphersuite、または AP-dtls-version に設定された値を表示します。これらのパラメータを再設定した後はリロードする必要があります。
CC モード	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが CC モードで動作している場合、AES128-SHA オプションは AP-dtls-ciphersuite でサポートされません。
CC モード	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが FIPS モードで動作している場合は、AES128-SHA オプションが AP-dtls-ciphersuite でサポートされます。
CC モード	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラを CC モードで動作させる場合は、FIPS モードと CC モードの両方を有効にする必要があります。
LSC	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと LSC サーバの間でセキュアな通信を確保するには、ESTCA を LSC サーバとして展開する必要があります（これにより、TLS を使用して関連する通信が保護されます）。
LSC	Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、LSC サーバとの通信を保護する HTTPS をサポートしていません。

機能	説明
LSC	AP は関連する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが CC モードで動作している場合にのみ、LSC のプロビジョニング時に EC ベースのキーを生成します。
LSC	AP は関連する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが FIPS モードで動作している場合、LSC のプロビジョニング時に RSA ベースのキーを生成します。
LSC	AP は関連する Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが非 FIPS モードまたは非 CC モードで動作している場合、LSC のプロビジョニング時に RSA ベースのキーを生成します。
パスワードの難読化	パスワードの難読化には、次のコマンドを使用できます。 • **key config-key password-encrypt** • **service password-encryption** • **password encryption aes** • **passwd key obfuscate**
CC モード	**wlancc** ステータスを変更すると、AP はただちにリロードします。
FIPS モード	FIPS ステータスを変更しても、AP がただちにリロードすることはありません。
Cisco 1562 AP	Cisco 1562 AP が Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続できるようにするには、AP のイーサネット MAC をユーザ名リストに含める必要があります。
AP シリアル番号認証	シリアル番号認証が可能なのは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが FIPS モードおよび CC モードで、LSC ベースのトラストポイント/証明書（SUDI トラストポイントではない）を使用した場合のみです。

機能	説明
ディスプレー	FIPS適合性は、コントローラがCCモードで、LSC証明書に互換性がある場合にのみ**Suitable**と表示されます。ワイヤレス管理と証明書CNの両方で、コントローラのホスト名と、使用されている RSA キー（2048 以上）または EC キーの長さが一致する必要があります。
RADSEC	FIPS モードまたは CC モードで動作している場合、RSA キーサイズが（RADSECに基づいて証明書の）2048 ビット以上である必要があります。それ以外の場合、RADSEC は失敗します。

第 VII 部

モビリティ



第 79 章

モビリティ

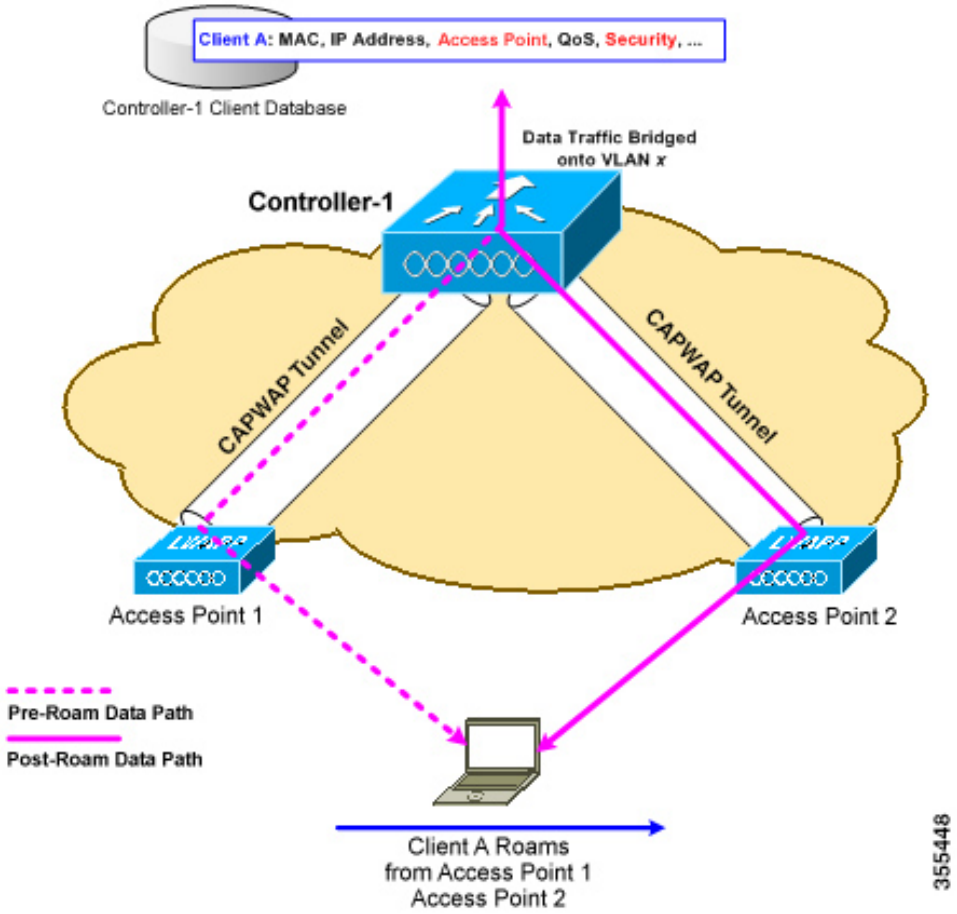
モビリティの概要

モビリティまたはローミングは、ワイヤレス LAN クライアントができるだけ低遅延で、あるアクセス ポイントから別のアクセス ポイントへの確実かつスムーズなアソシエーションを維持する機能です。この項では、コントローラが無線ネットワークに存在する場合のモビリティの動作について説明します。

あるワイヤレス クライアントがアクセス ポイントにアソシエートして認証すると、アクセス ポイントのコントローラは、クライアントデータベースにそのクライアントに対するエントリを設定します。このエントリには、クライアントの MAC アドレス、IP アドレス、セキュリティ コンテキストおよびアソシエーション、Quality of Service（QoS）コンテキスト、WLAN、およびアソシエートされたアクセスポイントが含まれます。コントローラはこの情報を使用してフレームを転送し、ワイヤレス クライアントとの間のトラフィックを管理します。

図 *16 :* コントローラ内ローミング

この図には、同一のコントローラに接続されている 2 つのアクセス ポイント間をワイヤレス クライアントがローミングする様子が示されています。

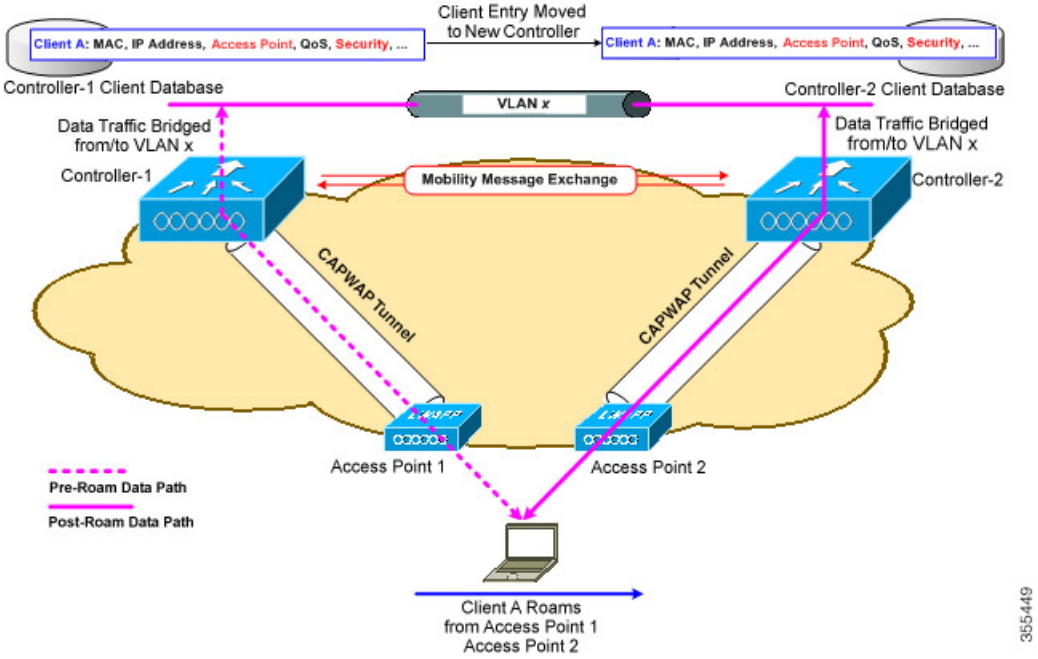


ワイヤレス クライアントがそのアソシエーションをあるアクセス ポイントから別のアクセス ポイントに移動する場合、コントローラはクライアントのデータベースを新たにアソシエートされたアクセス ポイントでアップデートするだけです。必要に応じて、新たなセキュリティ コンテキストとアソシエーションも確立されます。

しかし、クライアントが 1 つのコントローラに join されたアクセス ポイントから別のコントローラに join されたアクセス ポイントにローミングする際には、プロセスはより複雑になります。また、同一のサブネット上でこれらのコントローラが動作しているかどうかによっても異なります。

図 *17* : コントローラ間ローミング

次の図は、コントローラのワイヤレス LAN インターフェイスが同じ IP サブネット上に存在する場合に発生するコントローラ間ローミングを表したものです。



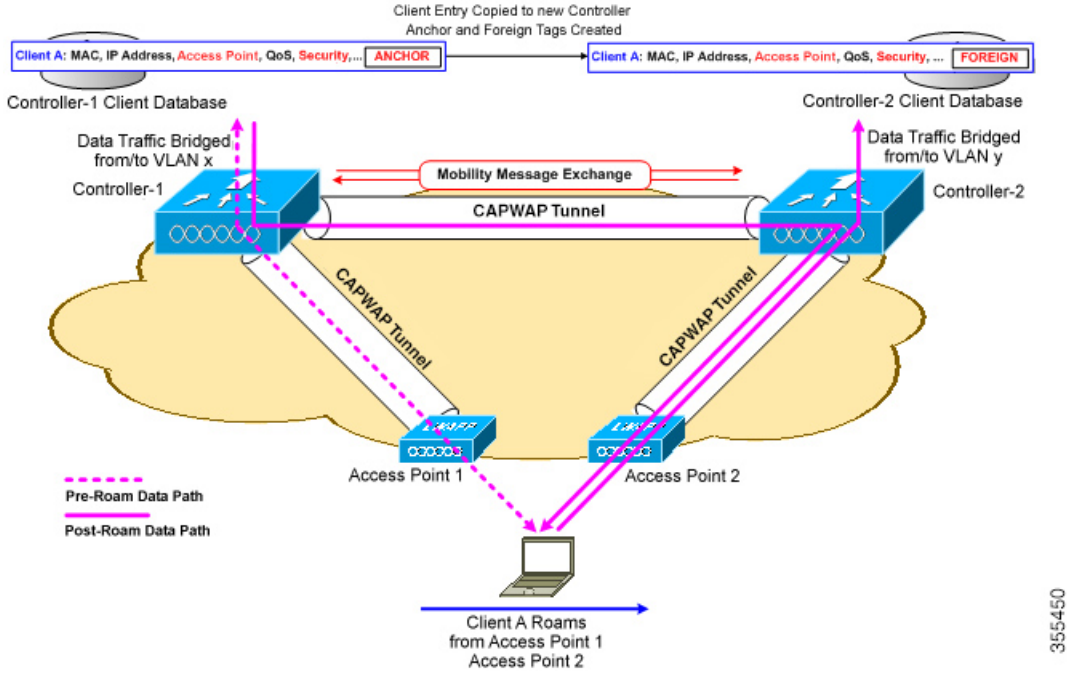
新たなコントローラに関連付けられているアクセスポイントにクライアントが接続すると、そのコントローラはモビリティメッセージを元のコントローラと交換し、クライアントのデータベース エントリが新たなコントローラに移動されます。新たなセキュリティ コンテキストとアソシエーションが必要に応じて確立され、クライアントのデータベース エントリは新たなアクセス ポイントに対してアップデートされます。このプロセスは、ユーザには透過的に行われます。

（注） 802.1X/Wi-Fi Protected Access（WPA）セキュリティで設定したすべてのクライアントは、IEEE 標準に準拠するために完全な認証を行います。

重要 サブネット間ローミングは SDA ではサポートされていません。

図 *18* : サブネット間ローミング

次の図は、コントローラのワイヤレス LAN インターフェイスが異なる IP サブネット上に存在する場合に発生するサブネット間ローミングを表したものです。



サブネット間ローミングは、コントローラがクライアントのローミングに関するモビリティメッセージを交換する点でコントローラ間ローミングと似ています。ただし、クライアントのデータベースエントリが新しいコントローラに移動されるのではなく、元のコントローラのクライアントデータベース内で該当クライアントにアンカーエントリのマークが付けられます。このデータベースエントリが新しいコントローラのクライアントデータベースにコピーされ、新しいコントローラでフォーリンエントリのマークが付けられます。ローミングはワイヤレスクライアントには透過的なまま行われ、クライアントは元の IP アドレスを保持します。

サブネット間ローミングでは、アンカー コントローラとフォーリン コントローラの両方の WLAN に同一のネットワーク アクセス権限を設定する必要があります。ソースベースのルーティングやソースベースのファイアウォールは設定しないでください。そのようにしない場合、ハンドオフ後クライアントにネットワーク接続上の問題が発生することがあります。

コントローラと RADIUS サーバを使用した静的アンカー セットアップでは、VLAN と QoS を動的に割り当てる AAA オーバーライドが有効になっている場合、フォーリン コントローラがレイヤ 2 認証（802.1x）後に適切な VLAN を使用してアンカー コントローラを更新します。レイヤ 3 RADIUS 認証の場合、認証の RADIUS 要求は、アンカー コントローラによって送信されます。

（注） Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ のモビリティ トンネルは、制御パス（UDP 16666）およびデータ パス（UDP 16667）を使用する CAPWAP トンネルです。デフォルトで、制御パスは DTLS で暗号化されます。データ パスの DTLS は、モビリティ ピアを追加する場合に有効化できます。

関連トピック

無線ゲスト アクセス （1119 ページ）

SDA ローミング

SDA では、他にも 2 つのローミング タイプ（xTR 内と xTR 間）がサポートされています。SDA において、xTR はアクセス スイッチ（ファブリック エッジ ノード）を意味し、入力トンネル ルータと出力トンネル ルータの両方の機能を果たします。

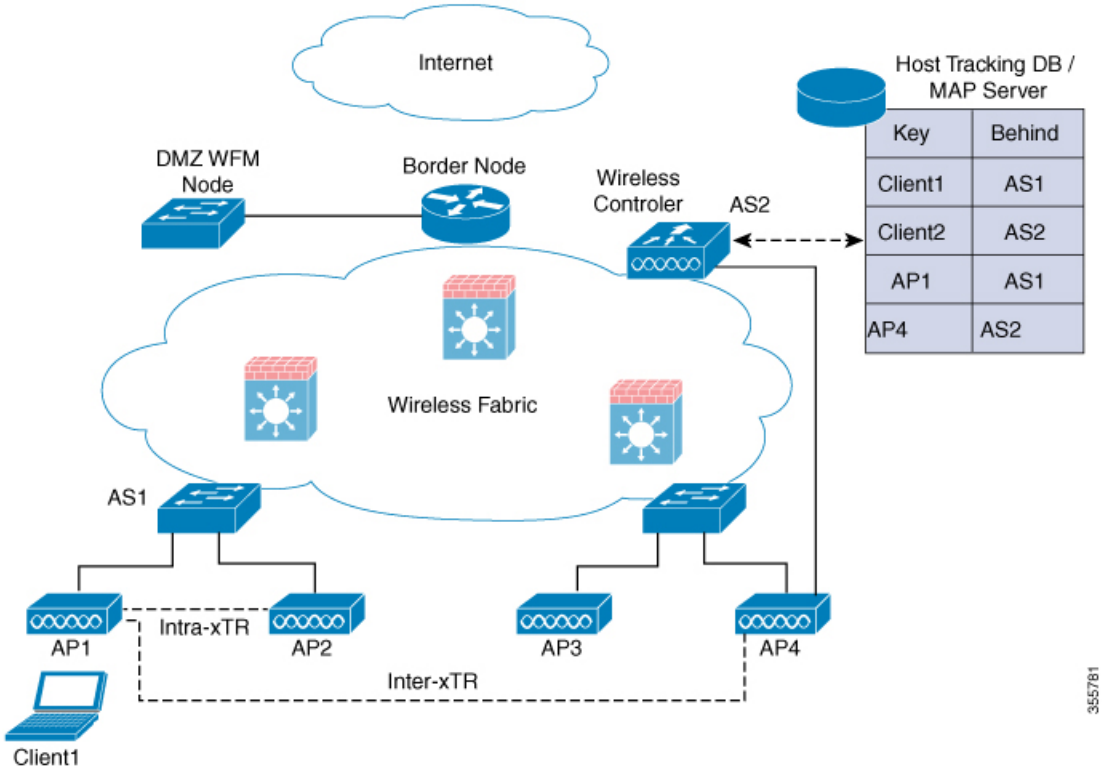
ファブリックが有効になっている WLAN 上のクライアントが同じアクセス スイッチ上のアクセス ポイント間で行うローミングは、xTR 内ローミングと呼ばれます。この場合、ローカルのクライアント データベースとクライアント履歴テーブルは、新たに関連付けられたアクセス ポイントの情報で更新されます。

ファブリックが有効になっている WLAN 上のクライアントがアクセス スイッチが異なるアクセス ポイント間で行うローミングは、xTR 間ローミングと呼ばれます。この場合は、マップ サーバもクライアント ロケーション（RLOC）情報で更新されます。また、ローカルのクライアント データベースが、新たに関連付けられたアクセス ポイントの情報で更新されます。

図 *19 : SDA* ローミング

次の図は、クライアントが 1 つのアクセス ポイントから同じスイッチ上の別のアクセス ポイント、またはファブリック トポロジ内の異なるスイッチ上のアクセス ポイントに移動すると

きに発生する、xTR 間ローミングと xTR 内ローミングを示しています。



モビリティ関連の用語の定義

- 接続ポイント：ステーションの接続ポイントは、ネットワークへの接続時にデータ パスが最初に処理される場所です。現在サービスを提供しているアクセス スイッチ、またはコントローラがこれに該当します。
- Point of Presence：ステーションの Point of Presence は、ステーションがアドバタイズされているネットワーク内の場所です。たとえば、アクセス スイッチがルーティング プロトコルを介してステーションへ到達可能性をアドバタイズしている場合、ルートがアドバタイズされているインターフェイスはステーションの Point of Presence と見なされます。
- ステーション：ネットワークに接続し、ネットワークからサービスを要求するユーザデバイス。

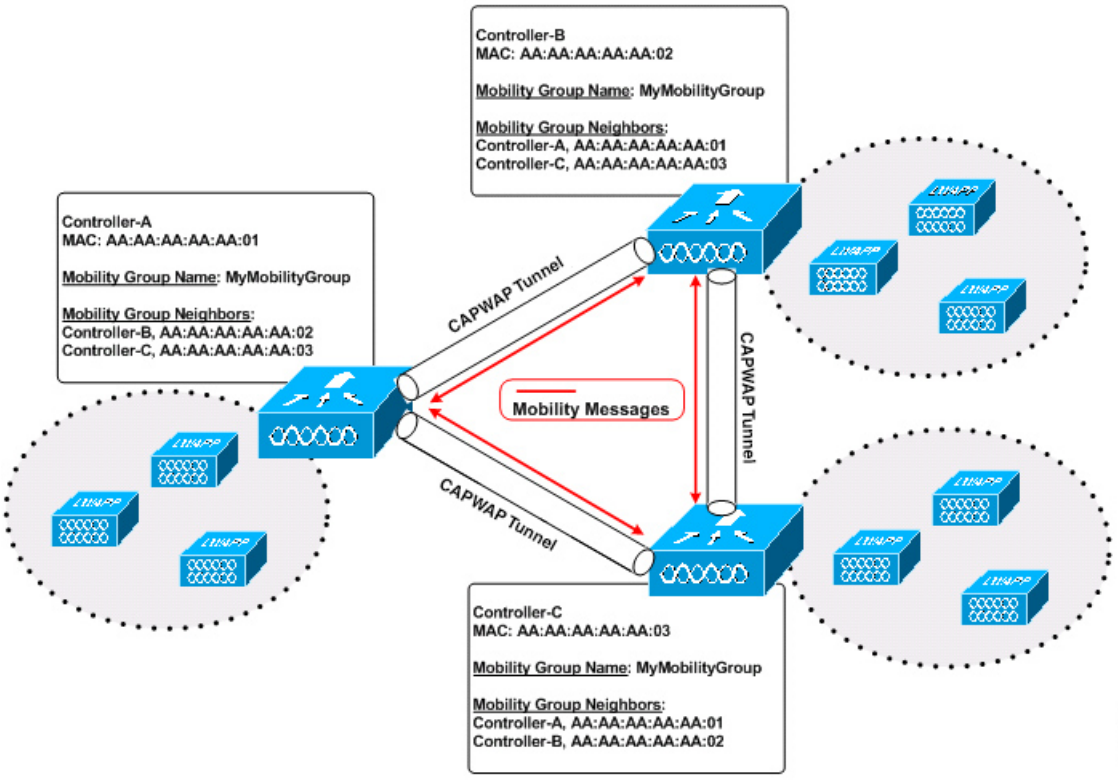
モビリティ グループ

モビリティ グループは、同じモビリティ グループ名で定義されるコントローラのセットで、ワイヤレス クライアントのローミングをシームレスに行う範囲を定義します。モビリティ グループを作成することで、コントローラ間またはサブネット間のローミングが発生した際に、ネットワーク内の複数のコントローラが動的に情報を共有してデータ トラフィックを転送できるようになります。同じモビリティ グループ内のコントローラは、相互のアクセス ポイントを不正なデバイスとして認識しないように、クライアントデバイスのコンテキストと状態およ

びアクセス ポイントのリストを共有できます。この情報を使用して、ネットワークはコントローラ間のワイヤレス LAN ローミングとコントローラの冗長性をサポートできます。

（注） AP がコントローラ間を移動する際（両方のコントローラがモビリティ ピアの場合）、移動前に最初のコントローラに関連付けられていたクライアントは、移動後も最初のコントローラにアンカーされる可能性があります。このような状況を防ぐには、コントローラのモビリティ ピア設定を削除します。

図 *20 :* 単一のモビリティ グループの例



上の図に示すように、各コントローラはモビリティ グループの他の一連のメンバーとともに設定されています。新たなクライアントがコントローラに join されると、コントローラはユニキャスト メッセージ（または、モビリティ マルチキャストが設定されている場合はマルチキャスト メッセージ）をそのモビリティ グループの全コントローラに送信します。クライアントが以前に接続されていたコントローラは、クライアントのステータスを送信します。

注意事項および制約事項

- 次の AireOS および Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ プラットフォームが、SDA コントローラ間モビリティ（AireOS コントローラから Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ）でサポートされています。

AireOS

- Cisco 3504
- Cisco 5520
- Cisco 8540

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

- クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ
- Cisco Catalyst 9800-40 ワイヤレス コントローラ

- 次のコントローラ プラットフォームが SDA コントローラ間モビリティでサポートされています。

Catalyst スイッチ

- Cisco 9300

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ

- クラウドの Cisco Catalyst 9800 ワイヤレス コントローラ
- Cisco Catalyst 9800-40 ワイヤレス コントローラ

- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと AireOS のデータ DTLS 設定が同じであることを確認してください。Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは設定の不一致がサポートされないため、モビリティ データ パスがダウンします。
- コントローラ間ローミングのシナリオでは、WLAN とポリシー プロファイルの設定が両方のコントローラで同一である必要があります。
- ポリシー プロファイルに含まれるポリシー プロファイル名およびクライアント VLAN が、同じ WLAN プロファイルがマッピングされているコントローラ間で異なる場合があります。
- コントローラ内ローミングのシナリオでは、WLAN がマッピングされた同じポリシー プロファイル間でクライアント ローミングがサポートされます。
- モビリティ トンネルでは、データ DTLS と SSC ハッシュ キーがメンバー間で同一である必要があります。
- クライアントが Web 認証状態でローミングすると、モバイル クライアントではなく、別のコントローラ上の新しいクライアントと見なされます。
- モビリティ ピアのコントローラは、同じ DHCP サーバを使用して、VLAN 内でのクライアント モビリティ移動カウントを更新する必要があります。
- モビリティ移動カウントは、コントローラ間ローミング時にのみクライアントの詳細で更新されます。コントローラ内ローミングは、クライアント統計情報とモビリティ履歴で確認できます。

- モビリティでは、IPv4 アドレスの放射性トレースはサポートされていません。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのアンカー VLAN は、Cisco AireOS コントローラではアクセス VLAN として表されます。
- クライアントがローミングしている間、そのモビリティ ロールは Unknown と表示されます。これは、ローミング クライアントが IP 学習状態にあるためです。このようなシナリオでは、多数のクライアントが新しいインスタンスに追加され、古いインスタンスでは削除されます。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラと Cisco AireOS コントローラの間では、IPv4 トンネルのみがサポートされています。
- HA シナリオでは、MAC アドレスを使用してワイヤレス モビリティを明示的に設定してください。設定しないと、SSO 後にモビリティ トンネルがダウンします。

モビリティの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Mobility]** を選択します。
[Wireless Mobility] ページが表示され、グローバル設定とピア設定を実行できます。

ステップ 2 [Global Configuration] セクションで次のタスクを実行します。

a) モビリティ グループの名前を入力します。
b) モビリティ グループのマルチキャスト IP アドレスを入力します。
c) [Keep Alive Interval] フィールドで、モビリティ リスト メンバーに ping 要求を送信する回数を指定します。この回数を超えると、メンバーは到達不能と判断されます。有効な範囲は 3 ～ 20 で、デフォルト値は 3 です。
d) [Mobility Keep Alive Count] で、モビリティ リスト メンバーへの ping 要求の送信間隔を秒単位で指定します。有効な範囲は 1 ～ 30 秒です。
e) モビリティ グループの DSCP 値を入力します。
f) モビリティ MAC アドレスを入力します。
g) [Apply] をクリックします。

ステップ 3 [Peer Configuration] タブで、次のタスクを実行します。

a) [Mobility Peer Configuration] セクションの [Add] をクリックします。
b) 表示される [Add Mobility Peer] ウィンドウで、モビリティ ピアの IP アドレスを入力します。
c) また、NAT を使用する場合は、任意のパブリック IP アドレスを入力してモビリティ ピアの NATed アドレスを入力します。NAT を使わない場合、パブリック IP アドレスは使用されず、デバイスにはモビリティ ピアの直接 IP アドレスが表示されます。
d) モビリティ ピアを追加するモビリティ グループを入力します。
e) [Data Link Encryption] に必要なステータスを選択します。

f) 必要に応じて [SSC Hash] を指定します。
g) [Save & Apply to Device] をクリックします。
h) [Non-Local Mobility Group Multicast Configuration] セクションの [Add] をクリックします。
i) モビリティ グループ名を入力します。
j) モビリティ グループのマルチキャスト IP アドレスを入力します。
k) **[保存（Save）]** をクリックします。

モビリティの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility group name** *group-name* 例： `Device(config)# wireless mobility group name Mygroup`	**Mygroup** という名前のモビリティ グループを作成します。
ステップ 2	**wireless mobility mac-address** *mac-addr* 例： `Device(config)# wireless mobility mac-address 00:0d:ed:dd:25:82`	モビリティ メッセージで使用される MAC アドレスを設定します。
ステップ 3	**wireless mobility dscp** *value-0-to-63* 例： `Device(config)# wireless mobility dscp 10`	（任意）モビリティ コントローラ間の DSCP 値を設定します。
ステップ 4	**wireless mobility group keepalive interval** *time-in-seconds* 例： `Device(config)# wireless mobility group keepalive interval 5`	（任意）モビリティ メンバーに送信される 2 つのキープアライブの間隔を設定します。有効な範囲は 1 ～ 30 秒です。 （注） モビリティ トンネルを介して接続されているコントローラの場合は、両方のコントローラのキープアライブ間隔値が同じであることを確認します。
ステップ 5	**wireless mobility group keepalive count** *count* 例：	（任意）メンバーのステータスがDOWNに移行するまでのキープアライブ再試行回数を設定します。

	コマンドまたはアクション	目的
	`Device(config)# wireless mobility group keepalive count 3`	
ステップ 6	次のオプションを使用して、IPv4 または IPv6 を設定します。 • **wireless mobility mac-address** *mac-address* **ip** *peer-ip-address* **group** *group-name***data-link-encryption** • **wireless mobility mac-address** *mac-address* **ip** *peer-ip-address* **public-ip** *public-ip-address* **group** *group-name* 例： `Device(config#) wireless mobility mac-address 001E.BD0C.5AFF ip 9.12.32.10 group test-group data-link-encryption` `Device(config#) wireless mobility mac-address 001E.BD0C.5AFF ip fd09:9:2:49::55 public-ip fd09:9:2:49::55 group scalemobility`	特定のグループにピア IPv4 または IPv6 アドレスを追加します。 ローカル グループからピアを削除するには、このコマンドの **no** 形式を使用します。
ステップ 7	**wireless mobility multicast** {**ipv4** | **ipv6** }*ip-address* or **wireless mobility group multicast-address** *group-name* {**ipv4** | **ipv6** } *ip-address* 例： `Device(config)# wireless mobility multicast ipv4 224.0.0.4` 例： `Device(config)# wireless mobility group multicast-address Mygroup ipv4 224.0.0.5`	（任意）ローカル モビリティ グループまたは非ローカル モビリティ グループのマルチキャスト IPv4 または IPv6 アドレスを設定します。 （注） **モビリティ マルチキャスト**：コントローラはクライアントの接続時またはローミング時に、ユニキャスト メッセージではなくマルチキャスト メッセージをモビリティ ローカル グループまたは非ローカル グループの全メンバーに送信します。 ローカル モビリティ グループのマルチキャスト IPv4 アドレスとして 224.0.0.4 を設定します。 非ローカル モビリティ グループのマルチキャスト IPv4 アドレスとして 224.0.0.5 を設定します。

リリース間コントローラ モビリティの設定

リリース間コントローラモビリティ（IRCM）は、異なるソフトウェアリリースを実行しているコントローラ間のインターワーキングを可能にする機能セットです。IRCMは、Cisco AireOSおよびCisco IOSを実行しているコントローラ間（Cisco 8540 WLCからCisco Catalyst 9800シリーズ ワイヤレス コントローラなど）で、レイヤ2およびレイヤ3ローミング、ゲストアクセスまたはターミネーションなどの機能について、シームレスなモビリティおよびワイヤレスサービスを実現します。

コントローラでモビリティ ピアを設定するには、次の手順を実行します。

始める前に

- IPv6は、ファブリック クライアント ローミング用のSDA IRCMではサポートされていません。IPv6は、非ファブリック クライアント ローミング用のIRCMでサポートされています。
- 暗号化モビリティ機能をサポートするAireOSコントローラを使用していることを確認します。
- AVCはIRCMではサポートされていません。
- 混合展開では、WLANプロファイル名とポリシー プロファイル名が同じです。
- 混合展開では、AireOSコントローラがリリース8.5以降のリリースにアップグレードされ、Cisco Catalyst 9800シリーズ ワイヤレス コントローラと連携することを確認します。
- AireOSが暗号化モビリティでのモビリティ マルチキャストをサポートしていないため、モビリティ グループ マルチキャストはサポートされません。
- インスタンスで表示されるクライアント数の合計が、ローミング スケールでサポートされている数を超えている場合があります。この不整合は、クライアントのローミング レートが非常に高い場合に、システムがレコードを更新する時間を必要とすることで発生します。この場合、非常に短い時間に複数のwncdに表示されるクライアントが複数回カウントされています。show CLI、WebUI、DNAC、またはSNMPのいずれかの方法を使用する前に、プロセスで一貫性のあるデータを取得できる十分な時間を設けることを推奨します。
- リンク ローカル ブリッジングはサポートされていません。ピアAireOSコントローラでも無効にしてください。

次のクライアント機能は、AireOSコントローラとCisco Catalyst 9800シリーズ ワイヤレス コントローラの間のIPv6クライアント モビリティをサポートしています：アカウンティング、L3セキュリティ（Webauth）、ポリシー（ACLとQoS）、SLAACとDHCPv6を介したIPアドレスの割り当ておよび学習、Ipv6 ソース ガード、複数のIPv6アドレス学習、IPv6マルチキャスト、およびSISF IPv6機能（RAガード、RAスロットリング、DHCPv6ガード、およびND抑制）。

次の IPv6 機能は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラではサポートされていません。

- 設定可能な IPv6 タイマー
- AP での RA ガードの有効化
- IPv6 のグローバルな無効化

（注）
- IPv6 CWA は、AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの両方ではサポートされません。
- クライアントあたり最大 8 つの IPv6 アドレスのみがサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	次のオプションを使用して、IPv4 または IPv6 を設定します。 • **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip* **group** *group-name***data-link-encryption** • **wireless mobility group member mac-address** *mac-address* **ip** *peer-ip-address* **public-ip** *public-ip-address* **group** *group-name* 例： `Device(config#) wireless mobility group member mac-address 001E.BD0C.5AFF ip 9.12.32.10 group test-group data-link-encryption` `Device(config#) wireless mobility group member mac-address 001E.BD0C.5AFF ip fd09:9:2:49::55 public-ip fd09:9:2:49::55 group scalemobility`	特定のグループにピア IPv4 または IPv6 アドレスを追加します。 ローカル グループからピアを削除するには、このコマンドの **no** 形式を使用します。
ステップ 3	**wireless mobility group name** *group-name* 例： `Device(config#) wireless mobility group name test-group`	ローカルグループの名前を追加します。デフォルトのローカル グループ名は「default」です。

	コマンドまたはアクション	目的
ステップ 4	**wireless mobility mac-address** *mac-address* 例： `Device(config#) wireless mobility mac-address 000d.bd5e.9f00`	（任意）モビリティ メッセージで使用する MAC アドレスを設定します。
ステップ 5	**wireless mobility group member ip** *peer-ip* 例： `Device(config#) wireless mobility group member ip 9.12.32.15`	ローカル グループにピアを追加します。 ローカル グループからピアを削除するには、このコマンドの **no** 形式を使用します。
ステップ 6	**wireless mobility dscp** *dscp-value* 例： `Device(config#) wireless mobility dscp 52`	（任意）DSCP を設定します。デフォルト値は 48 です。
ステップ 7	**wireless mobility group keepalive count** *count* 例： `Device(config#) wireless mobility group keepalive count 10`	モビリティの制御パスおよびデータ パスのキープアライブ数を設定します。デフォルト値は 3 です。
ステップ 8	**wireless mobility group keepalive interval** *interval* 例： `Device(config#) wireless mobility group keepalive interval 30`	モビリティの制御パスおよびデータ パスのキープアライブ間隔を設定します。デフォルト値は 10 です。 （注） モビリティ トンネルを介して接続されているコントローラの場合は、両方のコントローラのキープアライブ間隔値が同じであることを確認します。

モビリティの確認

モビリティ マネージャの概要を表示するには、次のコマンドを使用します。

```
Device# show wireless mobility summary
```

モビリティ ピアの情報を表示するには、次のコマンドを使用します。

```
Device# show wireless mobility peer ip 10.0.0.8
```

モビリティ グループに認識されているアクセス ポイントのリストを表示するには、次のコマンドを使用します。

```
Device# show wireless mobility ap-list
```

モビリティ マネージャの統計情報を表示するには、次のコマンドを使用します。

クライアントのモビリティ情報を表示するには、次のコマンドを使用します。

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 detail
```

サブドメイン内のアクティブクライアントのローミング履歴を表示するには、次のコマンドを使用します。

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 mobility history
```

モビリティマネージャのクライアント固有の統計情報を表示するには、次のコマンドを使用します。

```
Device# show wireless client mac-address 00:0d:ed:dd:35:80 stats mobility
```

コントローラ間ローミングが成功したかどうかを確認するには、次のコマンドを使用します。

- **show wireless client mac** *mac-address* **detail**：（ローミング先のコントローラ）ローミングタイプは L2 と表示され、ローミング数が 1 増えます。
- **show wireless client summary**：（ローミング元のコントローラ）クライアントエントリは出力に含まれません。

SDA モビリティの確認

コントローラ内（xTR内）ローミングが成功したかどうかを確認するには、次のコマンドを使用します。

- **show wireless client summary**：クライアントが同じ xTR 上の AP 間でローミングした場合は、新しい AP が表示されます。
- **show wireless client mac** *mac-address* **detail**：ローミング前と同じ RLOC が表示されます。

コントローラ内（xTR間）ローミングが成功したかどうかを確認するには、次のコマンドを使用します。

- **show wireless fabric client summary**：クライアントが別の xTR 上の AP にローミングした場合は、新しい AP が表示されます。
- **show wireless client mac** *mac-address* **detail**：クライアントがローミングした新しい xTR の RLOC が表示されます。

コントローラ内ローミング前後のクライアントステータスを確認するには、次の手順を実行します。

1. コントローラで **show wireless client summary** コマンドを使用して、クライアントが古い AP 上にあるかどうかを確認します。

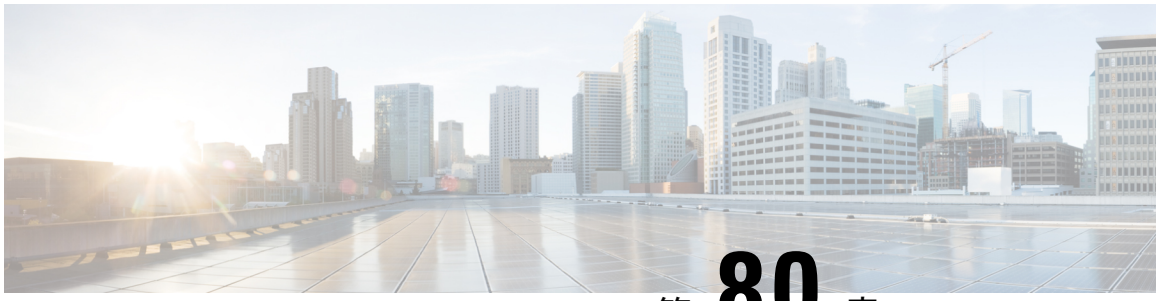
2. xTR1 で **show mac addr dyn** コマンドを使用して、クライアント MAC が古い AP に対してリストされているかどうかを確認します。
3. MAP サーバで **show lisp site detail** コマンドを使用して、クライアント IP が現在の xTR1 から登録され、クライアント MAC が現在の xTR1 と WLC1 の両方から登録されているかどうかを確認します。
4. WLC 内ローミングの後、クライアントが新しい AP 上にあるかどうかを確認するには、WLC1 および xTR1 で **show wireless client summary** コマンドと **show mac addr dyn** コマンドを使用します。
5. xTR 間ローミング（古い AP と新しい AP の xTR が異なる）の後、クライアントが（新しい xTR2 に接続されている）新しい AP 上にあるかどうかを確認するには、WLC1 および xTR2 で **show wireless client summary** コマンドと **show mac addr dyn** コマンドを使用します。
6. MAP サーバで **show lisp site detail** コマンドを使用して、クライアントが新しい xTR2 から登録されているかどうかを確認します。

SDA 用 MAP サーバでのローミングの確認

SDA のローミング情報を確認するには、次のコマンドを使用します。

ローミングの前後に MAP サーバで次のコマンドを実行し、クライアント IP が現在の xTR から登録され、クライアント MAC が現在の xTR と WLC の両方から登録されているかどうかを確認します。

```
Device# show lisp site detail
```



第 80 章

スタティック IP クライアント モビリティ

スタティック IP クライアント モビリティについて

ワイヤレス クライアントのスタティック IP アドレスの設定が必要になる場合があります。これらのワイヤレス クライアントは、ネットワーク内で移動するときに他のコントローラとの関連付けを試みる可能性があります。クライアントが、固定 IP と同じサブネットをサポートしないコントローラにアソシエートしようとすると、クライアントはネットワーク接続に失敗します。ただし現在は、スタティック IP アドレスを持つクライアントに対してスタティック IP モビリティを有効化できるようになりました。

スタティック IP アドレスを持つスタティック IP クライアントは、同じモビリティ グループ内の別のコントローラへのトラフィックをトンネリングすることで、クライアントのサブネットがサポートされている他のコントローラにアソシエートできます。この機能により、クライアントがスタティック IP アドレスを使用していてもネットワークが処理されるように WLAN を設定できます。

関連トピック

無線ゲスト アクセス （1119 ページ）

機能制限

- この機能はファブリックおよびスイッチ用の Cisco Catalyst 9800 ワイヤレス コントローラ プラットフォームではサポートされません。
- IPv6 はサポートされていません。
- FlexConnect モードはサポートされていません。

- WebAuth（LWA と CWA）はサポートされていません。
- オープン認証、Dot1x 認証、および PSK 認証メカニズムのみがサポートされます。
- モビリティ アンカー設定を含まない WLAN でのみサポートされます。モビリティ アンカーがすでに WLAN に設定されていて、スタティック IP モビリティが有効になっている場合、この機能はサポートされません。
- 有効になっているスタティック IP モビリティにすべてのピアが設定されている場合にのみサポートされます。
- IRCM はサポートされません。

スタティック IP クライアント モビリティの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞ を選択します。

ステップ 2 [Policy] ページで、ポリシー プロファイル名をクリックするか、[Add] をクリックして新しく作成します。

ステップ 3 [Mobility] タブをクリックします。

ステップ 4 [Static IP Mobility] フィールドを [Enabled] 状態に設定します。

ステップ 5 [Update & Apply to Device] をクリックします。

スタティック IP クライアント モビリティの設定（CLI）

スタティック IP クライアント モビリティを設定するには、次の手順に従います。

始める前に

- ネットワーク内の少なくとも 1 台のピア コントローラで、スタティック IP クライアントに対応するように SVI インターフェイス（L3 VLAN インターフェイス）を設定します。
- クライアントがコントローラに接続するには、デバイスで（ポリシープロファイル設定の VLAN 番号に基づいて）VLAN が設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-policy-name* 例： `Device(config)# wireless profile policy static-ip-policy`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**static-ip-mobility** 例： `Device(config-wireless-policy)# static-ip-mobility`	スタティック IP モビリティを有効にします。

スタティック IP クライアント モビリティの確認

次のコマンドを使用して、スタティック IP クライアント モビリティの設定を確認します。

```
Device# show wireless profile policy detailed static-ip-policy


Policy Profile Name           : static-ip-policy
Description                   :
Status                        : DISABLED
VLAN                          : 1
Wireless management interface VLAN        : 34
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
WLAN Switching Policy
  Central Switching           : ENABLED
  Central Authentication      : ENABLED
  Central DHCP                : DISABLED
  Flex NAT PAT            : DISABLED
  Central Assoc               : DISABLED
WLAN Flex Policy
  VLAN based Central Switching          : DISABLED
WLAN ACL
  IPv4 ACL                    : Not Configured
  IPv6 ACL                    : Not Configured
  Layer2 ACL                  : Not Configured
  Preauth urlfilter list      : Not Configured
  Postauth urlfilter list     : Not Configured
WLAN Timeout
  Session Timeout             : 1800
  Idle Timeout                : 300
  Idle Threshold              : 0
WLAN Local Profiling
  Subscriber Policy Name      : Not Configured
  RADIUS Profiling            : DISABLED
  HTTP TLV caching            : DISABLED
```

```
  DHCP TLV caching            : DISABLED
WLAN Mobility
  Anchor                      : DISABLED
AVC VISIBILITY                : Disabled
Flow Monitor IPv4
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
Flow Monitor IPv6
  Flow Monitor Ingress Name   : Not Configured
  Flow Monitor Egress Name    : Not Configured
NBAR Protocol Discovery       : Disabled
Reanchoring                   : Disabled
Classmap name for Reanchoring
  Reanchoring Classmap Name   : Not Configured
QOS per SSID
  Ingress Service Name        : Not Configured
  Egress Service Name         : Not Configured
QOS per Client
  Ingress Service Name        : Not Configured
  Egress Service Name         : Not Configured
Umbrella information
  Ciso Umbrella Parameter Map : Not Configured
Autoqos Mode                  : None
Call Snooping                 : Disabled
Fabric Profile
  Profile Name                : Not Configured
Accounting list
  Accounting List               : Not Configured
DHCP
  required                    : DISABLED
  server address              : 0.0.0.0
 Opt82
  DhcpOpt82Enable             : DISABLED
  DhcpOpt82Ascii              : DISABLED
  DhcpOpt82Rid                : DISABLED
  APMAC                       : DISABLED
  SSID                        : DISABLED
  AP_ETHMAC                   : DISABLED
  APNAME                      : DISABLED
  POLICY TAG                  : DISABLED
  AP_LOCATION                 : DISABLED
  VLAN_ID                     : DISABLED
Exclusionlist Params
  Exclusionlist               : ENABLED
  Exclusion Timeout           : 60
AAA Policy Params
  AAA Override                : DISABLED
  NAC                         : DISABLED
  AAA Policy name             : default-aaa-policy
WGB Policy Params
  Broadcast Tagging           : DISABLED
  Client VLAN                 : DISABLED
Mobility Anchor List
  IP Address                                  Priority
  -------------------------------------------------------------
```

```
Device# show run | section profile policy

wireless profile policy default-policy-profile
 central switching
 description "default policy profile"
 static-ip-mobility
 vlan 50
 no shutdown
```

第 VIII 部

ハイ アベイラビリティ

第 81 章

ハイ アベイラビリティ

ハイ アベイラビリティについて

ハイ アベイラビリティ（HA）によって、コントローラのフェールオーバーが原因で生じるワイヤレス ネットワークのダウンタイムを短縮することができます。

2 台のコントローラが障害保護のために 2 つの個別の Cisco Unified Computing System（UCS）ボックスに導入され、1：1（アクティブ：スタンバイ）の冗長性を形成します。アクティブな UCS ボックスに障害が発生すると、スイッチオーバーが行われてスタンバイがアクティブになります。

2 台のコントローラは、1 つの管理 IP アドレスを持つ単一ノードとして管理される仮想シャーシを形成します。アクティブ ボックスが IP アドレスを所有しています。これは、管理 IP への接続が常にアクティブボックスに到達することを意味します。コントローラ内のすべてのインターフェイスは、仮想ネットワーク インターフェイス コントローラ（vNIC）です。

（注） iOS は DHCP アドレスと同期しません。同期がサポートされている場合も、スタンバイ SVI インターフェイスには異なる MAC アドレスがあり、DHCP サーバはアクティブになるために割り当てられた同一の IP を提供しません。

スタンバイ ボックスは、アクティブ ボックスがカバーする同一の設定（すべてのインターフェイスを含む）をカバーします。同じインターフェイスセットが、スイッチオーバー後も保持されます。つまり、スタンバイ ボックスのインターフェイス状態はアクティブ ボックスでの同じ状態を反映します。たとえば、インターフェイスがアクティブ ボックスでアップ状態の場合、スイッチオーバー後の新しいアクティブ ボックスでもアップ状態になります。

（注） アクティブ ボックスとスタンバイ ボックスは、同じインターフェイス名でペアリングする必要があります。

（注） スタティック IP アドレッシングはスタンバイに同期できますが、スタンバイ コントローラの IP アドレスを使用することはできません。

アクティブ ボックスとスタンバイ ボックスは、どちらも専用 HA ポートを使用して 2 台のコントローラ間でHA トラフィックを送信します。「ハイ アベイラビリティ」の項で説明されているように、**chassis ha-interface <x>** コマンドを実行して、専用 HA ポートを設定します。HA ポートは、次の機能を提供します。

- IOSd が起動する前に、2 台の UCS ボックス間の通信を有効にする。
- ロールの選択やキープアライブなどの HA 制御メッセージを転送する。
- 2 台の UCS ボックス間に IPC のトランスポートを提供する。

（注） 専用 HA ポートを 1 GB インターフェイスにのみマッピングできます。

これにより、コントローラの 1：1 HA モデルが 2 台の UCS ボックスで実行されます。

（注） HA ポートには、SFP 接続または RJ-45 接続のいずれかを選択できます。

次の Cisco SFP がサポートされています。

- GLC-SX-MMD
- GLC-LH-SMD

SFP 接続または RJ-45 接続のいずれかが存在する場合、HA は 2 台の UCS ボックス間で機能します。

SFP HA 接続は、RJ-45 HA 接続よりも優先されます。RJ-45 HA の稼働中に SFP が接続されると、HA ペアがリロードされます。リロードは、SFP 間のリンクが接続されていない場合も発生します。

IPv4 および IPv6 マルチキャスト

IPv4 マルチキャストと IPv6 マルチキャストはどちらも HA 対応です。IGMP スヌーピングの場合、マルチキャスト グループとメンバーシップがアクティブ ボックスで作成および管理されます。その後、マルチキャスト パケットがスヌーピングされて処理されます。同じマルチキャスト グループおよびメンバーシップがスタンバイ ボックスと同期され、再作成されてデータ プレーンに組み込まれます。各マルチキャスト グループのレプリケーション リスト（CAPWAP インターフェイス）を組み込む必要がありますので注意してください。スイッチオーバー後も、マルチキャスト パケットはグループのすべてのクライアントに到達します。

AP SSO

AP SSO では、必要に応じて次の機能が提供されます。

- アクティブ ボックスからスタンバイ ボックスの永続メモリにライブ AP の状態を同期する。
- スタンバイ ボックスのデータ プレーンに AP の状態を組み込む。

SSO 後の状態は次のとおりです。

- AP のダウンタイムなし。
- AP は SSO を認識していない。

このように、AP は引き続き同様に動作します。SSO では、RUN 状態に達した AP のみが保持されます。

（注） すべての AP セッションと一時的な状態がスタンバイに同期されます。

クライアント SSO

クライアント SSO は、RUN 状態に達したクライアントに対してサポートされています。これは通常、クライアントが認証され、IP アドレスが取得された時点で行われます。

対応する受信側ハンドラは、次の場合に呼び出されます。

- クライアント SSO レコードがスタンバイ ボックスに同期された。
- スタンバイ ボックスで依存関係が解決された。

この時点で、関連するすべてのクライアント レコードがスタンバイに同期されると、クライアントの状態がデータプレーンに組み込まれます。

（注） スイッチオーバー後は、クライアントへの TCP 接続は保持されません。

関連トピック

無線ゲスト アクセス （1119 ページ）

ハイ アベイラビリティの前提条件

外部インターフェイスと IP

すべてのインターフェイスはアクティブ ボックスでのみ設定されますが、スタンバイ ボックスと同期されるため、両方のコントローラで同じインターフェイスセットが設定されます。外部ノードの場合は、接続されているコントローラに関係なく、インターフェイスが同じ IP アドレスに接続します。

このため、モビリティ グループ内の AP、クライアント、DHCP、Cisco Identity Services Engine（ISE）サーバ、および他のコントローラ メンバーは、常に同じ IP アドレスに接続します。SSO スイッチオーバーは、これらに対して透過的です。ただし、外部ノードからコントローラへの TCP 接続がある場合は、TCP 接続をリセットして再確立する必要があります。

HA インターフェイス

これは、HA転送用に予約された専用インターフェイスです。最初（IOSdが起動する前）にこのインターフェイスが起動するため、IPC 接続と HA ロール ネゴシエーションはどちらも、このインターフェイスを介してパケットの送信と同様に実行されます。

HA インターフェイスは次の目的で使用されます。

- IOSd が起動する前のコントローラ ペア間の接続を可能にする。
- コントローラ ペア全体での IPC トランスポートを可能にする。
- コントローラ ペア間で交換される制御メッセージ全体の冗長性を有効にする。制御メッセージには、HA ロールの解決、キープアライブ、通知、HA 統計情報などがあります。

（注） コントローラでブート変数を手動で設定する必要があります。詳細については、「コントローラでのブート変数の手動設定」の項を参照してください。

ハイ アベイラビリティの制約事項

- HA 接続では、IPv4 のみがサポートされます。
- 2つのHAインターフェイスを同じサブネット上に設定する必要があります。このサブネットをデバイス上の他のインターフェイスと共有することはできません。HA インターフェイスは、IP アドレスとして 10.10.10.x/24 ネットワークを使用することはできません。

- TCP セッションはスイッチオーバー後に保持されず、再確立する必要があるため、TCP セッションの状態を同期することはできません。
- RUN 状態に達していないクライアントはスイッチオーバー後に削除されるため、クライアント SSO の対象にはなりません。
- 統計情報テーブルはアクティブ コントローラからスタンバイ コントローラに同期されません。したがって、スイッチオーバー後に **show wireless stats ap discovery chassis active r0** コマンドを実行しても AP エントリは表示されません。
- コントローラの HA インターフェイスをホストする VM のマシン スナップショットはサポートされていません。これは、HA コントローラのクラッシュの原因となる可能性があります。
- モビリティ側の制約事項：
  - 完全なモビリティ状態に達していないクライアントは、SSO 後に削除されます。
- キャッシュ タイマーは、持続したままアクティブからスタンバイに同期される必要があります。同期後、アクティブ ボックスからの削除を容易にするために、スタンバイでアクティブ ボックスの値に 30 秒が加算されてタイマーが再開されます。SSO 中は、セッション タイムアウト値も持続されます。
- アプリケーション分類の大部分は、SSO 後に保持されない場合があります。
  - AVC の制限：スイッチオーバー後、スタンバイ ボックスへのコンテキスト転送または同期は行われず、新しいアクティブ フローを再学習する必要があります。AVC QoS は、分類が失敗した場合は有効になりません。
  - 音声ポリシーは RTP または RTCP プロトコルに基づいているため、スイッチオーバー後に音声コールを認識することはできません。
  - AVC の制限により、自動 QoS は有効ではありません。

コントローラでのブート変数の手動設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例**： `Device# 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	**boot system bootflash** *image_path* **例**：	ROMMON でブート イメージを設定します。

	コマンドまたはアクション	目的
	Device(config)# **boot system**	
ステップ 3	**config-register 0x2102** 例： Device(config)# **config-register 0x2102**	コンフィギュレーション レジスタを 0x2102 に設定します。
ステップ 4	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

高可用性の設定（GUI）

次の手順を実行して、選択したアクセス ポイントのハイ アベイラビリティ パラメータを設定できます。

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] > の順に選択します。

ステップ 2 AP 名をクリックします。[Edit AP] 画面が表示されます。

ステップ 3 [High Availability] タブをクリックします

ステップ 4 プライマリ コントローラの名前と管理 IP アドレス（IPv4/IPv6）を入力します。同様に、セカンダリ コントローラおよびターシャリ コントローラの名前と管理 IP アドレスを入力します。

ステップ 5 [AP Failover Priority] ドロップダウンリストから、使用可能なオプションのいずれかを選択します。次のオプションを使用できます。

- Low
- 中
- 高
- [Critical]

ステップ 6 [Update & Apply to Device] ボタンをクリックします。

ハイ アベイラビリティの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**chassis ha-interface GigabitEthernet** *num* **local-ip** *local-chassis-ip-addr network-mask* **remote-ip** *remote-chassis-ip-addr* 例： `Device# chassis ha-interface GigabitEthernet 2 local-ip 1.1.1.2 255.255.255.0 remote-ip 1.1.1.3`	シャーシHAインターフェイスを設定します。 （注） このコマンドは、冗長ペアの両方のデバイスで発行します。 • *num*：GigabitEthernet インターフェイス番号。有効な範囲は 0 ～ 32 です。 • *local-chassis-ip-addr*：ローカル シャーシ HA インターフェイスの IP アドレスを入力します。 • *network-mask*：ネットワーク マスクかプレフィックス長を /nn または A.B.C.D の形式で入力します。 • *remote-chassis-ip-addr*：リモート シャーシの IP アドレスを入力します。 （注） 変更を有効にするには、デバイスをリロードします。
ステップ 2	**chassis** *chassis-num* **priority** *chassis-priority* 例： `Device# chassis 1 priority 1`	指定されたデバイスのプライオリティを設定します。 （注） デバイスのプライオリティを変更すると、そのデバイスの設定が変更されることがあります。新しいデバイスのプライオリティは、次回のリブート後に有効になります。 • *chassis-num*：シャーシ番号を入力します。有効な範囲は 1 ～ 2 です。 • *chassis-priority*：シャーシのプライオリティを入力します。有効な範囲

	コマンドまたはアクション	目的
		は1～2です。デフォルト値は1です。 （注） 両方のデバイスが同時に起動すると、プライオリティが高いデバイスがアクティブになり、もう一方はスタンバイになります。両方のデバイスに同じプライオリティ値が設定されている場合、MACアドレスが小さいデバイスがアクティブとして機能し、そのピアがスタンバイとして機能します。 **chassis-num** の詳細を取得するには、**show chassis** コマンドを実行します。
ステップ3	**chassis timer peer-timeout** {*timeout* | **default**} 例： `Device# chassis timer peer-timeout 500`	ピア キープアライブ タイムアウト値を設定します。 （注） このコマンドの実行後にデバイスをリロードする必要はありません。また、このコマンドは両方のデバイスに同時に同じタイムアウト値を設定します。 *timeout*：ピア タイムアウト値を入力します。範囲は500ミリ秒～16秒です。デフォルトは500ミリ秒です。

ハイ アベイラビリティ設定の確認

HA設定の詳細を表示するには、次のコマンドを使用します。

```
Device# show romvar
ROMMON variables:
 LICENSE_BOOT_LEVEL =
 MCP_STARTUP_TRACEFLAGS = 00000000:00000000
 BOOTLDR =
 CRASHINFO = bootflash:crashinfo_RP_00_00_20180202-034353-UTC
 STACK_1_1 = 0_0
 CONFIG_FILE =
 BOOT =
bootflash:boot_image_test,1;bootflash:boot_image_good,1;bootflash:rp_super_universalk9.vwlc.bin,1;
```

```
RET_2_RTS =
SWITCH_NUMBER = 1
CHASSIS_HA_REMOTE_IP = 10.0.1.9
CHASSIS_HA_LOCAL_IP = 10.0.1.10
CHASSIS_HA_LOCAL_MASK = 255.255.255.0
CHASSIS_HA_IFNAME = GigabitEthernet2
CHASSIS_HA_IFMAC = 00:0C:29:C9:12:0B
RET_2_RCALTS =
BSI = 0
RANDOM_NUM = 647419395
```

AP またはクライアントの SSO 統計情報の確認

AP SSO の統計情報を表示するには、次のコマンドを使用します。

```
Device# show wireless stat redundancy statistics ap-recovery wnc all
AP SSO Statistics

Inst    Timestamp     Dura(ms)   #APs  #Succ  #Fail  Avg(ms)  Min(ms)  Max(ms)
-------------------------------------------------------------------------------
   0    00:06:29.042        98     34     34      0        2        1       35
   1    00:06:29.057        56     33     30      3        1        1       15
   2    00:06:29.070        82     33     33      0        2        1       13


Statistics:

WNCD Instance   : 0
No. of AP radio recovery failures          : 0
No. of AP BSSID recovery failures          : 0
No. of CAPWAP recovery failures            : 0
No. of DTLS recovery failures              : 0
No. of reconcile message send failed       : 0
No. of reconcile message successfully sent : 34
No. of Mesh BSSID recovery failures: 0
No. of Partial delete cleanup done : 0

WNCD Instance   : 1
No. of AP radio recovery failures          : 0
No. of AP BSSID recovery failures          : 0
No. of CAPWAP recovery failures            : 3
No. of DTLS recovery failures              : 0
No. of reconcile message send failed       : 0
No. of reconcile message successfully sent : 30
No. of Mesh BSSID recovery failures: 0
No. of Partial delete cleanup done : 0

WNCD Instance   : 2
No. of AP radio recovery failures          : 0
No. of AP BSSID recovery failures          : 0
No. of CAPWAP recovery failures            : 0
No. of DTLS recovery failures              : 0
No. of reconcile message send failed       : 0
No. of reconcile message successfully sent : 33
No. of Mesh BSSID recovery failures: 0
No. of Partial delete cleanup done : 0
```

クライアント SSO の統計情報を表示するには、次のコマンドを使用します。

```
Device# show wireless stat redundancy statistics client-recovery wncd all
Client SSO statistics
```

```
----------------------

WNCD instance  : 1
Reconcile messages received from AP                    : 1
Reconcile clients received from AP                     : 1
Recreate attempted post switchover                     : 1
Recreate attempted by SANET Lib                        : 0
Recreate attempted by DOT1x Lib                        : 0
Recreate attempted by SISF Lib                         : 0
Recreate attempted by SVC CO Lib                       : 1
Recreate attempted by Unknown Lib                      : 0
Recreate succeeded post switchover                     : 1
Recreate Failed post switchover                        : 0
Stale client entries purged post switchover            : 0

Partial delete during heap recreate                    : 0
Partial delete during force purge                      : 0
Partial delete post restart                            : 0
Partial delete due to AP recovery failure              : 0
Partial delete during reconcilation                    : 0

Client entries in shadow list during SSO               : 0
Client entries in shadow default state during SSO      : 0
Client entries in poison list during SSO               : 0

Invalid bssid during heap recreate                     : 0
Invalid bssid during force purge                       : 0
BSSID mismatch with shadow rec during reconcilation    : 0
BSSID mismatch with shadow rec reconcilation(WGB client): 0
BSSID mismatch with dot11 rec during heap recreate     : 0

AID mismatch with dot11 rec during force purge         : 0
AP slotid mismatch during reconcilation                : 0
Zero aid during heap recreate                          : 0
AID mismatch with shadow rec during reconcilation      : 0
AP slotid mismatch shadow rec during reconcilation     : 0
Client shadow record not present                       : 0
```

モビリティの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless stat redundancy statistics client-recovery mobilityd
Mobility Client Deletion Reason Statistics
------------------------------------------
Mobility Incomplete State         : 0
Inconsistency in WNCD & Mobility  : 0
Partial Delete                    : 0

General statistics
--------------------
Cleanup sent to WNCD, Missing Delete case   : 0
```

クライアント SSO の SISF に関する統計情報を表示するには、次のコマンドを使用します。

```
Device# show wireless stat redundancy statistics client-recovery sisf
Client SSO statistics for SISF
--------------------------------
Number of recreate attempted post switchover    : 1
Number of recreate succeeded post switchover    : 1
Number of recreate failed because of no mac     : 0
Number of recreate failed because of no ip      : 0
Number of ipv4 entry recreate success           : 1
Number of ipv4 entry recreate failed            : 0
Number of ipv6 entry recreate success           : 0
Number of ipv6 entry recreate failed            : 0
Number of partial delete received               : 0
```

```
Number of client purge attempted                : 0
Number of heap and db entry purge success       : 0
Number of purge success for db entry only       : 0
Number of client purge failed                   : 0
Number of garp sent                             : 1
Number of garp failed                           : 0
Number of IP entries validated in cleanup       : 0
Number of IP entry address errors in cleanup    : 0
Number of IP entry deleted in cleanup           : 0
Number of IP entry delete failed in cleanup     : 0
Number of IP table create callbacks on standby  : 0
Number of IP table modify callbacks on standby  : 0
Number of IP table delete callbacks on standby  : 0
Number of MAC table create callbacks on standby : 1
Number of MAC table modify callbacks on standby : 0
Number of MAC table delete callbacks on standby : 0
```

HA 冗長性の概要を表示するには、次のコマンドを使用します。

```
Device# show wireless stat redundancy summary
HA redundancy summary

---------------------

AP recovery duration (ms)        : 264
SSO HA sync timer expired        : No
```

ハイ アベイラビリティの確認

表 *28:* シャーシと冗長性のモニタリング用コマンド

コマンド名	説明
show chassis	シャーシ情報を表示します。
show redundancy	アクティブ ボックスとスタンバイ ボックスに関する詳細を表示します。

表 *29:* アクティブ シャーシとスタンバイ シャーシの電源装置、ファン ステータス、およびシリアル番号のモニタリング用コマンド

コマンド名	説明
show inventory	スタンバイ シャーシおよびアクティブ シャーシの電源装置、ファン、シャーシの詳細を表示します。

ハイ アベイラビリティの削除

すべての HA 関連のパラメータ（ローカル IP、リモート IP、HA インターフェイス、マスク、タイムアウト、プライオリティなど）をクリアするには、次のコマンドを実行します。

chassis clear

（注） 変更を有効にするには、デバイスをリロードします。

ハイ アベイラビリティの SNMP の設定

前提条件

- 管理ポートが稼働している必要があります。
- SNMP コマンドをクエリする場合、管理ポートには 10x のネットワーク IP アドレスが必要です。これは、SNMP の **getmany** を発行する IP アドレスが **10.x.x.x** ネットワークにあるためです。

ハイ アベイラビリティの SNMP の設定

手順

	コマンドまたはアクション	目的
ステップ 1	**show interface ip brief** 例： `Device# show interface ip brief`	管理ポートの IP アドレスが稼働しているかどうかを確認します。
ステップ 2	**show run | sec GigabitEthernet0** 例： `Device# show run | sec GigabitEthernet0`	IP インターフェイスの詳細を表示します。
ステップ 3	**show run | sec SNMP** 例： `Device# show run | sec SNMP`	SNMP サーバの詳細を表示します。
ステップ 4	**snmp-server community public RW** 例： `Device# snmp-server community public RW`	SNMP サーバを設定します。
ステップ 5	**end** 例： `Device# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ENTITY-MIB

ENTITY-MIB は、論理エンティティと物理エンティティを表す一連の管理対象オブジェクト、およびそれらの関係に関する情報を提供します。

表 *30 : MIB* オブジェクトと注記

MIB オブジェクト	注
entPhysicalSerialNum	モニタリングする必要がある唯一の MIB オブジェクトです。
entPhyiscalIndex	インスタンスの作成時にエンティティ MIB によって設定される読み取り専用の一意の ID です。
entPhysicalName	**chassis** *chassis_num* を参照します。 *chassis_num*：スタンドアロンまたはデュアル シャーシを指します。 **entPhysicalName** の長さは 32 文字未満にする必要があります。

ENTITY-STATE-MIB

ENTITY-STATE-MIB は、ENTITY-MIB によって提供される機能を拡張するオブジェクトを定義します。この MIB は、次の *entPhysicalClass* 値を持つエンティティをサポートします。

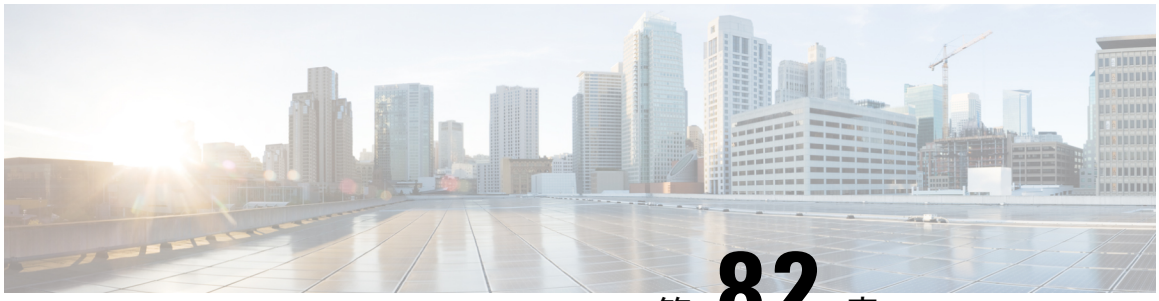
- chassis
- powerSupply
- ファン

表 *31 : MIB* オブジェクトと注記

MIB オブジェクト	注
entStateOper	モニタリングする必要がある唯一の MIB オブジェクトです。

第 IX 部

QoS



第 82 章

QoS

ワイヤレス QoS について

ワイヤレス QoS の概要

Quality of Service（QoS）では、特定のトラフィックを他のトラフィック タイプよりも優先的に処理することで、トラフィックに優先順位を付けることができます。QoS を設定しない場合、デバイスはパケットの内容やサイズに関係なく、各パケットにベストエフォート型のサービスを提供します。デバイスは信頼性、遅延限界、スループットを保証せずにパケットを送信します。

ターゲットは、ポリシーが適用されるエンティティです。SSID およびクライアントに対するワイヤレス QoS ポリシーは、ダウンストリーム方向で適用されます。つまり、トラフィックがデバイスからワイヤレス クライアントに流れているときに適用されます。有線ソースからワイヤレス ターゲットへのトラフィック フローは、ダウンストリーム トラフィックと呼ばれます。ワイヤレス ソースから有線ターゲットへのトラフィック フローは、アップストリーム トラフィックと呼ばれます。

次は、ワイヤレス QoS によって提供される特定の機能の一部です。

- ワイヤレス QoS ターゲットに対する SSID ポリシーおよびクライアント ポリシー
- ワイヤレス トラフィックのポリシング
- Approximate Fair Drop（AFD）
- QoS のモビリティ サポート
- Cisco Unified Wireless Controller で使用可能な貴金属 QoS ポリシーとの互換性

関連トピック

無線ゲスト アクセス （1119 ページ）

ワイヤレス QoS ターゲット

ここでは、デバイスで使用可能なさまざまなワイヤレスQoSターゲットについて説明します。

SSID ポリシー

入力と出力の両方向でSSIDのQoSポリシーを作成できます。デフォルトでは、SSIDポリシーはありません。ポリシーは、BSSID 単位で適用できます。

SSID のポリシング ポリシーとマーキング ポリシーを設定できます。

クライアント ポリシー

クライアントポリシーは、入力方向と出力方向に適用できます。クライアントではポリシングポリシーおよびマーキング ポリシーを設定できます。デバイスのワイヤレス制御モジュールは、WMMクライアントでアドミッションコントロールが有効になっている場合に、デフォルトクライアント ポリシーを適用します。

次の方法を使用して、クライアント ポリシーを設定できます。

- Cisco IOS MQC CLI
- AAA オーバーライド

ワイヤレス ターゲットでサポートされる QoS 機能

次の表に、ワイヤレス ターゲットで使用可能なさまざまな機能について説明します。

表 *32*：ワイヤレス ターゲットで使用可能な *QoS* 機能

Target	機能	Traffic	ポリシーが適用される方向
SSID	• Set • ポリシング • ドロップ	非リアルタイム、リアルタイム	アップストリームおよびダウンストリーム
クライアント	• Set • ポリシング • ドロップ	非リアルタイム、リアルタイム	アップストリームおよびダウンストリーム

ワイヤレス QoS モビリティ

ワイヤレス QoS モビリティによって、ネットワーク内のどの場所でも同じサービスが提供されるように QoS ポリシーを設定することができます。ワイヤレス クライアントは 1 つの場所から別の場所にローミングできるため、異なるデバイスに関連付けられた別のアクセスポイントにクライアントを関連付けることができます。ワイヤレスクライアントのローミングは、次の 2 つのタイプに分類できます。

- デバイス内ローミング
- デバイス間ローミング

（注） 外部 WLC では、クライアントの統計情報は表示されません。

（注） クライアント ポリシーは、モビリティ グループ内のすべてのデバイスで使用できる必要があります。クライアントに一貫した操作ができるように、同じ SSID ポリシーをモビリティ グループのすべてのデバイスに適用する必要があります。

ワイヤレス QoS の貴金属ポリシー

貴金属ポリシーは、コントローラで使用可能なシステム定義のポリシーです。

次のポリシーを使用できます。

- プラチナ：VoIP クライアントに使用されます。
- ゴールド：ビデオ クライアントに使用されます。
- シルバー：ベスト エフォートであると考えられるトラフィックに使用されます。
- ブロンズ：NRT トラフィックに使用されます。

これらのポリシー（プロファイルとも呼ばれる）は、トラフィックに基づいてポリシー プロファイルに適用できます。Cisco IOS MQC 設定を使用した設定を推奨します。ポリシーは、必要な貴金属ポリシーに基づくシステムで利用可能です。SSID の入力および出力ポリシーに対してのみ貴金属ポリシーを設定できます。

クライアントのメタル ポリシーは、AAA を使用してプッシュできます。

適用されたポリシーに基づいて、パケット内の 802.11e（WMM）および DSCP フィールドが影響を受けます。

ワイヤレス QoS の前提条件

ワイヤレス QoS を設定する前に、次の事項を十分に理解しておく必要があります。

- ワイヤレスの概念とネットワーク トポロジ。
- QoS 実装について。
- モジュラ QoS CLI（MQC）
- 使用するアプリケーションのタイプおよびネットワークのトラフィック パターン
- ネットワークの帯域幅要件および速度

ワイヤレス ターゲットの QoS に関する制約事項

一般的な制約事項

ターゲットとは、ポリシーが適用されるエンティティです。有線またはワイヤレス ターゲットにポリシーを適用できます。有線ターゲットには、ポートまたは VLAN を指定できます。 ワイヤレス ターゲットには、ポート、無線、SSID、またはクライアントを設定できます。ユーザは、ポート、SSID、およびクライアント ポリシーだけを設定できます。ユーザは、無線ポリシングを設定できません。ポート、無線、SSID、クライアントの QoS ポリシーはダウンストリーム方向に適用されます。アップストリーム方向では、SSIDおよびクライアント ターゲットだけがサポートされます。ダウンストリームは、トラフィックがdeviceからワイヤレス クライアントに流れていることを示します。アップストリームは、トラフィックがワイヤレス クライアントからdeviceに流れていることを示します。

- ポート、SSID、および（AAA および Cisco IOS コマンドライン インターフェイスを使用する）クライアント ポリシーのみがユーザ設定可能です。無線ポリシーはワイヤレス制御モジュールで設定されるため、ユーザ設定できません。
- ポートおよび無線ポリシーは、出力方向にのみ適用できます。
- SSID およびクライアント ターゲットには、マーキングおよびポリシング ポリシーのみを設定できます。
- 方向単位ターゲットあたり 1 つのポリシーがサポートされています。
- 出力 class-default SSID ポリシーの場合、平均シェーピング レートを設定した後にキュー バッファの割合を 0 に設定する必要があります。
- WLAN グループや QoS ポリシーは削除できません。

SSID に対するワイヤレス QoS の制約事項

次に、SSID で QoS 機能を適用するときの制約事項を示します。

- 入力ポリシーでは 1 つのテーブル マップがサポートされます。
- テーブル マップは、親 class-default でのみサポートされます。最大 2 つのテーブル マップが出力方向でサポートされ、QoS グループが関係する場合、3 つのテーブル マップを設定できます。

（注） テーブル マップは、クライアント ターゲットではサポートされません。

- プライオリティのないポリシングは出力方向でサポートされません。
- SSID レベルのプライオリティ設定は、RT1 および RT2 ポリサー（ポリサー用 AFD）を設定する目的でのみ使用されます。プライオリティの設定にシェーピング レートは含まれません。そのため、プライオリティはポリシングのない SSID ポリシーに対して制限されます。
- DSCP2DSCP および COS2COS テーブルでのマッピングは、ポート レベル ポリシーの音声およびビデオ クラスの分類機能に基づいている必要があります。
- 子ポリシーの class-default ではアクションは許可されません。
- SSID の入力ポリシーでは、UP および DSCP フィルタ（一致基準）のみがサポートされます。ACL およびプロトコルの一致基準はサポートされません。

クライアントのワイヤレス QoS の制約事項

次に、クライアント ターゲットでの QoS ポリシーの適用に関する制約事項を示します。

- デフォルトのクライアント ポリシーは、ACM イネーブルの WMM クライアント上でのみイネーブルにされます。
- キューイングはサポートされていません。
- イネーブル状態の WLAN では、クライアント ポリシーの付加、削除また変更はサポートされません。ポリシーを適用、削除、または変更するには、WLAN をシャットダウンする必要があります。
- テーブル マップ設定は、ターゲット クライアントでサポートされていません。
- class-default で一緒に設定されたポリシングとセットは、出力方向でブロックされます。

```
policy-map foo
class class-default
police X
set dscp Y
```

- 親ポリシーが他のユーザ定義クラス マップを含む場合、子ポリシーは class-default でサポートされません。
- フラットな出力クライアント ポリシーでは、class-default 内のポリシングおよび他のクラス内のマーキング アクションはサポートされません。
- クライアント ポリシーのポリシー マップ クラスのフィルタすべてに、同じ属性が必要です。IPv4 または IPv6 アドレスなどのプロトコル固有の属性で一致するフィルタは、異なる属性セットと見なされます。

- ACL で一致するフィルタでは、アクセス リストのすべての ACE（アクセス コントロール エントリ）に同じ種類と同じ数の属性が必要です。
- クライアント出力ポリシーでは、マーキング属性で一致するフィルタにおいて、policy-map 内のすべてのフィルタが同じマーキング属性で一致する必要があります。たとえば、フィルタが DSCP で一致する場合、ポリシー内のすべてのフィルタが DSCP で一致する必要があります。

ワイヤレス QoS の設定方法

クラス マップの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Services]** > **[QoS]** を選択します。

ステップ 2 [Add] をクリックして、[Add QoS] ウィンドウを表示します。

ステップ 3 [Add Class-Maps] をクリックします。

ステップ 4 [AVC/User Defined] ドロップダウンリストから [AVC] を選択し、次のように設定します。

a) [Match Any] または [Match All] のいずれかを選択します。

b) 必要な [Mark Type] を選択し、適切な [Mark Value] を指定します。

c) 必要な [Mark Type] を選択します。[DSCP] を選択した場合は、適切な [Mark Value] を指定する必要があります。

d) 特定の送信元からのトラフィックをドロップするには、[Drop] チェック ボックスをオンにします。

（注） [Drop] が有効になっている場合、[Mark Type] および [Police(kbps)] オプションは無効になります。

e) 選択した一致タイプに基づいて、[Available Protocol(s)] リストから必要なプロトコルを選択し、[Selected Protocol(s)] リストに移動します。選択したこれらのプロトコルによってトラフィックがドロップされます。

f) [Save] をクリックします。

ステップ 5 [User Defined] を選択してユーザ定義の QoS ポリシーを有効化し、次のように設定します。

a) [Match Any] または [Match All] のいずれかを選択します。

b) 必要な [Match Type] を選択し、適切な [Match Value] を指定します。

c) 必要な [Mark Type] を選択してマーク ラベルに関連付けます。[DSCP] を選択した場合は、適切な [Mark Value] を指定する必要があります。

d) 特定の送信元からのトラフィックをドロップするには、[Drop] チェック ボックスをオンにします。

（注） [Drop] が有効になっている場合、[Mark Type] および [Police(kbps)] オプションは無効になります。

e) [Save] をクリックします。

ステップ 6 [Save & Apply to Device] をクリックします。

クラス マップの設定（CLI）

音声およびビデオ トラフィックのクラス マップを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**class-map** *class-map-name* 例： `Device(config)# class-map test`	クラス マップを作成します。
ステップ 3	**match dscp** *dscp-value* 例： `Device(config-cmap)# match dscp 46`	IPv4 および IPv6 パケットの DSCP 値を照合します。 （注） クラス マップのデフォルトでは、値は match-all です。

WLAN の貴金属ポリシーの設定（GUI）

始める前に

ポリシー プロファイルが設定されていることを確認します。プロファイル ポリシー単位で貴金属 QoS ポリシーを設定できます。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞を選択します。

ステップ 2 [Policy Profile] ページでポリシー プロファイルの名前をクリックします。

ステップ 3 [Edit Policy Profile] ウィンドウで [QoS and AVC] タブをクリックします。

ステップ 4 [QoS SSID Policy] で、WLAN の適切な [Ingress] および [Egress] ポリシーを選択します。

- プラチナ
- Gold
- Silver
- ブロンズ

（注） 入力ポリシーを出力ポリシーと区別するには、サフィックス -up を使用します。たとえば、Platinum 入力ポリシーは platinum-up という名前になります。

ステップ 5 [Update & Apply to Device] をクリックします。

WLAN の貴金属ポリシーの設定（CLI）

プロファイル ポリシー単位で貴金属 QoS ポリシーを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless policy profile** *policy-name* 例： `Device`**`wireless policy profile pp1`**	ワイヤレス ポリシー プロファイル コンフィギュレーション サブモードを開始します。
ステップ 3	**shutdown** 例： `Device`**`shutdown`**	ワイヤレス ポリシー プロファイルを無効にします。
ステップ 4	**service-policy** {**input** | **output**} *policy-name* 例： `Device(config-wlan)# service-policy output platinum` 例： `Device(config-wlan)# service-policy input platinum-up`	ポリシー プロファイルに QoS ポリシーを設定します。貴金属ポリシーを設定するには、**platinum**、**gold**、**silver**、または **bronze** のいずれかのキーワードを入力する必要があります。この例に示すように、アップストリーム ポリシーは **platinum-up** キーワードを使って指定します。 （注） アップストリーム ポリシーは、ダウンストリーム ポリシーと異なります。アップストリーム ポリシーには -up サフィックスがあります。

	コマンドまたはアクション	目的
ステップ 5	**[no] shutdown** 例： `Device`**`no shutdown`**	ワイヤレス ポリシー プロファイルを有効にします。
ステップ 6	**end** 例： `Device(config)#` **`end`**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー マップの設定（CLI）

音声およびビデオ トラフィックのクラス マップを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device#` **`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	**policy-map** *policy-map-name* 例： `Device(config)#` **`policy-map testpolicy`**	ポリシー マップを作成します。
ステップ 3	**class** *class-map-name* 例： `Device(config-pmap)#` **`class testmap`**	ポリシー基準を作成します。
ステップ 4	**set dscp** *value* 例： `Device(config-pmap)#` **`set dscp 45`**	パケットに新しいDSCP値を設定して、IP トラフィックを分類します。
ステップ 5	**police** *bit_rate_value* 例： `Device(config-pmap)#` **`police 2M`**	ビット レートにポリサーを追加します。

ポリシー マップの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Local Policy]** を選択します。

ステップ 2 [Local Policies] ページで [Policy Map] タブをクリックします。

ステップ 3 [Policy Map] タブで [Add] をクリックします。

ステップ 4 表示される [Create Policy Map Configuration] ウィンドウで、ポリシー マップの名前を入力します。

ステップ 5 [Match Criteria List] セクションで [Add] をクリックします。

ステップ 6 [Service Template] ドロップダウンリストから、ポリシーにマッピングするサービステンプレートを選択します。

ステップ 7 [Device Type] ドロップダウン リストから、デバイス タイプを選択します。デバイス タイプの一致基準は、選択したデバイス タイプに合わせて eq、not-eq、または regex にすることができます。

ステップ 8 [User Role] ドロップダウンリストから一致基準を選択し、ユーザ ロールを入力します。ユーザ ロールの一致基準には、eq、not-eq、または regex を使用できます。

ステップ 9 [User Name] ドロップダウンリストから一致基準を選択し、ユーザ名を入力します。ユーザ名の一致基準には、eq、not-eq、または regex を使用できます。

ステップ 10 [OUI] ドロップダウンリストから OUI を選択します。

ステップ 11 [MAC Address] ドロップダウンリストから一致基準を選択し、MAC アドレスを入力します。一致基準には eq または not-eq を使用できます。

ステップ 12 [Add Criteria] をクリックして一致基準を追加します。

ステップ 13 [Save & Apply to Device] をクリックします。

QoS プロファイル ポリシーの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞ を選択します。

ステップ 2 [Policy Profile] ページでポリシー プロファイルの名前をクリックします。

ステップ 3 [Edit Policy Profile] ウィンドウで [QoS and AVC] タブをクリックします。

ステップ 4 [QoS SSID Policy] で、WLAN の適切な [Ingress] および [Egress] ポリシーを選択します。

- プラチナ
- Gold
- Silver
- ブロンズ

（注） 入力ポリシーを出力ポリシーと区別するには、サフィックス -up を使用します。たとえば、Platinum 入力ポリシーは platinum-up という名前になります。

ステップ 5 [QoS Client Policy] で、クライアントの適切な [Ingress] および [Egress] ポリシーを選択します。

ステップ 6 [Update & Apply to Device] をクリックします。

QoS プロファイル ポリシーの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy qostest`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**service-policy client** {**input** | **output**} *policy-name* 例： `Device(config-wireless-policy)# service-policy client input policy-map-client`	ポリシーを適用します。選択できるオプションは、次のとおりです。 • **input**：クライアント ポリシーをポリシー プロファイルの入力方向に割り当てます。 • **output**：クライアント ポリシーをポリシー プロファイルの出力方向に割り当てます。
ステップ 4	**service-policy** {**input** | **output**} *policy-name* 例： `Device(config-wireless-policy)# service-policy input policy-map-ssid`	ポリシーを適用します。選択できるオプションは、次のとおりです。 • **input**：WLAN のすべてのクライアントにポリシー マップを割り当てます。 • **output**：WLAN のすべてのクライアントにポリシー マップを割り当てます。

	コマンドまたはアクション	目的
ステップ 5	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	設定を保存します。

QoS ポリシー タグの設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。

ステップ 2 [Manage Tags] ページの [Policy] タブで [Add] をクリックします。

ステップ 3 表示される [Add Policy Tag] ウィンドウに、ポリシー タグの名前と説明を入力します。

ステップ 4 必要な WLAN ID および WLAN プロファイルを適切なポリシー プロファイルにマッピングします。

ステップ 5 [Update & Apply to Device] をクリックします。

QoS ポリシー タグの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag policy** *policy-tag-name* 例： `Device(config-policy-tag)# wireless tag policy qostag`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device(config-policy-tag)# wlan test policy qostest`	ポリシー プロファイルを WLAN プロファイルにマッピングします。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-policy-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 5	**show wireless tag policy summary** 例： `Device# show wireless tag policy summary`	設定されたポリシータグを表示します。 （注） ポリシー タグの詳細情報を表示するには、**show wireless tag policy detailed** *policy-tag-name* コマンドを使用します。

AP へのポリシー タグの付加

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap** *mac-address* 例： `Device(config)# ap F866.F267.7DFB`	Cisco AP を設定し、AP プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag qostag`	ポリシー タグを AP にマッピングします。
ステップ 4	**end** 例： `Device(config-ap-tag)# end`	設定を保存し、コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。
ステップ 5	**show ap tag summary** 例： `Device# show ap tag summary`	AP の詳細と AP に関連付けられているタグを表示します。

SIP コール アドミッション制御（CAC）

コール アドミッション制御（CAC）は音声トラフィックのみに適用される概念で、データ トラフィックには適用されません。CAC を実装する場合、クライアントは帯域幅を予約するためにトラフィック仕様（TSPEC）を送信する必要があります。SIP CAC 機能は、SIP コールをサポートするために CAC を有効にします。使用可能な SIP 電話機のほとんどには、TSPEC が実装されていません。CAC を呼び出して帯域幅を予約するには、TSPEC が必要です。

この機能を使用すると、特定の SIP コールに帯域幅パラメータを手動で設定し、その設定を使用して、新しいコールを受信するたびに帯域幅を予約できます。

（注） クライアントが SIP と TSPEC の両方をサポートしている場合は、TSPEC を使用した帯域幅予約が優先されます。

制約事項と制限

- コントローラで SIP コール スヌープが有効になっている場合にのみ、SIP CAC を有効化できます。

SIP CAC の設定

SIP CAC は、実行できる SIP 呼び出しの総数を制御します。

手順

	コマンドまたはアクション	目的
ステップ 1	**Configure Terminal** 例： `Device# 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	**wireless profile policy <policy-name>** 例： `Device(config)# wireless profile policy policy-name`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**shutdown** 例： `Device(config)# Shutdown`	ワイヤレス ポリシー プロファイルを無効にします。
ステップ 4	**service-policy** {**input** | **output**} *policy-name* 例：	ポリシー プロファイルに Platinum メタル QoS ポリシーを設定します。この例に示されるように、platinum-up キー

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# service-policy input platinum-up` `Device(Config-wireless-policy)# service-policy output platinum`	ワードでアップストリームポリシーが指定されます。 （注） アップストリーム ポリシーは、ダウンストリーム ポリシーと異なります。アップストリーム ポリシーには -up サフィックスがあります。 （注） コールスヌープが有効になっている場合は、Platinum で SSID ポリシーを設定する必要があります。
ステップ 5	**call-snoop** 例： `Device(config-wireless-policy)# call-snoop`	WLAN のコール スヌーピングを有効にします。
ステップ 6	**[no] shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ワイヤレス ポリシー プロファイルを有効にします。
ステップ 7	**ap dot11** {**5ghz** | **24ghz**} **cac** {**voice** | **video**} **acm** 例： `Device(config-wireless-policy)#ap dot11 5ghz cac voice acm`	無線の静的 ACM をイネーブルにします。SIP スヌーピングをイネーブルにする場合、静的 CAC ではなく、負荷ベースの CAC を使用します。
ステップ 8	**ap dot11** {**5ghz** | **24ghz**} **cac voice sip** 例： `Device(config)#ap dot11 5ghz cac voice sip`	SIP-Based CAC を設定します。
ステップ 9	**ap dot11** {**5ghz** | **24ghz**} **cac voice sipbandwidth** <*bandwidth*> **sample-interval** <*interval-value*> 例： `Device(config)#ap dot11 24ghz cac voice sip bandwidth <8-64> sample-interval <10-80>`	（任意）帯域幅と間隔値を設定します。 たとえば、帯域幅を <8-64> と入力します（G729 の 8 kbps と G711 の 64 kbps）。間隔値として、パケット化間隔 10 ～ 80 ミリ秒（G711 または G729 コーデックの 10、20、30、40、80 ミリ

	コマンドまたはアクション	目的
		秒。デフォルトは 20）を意味する <10-80> を入力します。
ステップ 10	**end** 例： `Device(config)#end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。

SIP CAC の確認

SIP CAC 機能を確認するには、次の Show コマンドを使用します。

```
Device # show ap cac voice
AP Name: AP5897.bdd0.61d4
Slot#   Radio       Calls   BW-Max  BW-Alloc    BW-InUse
-------------------------------------------------------
0       802.11b/g   1       23437         765         3


AP Name: AP70DF.2FA2.39E0
Slot#   Radio       Calls   BW-Max  BW-Alloc    BW-InUse
-------------------------------------------------------


AP Name: APA023.9F11.C6DC
Slot#   Radio       Calls   BW-Max  BW-Alloc    BW-InUse
-------------------------------------------------------
0       802.11b/g   1       23437   765         3
```

SIP 音声コール スヌーピング

この機能により、アクセス ポイントは Session Initiation Protocol（SIP）コールの確立、終了、および失敗を検出し、コントローラにレポートできます。各 WLAN に対して、SIP スヌーピングおよびレポートを有効または無効にできます。VoIP Media Session Aware（MSA）スヌーピングを有効にすると、この WLAN をアドバタイズするアクセス ポイント無線は SIP 音声パケットを検索します。

ポート番号 5060（標準の SIP シグナリング ポート）を宛先または送信元とする SIP パケットは、追加インスペクションの対象と見なされます。アクセス ポイントでは、Wi-Fi Multimedia（WMM）クライアントと非 WMM クライアントがコールを確立している段階、コールがアクティブになった段階、コールの終了処理の段階を追跡します。両方のクライアント タイプのアップストリームパケット分類は、アクセスポイントで行われます。ダウンストリームパケット分類は、WMM クライアントはコントローラで、非 WMM クライアントはアクセス ポイントで行われます。アクセス ポイントは、コールの確立、終了、失敗など、主要なコール イベントをコントローラに通知します。

（注） この機能は、中央スイッチング モード、IOS および ClickOS AP、メッシュ AP ブリッジ モードでサポートされますが、ファブリックではサポートされません。

（注） L3 ローミングを使用して SIP コールを実行する場合は、コントローラが NTP サーバと同期している必要があります。または、その時刻が同じである必要があります。

SIP 音声コール スヌーピングの設定

始める前に

- コール スヌープを有効にするには、BSSID Platinum ポリシーを最初に設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**Configure Terminal** 例： `Device# 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	**wireless profile policy** <*policy-name*> 例： `Device(config)# wireless profile policy policy-name`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**shutdown** 例： `Device(config)# Shutdown`	ワイヤレス ポリシー プロファイルを無効にします。
ステップ 4	**service-policy** {**input** | **output**} *policy-name* 例： `Device(config-wireless-policy)# service-policy input platinum-up` `Device(Config-wireless-policy)# service-policy output platinum`	ポリシー プロファイルに Platinum メタル QoS ポリシーを設定します。例に示すように、アップストリーム ポリシーは **platinum-up** キーワードで指定されます。 （注） アップストリーム ポリシーは、ダウンストリーム ポリシーと異なります。アップストリーム ポリシーには -up サフィックスがあります。

	コマンドまたはアクション	目的
		（注） コール スヌープが有効になっている場合は、Platinum で SSID ポリシーを設定する必要があります。
ステップ 5	**call-snoop** 例： `Device(config-wireless-policy)# call-snoop`	WLAN のコール スヌーピングを有効にします。
ステップ 6	**[no] shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ワイヤレス ポリシー プロファイルを有効にします。
ステップ 7	**end** 例： `Device(config)#end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

SIP 音声コール スヌーピングの確認

call-snoop コマンドが有効になっているかどうかを確認するには、次のコマンドを使用します。

```
Device# sh wireless profile policy detailed <policy-name>
Classmap name for Reanchoring
  Reanchoring Classmap Name   : Not Configured
QOS per SSID
  Ingress Service Name        : platinum-up
  Egress Service Name         : platinum
QOS per Client
  Ingress Service Name        : voice-client
  Egress Service Name         : voice-client
Umbrella information
  Ciso Umbrella Parameter Map : Not Configured
Autoqos Mode                  : None
Call Snooping                 : Enabled
Fabric Profile
  Profile Name                : Not Configured
Accounting list
```

QoS 耐障害性

ここでは、QoS の耐障害性（FT）設定について説明します。耐障害性はフレックス モードにのみ適用されます。

アクセス ポイント（AP）がスタンドアロン モードになると、クライアントは AP に接続したままになります。BSSID およびクライアントに適用されているすべての QoS ポリシーは変更されることなく、通常どおり機能します。

AP がコントローラに再接続すると、AP は接続モードに戻ってクライアントが AP に参加したままになります。BSSID およびクライアントの既存のポリシーは消去されます。コントローラは、BSSID およびクライアントのポリシーを送信します。これらのポリシーは AP に適用されます。

QoS 耐障害性の設定

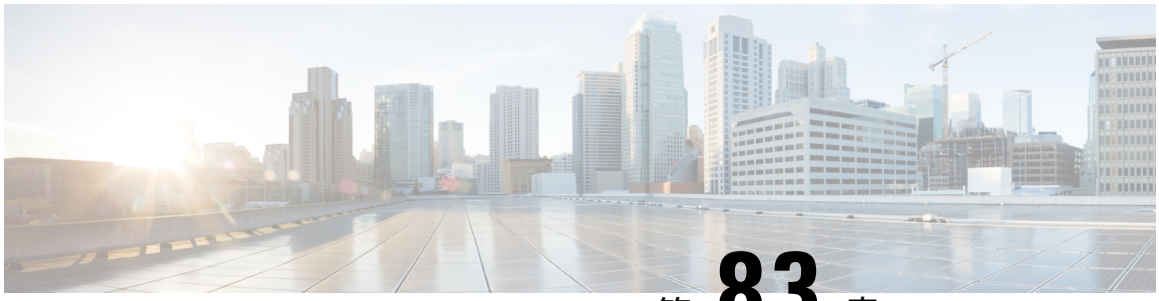
手順

	コマンドまたはアクション	目的
ステップ 1	**Configure Terminal** 例： `Device# 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	**wireless profile policy <policy-name>** 例： `Device(config)# wireless profile policy policy-name`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**shutdown** 例： `Device(config)# Shutdown`	ワイヤレス ポリシー プロファイルを無効にします。
ステップ 4	**service-policy client** {**input** | **output**} *policy-name* 例： `Device(config-wireless-policy)# service-policy client input policy-map-client`	ポリシーを適用します。選択できるオプションは、次のとおりです。 • **input**：クライアント ポリシーをクライアントの入力方向に割り当てます。 • **output**：クライアント ポリシーをクライアントの出力方向に割り当てます。
ステップ 5	**service-policy** {**input** | **output**} *policy-name* 例： `Device(config-wireless-policy)# service-policy input policy-map-ssid`	ポリシーを適用します。選択できるオプションは、次のとおりです。 • **input**：WLAN のすべてのクライアントにポリシー マップを割り当てます。

	コマンドまたはアクション	目的
		• **output**：WLAN のすべてのクライアントにポリシーマップを割り当てます。
ステップ 6	**vlan vlan-id** 例： `Device(config-wireless-policy)# vlan 24`	VLAN 名または VLAN ID を設定します。
ステップ 7	**[no] shutdown** 例： `Device(config-wireless-policy)# no shutdown`	設定を保存します。
ステップ 8	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site rr-xyz-site`	サイト タグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 9	**no local-site** 例： `Device(config-site-tag)# no local-site`	このサイトをローカル サイトとして設定します。
ステップ 10	**exit** 例： `Device(config-site-tag)# exit`	サイト タグ コンフィギュレーション モードを終了します。
ステップ 11	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy rr-xyz-policy-tag`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 12	**wlan** *wlan-profile-name* **policy** *policy-name* 例： `Device(config-policy-tag) # wlan qos-ft policy flex-policy`	ポリシー プロファイルを WLAN プロファイルにマッピングします。
ステップ 13	**wlan** *wlan-profile-name wlan-identifier ssid-network-name* 例： `Device(config) # wlan qos-ft 2 qos-ft`	WLAN と SSID を設定します。SSID（ネットワーク名）には、最大32文字の英数字を使用できます。
ステップ 14	**no security wpa** 例：	WPA セキュリティを無効にします。

	コマンドまたはアクション	目的
	`Device(config-wlan)# no security wpa`	
ステップ 15	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 16	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 17	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 18	**no shutdown** 例： `Device(config-wlan)# no shutdown`	設定を保存します。
ステップ 19	**exit** 例： `Device(config-wlan)# exit`	WLAN コンフィギュレーション モードを終了します。
ステップ 20	**ap** *Ethernet-ap-mac-address* 例： `Device(config)#ap A123.1F2B.12B0`	AP コンフィギュレーション モードを開始します。
ステップ 21	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)#policy-tag flex-tag`	AP にポリシー タグを関連付けます。
ステップ 22	**site-tag** *site-tag-name* 例： `Device(config-ap-tag)# site-tag site-flex`	AP にサイト タグを関連付けます。
ステップ 23	**end** 例： `Device(config-ap-tag)# end`	特権 EXEC モードに戻ります。
ステップ 24	**show ap summary** 例：	入力内容を確認します。

	コマンドまたはアクション	目的
	`Device# show ap summary`	



第 83 章

ワイヤレス自動 QoS

-
- 自動 QoS について （839 ページ）
- ワイヤレス自動 QoS の設定方法 （840 ページ）

自動 QoS について

ワイヤレス自動 QoS は、ワイヤレス QoS 機能の展開を自動化します。事前定義された一連のプロファイルが含まれており、顧客はこれを変更してさまざまなトラフィック フローに優先順位を付けることができます。自動 QoS はトラフィックを照合し、各一致パケットを qos-group に割り当てます。これにより、出力ポリシー マップは、プライオリティ キューを含む特定のキューに、特定の qos-group を配置できます。

自動 QoS ポリシー設定

表 *33*：自動 *QoS* ポリシー設定

モード	クライアント入力	クライアント出力	BSSID 入力	BSSID 出力	ポート入力	ポート出力	無線機
音声	該当なし	該当なし	P3	P4	該当なし	P7	ACM
ゲスト	該当なし	該当なし	P5	P6	該当なし	P7	
ファストレーン	該当なし	該当なし	該当なし	該当なし	該当なし	P7	edca-parameters fastlane
エンタープライズ AVC	該当なし	該当なし	P1	P2	該当なし	P7	

P	AutoQos-4.0-wlan-ET-SSID-Input-AVC-Policy
P	AutoQos-4.0-wlan-ET-SSID-Output-Policy

P	platinum-up
P	platinum
P	AutoQos-4.0-wlan-GT-SSID-Input-Policy
P	AutoQos-4.0-wlan-GT-SSID-Output-Policy
P	AutoQos-4.0-wlan-Port-Output-Policy

ワイヤレス自動 QoS の設定方法

プロファイル ポリシーのワイヤレス自動 QoS の設定

プロファイル ポリシーの自動 QoS を有効にすることができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device`**`enable`**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**wireless autoqos policy-profile** *policy-name* **mode { enterprise-avc | fastlane | guest | voice}** 例： `Device# wireless autoqos policy-profile test-profile mode voice`	自動 QoS ワイヤレス ポリシーを設定します。 • enterprise-avc：自動 QoS ワイヤレス エンタープライズ AVC ポリシーを有効にします。 • fastlane：自動 QoS ワイヤレス ファストレーン ポリシーを有効にします。 • guest：自動 QoS ワイヤレス ゲスト ポリシーを有効にします。 • voice：自動 QoS ワイヤレス 音声ポリシーを有効にします。

	コマンドまたはアクション	目的
		（注） 自動 QoS MIB 属性は、サービス ポリシーの完全な機能をサポートしていません。サービス ポリシーは手動で設定する必要があります。現在は自動 QoS モードのみがサポートされています。

次のタスク

（注） 自動 QoS を有効にした後、ポリシーがインストールされるまで数秒待ってから、必要に応じて自動 QoS ポリシー マップの変更を試みるか、変更が拒否された場合は再試行します。

ワイヤレス自動 QoS の無効化

ワイヤレス自動 QoS をグローバルに無効化する手順は次のとおりです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device`**`enable`**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**shutdown** 例： `Device`**`shutdown`**	ポリシー プロファイルをシャット ダウンします。
ステップ 3	**wireless autoqos disable** 例： `Device# wireless autoqos disable`	ワイヤレス自動 QoS をグローバルに無効化します。
ステップ 4	**[no] shutdown** 例： `no shutdown`	ワイヤレス ポリシー プロファイルを有効にします。

自動 QoS 設定のロールバック

始める前に

（注） 自動 QoS MIB 属性は、サービス ポリシーの完全な機能をサポートしていません。現在は自動 QoS モードのみがサポートされています。サービス ポリシーは手動で設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device`**`enable`**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**clear platform software autoqos config template { enterprise_avc | guest}** 例： `Device# clear platform software autoqos config template guest`	自動 QoS 設定をリセットします。 • enterprise-avc：自動 QoS エンタープライズ AVC ポリシー テンプレートをリセットします。 • guest：自動 QoS ゲスト ポリシー テンプレートをリセットします。

ワイヤレス自動 QoS ポリシー プロファイルのクリア

手順

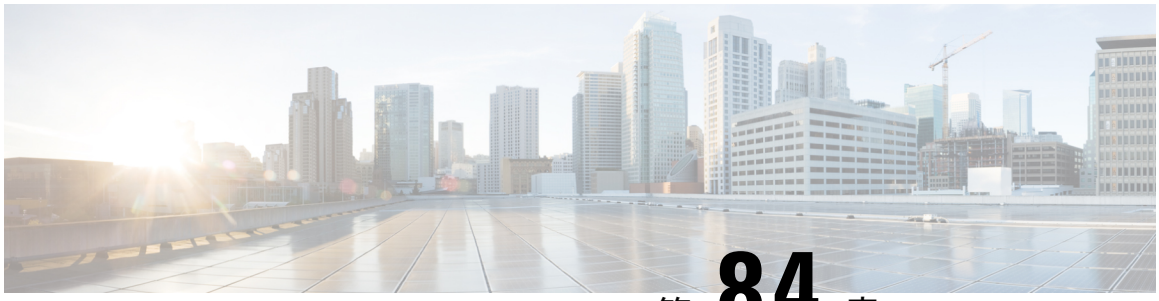
	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device`**`enable`**	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**shutdown** 例： `Device`**`shutdown`**	ポリシー プロファイルをシャット ダウンします。
ステップ 3	**wireless autoqos policy-profile** *policy-name***mode clear** 例：	設定されている自動 QoS ワイヤレス ポリシーをクリアします。

	コマンドまたはアクション	目的
	`Device# wireless autoqos policy-profile test-profile mode clear`	
ステップ 4	**[no] shutdown** 例： `no shutdown`	ワイヤレス ポリシー プロファイルを有効にします。

ポリシー プロファイルの自動 QoS の表示

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device**enable**`	特権 EXEC モードをイネーブルにします。パスワードを入力します（要求された場合）。
ステップ 2	**show wireless profile policy detailed** *policy-profile-name* 例： `Device# **show wireless profile policy detailed testqos**`	ポリシー プロファイル詳細パラメータを表示します。



第 84 章

ネイティブ プロファイリング

ネイティブ プロファイリングについて

HTTP と DHCP に基づいてデバイスをプロファイルし、ネットワーク上のエンドデバイスを識別できます。デバイスベースのポリシーを設定して、ネットワーク上でユーザまたはデバイスポリシーごとに適用できます。

ポリシーを使用すれば、モバイルデバイスのプロファイリングと、プロファイルしたデバイスの特定の VLAN への基本オンボーディングが可能になります。また、ACL と QoS を割り当てたり、セッション タイムアウトを設定したりできます。

ポリシーは 2 つの異なるコンポーネントとして設定できます。

- ネットワークに接続しているクライアントに固有のサービステンプレートとしてポリシー属性を定義し、ポリシー一致基準を適用する。
- ポリシーへの一致基準の適用。

（注） ネイティブ プロファイルの設定に進む前に、HTTP プロファイリングと DHCP プロファイリングが有効になっていることを確認してください。

ネイティブ プロファイリングを設定するには、次のいずれかの手順を使用します。

- サービス テンプレートを作成する
- クラス マップの作成

（注） サービス テンプレートは、クラス マップまたはパラメータ マップのいずれかを使用して適用できます。

- パラメータ マップを作成し、サービス テンプレートをパラメータ マップに関連付ける
  - ポリシー マップの作成
    1. クラス マップを使用する場合：クラス マップをポリシー マップに関連付けて、サービス テンプレートをクラス マップに関連付けます。
    2. パラメータ マップを使用する合：パラメータ マップをポリシー マップに関連付けます。
  - ポリシー マップをポリシー プロファイルに関連付けます。

関連トピック

無線ゲスト アクセス （1119 ページ）

クラス マップの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Services]** > **[QoS]** をクリックします。

ステップ 2 [Qos – Policy] 領域で、[Add] をクリックして新しい QoS ポリシーを作成するか、編集するポリシーをクリックします。

ステップ 3 [Add Class Map] を追加し、詳細を入力します。

ステップ 4 [Save] をクリックします。

ステップ 5 [Update and Apply to Device] をクリックします。

クラス マップの作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**class-map type control subscriber match-any** *class-map-name* 例： `Device(config)# class-map type control subscriber match-any cls_user`	クラスマップのタイプと名前を指定します。
ステップ 3	**match username** *username* 例： `Device(config-filter-control-classmap)# match username ciscoise`	クラスマップ属性フィルタ基準を指定します。
ステップ 4	**class-map type control subscriber match-any** *class-map-name* 例： `Device(config)# class-map type control subscriber match-any cls_userrole`	クラスマップのタイプと名前を指定します。
ステップ 5	**match user-role** ユーザ ロール 例： `Device(config-filter-control-classmap)# match user-role engineer`	クラスマップ属性フィルタ基準を指定します。
ステップ 6	**class-map type control subscriber match-any** *class-map-name* 例： `Device(config)# class-map type control subscriber match-any cls_oui`	クラスマップのタイプと名前を指定します。
ステップ 7	**match oui** *oui-address* 例： `Device(config-filter-control-classmap)# match oui 48.f8.b3`	クラスマップ属性フィルタ基準を指定します。
ステップ 8	**class-map type control subscriber match-any** *class-map-name* 例：	クラスマップのタイプと名前を指定します。

	コマンドまたはアクション	目的
	`Device(config)# class-map type control subscriber match-any cls_mac`	
ステップ 9	**match mac-address** *mac-address* 例： `Device(config-filter-control-classmap)# match mac-address 0040.96b9.4a0d`	クラスマップ属性フィルタ基準を指定します。
ステップ 10	**class-map type control subscriber match-any** *class-map-name* 例： `Device(config)# class-map type control subscriber match-any cls_devtype`	クラスマップのタイプと名前を指定します。
ステップ 11	**match device-type** *device-type* 例： `Device(config-filter-control-classmap)# match device-type windows`	クラスマップ属性フィルタ基準を指定します。
ステップ 12	**match join-time-of-day** *start-time end-time* 例： `Device(config-filter-control-classmap)# match join-time-of-day 10:30 12:30`	時刻の一致を指定します。 ここで照合の対象となるのは、接続時刻です。たとえば、一致フィルタが午前 11:00 から午後 2:00 に設定されている場合、午前 10:59 に接続したデバイスは、クレデンシャルの取得が午前 11:00 以降であっても一致と見なされません。 ここで、各変数は次のように定義されます。 *start-time* と *end-time* は 24 時間形式で指定します。 設定を確認するには、**show class-map type control subscriber name** *name* コマンドを使用します。 （注） このコマンドを使用するには、AAA オーバーライドも無効にする必要があります。

サービス テンプレートの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Local Policy]** を選択します。

ステップ 2 [Local Policy] ページの [Service Template] タブで、[ADD] をクリックします。

ステップ 3 [Create Service Template] ウィンドウで、次のパラメータを入力します。

- [Service Template Name]：テンプレートの名前を入力します。
- [VLAN ID]：テンプレートの VLAN ID を入力します。有効な範囲は 1 ～ 4094 です。
- [Session Timeout (secs)]：テンプレートのタイムアウト時間を設定します。有効な範囲は 1 ～ 65535 です。
- [Access Control List]：ドロップダウンリストからアクセス制御リストを選択します。
- [Ingress QOS]：ドロップダウンリストからクライアントの入力 QoS ポリシーを選択します
- [Egress QOS]：ドロップダウンリストからクライアントの出力 QoS ポリシーを選択します

ステップ 4 [Save & Apply to Device] をクリックします。

サービス テンプレートの作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**service-template** *service-template-name* 例： `Device(config)# service-template svc1`	サービス テンプレート コンフィギュレーション モードを開始します。
ステップ 3	**vnid** *vnid* 例： `Device(config-service-template)# vnid test`	VXLAN ネットワーク ID（VNID）を指定します。 設定を確認するには、**show service-template** *service-template-name* コマンドを使用します。

	コマンドまたはアクション	目的
ステップ 4	**access-group** *access-list-name* 例： `Device(config-service-template)# access-group acl-auto`	適用するアクセスリストを指定します。
ステップ 5	**vlan** *vlan-id* 例： `Device(config-service-template)# vlan 10`	VLAN ID を指定します。有効な範囲は 1 ～ 4094 です。
ステップ 6	**absolute-timer** *timer* 例： `Device(config-service-template)# absolute-timer 1000`	サービス テンプレートのセッション タイムアウト値を指定します。有効な範囲は 1 ～ 65535 です。
ステップ 7	**service-policy qos input** *qos-policy* 例： `Device(config-service-template)# service-policy qos input in_qos`	クライアントの入力 QoS ポリシーを設定します。
ステップ 8	**service-policy qos output** *qos-policy* 例： `Device(config-service-template)# service-policy qos output out_qos`	クライアントの出力 QoS ポリシーを設定します。

パラメータ マップの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**parameter-map type subscriber attribute-to-service** *parameter-map-name* 例： `Device(config)# parameter-map type subscriber attribute-to-service param`	パラメータ マップのタイプと名前を指定します。

	コマンドまたはアクション	目的
ステップ 3	*map-index* **map device-type eq** *filter-name* 例： `Device(config-parameter-map-filter)# 1 map device-type eq "windows" mac-address eq 3c77.e602.2f91 username eq "cisco"`	パラメータ マップ属性フィルタ基準を指定します。ここに示す例では、複数のフィルタが使用されています。
ステップ 4	*map-index* **service-template** *service-template-name* **precedence** *precedence-num* 例： `Device(config-parameter-map-filter-submode)# 1 service-template svc1 precedence 150`	サービス テンプレートとその優先順位を指定します。

ポリシー マップの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Local Policy]** > **[Policy Map]** タブを選択します。

ステップ 2 [Policy Map Name] テキスト フィールドに、ポリシー マップの名前を入力します。

ステップ 3 [Add] をクリックします。

ステップ 4 [Service Template] ドロップダウンリストからサービス テンプレートを選択します。

ステップ 5 次のパラメータでは、ドロップダウンリストからフィルタのタイプを選択し、必要な一致基準を入力します。

- Device Type
- ユーザ ロール
- ユーザ名
- OUI
- MAC アドレス

ステップ 6 [Add Criteria] をクリックします。

ステップ 7 [Update & Apply to Device] をクリックします。

ポリシー マップの作成（CLI）

始める前に

ポリシー マップまたはパラメータ マップを削除する場合は、事前にターゲットから削除するか、WLAN プロファイルをシャット ダウンするか、セッションを削除する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**policy-map type control subscriber** *policy-map-name* 例： `Device(config)# policy-map type control subscriber polmap5`	ポリシーマップ タイプを指定します。
ステップ 3	**event identity-update match-all** 例： `Device(config-event-control-policymap)# event identity-update match-all`	ポリシーマップに対して一致基準を指定します。
ステップ 4	次に示すように、クラスマップまたはパラメータ マップのいずれかを使用してサービステンプレートを適用できます。 • *class-num* **class** *class-map-name* **do-until-failure** • *action-index* **activate service-template** *service-template-name* • *action-index* **map attribute-to-service table** *parameter-map-name* 例： 次の例は、サービステンプレートを含むクラスマップを適用する方法を示しています。 `Device(config-class-control-policymap)# 10 class cls_mac do-until-failure` `Device(config-action-control-policymap)# 10 activate service-template svc1` 例：	ローカルプロファイリング ポリシーのクラスマップ番号を設定し、アクションの実行方法を指定するか、サービステンプレートをアクティブ化するか、identity-update 属性を自動設定テンプレートにマッピングします。

	コマンドまたはアクション	目的
	次の例は、パラメータ マップを適用する方法を示しています（パラメータ マップ「param」の作成時にサービス テンプレートがすでに関連付けられています）。 `Device(config-action-control-policymap)#1 map attribute-to-service table param`	
ステップ 5	**end** 例： `Device(config-action-control-policymap)# end`	コンフィギュレーション モードを終了します。
ステップ 6	**configure terminal** 例： `Device# 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 7	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-wlan-policy`	ワイヤレス ポリシー プロファイルを設定します。 **注意** 名前付きワイヤレス プロファイル ポリシーでネイティブ プロファイリングの AAA オーバーライドを設定しないでください。
ステップ 8	**description** *profile-policy-description* 例： `Device(config-wireless-policy)# description "default policy profile"`	ポリシー プロファイルの説明を追加します。
ステップ 9	**dhcp-tlv-caching** 例： `Device(config-wireless-policy)# dhcp-tlv-caching`	WLAN で DHCP TLV キャッシングを設定します。
ステップ 10	**http-tlv-caching** 例： `Device(config-wireless-policy)# http-tlv-caching`	WLAN でクライアント HTTP TLV キャッシングを設定します。
ステップ 11	**subscriber-policy-name** *policy-name* 例： `Device(config-wireless-policy)# subscriber-policy-name polmap5`	サブスクライバ ポリシー名を設定します。

	コマンドまたはアクション	目的
ステップ 12	**vlan** *vlan-id* 例： `Device(config-wireless-policy)# vlan 1`	VLAN 名または VLAN ID を設定します。
ステップ 13	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	設定を保存します。

ローカルモードでのネイティブプロファイリングの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy np_local_policy`	ワイヤレス ポリシー プロファイルを設定します。
ステップ 3	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 4	**dhcp-tlv-caching** 例： `Device(config-wireless-policy)# dhcp-tlv-caching`	WLAN で DHCP TLV キャッシングを設定します。
ステップ 5	**http-tlv-caching** 例： `Device(config-wireless-policy)# http-tlv-caching`	WLAN でクライアント HTTP TLV キャッシングを設定します。
ステップ 6	**subscriber-policy-name***subsciber-policy* 例：	サブスクライバ ポリシー名を設定します。

	コマンドまたはアクション	目的
	`Device(config-wireless-policy)# subscriber-policy-name polmap1`	
ステップ 7	**vlan***vlan-id* 例： `Device(config-wireless-policy)# vlan 1`	VLAN 名または VLAN ID を設定します。
ステップ 8	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	設定を保存します。
ステップ 9	**exit** 例： `Device(config-wireless-policy)# exit`	ワイヤレス ポリシー コンフィギュレーション モードを終了します。
ステップ 10	**wireless tag site** *site-name* 例： `Device(config)# wireless tag site np_local_site`	サイト タグを設定し、サイト タグ コンフィギュレーション モードを開始します。
ステップ 11	**local-site** 例： `Device(config-site-tag)# local-site`	このサイトをローカル サイトとして設定します。
ステップ 12	**exit** 例： `Device(config-site-tag)# exit`	サイト タグ コンフィギュレーション モードを終了します。
ステップ 13	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy new1`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 14	**wlan** *wlan-profile-name* **policy** *policy-name* 例： `Device(config-policy-tag)# wlan godavari-cwa policy np_local_policy`	ポリシー プロファイルを WLAN プロファイルにマッピングします。
ステップ 15	**exit** 例： `Device(config-policy-tag)# exit`	ポリシー タグ コンフィギュレーション モードを終了します。
ステップ 16	**wlan** *wlan-profile-name wlan-id ssid* 例：	WLAN と SSID を設定します。

	コマンドまたはアクション	目的
	`Device(config)# wlan godavari-cwa 199 gcae`	
ステップ 17	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 18	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 19	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 20	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 21	**no shutdown** 例： `Device(config-wlan)# no shutdown`	設定を保存します。
ステップ 22	**exit** 例： `Device(config-wlan)# exit`	WLAN コンフィギュレーション モードを終了します。
ステップ 23	**ap** *ap-mac-address* 例： `Device(config)# ap D46D.50A6.ED40`	AP コンフィギュレーション モードを開始します。
ステップ 24	**policy-tag** *policy-tag* 例： `Device(config-ap-tag)# policy-tag new1`	AP にポリシー タグを関連付けます。
ステップ 25	**site-tag** *site-tag* 例： `Device(config-ap-tag)# site-tag np_local_site`	AP にサイト タグを関連付けます。
ステップ 26	**end** 例：	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
	`Device(config-wlan)# end`	
ステップ 27	**show ap summary** 例： `Device# show ap summary`	（任意）APがフレックス モードかローカル モードかを表示します。

ネイティブ プロファイル設定の確認

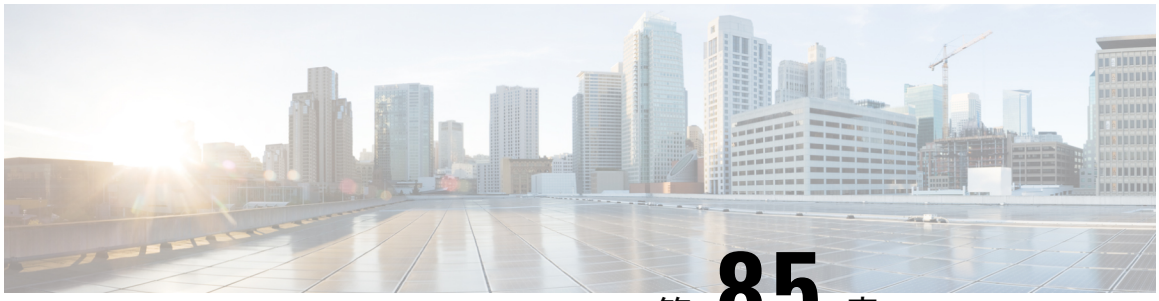
ネイティブ プロファイル設定を確認するには、次の **show** コマンドを使用します。

```
Device# show wireless client device summary

Active classified device summary
MAC Address       Device-type                      User-role
   Protocol-map
-------------------------------------------------------------------------------------------------
1491.82b8.f94b    Microsoft-Workstation            sales
              9
1491.82bc.2fd5    Windows7-Workstation             sales
             41


Device# show wireless client device cache

Cached classified device info

MAC Address       Device-type                      User-role
   Protocol-map
-------------------------------------------------------------------------------------------------
2477.031b.aa18    Microsoft-Workstation
              9
30a8.db3b.a753    Un-Classified Device
              9
4400.1011.e8b5    Un-Classified Device
              9
980c.a569.7dd0    Un-Classified Device

Device# show wireless client mac-address 4c34.8845.e32c detail | s
Session Manager:
  Interface :
  IIF ID            : 0x90000002
  Device Type       : Microsoft-Workstation
  Protocol Map      : 0x000009
  Authorized        : TRUE
  Session timeout   : 1800
  Common Session ID: 78380209000000174BF2B5B9
  Acct Session ID   : 0
  Auth Method Status List
   Method : MAB
    SM State         : TERMINATE
    Authen Status    : Success
  Local Polices:
   Service Template : wlan_svc_C414.3CCA.0A51 (priority 254)
    Absolute-Timer   : 1800
  Server Polices:
  Resultant Policies:
  Filter-ID         : acl-auto
  Input QOS         : in_qos
```

```
  Output QOS       : out_qos
  Idle timeout     : 60 sec
  VLAN              : 10
  Absolute-Timer   : 1000
```

クラス マップ名のクラス マップの詳細を確認するには、次の **show** コマンドを使用します。

```
Device# show class-map type control subscriber name test
Class-map               Action                       Exec  Hit  Miss  Comp
---------                ------                      ----  ---  ----   ---
match-any test     match day Monday                    0     0    0     0
match-any test     match join-time-of-day 8:00 18:00   0     0    0     0
Key:
  "Exec" - The number of times this line was executed
  "Hit"  - The number of times this line evaluated to TRUE
  "Miss" - The number of times this line evaluated to FALSE
  "Comp" - The number of times this line completed the execution of its
       condition without a need to continue on to the end
```



第 85 章

Air Time Fairness

Air Time Fairness について

ネットワーク管理者は Cisco Air Time Fairness（ATF）を使用して、定義済みのカテゴリでデバイスをグループ化し、一部のグループに他のグループよりも頻繁に WLAN からトラフィックを受信させることができます。これにより、一部のグループは他のグループよりも長い通信時間を利用できることになります。

Cisco ATF には次の機能があります。

- ユーザ グループまたはデバイス カテゴリに対して Wi-Fi の通信時間を割り当てる。
- Air Time Fairness は、ネットワークではなくネットワーク管理者が定義する
- 簡単な仕組みで通信時間を割り当てることができる。
- WLAN の状態の変化に動的に対応できる。
- サービス レベル契約を効率的に実行できる。
- 各種の標準規格に準拠した Wi-Fi QoS のメカニズムを強化できる。

クライアント グループごとの通信時間の長さに関する公平性をネットワーク管理者が自身の環境で定義できれば、トラフィック量も制御できます。

通信時間をパーセンテージ単位で制御するために、クライアントまたは SSID のアップリンク送信とダウンリンク送信の両方を含む通信時間が継続的に測定されます。

AP が正確に制御できるのは、ダウンリンク方向（AP からクライアント方向）の通信時間のみです。クライアントから AP へのアップリンク方向の通信時間は、測定可能ですが制御できま

せん。APは、クライアントに発信するパケットの通信時間を制限できますが、APが測定できるのはその AP がクライアントから受信したパケットの通信時間のみです。これは、AP は受信時の通信時間を正確には制限できないためです。

Cisco ATF では、通信時間の限度（全通信時間に対する割合）を設定して SSID 単位で適用します。この場合、SSID はクライアント グループを定義するパラメータとして使用されます。他のパラメータも、クライアント グループの定義に利用できます。さらに、1 つの通信時間の限度を個々のクライアントに適用できます。

SSID（またはクライアント）の通信時間の限度を超えると、ダウンリンク方向のパケットはドロップされます。ダウンリンク パケット（AP からクライアント方向）をドロップすると通信時間が解放されます。これに対して、アップリンク パケット（クライアントから AP 方向）をドロップしても、通信時間の解放にはつながりません。これは、そのパケットがクライアントによって無線で送信済みであるためです。

クライアント フェア シェアリング

Cisco Air Time Fairness は、SSID または WLAN に関連付けられたクライアントで実施できます。これにより、SSID または WLAN 内のすべてのクライアントは、それぞれの無線帯域幅の使用率に基づいて均等に扱われます。この機能は、1 つまたは少数のクライアントが SSID または WLAN に割り当てられたすべての通信時間を消費することで、同じ SSID または WLAN に関連付けられた他のクライアントが Wi-Fi を利用できなくなる場合に便利です。

- 各クライアントに割り当てる通信時間の割合は、クライアントの接続または切断のたびに計算し直されます。
- クライアント フェア シェアリングを適用できるのは、ダウンストリーム トラフィックのみです。
- クライアントはポリシー レベルで、低、中、高の使用率グループに分類できます。
- クライアントベースの ATF メトリックは、送信完了ルーチンで累積します。これにより、使用率が中から低のグループのクライアントが未使用の通信時間をシェア プール バケットに累積して、使用率が高いクライアントに通信時間を融通することができます。

サポート対象のアクセス ポイント プラットフォーム

Cisco ATF は、次の Cisco IOS アクセス ポイントでサポートされています。

- Cisco Aironet 1260 シリーズ アクセス ポイント
- Cisco Aironet 2600 シリーズ アクセス ポイント
- Cisco Aironet 3500 シリーズ アクセス ポイント
- Cisco Aironet 3600 シリーズ アクセス ポイント
- Cisco Aironet 3700 シリーズ アクセス ポイント

（注） AP が ATF をサポートしている場合、Cisco ATF はメッシュでサポートされます。

Cisco ATF モード

Cisco ATF は以下のモードで動作します。

- 次の操作をユーザが実行できる監視モード：
  - 通信時間の表示
  - すべての AP 送信の通信時間の報告
  - レポートの表示
    - SSID または WLAN 単位
    - AP グループ単位
    - AP 単位
    - クライアントごと
  - 通信時間の使用量の定期報告
  - モニタ モードの一部としての適用なし
- 次の操作をユーザが実行できるポリシー適用モード：
  - 設定したポリシーに基づいて通信時間を適用
  - 次の項目に通信時間を適用
    - 単独の WLAN
    - Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ ネットワークに接続されているすべての AP
    - 単独の AP グループ
    - AP
    - クライアント 1 台

Cisco Air Time Fairness の制限

- Cisco ATF を実装できるのはダウンストリーム方向のデータ フレームのみです。
- SSID 単位モードで ATF を設定する場合は、すべての WLAN を無効にしてから ATF 設定コマンドを入力します。すべての ATF コマンドを入力した後に WLAN を有効にします。

Cisco Air Time Fairness （ATF）の使用例

パブリック ホットスポット（スタジアム/空港/コンベンション センターなど）

この例では、パブリック ネットワークが複数のサービス プロバイダーおよび施設との間で WLAN を共有しています。各サービス プロバイダーのサブスクライバをグループ化して、一定割合の通信時間を割り当てることができます。

Education

たとえば大学では、学生、教員、およびゲスト間で WLAN を共有しています。ゲスト ネットワークは、サービスプロバイダーによってさらに分割できます。各グループに一定割合の通信時間を割り当てることができます。

エンタープライズ/サービス/小売

この場合、施設は、従業員とゲスト間で WLAN を共有しています。ゲスト ネットワークは、サービス プロバイダーによってさらに分割できます。ゲストをサービス レベルによってサブグループ化し、サブグループごとに一定割合の通信時間を割り当てることができます（有料グループには、無料グループよりも多く割り当てるなど）。

時間を共有する管理型ホットスポット

この場合、サービス プロバイダーや企業などのホットスポットを管理するビジネス エンティティは、通信時間を割り当てて他のビジネス エンティティにリースすることができます。

次に、Cisco ATF の設定手順の概要を示します。

1. モニタ モードを有効にして、ネットワーク使用量を特定します（任意）。
2. Cisco ATF ポリシーを作成します。
3. ネットワーク、AP グループ、または個別の AP 単位で WLAN ATF ポリシーを追加します。AP または AP グループに設定したポリシーは、ネットワーク ポリシーごとにオーバーライドします。
4. 最適化を有効にする必要があるかどうかを特定します。
5. Cisco ATF の統計情報を定期的に確認します。

Cisco Air Time Fairness（ATF）の設定

Cisco ATF ポリシーの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile airtime-fairness** *atf-policy-name atf-profile-id* 例： `Device(config)# wireless profile airtime-fairness atf-policy-name 1`	新しい Cisco ATF ポリシーを作成します。 • *atf-policy-name*：ATF プロファイル名を入力します。 • *atf-profile-id*：ATF プロファイル ID を入力します。範囲は 0 ～ 511 です。
ステップ 3	**weight** *policy-weight* 例： `Device(config-config-atf)# weight 5`	Cisco ATF ポリシーにウェイトを追加します。 • *policy-weight*：ポリシー ウェイトを入力します。範囲は 5 ～ 100 です。
ステップ 4	**client-sharing** 例： `Device(config-config-atf)# client-sharing`	Cisco ATF ポリシーのクライアント共有を有効または無効にします。
ステップ 5	**end** 例： `Device(config-config-atf)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AP のポリシー プロファイルへの Cisco ATF ポリシーの適用（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Air Time Fairness] を選択し、以下を設定します。

ステップ 2 ATF ポリシーの名前、ID、およびウェイトを指定します。合計が 100 を超えるできるよう、パーセンテージではなくウェイト比率が使用されます。設定可能なウェイトの最小値は 5 です。

ステップ 3 スライダを使用して、**クライアント共有**機能を有効または無効にします。

ステップ 4 [Save & Apply to Device] をクリックして、ATF 設定を保存します。

ステップ 5 ポリシーを削除するには、該当するポリシーの横にあるチェック ボックスをオンにして [Delete] をクリックします。

ステップ 6 既存の ATF ポリシーを編集するには、編集するポリシーの横にあるチェック ボックスをオンにします。ポリシーの詳細が [Edit ATF Policy] ウィンドウに表示されます。ポリシーのウェイトおよびクライアント共有の詳細を変更できます。

AP のポリシー プロファイルへの Cisco ATF ポリシーの適用

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy profile-name`	WLAN のポリシー プロファイルを作成します。 • *profile-name*：ポリシー プロファイルのプロファイル名です。
ステップ 3	**dot11** {**24ghz** | **5ghz**} **airtime-fairness** *atf-policy-name* 例： `Device(config-wireless-policy)# dot11 24ghz airtime-fairness atf-policy-name`	2.4 または 5 GHz 無線の Air Time Fairness ポリシーを設定します。 • *atf-policy-name*：Air Time Fairness ポリシーの名前です。Cisco ATF ポリシーの作成の詳細については、「Cisco ATF ポリシーの作成」を参照してください。

	コマンドまたはアクション	目的
		（注） 2.4 GHz と 5 GHz の両方の無線に同じ ATF ポリシーを割り当てることも、2 つの異なる ATF ポリシーを割り当てることもできます。
ステップ 4	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AP に関連付けられた RF プロファイルの ATF の有効化

Cisco ATF は、2.4 または 5 GHz 無線で個別に有効化する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11** {**24ghz** | **5ghz**} **rf-profile** *rf-profile* 例： `Device(config)# ap dot11 24ghz rf-profile rfprof24_1`	2.4 または 5 GHz 無線の RF プロファイルを設定します。
ステップ 3	**airtime-fairness mode** {**enforce-policy** | **monitor**} 例： `Device(config-rf-profile)# airtime-fairness mode enforce-policy`	次のいずれかのモードで Air Time Fairness を設定します。 • ポリシー適用：このモードは ATF が動作していることを示します。 • モニタ：このモードは、通信時間に関する情報を収集して通信時間の使用状況を報告します。
ステップ 4	**airtime-fairness optimization** 例： `Device(config-rf-profile)# airtime-fairness optimization`	Air Time Fairness の最適化を有効にします。 最適化は、現在の WLAN が通信時間の限度に達し、他の使用可能な WLAN が通信時間を十分に使用できない場合に有効です。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-rf-profile)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

Cisco ATF 設定の確認

Cisco ATF 設定を確認するには、次のコマンドを使用します。

表 *34 : Cisco ATF* 設定を確認するためのコマンド

コマンド	説明
show wireless profile airtime-fairness summary	Air Time Fairness プロファイルの要約を表示します。
show wireless profile airtime-fairness mapping	ワイヤレス プロファイルとの ATF ポリシー マッピングを表示します。
show ap airtime-fairness summary	すべての無線の ATF 設定のサマリーを表示します。
show ap dot11 24ghz airtime-fairness	2.4 GHz 無線の ATF 設定を表示します。
show ap dot11 5ghz airtime-fairness	5 GHz 無線の ATF 設定を表示します。
show ap name *ap-name* **airtime-fairness**	AP の ATF 設定または統計情報を表示します。
show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **airtime-fairness statistics summary**	2.4 または 5 GHz 無線の ATF 統計情報を表示します。

Cisco ATF の統計情報の確認

表 *35 : WLAN* ごとの *ATF* 統計情報

コマンド	説明
show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **airtime-fairness wlan** *wlan_name* **statistics**	WLAN に関連する ATF 統計情報を表示します。

表 *36* : *ATF* ポリシーごとの *ATF* 統計情報

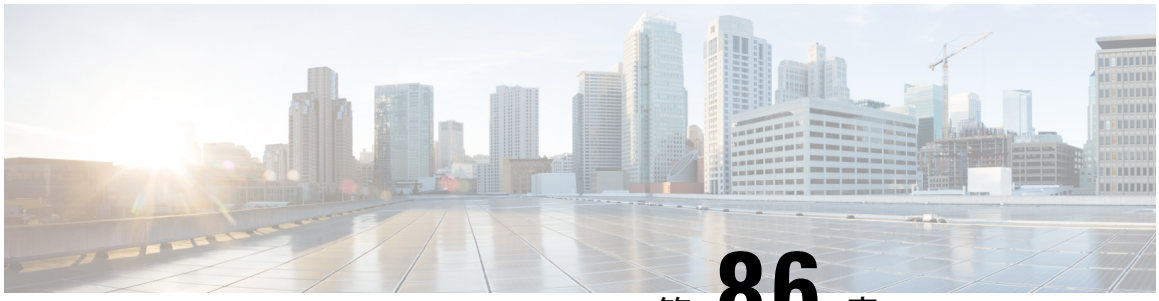
コマンド	説明
show ap name *ap-name* **dot11** {**24ghz** | **5ghz**} **airtime-fairness policy** *policy-name* **statistics**	ATF ポリシーに関連する ATF 統計情報を表示します。

表 *37* : クライアントごとの *ATF* 統計情報

コマンド	説明
show ap airtime-fairness statistics client *mac_address*	クライアントに関連する ATF 統計情報を表示します。

第 X 部

IPv6



第 86 章

IPv6 クライアントの IP アドレス ラーニング

IPv6 クライアント アドレス ラーニングについて

クライアント アドレス ラーニングは、アソシエーション、再アソシエーション、非認証、タイムアウト時に、ワイヤレス クライアントの IPv4 および IPv6 アドレス、deviceによって維持されるクライアント遷移ステートについて学習するために、deviceで設定されます。

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLACC）
- ステートフル DHCPv6
- 静的設定

これらの方法のいずれの場合も、IPv6 クライアントは常にネイバー送信要求 DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。device はクライアントの NDP および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習します。

（注） APはIPv6スタティックアドレスでのみIPv6コントローラに接続できます。自動設定を備え、複数の IPv6 アドレスを持つ AP は、IPv6 コントローラに接続できません。

関連トピック

無線ゲスト アクセス （1119 ページ）

SLAAC アドレス割り当て

IPv6 クライアント アドレス割り当て用の最も一般的な方法は、ステートレス アドレス自動設定（SLAAC）です。SLAACはクライアントがIPv6プレフィクスに基づいてアドレスを自己割り当てするシンプルなプラグアンドプレイ接続を提供します。このプロセスが実現しました。

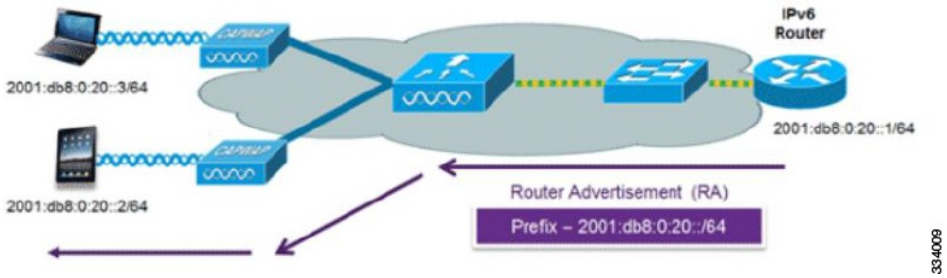
次のように、ステートレス アドレス自動設定（SLAAC）は設定されています。

- ホストは、ルータ送信要求メッセージを送信します。
- ホストは、ルータ アドバタイズメント メッセージを待機します。
- ホストは、ルータ アドバタイズメント メッセージから IPv6 プレフィックスの最初の 64 ビットを取得し、これを 64 ビット EUI-64 アドレス（イーサネットの場合、MAC アドレスから作成されます）と組み合わせて、グローバル ユニキャスト メッセージを作成します。ホストは、デフォルト ゲートウェイとして、ルータ アドバタイズメント メッセージの IP ヘッダーに含まれる送信元 IP アドレスも使用します。
- 重複アドレス検出は、選択されるランダムアドレスが他のクライアントと重複しないように、IPv6 クライアントによって実行されます。
- アルゴリズムの選択はクライアントに依存し、多くの場合は設定できます。

次の 2 種類のアルゴリズムに基づいて IPv6 アドレスの最後の 64 ビットが学習可能です。

- インターフェイスの MAC アドレスに基づく EUI-64、または
- ランダムに生成されるプライベート アドレス。

図 *21 : SLAAC* アドレス割り当て

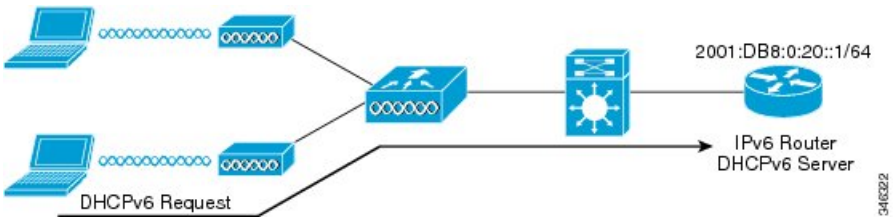


Cisco 対応 IPv6 ルータからの次の Cisco IOS コンフィギュレーション コマンドを使用して、SLAAC のアドレッシングとルータ アドバタイズメントをイネーブルにします。

```
ipv6 unicast-routing
interface Vlan20
description IPv6-SLAAC
ip address 192.168.20.1 255.255.255.0
ipv6 address FE80:DB8:0:20::1 linklocal
ipv6 address 2001:DB8:0:20::1/64
ipv6 enable
end
```

ステートフル DHCPv6 アドレス割り当て

図 *22 :* ステートフル *DHCPv6* アドレス割り当て



DHCPv6 の使用は、SLAAC がすでに導入されている場合は、IPv6 クライアント接続で要求されません。DHCPv6 にはステートレスおよびステートフルという 2 種類の動作モードがあります。

DHCPv6 ステートレス モードは、ルータ アドバタイズメントで使用できない追加のネットワーク情報をクライアントに提供するために使用しますが、これは IPv6 アドレスではありません。すでに SLAAC によって提供されているためです。この情報には DNS ドメイン名、DNS サーバ、その他の DHCP ベンダー固有オプションを含めることができます。このインターフェイス設定は、SLAAC をイネーブルにしてステートレス DHCPv6 を実装する Cisco IOS IPv6 ルータ用です。

```
ipv6 unicast-routing
ipv6 dhcp pool IPV6_DHCPPOOL
address prefix 2001:db8:5:10::/64
domain-name cisco.com
dns-server 2001:db8:6:6::1
interface Vlan20
description IPv6-DHCP-Stateless
ip address 192.168.20.1 255.255.255.0
ipv6 nd other-config-flag
ipv6 dhcp server IPV6_DHCPPOOL
ipv6 address 2001:DB8:0:20::1/64
end
```

静的 IP アドレス割り当て

クライアントにスタティックに設定されたアドレス。

ルータ要求

ルータ送信要求メッセージは、ローカル ルーティングに関する情報を入手できる、またはステートレス自動設定を設定できるルータ アドバタイズメントを送信するようにローカル ルータを促進するために、ホスト コントローラによって発行されます。ルータ アドバタイズメントは定期的に送信され、起動時または再起動操作後などに、ホストはルータ送信要求を使用して即時ルータ アドバタイズメントを要求します。

Router Advertisement

ルータ アドバタイズメント メッセージは、ルータから定期的に送信されるか、ホストからのルータ送信要求メッセージへの応答として送信されます。これらのメッセージに含まれる情報は、ホストでステートレス自動設定を実行し、ルーティング テーブルを変更するために使用されます。

ネイバー探索

IPv6 ネイバー ディスカバリとは、近隣のノード間の関係を決定するメッセージとプロセスのことです。ネイバー ディスカバリは、IPv4 で使用されていた ARP、ICMP ルータ探索、および ICMP リダイレクトに代わるものです。

信頼できるバインディング テーブル データベースを構築するために、IPv6 ネイバー ディスカバリ検査によってネイバー ディスカバリ メッセージが分析され、準拠しない IPv6 ネイバー ディスカバリ パケットはドロップされます。 内のネイバー バインディング テーブルでは、各 IPv6 アドレスと、アソシエートされた MAC アドレスが追跡されます。クライアントは、ネイバー バインディング タイマーに従って、テーブルから消去されます。

ネイバー探索抑制

ワイヤレス クライアントの IPv6 アドレスは、deviceによってキャッシュされます。deviceが IPv6 アドレスを検索する NS マルチキャストを受信して、deviceによって特定された目的のアドレスがクライアントのいずれかに属している場合、deviceはクライアントに代わって NA メッセージで応答します。このプロセスによって IPv4 のアドレス解決プロトコル（ARP）テーブルと同等のテーブルが生成されますが、より効率的であり、たいていの場合、使用されるメッセージは少なくなります。

（注） deviceがプロキシのように動作し NA で応答するのは、**ipv6 nd suppress** コマンドが設定されている場合だけです。

deviceにワイヤレス クライアントの IPv6 アドレスがない場合、device は NA で応答せず、NS パケットをワイヤレス側に転送します。この問題を解決するために、NS マルチキャスト フォワーディング ノブが用意されています。このノブがイネーブルの場合、deviceは存在しない

（キャッシュ欠落）IPv6 アドレスの NS パケットを取得し、ワイヤレス側に転送します。このパケットは、目的のワイヤレス クライアントに到達し、クライアントは NA で応答します。

このキャッシュ ミス シナリオが発生するのはまれで、完全な IPv6 スタックが実装されていないクライアントが、NDP 時にそれらの IPv6 アドレスをアドバタイズしない可能性はほとんどありません。

RA ガード

RA ガード機能は、ワイヤレス クライアントから送信されるルータ アドバタイズメントをドロップすることで、IPv6 ネットワークのセキュリティを強化します。この機能が設定されていないと、誤設定されたか、または悪意のある IPv6 クライアントが、多くの場合は高順位でクライアント自体をネットワークのルータとしてアナウンスし、正規の IPv6 ルータよりも優先される可能性があります。デフォルトでは、RA ガードは常にコントローラ上で有効になっています。

RA スロットリング

RA スロットリングは、コントローラがワイヤレス ネットワーク宛ての RA パケットを強制的に制限できるようにします。RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。クライアントが RS パケットを送信すると、RA がクライアントに返送されます。この RA は、コントローラを通過でき、クライアントにユニキャストされます。このプロセスによって、新しいクライアントやローミング クライアントが RA スロットリングの影響を受けないようにすることができます。

IPv6 クライアント アドレス ラーニングの前提条件

IPv6 クライアント アドレス ラーニングを設定する前に、IPv6 をサポートするようにワイヤレス クライアントを設定します。

ワイヤレス IPv6 クライアント接続を有効にするには、基礎となる有線ネットワークで、SLAAC または DHCPv6 などの IPv6 ルーティングおよびアドレス割り当て機能をサポートしている必要があります。ワイヤレス LAN コントローラには、IPv6 ルータに隣接する L2 が必要です。

RA スロットル ポリシーの設定（CLI）

強制的に制限できるように RA スロットル ポリシーを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ipv6 nd ra-throttler policy ra-throttler1** 例： `Device(config)# ipv6 nd ra-throttler policy ra-throttler1`	ルータ アドバタイズメント（RA）スロットラ ポリシー名を定義して、IPv6 RA スロットル ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**throttleperiod500** 例： `Device(config-nd-ra-throttle)# throttleperiod 500`	IPv6 RA スロットラ ポリシーのスロットル期間を設定します。
ステップ 4	**max-through10** 例： `Device(config-nd-ra-throttle)# max-through 500`	スロットル期間ごとに、VLANあたりのマルチキャスト RA を制限します。
ステップ 5	**allow-atleast 5 at-most 10** 例： `Device(config-nd-ra-throttle)# allow-atleast 5 at-most 10`	RA スロットラ ポリシーのスロットル期間ごとに、デバイスあたりのマルチキャスト RA 数を制限します。

VLAN への RA スロットル ポリシーの適用（GUI）

手順

ステップ 1 **[Configuration]** > **[Services]** > **[RA Throttle Policy]** を選択します。

ステップ 2 [Add] をクリックします。[Add RA Throttle Policy] ダイアログボックスが表示されます。

ステップ 3 [Name] フィールドにポリシーの名前を入力します。

ステップ 4 [Medium Type] ドロップダウンリストから必要なオプションを選択します。

ステップ 5 [Throttle Period] フィールドに値を入力します。RA スロットリングは、VLAN に対する [Max Through] 制限に達した後、または特定のルータに対する [Allow At-Most] 値に達した後にのみ実行されます。

ステップ 6 [Max Through] フィールドに、スロットリングが実行される前に送信可能な、VLAN 上の RA パケットの最大数を入力します。[No Limit] オプションを使用すると、スロットリングは実行されず、RA パケット数が無制限になります。

ステップ 7 [Interval Option] を選択します。このオプションは、IPv6 RA パケットに設定された RFC 3775 値に基づいて、デバイスのさまざまな動作を許可します。

- [Ignore]：RA スロットルが、インターバル オプションの指定されたパケットを通常の RA として処理し、有効である場合はスロットリングが適用されるようにします。
- Inherit
- [Passthrough]：RFC 3775 インターバル オプションが指定された RA メッセージがスロットリングなしで通過することを許可します。
- [Throttle]：インターバル オプションが指定された RA パケットに、常にレート制限が適用されるようにします。

ステップ 8 [At Least Multicast RAs] フィールドに、スロットリングが実行される前にマルチキャストとして送信できる、ルータごとの RA パケットの最小数を入力します。

ステップ 9 [At Most Multicast RAs] フィールドに、スロットリングが実行される前にマルチキャストとして送信できる、ルータごとの RA パケットの最大数を入力します。[No Limit] オプションを使用すると、ルータを通過する RA パケット数が無制限になります。

ステップ 10 [Add & Apply to Device] ボタンをクリックします。

VLAN への RA スロットル ポリシーの適用（CLI）

VLAN に RA スロットル ポリシーを適用します。RA スロットリングを有効にすることにより、多数の RA パケットを送信するルータを最小限の頻度に調整することができ、その場合も IPv6 クライアントの接続は維持されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**vlan configuration 1** 例： `Device(config)# vlan configuration 1`	VLAN または VLAN の集合を設定して、VLAN コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 nd ra throttler attach-policy ra-throttler1** 例： `Device(config-vlan)# ipv6 nd ra throttler attach-policy ra-throttler1`	VLAN または VLAN の集合に IPv6 RA スロットル ポリシーを接続します。

インターフェイスでの IPv6 の設定

インターフェイスで IPv6 を設定するには、次の手順に従います。

始める前に

クライアント上の IPv6 および有線インフラストラクチャ上の IPv6 サポートをイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、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。
ステップ 4	**ip address fe80::1 link-local** 例： `Device(config-if)# ip address 198.51.100.1 255.255.255.0` `Device(config-if)# ipv6 address fe80::1 link-local` `Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64` `Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`	リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。
ステップ 6	**end** 例： `Device(config)# end`	インターフェイスモードを終了します。

スイッチでの DHCP プールの設定（GUI）

手順

ステップ 1 **[Administration]** > **[DHCP]** を選択します。

ステップ 2 [Add] ボタンをクリックします。[Create DHCP Pool] ダイアログ ボックスが表示されます。

ステップ 3 [DHCP Pool Name] フィールドにプール名を入力します。名前の長さは 236 文字以下にする必要があります。

ステップ 4 [IP Type] ドロップダウンリストから [IPv4] または [IPv6] のいずれかを選択します。

ステップ 5 [Network] フィールドに IP アドレスを入力します。

ステップ 6 [Subnet Mask] ドロップダウンリストから、使用可能なサブネット マスクのいずれかを選択します。

ステップ 7 [Starting ip] フィールドに IP アドレスを入力します。

ステップ 8 [Ending ip] フィールドに IP アドレスを入力します。

ステップ 9 必要に応じて DHCP プールを予約する場合は、[Reserved Only] フィールドのステータスを [Enabled] に設定します。

ステップ 10 [Lease] ドロップダウンリストから必要なオプションを選択します。

ステップ 11 [Lease] ドロップダウンリストから [User Defined] オプションを選択すると、[(0-365 days)]、[(0-23 hours)]、および [(0-59 minutes)] フィールドが有効になります。適切な値を入力します。

ステップ 12 [Save & Apply to Device] ボタンをクリックします。

スイッチでの DHCP プールの設定

インターフェイスで DHCP プールを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**ipv6 dhcp pool Vlan21** 例： `Device(config)# ipv6 dhcp pool vlan1`	コンフィギュレーション モードを開始し、VLAN の IPv6 DHCP プールを設定します。
ステップ 4	**address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10** 例： `Device(config-dhcpv6)# address prefix 2001:DB8:0:1:FFFF:1234::/64 lifetime 300 10`	コンフィギュレーション DHCP モードを開始し、VLAN のアドレス プールとそのライフタイムを設定します。
ステップ 5	**dns-server 2001:100:0:1::1** 例： `Device(config-dhcpv6)# dns-server 2001:20:21::1`	DHCP プールの DNS サーバを設定します。
ステップ 6	**domain-name example.com** 例： `Device(config-dhcpv6)# domain-name example.com`	完全な非修飾ホスト名になるようにドメイン名を設定します。
ステップ 7	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

スイッチでの DHCP を使用しないステートレス自動アドレス設定の設定（CLI）

DHCP を使用しないステートレス自動アドレス設定を指定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、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。
ステップ 4	**ip address fe80::1 link-local** 例： `Device(config-if)# ip address 198.51.100.1 255.255.255.0` `Device(config-if)# ipv6 address fe80::1 link-local` `Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64` `Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`	リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。
ステップ 5	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。
ステップ 6	**no ipv6 nd managed-config-flag** 例： `Device(config)# interface vlan 1` `Device(config-if)# no ipv6 nd managed-config-flag`	接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。

	コマンドまたはアクション	目的
ステップ 7	**no ipv6 nd other-config-flag** 例： `Device(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCPからの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

スイッチでの DHCP を使用したステートレス自動アドレス設定の指定

DHCP を使用したステートレス自動アドレス設定を指定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface vlan 1** 例： `Device(config)# interface vlan 1`	インターフェイスを作成し、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。
ステップ 4	**ip address fe80::1 link-local** 例： `Device(config-if)# ip address 198.51.100.1 255.255.255.0` `Device(config-if)# ipv6 address fe80::1 link-local` `Device(config-if)# ipv6 address 2001:DB8:0:1:FFFF:1234::5/64` `Device(config-if)# ipv6 address 2001:DB8:0:0:E000::F/64`	リンクローカル オプションを使用してインターフェイスで IPv6 アドレスを設定します。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 enable** 例： `Device(config)# ipv6 enable`	（任意）インターフェイス上で IPv6 をイネーブルにします。
ステップ 6	**no ipv6 nd managed-config-flag** 例： `Device(config)# interface vlan 1` `Device(config-if)# no ipv6 nd managed-config-flag`	接続されたホストで、アドレスの取得にステートフル自動設定が使用されないようにします。
ステップ 7	**ipv6 nd other-config-flag** 例： `Device(config-if)# no ipv6 nd other-config-flag`	接続されたホストで、DHCP からの非アドレス オプションの取得に（ドメインなど）ステートフル自動設定が使用されないようにします。
ステップ 8	**end** 例： `Device(config)# end`	インターフェイスモードを終了します。

ネイティブ IPv6

IPv6 について

IPv6 は、デジタル ネットワーク上のデータ、音声、およびビデオ トラフィックの交換に使用されるパケットベースのプロトコルです。IPv6 は IP に基づいていますがアドレス空間が大幅に拡大されており、メインヘッダーと拡張ヘッダーが簡素化されるなどの改善が行われています。IPv6 のアーキテクチャは、既存の IPv4 ユーザがエンドツーエンドのセキュリティ、Quality Of Service（QoS）、およびグローバルに一意のアドレスなどのサービスを引き続き利用しながら、簡単に IPv6 へ移行できるように設計されています。拡大された IPv6 アドレス空間により、ネットワークのスケーラビリティが可能となり、グローバルな到達可能性が提供されます。

（注） IPv4 アドレスを使用して IPv4 ネットワークで動作する機能は、IPv6 アドレスを使用して IPv6 ネットワークでも動作します。

一般的な注意事項

- IPv6 機能を動作させるには、コントローラで **ipv6 unicast-routing** コマンドを設定する必要があります。

- ワイヤレス管理インターフェイスには、スタティック IPv6 アドレスを 1 つだけ設定する必要があります。
- IPv6 ネイバー探索：ワイヤレス管理インターフェイスおよびクライアント VLAN でルータ アドバタイズメントを抑制する必要があります（IPv6 がクライアント VLAN で設定されている場合）。
- 優先モードは、AP 接続プロファイルに含まれます。優先モードを IPv6 として設定すると、AP は最初に IPv6 を介した接続を試みます。失敗した場合、AP は IPv4 にフォールバックします。
- AP およびクライアントの RA トレースには MAC アドレスを使用する必要があります。

サポートされない機能

- UDP Lite はサポートされていません。
- IPv6 を介した AP スニッファはサポートされていません。
- IPv6 は、HA ポート インターフェイスではサポートされていません。
- IPv6 を介した自動 RF グループ化はサポートされていません。静的 RF グループ化のみがサポートされます。

IPv6 アドレッシングの設定

IPv6 を設定するには、次の手順に従います。

IPv4 アドレスを使用して IPv4 ネットワークで動作する機能はすべて、IPv6 アドレスを使用して IPv6 ネットワークでも動作します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ipv6 unicast-routing** *vlan-id* 例： `Device(config)# ipv6 unicast-routing`	ユニキャスト用に IPv6 を設定します。
ステップ 3	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 49`	インターフェイスを作成して、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。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 address** *ipv6-address* 例： `Device(config-if)# ipv6 address FD09:9:2:49::53/64`	グローバル IPv6 アドレスを指定します。
ステップ 5	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	インターフェイス上で IPv6 をイネーブルにします。
ステップ 6	**ipv6 nd ra suppress all** 例： `Device(config-if)# ipv6 nd ra suppress all`	インターフェイス上で IPv6 ルータ アドバタイズメントの送信を抑制します。
ステップ 7	**exit** 例： `Device(config-if)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 8	**wireless management interface vlan** *vlan-id* 例： `Device(config)# wireless management interface vlan 49`	ワイヤレス管理 VLAN でサポートされている AP に接続されているポートを設定します。
ステップ 9	**ipv6 route** *ipv6-address* 例： `Device(config)# ipv6 route ::/0 FD09:9:2:49::1`	IPv6 スタティック ルートを指定します。

AP 接続プロファイルの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Services]** > **[AP Join]** を選択します。

ステップ 2 [AP Join Profile] ページで [General] タブを選択し、[Add] をクリックします。

ステップ 3 [Name] フィールドに AP 接続プロファイルの名前を入力します。

ステップ 4 （任意）AP 接続プロファイルの説明を入力します。

ステップ 5 **[CAPWAP]** > **[Advanced]** タブをクリックします。

ステップ 6 [Preferred Mode] ドロップダウンリストから [IPv6] を選択します。AP の優先モードを IPv6 に設定します。

ステップ 7 [Save & Apply to Device] をクリックします。

AP 接続プロファイルの作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *ap-profile* 例： `Device(config)# ap profile xyz-ap-profile`	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。
ステップ 3	**description** *ap-profile-name* 例： `Device(config-ap-profile)# description "xyz ap profile"`	AP プロファイルの説明を追加します。
ステップ 4	**preferred-mode ipv6** 例： `Device(config-ap-profile)# preferred-mode ipv6`	APの優先モードをIPv6に設定します。

プライマリ コントローラとバックアップ コントローラの設定（GUI）

始める前に

プライマリ コントローラとバックアップ コントローラを設定する前に、AP参加プロファイルがすでに設定済みであることを確認します。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [AP Join] > > を選択します。

ステップ 2 [AP Join Profile] ページで、AP 参加プロファイル名をクリックします。

ステップ 3 [Edit AP Join Profile] ウィンドウで [CAPWAP] タブをクリックします。

ステップ 4 [Backup Controller Configuration] の [High Availability] タブで、[Enable Fallback] チェック ボックスをオンにします。

ステップ 5 プライマリ コントローラとセカンダリ コントローラの名前および IP アドレスを入力します。

ステップ 6 [Update & Apply to Device] をクリックします。

プライマリ コントローラとバックアップ コントローラの設定（CLI）

選択したアクセス ポイントのプライマリおよびセカンダリ コントローラを設定するには、次の手順に従います。

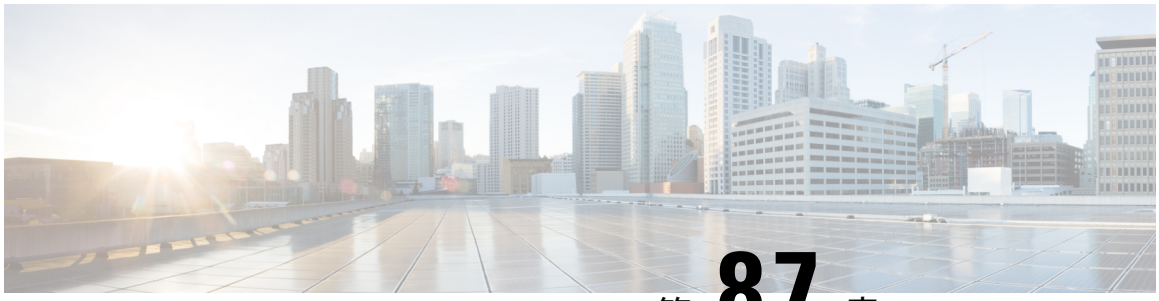
手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap profile** *profile-name* 例： `Device(config)# ap profile yy-ap-profile`	APプロファイルを設定し、APプロファイル コンフィギュレーション モードを開始します。
ステップ 3	**capwap backup primary** *primary-controller-name primary-controller-ip* 例： `Device(config)# capwap backup primary WLAN-Controller-A 10.2.3.4`	プライマリ バックアップ コントローラ名を使用して AP CAPWAP パラメータを設定します。
ステップ 4	**ap capwap backup secondary** *secondary-controller-name secondary-controller-ip* 例： `Device(config)# capwap backup secondary WLAN-Controller-B 10.2.3.5`	セカンダリ バックアップ コントローラ名を使用して AP CAPWAP パラメータを設定します。
ステップ 5	**syslog host** *ipaddress* 例： `Device(config)# syslog host 10.5.6.7`	Cisco AP のシステム ロギングを設定します。
ステップ 6	**tftp-downgrade** *tftp-server-ip imagename* 例： `Device(config)# tftp-downgrade 10.6.7.8 testimage`	すべての Cisco AP の TFTP サーバから AP イメージのダウングレードを開始します。

IPv6 設定の確認

次の **show** コマンドを使用して、IPv6 設定を確認します。

```
Device# show wireless interface summary

Wireless Interface Summary


Interface Name Interface Type VLAN ID IP Address      IP Netmask     MAC Address
-----------------------------------------------------------------------------------
Vlan49         Management     49      0.0.0.0       255.255.255.0    001e.f64c.1eff
                                      fd09:9:2:49::54/64
```



第 87 章

IPv6 ACL の設定

IPv6 ACL について

アクセス コントロール リスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます）。deviceで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、またはワイヤレス クライアントとやり取りするデータ トラフィックの制御用の WLAN、あるいは中央処理装置（CPU）宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

Web 認証用に事前認証 ACL を作成することもできます。このような ACL は、認証が完了するまでに特定のタイプのトラフィックを許可するために使用されます。

IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

（注） ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

IPv6 ACL の概要

ACL のタイプ

ユーザあたりの IPv6 ACL

ユーザあたりの ACL の場合、テキスト文字列としての完全なアクセス コントロール エントリ（ACE）が Cisco Secure Access Control Server（Cisco Secure ACS）で設定されます。

ACE はコントローラで設定されません。ACE は `ACCESS-Accept` 属性でdeviceに送信され、クライアント用に直接適用されます。ワイヤレス クライアントが外部deviceにローミングするときに、ACE が、AAA 属性としてモビリティ ハンドオフ メッセージで外部deviceに送信されます。ユーザあたりの ACL を使用した出力方向はサポートされていません。

フィルタ ID IPv6 ACL

filter-Id ACL の場合、完全な ACE および `acl name(filter-id)` がdeviceで設定され、`filter-id` のみが Cisco Secure ACS で設定されます。

`filter-id` は ACCESS-Accept 属性でdeviceに送信され、deviceは ACE の filter-id をルックアップしてから、クライアントに ACE を適用します。クライアント L2 が外部deviceにローミングするときに、filter-id だけがモビリティ ハンドオフ メッセージで外部deviceに送信されます。ユーザあたりの ACL を使用した出力フィルタ ACL はサポートされていません。外部deviceは filter-id と ACE を事前に設定する必要があります。

ダウンロード可能 IPv6 ACL

ダウンロード可能 ACL（dACL）の場合、完全な ACE および `dacl` 名は Cisco Secure ACS のみで設定されます。

Cisco Secure ACS はその `ACCESS-Accept` 属性で `dacl` 名をdeviceに送信します。デバイスは `dacl` 名を取得し、ACE のために `dACL` 名を `ACCESS-request` 属性を使用して Cisco Secure ACS に送り返します。

IPv6 ACL の設定の前提条件

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。また、スイッチが Network Essentials ライセンスで稼働している場合、入力ルータ ACL を作成し、それを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

IPv6 ACL の設定の制約事項

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。IPv6 がサポートするのは名前付き ACL だけです。IPv6 ACL は Flex 接続モードをサポートしていません。

deviceは Cisco IOS がサポートする IPv6 ACL の大部分をサポートしますが、一部例外もあります。

- deviceは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- deviceは再帰 ACL（**reflect** キーワード）をサポートしません。
- deviceは IPv6 フレームに MAC ベース ACL を適用しません。
- ACL を設定する場合、ACL に入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。ハードウェア転送が必要なインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、deviceはインターフェイスで ACL がサポートされるかどうかを判別します。サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロール エントリ（ACE）を追加しようとする場合、deviceは現在インターフェイスに適用されている ACL に ACE が追加されることを許可しません。

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングするには、次の手順に従います。

1. IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
2. IPv6 ACL が、トラフィックをブロックする（deny）または通過させる（permit）よう設定します。
3. トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。
4. インターフェイスに IPv6 ACL を適用します。ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージ プロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（例えば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリが満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。

IPv6 ACL の設定方法

IPv6 ACL の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 3	**ipv6 access-list** *acl_name* 例： `Device# ipv6 access-list access-list-name`	名前を使用して IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 4	**{deny|permit} protocol** 例： `{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	条件が一致した場合にパケットを拒否する場合は deny、許可する場合は permit を指定します。次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • source-ipv6-prefix/prefix-length または destination-ipv6-prefix/ prefix-length は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • host source-ipv6-address または destination-ipv6-address には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。オペランドには、lt（より小さい）、gt（より大きい）、eq（等しい）、neq（等しくない）、range（包含範囲）があります。

	コマンドまたはアクション	目的
		source-ipv6-prefix/prefix-length 引数のあとの operator は、送信元ポートに一致する必要があります。destination-ipv6-prefix/prefix-length 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）port-number は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）dscp value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。指定できる範囲は 0 ～ 63 です。 • （任意）fragments を入力して、先頭ではないフラグメントを確認します。このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）log を指定すると、エントリと一致するパケットに関するログ メッセージがコンソールに送信されます。log-input を指定すると、ログエントリに入力インターフェイスが追加されます。ロギングはルータ ACL でだけサポートされます。 • （任意）routing を入力して、IPv6 パケットのルーティングを指定します。 • （任意）sequence value を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。指定できる範囲は 1 ～ 4294967295 です。

	コマンドまたはアクション	目的
		• （任意）time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 5	**{deny|permit} tcp** **例：** `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。パラメータはステップ 3 で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • ack：確認応答（ACK）ビットセット • established：確立された接続。TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin：終了ビットセット。送信元からのデータはそれ以上ありません。 • neq {port | protocol}：所定のポート番号上にないパケットだけを照合します。 • psh：プッシュ機能ビット セット • range {port | protocol}：ポート番号の範囲内のパケットだけを照合します。 • rst：リセット ビット セット • syn：同期ビット セット • urg：緊急ポインタ ビット セット
ステップ 6	**{deny|permit} udp** **例：** `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length`	（任意）UDP アクセス リストおよびアクセス条件を定義します。 ユーザ データグラム プロトコルの場合は、udp を入力します。UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator

	コマンドまたはアクション	目的
		[port]] のポート番号またはポート名は、UDP ポートの番号または名前でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 7	**{deny|permit} icmp** 例： `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]`	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージプロトコルの場合は、icmp を入力します。ICMP パラメータはステップ 3a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージ タイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。 • icmp-type：ICMP メッセージ タイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-code：ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ～ 255 です。 • icmp-message：ICMP パケットを ICMP メッセージ タイプ名または ICMP メッセージ タイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのタイプ名およびコード名のリストについては、? キーを使用するか、またはこのリリースのコマンドリファレンスを参照してください。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーションモードを終了できます。
ステップ 9	**show ipv6 access-list** 例：	アクセス リストの設定を確認します。

	コマンドまたはアクション	目的
	`show ipv6 access-list`	
ステップ 10	**copy running-config startup-config** 例： `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。

WLAN IPv6 ACL の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `DeviceController # configure terminal`	端末を設定します。
ステップ 2	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy test1`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**ipv6 acl** *acl_name* 例： `Device(config-wireless-policy)# ipv6 acl testacl`	名前付き WLAN ACL を作成します。
ステップ 4	**ipv6 traffic-filter web** *acl_name-preauth* 例： `Device(config-wlan)# ipv6 traffic-filter web preauth1`	Web 認証の事前認証 ACL を作成します。

IPv6 ACL の確認

IPv6 ACL の表示

IPv6 ACL を表示するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**show access-list** 例： `Device# show access-lists`	deviceに設定されたすべてのアクセス リストを表示します。
ステップ 4	**show ipv6 access-list** *acl_name* 例： `Device# show ipv6 access-list [access-list-name]`	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

IPv6 ACL の設定例

例：IPv6 ACL の作成

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。また、この2番めの拒否エントリは、すべての一致をコンソールに表示します。リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。リスト内の 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番めの許可エントリは必要です。

（注） ロギングは、レイヤ 3 インターフェイスでのみサポートされます。

```
Device(config)# ipv6 access-list CISCO
Device(config-ipv6-acl)# deny tcp any any gt 5000
Device (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Device(config-ipv6-acl)# permit icmp any any
Device(config-ipv6-acl)# permit any any
```

例：ワイヤレス環境でのポリシー プロファイルへの IPv6 ACL の適用

次に、ワイヤレス環境でポリシー プロファイルに IPv6 ACL を適用する例を示します。

（注） すべての IPv6 ACL をポリシー プロファイルに関連付ける必要があります。

1. IPv6 ACL を作成する。

```
Device(config)# ipv6 access-list <acl-name>
Device(config-ipv6-acl)# permit tcp 2001:DB8::/32 any
Device(config-ipv6-acl)# permit udp 2001:DB8::/32 any
```

2. ポリシー プロファイルに IPv6 ACL を適用する。

```
Device(config)# wireless profile policy <policy-profile-name>
Device(config-wireless-policy)# shutdown
Device(config-wireless-policy)# ipv6 acl <acl-name>
Device(config-wireless-policy)# no shutdown
```

例：IPv6 ACL の表示

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Device #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

次に、show ipv6 access-lists 特権 EXEC コマンドの出力例を示します。出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Device# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

例：RA スロットリングの設定

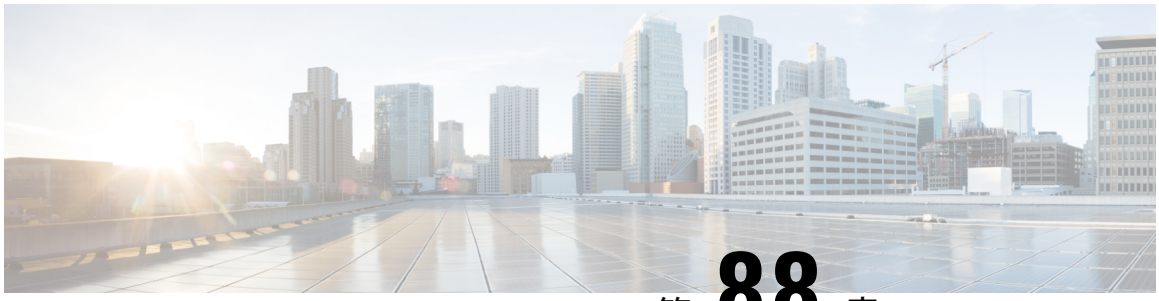
このタスクでは、省電力のワイヤレス クライアントが頻繁な非請求の定期的 RA に影響されないように、RA スロットル ポリシーを作成する方法について説明します。非請求タイプのマルチキャスト RA は、コントローラによってスロットルされます。

始める前に

クライアント マシンで IPv6 をイネーブルにします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ipv6 nd ra-throttler policy Mythrottle** 例： `Device (config)# ipv6 nd ra-throttler policy Mythrottle`	Mythrottle という RA スロットラ ポリシーを作成します。
ステップ 3	**throttle-period 20** 例： `Device (config-nd-ra-throttle)# throttle-period 20`	スロットリングを適用する時間間隔セグメントを特定します。
ステップ 4	**max-through 5** 例： `Device (config-nd-ra-throttle)# max-through 5`	許容する初期 RA の数を特定します。
ステップ 5	**allow at-least 3 at-most 5** 例： `Device (config-nd-ra-throttle)# allow at-least 3 at-most 5`	初期RAが送信された後に、間隔セグメントの終了まで許容されるRAの数を特定します。
ステップ 6	**switch (config)# vlan configuration 100** 例： `Device (config)# vlan configuration 100`	vlan あたりの設定を作成します。
ステップ 7	**ipv6 nd ra-th attach-policy attach-policy_name** 例： `Device (config)# ipv6 nd ra-throttle attach-policy attach-policy_name`	ルータ アドバタイズメント スロットリングをイネーブルにします。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。



第 88 章

IPv6 クライアント モビリティ

IPv6 クライアント モビリティについて

リンク層モビリティは、ローミング中にワイヤレス クライアントのレイヤ3アプリケーションがシームレスに動作を継続するには十分ではありません。Cisco IOSd のワイヤレス モビリティ モジュールは、モビリティ トンネリングを使用して、クライアントが異なるスイッチ上の異なるサブネット間をローミングするときに、クライアントのレイヤ 3 PoP（Point of Presence）用のシームレスな接続を維持します。

IPv6 は、プロトコルの TCP/IP スイートの IPv4 に代わることを目的とした次世代ネットワーク層インターネット プロトコルです。この新しいバージョンでは、一意のグローバル IP アドレスを必要とするユーザとアプリケーションに対応するためのインターネット グローバル アドレス空間を増大させます。IPv6 は、128 ビットの送信元アドレスおよび宛先アドレスを組み込むことにより、32 ビットの IPv4 アドレスよりも格段に多くのアドレスを提供します。

コントローラをまたいだ IPv6 クライアントをサポートするには、IPv6 クライアントが同じレイヤ 3 ネットワーク上にとどまるように、ICMPv6 メッセージを特別に処理する必要があります。deviceは、ICMPv6 メッセージを代行受信することで IPv6 クライアントを追跡し、シームレスなモビリティを提供して、ネットワーク攻撃からネットワークを保護します。NDP（ネイバー ディスカバリ パケット）パケットは、マルチキャストからユニキャストに変換され、クライアントごとに個別に配信されます。この固有なソリューションによって、ネイバーディスカバリ パケットとルータ アドバタイズメント パケットの VLAN 間でのリークを防止できます。クライアントは、特定のネイバー ディスカバリ パケットおよびルータ アドバタイズメントパケットを受信することでIPv6アドレス指定が適切であることを確認し、不要なマルチキャスト トラフィックを回避します。

IPv6 モビリティの設定は、IPv4 モビリティと同一であり、シームレスなローミングを実現するためにクライアント側で別個のソフトウェアを使用する必要はありません。deviceは、同じモビリティ グループに属している必要があります。IPv4 と IPv6 の両クライアント モビリティが、デフォルトで有効になります。

IPv6 クライアント モビリティは次のことに使用されます。

- レイヤ 2 およびレイヤ 3 ローミングでのクライアント IPv6 複数アドレスの維持
- IPv6 ネイバー探索プロトコル（NDP）パケットの管理
- クライアントの IPv6 アドレスの学習

（注） SDA ワイヤレスおよびローカル モードでの IPv6 モビリティの設定は、IPv4 モビリティの場合と同様であり、シームレスなローミングを実現するためにクライアント側で別のソフトウェアを設定する必要はありません。設定情報については、「IPv4 モビリティ」の項を参照してください。

（注） SVI で IPv6 アドレスを設定する場合は、コントローラ上のすべてのクライアント VLAN SVI インターフェイスで **ipv6 nd ra suppress all** コマンドを設定する必要があります。これにより、複数のデバイスがルータとして自身をアドバタイズすることを防ぎます。

ルータ アドバタイズメントの使用

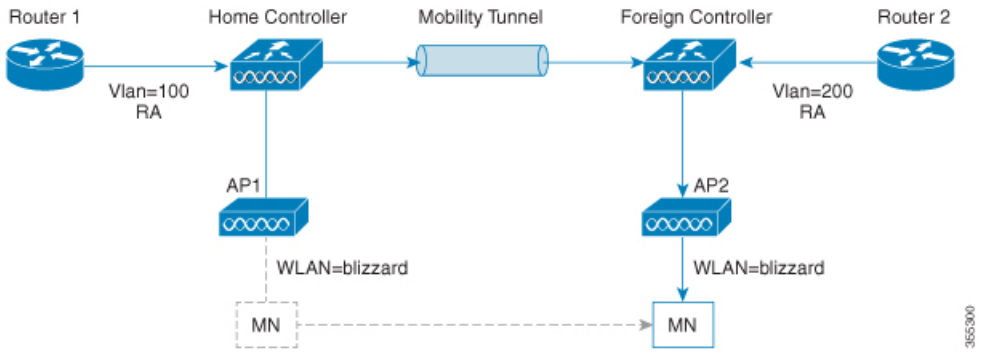
ネイバー探索プロトコル（NDP）はリンク層で動作し、リンク上の他のノードの検出を行います。他のノードのリンク層アドレスを特定し、使用可能なルータを検索し、他のアクティブなネイバー ノードのパスに関する到達可能性情報を維持します。

ルータ アドバタイズメント（RA）は、使用可能なルータを検出し、IPv6 アドレス、リンク MTU などを生成するネットワーク プレフィクスを取得するためにホストで使用される IPv6 ネイバー探索プロトコル（NDP）パケットの 1 つです。ルータは、定期的またはホスト ルータ送信要求メッセージへの応答として RA を送信します。

IPv6 ワイヤレス クライアント モビリティは IPv6 RA パケットを管理します。deviceは、リンクローカル全ノード マルチキャスト RA パケットをローカル、および RA が受信された同じ VLAN にマッピングされているローミング ワイヤレス ノードに転送します。

図 1 は、ローミング クライアント「MN」がフォーリン コントローラの VLAN 200 から RA を受信し、新しい IP アドレスを取得して L3 モビリティの PoP（Point of Presence）に入る仕組みを示しています。

図 *23* : ルータ *1* から有効な *RA* を受け取るローミング クライアント



RA スロットリング

頻繁な非請求タイプの定期的RAによる制約を受けないように省電力ワイヤレス クライアントを保護するため、コントローラで非請求タイプのマルチキャスト RA をスロットルできます。

IPv6 アドレス ラーニング

IPv6 クライアントで IPv6 アドレスを取得するには、次の 3 つの方法があります。

- ステートレス アドレス自動設定（SLAAC）
- ステートフル DHCPv6
- 静的設定

これらの方法の場合、IPv6 クライアントは常に NS DAD（重複アドレス検出）要求を送信して、ネットワークに重複する IP アドレスがないようにします。deviceはクライアントの NDP および DHCPv6 パケットをスヌープして、そのクライアント IP アドレスについて学習し、コントローラ データベースを更新します。データベースは、クライアントの新しい IP アドレスについて通知します。

複数の IP アドレスの処理

RUN 状態後に新しい IP アドレスが受信されると、追加の場合も削除の場合も、コントローラは表示目的でそのローカルデータベース上の新しいIPアドレスを更新します。基本的に、IPv6 は既存または IPv4 の場合と同じ PEM ステート マシン コード フローを使用します。IP アドレスが、たとえば、外部エンティティによってPrime Infrastructureから要求されると、コントローラは、すべての使用可能な IP アドレス、IPv4 および IPv6 を外部エンティティへの API/SPI インターフェイスに含めます。

IPv6 クライアントは、様々な目的でスタックから複数の IP アドレスを取得できます。たとえば、リンクローカル トラフィックのリンクローカル アドレスおよびルーティング可能な固有のローカル アドレスまたはグローバル アドレスがあります。

クライアントが DHCP 要求状態にあり、コントローラが IPv4 または IPv6 アドレス用にデータベースから最初の IP アドレスの通知を受信すると、PEM はクライアントを RUN 状態に移行させます。

RUN状態後に新しいIPアドレスが受信されるときは、追加の場合も削除の場合も、コントローラは表示目的でそのローカル データベース上の新しい IP アドレスを更新します。

IP アドレスが、たとえば、外部エンティティによって Prime Infrastructure から要求されると、コントローラは、使用可能な IP アドレス、IPv4 および IPv6 を外部エンティティに提供します。

IPv6 設定

deviceは IPv4 クライアントと同様にシームレスに IPv6 クライアントをサポートします。管理者は手動で VLAN を設定し、IPv6 および IPv6 のスヌーピングとスロットリングの機能を有効にする必要があります。これにより、deviceとそのさまざまなクライアントの間でNDPパケットをスロットリングできます。

IPv6 クライアント モビリティの前提条件

- ワイヤレス IPv6 クライアント接続をイネーブルにするには、基礎となる有線ネットワークで、SLAAC または DHCPv6 などの IPv6 ルーティングおよびアドレス割り当て機能をサポートしている必要があります。deviceは IPv6 ルータに対する L2 隣接関係が必要です。また、VLANはパケットがdeviceに着信するときにタグを付ける必要があります。APは、IPv6 ネットワーク上で接続を必要としません。すべてのトラフィックが AP とdevice間の IPv4 CAPWAP トンネル内でカプセル化されるためです。
- IPv6 クライアント モビリティを使用する場合、クライアントはスタティック ステートレス自動設定またはステートフル DHCPv6 IP アドレッシングのいずれかで IPv6 をサポートする必要があります。
- ステートフル DHCPv6 IP アドレッシングが円滑に動作できるようにするには、DHCPv6 サーバとして動作するように設定された DHCP for IPv6 機能をサポートするスイッチまたはルータ、または組み込み DHCPv6 サーバを備えた Windows 2008 サーバなどの専用サーバが必要です。

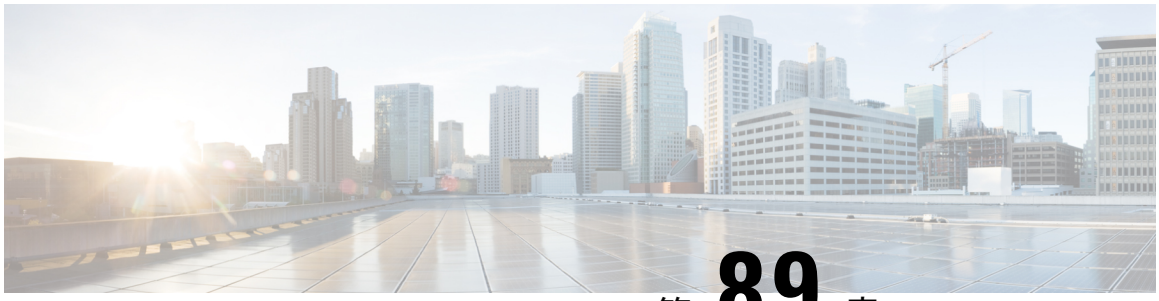
IPv6 クライアント モビリティのモニタリング

表 1 のコマンドは、deviceで IPv6 クライアント モビリティをモニタリングするために使用されます。

表 *38 : IPv6* クライアント モビリティ コマンドのモニタリング

コマンド	Description

show wireless client summary	アクティブなクライアントのワイヤレス固有設定を表示します。
show wireless client mac-address (mac-addr-detail)	アクティブなクライアントのワイヤレス固有設定をその MAC アドレスに基づいて表示します。



第 89 章

フレックスとメッシュでの IPv6 サポート

フレックス + メッシュ展開での IPv6 サポート

IPv6 は、サービス プロバイダーのバックホール転送です。フレックス + メッシュでの IPv6 サポート機能が、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでサポートされるようになりました。WLAN は IPv6 クライアントを受け入れてトラフィックを転送します。

フレックス + メッシュの IPv6 サポートの設定

コントローラで IPv6 ルーティングを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 vlan** *vlan-interface-number* 例： `Device(config)#interface vlan 89`	インターフェイスを作成して、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。
ステップ 3	**shutdown** 例： `Device(config-if)#shutdown`	インターフェイスの設定を無効にします。

	コマンドまたはアクション	目的
ステップ 4	**ipv6 enable** 例： `Device(config-if)#ipv6 enable`	インターフェイス上で IPv6 をイネーブルにします。
ステップ 5	**ipv6 address** *X:X:X:X::X/<0-128>* 例： `Device(config-if)#ipv6 address 1:1:1:1::1/64`	IPv6 プレフィックス オプションを使用して、インターフェイスで IPv6 アドレスを設定します。
ステップ 6	**no shutdown** 例： `Device(config-if)#no shutdown`	IPv6 アドレスを有効にします。
ステップ 7	**ipv6 mld version** *version-number* 例： `Device(config-if)#ipv6 mld version 1`	IPv6 MLD バージョンを有効にします。バージョンは、1 または 2 のいずれかです。
ステップ 8	**ip pim dense-mode** 例： `Device(config-if)#ip pim dense-mode`	PIM 高密度モードの動作を設定します。
ステップ 9	**no shutdown** 例： `Device(config-if)#no shutdown`	PIM 高密度モードの動作を有効にします。
ステップ 10	**end** 例： `Device(config-if)#end`	特権 EXEC モードに戻ります。
ステップ 11	**show ipv6 interface brief** 例： `Device#show ipv6 interface brief`	入力を確認します。
ステップ 12	**ping ipv6** *destination-address or hostname* 例： `Device#ping ipv6 1:1:1:1::10`	ゲートウェイの接続を確認します。

IPv6 としての優先 IP アドレスの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**Configure Terminal** 例： `Device# 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	**ap profile** *default-ap-profile* 例： `Device(config)# ap profile default-ap-profile`	AP プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**preferred-mode ipv6** 例： `Device(config-ap-profile)# preferred-mode ipv6`	IPv6 を使用してコントローラに接続します。
ステップ 4	**end** 例： `Device(config-ap-profile)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

フレックス + メッシュでの IPv6 の確認

コントローラの IPv6 設定を確認するには、次の **show** コマンドを使用します。

```
Device#show ip interface brief
Interface              IP-Address      OK? Method Status                Protocol
GigabitEthernet2       unassigned      YES unset  up                    up
GigabitEthernet0       unassigned      YES NVRAM  administratively down down
Capwap1                unassigned      YES unset  up                    up
Capwap2                unassigned      YES unset  up                    up
Vlan1                  unassigned      YES NVRAM  administratively down down
Vlan89                 9.10.89.90      YES NVRAM  up                    up
Ewlc-9.10.89.90#show running-config interface vlan 89
Building configuration...

Current configuration : 120 bytes
!
interface Vlan89
 ip address 9.10.89.90 255.255.255.0
 ip helper-address 9.1.0.100
 no mop enabled
 no mop sysid
end
```

第 XI 部

CleanAir

第 90 章

Cisco CleanAir

Cisco CleanAir について

Cisco CleanAir は、共有ワイヤレス スペクトラムに関する問題の予防的な管理を目的に設計されたソリューションです。この機能を使用すると、共有スペクトラムの全ユーザを確認できます（ネイティブデバイスと外部干渉源の両方）。また、この情報に基づいてネットワークが対処できるようにします。たとえば、干渉デバイスを手動で排除することや、システムによって自動的にチャネルを変更して干渉を受けないようにすることができます。CleanAir は、スペクトラム管理と無線周波数（RF）の可視性を提供します。

Cisco CleanAir システムは CleanAir 対応アクセス ポイントおよび Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで構成されます。アクセス ポイントは工業、科学、医療用（ISM）帯域で動作するすべてのデバイスの情報を収集し、これらの情報を潜在的な干渉源として特定および評価してコントローラに転送します。コントローラはアクセス ポイントを制御して干渉デバイスを表示し。

ライセンス不要の帯域で動作している各デバイスについては、Cisco CleanAir はその種類、ワイヤレス ネットワークに与える影響の程度、取るべき対策を提示します。これによって RF がシンプルになり、管理者が RF のエキスパートである必要がなくなります。

ワイヤレス LAN システムは、ライセンス不要の 2.4 GHz および 5 GHz ISM 帯域で動作します。電子レンジやコードレス電話、そして Bluetooth デバイスなどの多くのデバイスもこれらの帯域で稼働するため、Wi-Fi の動作に悪影響を与える可能性があります。

Voice over Wireless や IEEE 802.11n 無線通信などの非常に高度な WLAN サービスの一部は、ISM 帯域を合法的に使用する他の機器からの干渉によって、重大な影響を受ける可能性があります。Cisco CleanAir 機能の統合により、この RF 干渉の問題に対処できます。

Cisco CleanAir 関連の用語

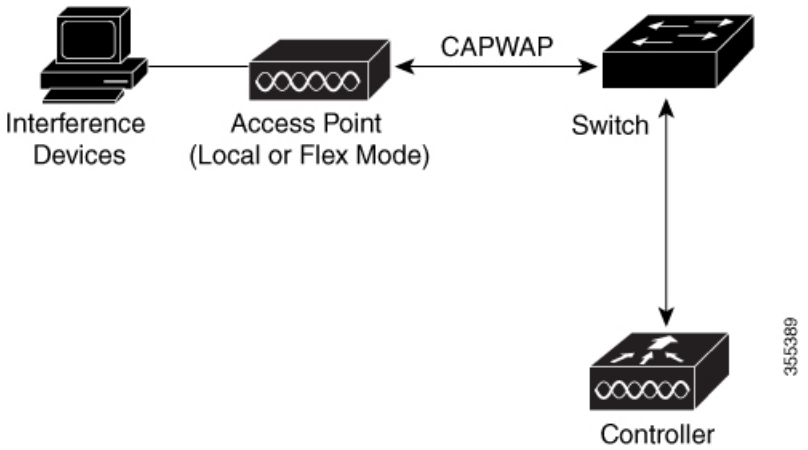
表 *39 : CleanAir* 関連の用語

用語	説明
AQI	電波品質の指標。AQI は空気汚染物質に基づいた電波品質の指標です。AQI が 0 の場合は不良で、AQI が 85 より大きいと良好です。
AQR	電波品質レポート。AQR には、特定されたすべての発生源からの干渉全体に関する情報（AQI で表される）や、最も重大な干渉カテゴリの概要が示されます。AQR は 15 分ごとにモビリティ コントローラに送信され、30 秒ごとに迅速モードで送信されます。
DC	デューティ サイクル。チャネルがデバイスで使用される時間の割合。
EDRRM	イベント駆動型 RRM。EDRRM は、緊急事態にあるアクセス ポイントが、正常な RRM 間隔をバイパスし、すぐにチャネルを変更できるようにします。
IDR	アクセス ポイントがコントローラに送信する干渉デバイス レポート。
ISI	干渉の重大度指標。ISI は、干渉の重大度の指標です。
RSSI	受信信号強度インジケータ。RSSI は受信した無線信号における電力の測定値です。アクセス ポイントはこの電力で干渉デバイスを認識します。

Cisco CleanAir のコンポーネント

Cisco CleanAir の基本的なアーキテクチャは、Cisco CleanAir 対応 AP およびdeviceで構成されます。

図 *24 : Cisco CleanAir* ソリューション



Cisco CleanAir テクノロジーを搭載したアクセス ポイントは、非 Wi-Fi 干渉源に関する情報を収集しそれを処理します。アクセス ポイントは、電波品質レポート（AQR）および干渉デバイス レポート（IDR）を収集してコントローラに送信します。

コントローラは CleanAir 対応のアクセス ポイントを制御および設定し、スペクトラム データを収集および処理します。コントローラはCleanAirの基本機能およびサービスを設定し、現在のスペクトラム情報を表示するローカル ユーザ インターフェイス（GUI および CLI）を提供します。また、コントローラはRRM TPC と DCM を使用して、干渉デバイスを検出、マージ、および軽減します。詳細については、「干渉デバイスのマージ」を参照してください。

Cisco CleanAir システムにおいて、deviceは次のような処理を実行します。

- アクセス ポイントにおける Cisco CleanAir 機能を設定する。
- Cisco CleanAir の機能の設定やデータ収集のためのインターフェイス（GUI、CLI）を提供する。
- スペクトラム データを表示する。
- アクセス ポイントから AQR を収集して処理し、電波品質データベースに保存する。AQR には、特定されたすべての発生源からの干渉全体に関する情報（電波品質の指標（AQI）で表す）や、最も重大な干渉カテゴリの概要が示されます。またCleanAirシステムでは、干渉の種類別レポートに未分類の干渉情報を含めることができ、未分類の干渉デバイスによる干渉が頻繁に生じる場合に対処することができます。
- アクセス ポイントから IDR を収集して処理し、干渉デバイス データベースに保存する。

（注） コントローラで Cisco CleanAir を無効にしてスペクトル インテリジェンス（SI）を有効にすると、CleanAir と電波品質レポートの両方が無効になります。ただし SI AP の電波品質は引き続き読み込まれ、**show ap dot11 5ghz/24ghz cleanair config** コマンドを実行すると、無効として表示されます。これは、SI AP が電波品質を報告する場合に想定される動作です。

この場合、スペクトル インテリジェンスは CleanAir 機能のサブセットです。スペクトル インテリジェンスの詳細については、『Spectrum Intelligence Deployment Guide』を参照してください。

Cisco CleanAir で検出できる干渉の種類

Cisco CleanAir アクセス ポイントでは、干渉を検出してその重大度をレポートすることができます。スペクトラム イベント駆動型 RRM は、このような緩和方法の 1 つです。

Wi-Fi チップをベースとする RF 管理システムには、次のような共通の特性があります。

- Wi-Fi 信号として識別できない RF エネルギーはノイズとして報告される。
- チャネル計画の割り当てに使用するノイズの測定値は、一部のクライアントデバイスに悪影響を及ぼす可能性のある不安定さや急速な変化を避けるために、一定の期間において平均化される傾向がある。
- 測定値が平均化されることで、測定値の精度が低下する。そのため、平均化された後、クライアントに混乱をもたらす信号が緩和を必要とするものに見えない場合がある。

• 現在使用できる RF 管理システムは、本質的にはすべて事後対応型である。

Cisco CleanAir はこれらと異なり、ノイズの発生源だけでなく、WLAN に対する潜在的な影響まで明確に特定することができます。このような情報を入手することにより、ネットワーク内におけるノイズを考慮し、理にかなった、可能であれば予防的な判断を行うことができます。通常、CleanAir には自発的干渉イベントが使用されます。

（注） イベント駆動型 RRM は、Cisco CleanAir 対応でローカル モードにあるアクセス ポイントによってのみ動作します。

（注） Qualcomm Atheros チップセットを使用するすべての AP は、無線が干渉を検出した場合も、電波品質を 100% として送信します。

突発的干渉は、ネットワーク上に突然発生する干渉であり、おそらくは、あるチャネル、またはある範囲内のチャネルが完全に妨害を受けます。Cisco CleanAir のスペクトラム イベント駆動型 RRM 機能を使用すると、電波品質（AQ）のしきい値を設定できます。このしきい値を超過した場合は、影響を受けたアクセス ポイントに対してチャネル変更がただちに行われます。ほとんどの RF 管理システムでは干渉を回避できますが、この情報がシステム全体に伝搬するには時間を要します。Cisco CleanAir では AQ 測定値を使用してスペクトラムを連続的に評価するため、対応策を 30 秒以内に実行します。たとえば、アクセス ポイントがビデオ カメラからの干渉を受けた場合は、そのカメラが動作し始めてから 30 秒以内にチャネル変更によってアクセス ポイントを回復させることができます。Cisco CleanAir では干渉源の識別と位置の特定も行うため、後からその装置の永続的な緩和処理も実行できます。

Bluetooth デバイスの場合、Cisco CleanAir 対応のアクセス ポイントで干渉の検出と報告を行うことができるのは、そのデバイスがアクティブに送信しているときだけです。Bluetooth デバイスには、さまざまな省電力モードがあります。たとえば、接続されたデバイス間でデータまたは音声がストリーム化されている最中に干渉が検出されます。

EDRRM および AQR の更新モード

EDRRM は、緊急事態にあるアクセス ポイントが、正常な RRM 間隔をバイパスしてすぐにチャネルを変更できるようにするための機能です。CleanAir アクセス ポイントは AQ を常に監視し、AQ を 15 分ごとに報告します。AQ は分類された干渉デバイスのみを報告します。EDRRM の主なメリットは短い処理時間です。干渉デバイスがアクティブ チャネルで動作しており、EDRRM をトリガーするのに十分な AQ の低下を引き起こした場合、クライアントはそのチャネルまたはアクセス ポイントを使用できなくなります。チャネルからアクセス ポイントを削除する必要があります。EDRRM はデフォルトではイネーブルになっていません。最初に CleanAir をイネーブルにしてから、EDRRM をイネーブルにします。

CleanAir の前提条件

Cisco CleanAir は、CleanAir 対応のアクセス ポイントにのみ設定できます。

次のアクセス ポイント モードを使用して、Cisco CleanAir スペクトラム モニタリングを実行できるのは、Cisco CleanAir 対応のアクセス ポイントだけです。

- Local：このモードでは、Cisco CleanAir 対応の各アクセス ポイント無線によって、現在の動作チャネルだけに関する電波品質と干渉検出のレポートが作成されます。
- FlexConnect：FlexConnect アクセス ポイントがコントローラに接続しているとき、その Cisco CleanAir 機能はローカル モードと同じになります。
- Monitor：Cisco CleanAir が監視モードで有効になっていると、そのアクセス ポイントによって、モニタされているすべてのチャネルに関する電波品質と干渉検出のレポートが作成されます。

  次のオプションを使用できます。

  - All：すべてのチャネル
  - DCA：DCA リストによって管理されるチャネル選択
  - Country：規制ドメイン内で合法なすべてのチャネル

（注） 一度感知された AP を手動でリブートすると、クラッシュが複数回が発生し、AP 無線は起動しません。コントローラにはエラー メッセージは表示されません。

CleanAir の制約事項

- 監視モードのアクセス ポイントは、Wi-Fi トラフィックまたは 802.11 パケットを送信しません。これらは無線リソース管理（RRM）計画から除外され、隣接アクセス ポイントのリストに含まれません。IDR クラスタリングは、deviceがネットワーク内の隣接アクセス ポイントを検出する機能に依存しています。複数のアクセスポイントから関係する干渉デバイスを検出する機能を使用できるのは、監視モードのアクセス ポイント間に限られます。
- スロット 2 のモニタ モード アクセス ポイントは 2.4 GHz でのみ動作します。
- ローカル モード アクセス ポイント 5 つに対してモニタ モード アクセス ポイント 1 つという比率をお勧めします。これは、最適なカバレッジに関するネットワーク設計やエキスパートのガイダンスによって異なる場合があります。
- チャネル幅が 160 MHz の場合、CleanAir はサポートされません。

CleanAir の設定方法

2.4 GHz 帯域の CleanAir の有効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[CleanAir]** を選択します。
ステップ 2 [CleanAir] ページで **[2.4 GHz Band]** > **[General]** タブをクリックします。
ステップ 3 [Enable CleanAir] チェックボックスをオンにします。
ステップ 4 [Apply] をクリックします。

2.4 GHz 帯域の CleanAir の有効化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz cleanair** 例： `Device(config)#ap dot11 24ghz cleanair` `Device(config)#no ap dot11 24ghz cleanair`	802.11b ネットワークで CleanAir 機能を有効にします。802.11b ネットワークで CleanAir を無効にするには、このコマンドの **no** 形式を実行します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

2.4 GHz デバイスの干渉レポートの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[CleanAir]** を選択します。

ステップ 2 [2.4 GHz Band] タブをクリックします。

ステップ 3 干渉タイプを選択し、[Interference Types to detect] セクションに追加します。

次の干渉タイプを使用できます。

- BLE Beacon：Bluetooth Low Energy ビーコン
- Bluetooth 検出
- Bluetooth リンク
- Canopy
- 連続トランスミッタ
- DECT-like Phone：Digital Enhanced Cordless Technology 電話機
- 802.11 FH：802.11 周波数ホッピング デバイス
- WiFi Inverted：スペクトル反転 Wi-Fi 信号を使用するデバイス
- Jammer
- 電子レンジ
- WiFi Invalid Channel：非標準の Wi-Fi チャネルを使用するデバイス
- TDD トランスミッタ
- Video Camera
- SuperAG：802.11 SuperAG デバイス
- WiMax Mobile
- WiMax Fixed
- 802.15.4
- Microsoft Device
- SI_FHSS

ステップ 4 [Apply] をクリックします。

2.4 GHz デバイスの干渉レポートの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 24ghz cleanair device {ble-beacon | bt-discovery | bt-link | canopy | cont-tx | dect-like | fh | inv | jammer | mw-oven | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile | xbox | zigbee }** 例： `Device(config)# ap dot11 24ghz cleanair device ble-beacon` `Device(config)# ap dot11 24ghz cleanair device bt-discovery` `Device(config)# ap dot11 24ghz cleanair device bt-link` `Device(config)# ap dot11 24ghz cleanair device canopy` `Device(config)# ap dot11 24ghz cleanair device cont-tx` `Device(config)# ap dot11 24ghz cleanair device dect-like` `Device(config)# ap dot11 24ghz cleanair device fh` `Device(config)# ap dot11 24ghz cleanair device inv` `Device(config)# ap dot11 24ghz cleanair device jammer` `Device(config)# ap dot11 24ghz cleanair device mw-oven` `Device(config)# ap dot11 24ghz cleanair device nonstd` `Device(config)# ap dot11 24ghz cleanair device report` `Device(config)# ap dot11 24ghz cleanair`	deviceに報告するように 2.4 GHz 干渉デバイスを設定します。設定を無効にするには、このコマンドの **no** 形式を実行します。 次に、キーワードの説明のリストを示します。 • **ble-beacon**：Bluetooth Low Energy ビーコン • **bt-discovery**：Bluetooth の検出 • **bt-link**：Bluetooth リンク • **canopy**：Canopy デバイス • **cont-tx**：連続トランスミッタ • **dect-like**：Digital Enhanced Cordless Communication 方式の電話機 • **fh**：802.11 周波数ホッピング デバイス • **inv**：スペクトル反転 Wi-Fi 信号を使用するデバイス • **jammer**：電波妨害装 • **mw-oven**：電子レンジ • **nonstd**：非標準 Wi-Fi チャネルを使用するデバイス • **report**：説明なし • **superag**：802.11 SuperAG デバイス • **tdd-tx**：TDD トランスミッタ • **video**：ビデオ カメラ

	コマンドまたはアクション	目的
	device superag `Device(config)# ap dot11 24ghz cleanair device tdd-tx` `Device(config)# ap dot11 24ghz cleanair device video` `Device(config)# ap dot11 24ghz cleanair device wimax-fixed` `Device(config)# ap dot11 24ghz cleanair device wimax-mobile` `Device(config)# ap dot11 24ghz cleanair device xbox` `Device(config)# ap dot11 24ghz cleanair device zigbee`	• **wimax-fixed**：WiMax 固定 • **wimax-mobile**：WiMax モバイル • **xbox**：Xbox デバイス • **zigbee**：802.15.4 デバイス
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

5 GHz 帯域の CleanAir の有効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[CleanAir]** を選択します。
ステップ 2 [CleanAir] ページで **[5 GHz Band]** > **[General]** タブをクリックします。
ステップ 3 [Enable CleanAir] チェックボックスをオンにします。
ステップ 4 [Apply] をクリックします。

5 GHz 帯域の CleanAir の有効化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**ap dot11 5ghz cleanair** 例： `Device(config)#ap dot11 5ghz cleanair` `Device(config)#no ap dot11 5ghz cleanair`	802.11a ネットワークで CleanAir 機能を有効にします。802.11a ネットワークで CleanAir を無効にするには、このコマンドの **no** 形式を実行します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

5 GHz デバイスの干渉レポートの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[CleanAir]** を選択します。

ステップ 2 [5 GHz Band] タブをクリックします。

ステップ 3 干渉タイプを選択し、[Interference Types to detect] セクションに追加します。

次の干渉タイプを使用できます。

- Canopy
- 連続トランスミッタ
- DECT-like Phone：Digital Enhanced Cordless Technology 電話機
- 802.11 FH：802.11 周波数ホッピング デバイス
- WiFi Inverted：スペクトル反転 Wi-Fi 信号を使用するデバイス
- Jammer
- WiFi Invalid Channel：非標準の Wi-Fi チャネルを使用するデバイス
- SuperAG：802.11 SuperAG デバイス
- TDD トランスミッタ
- WiMax Mobile
- WiMax Fixed
- Video Camera

ステップ 4 [Apply] をクリックします。

5 GHz デバイスの干渉レポートの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 5ghz cleanair device{canopy | cont-tx | dect-like | inv | jammer | nonstd | report | superag | tdd-tx | video | wimax-fixed | wimax-mobile}** 例： `Device(config)#ap dot11 5ghz cleanair device canopy` `Device(config)#ap dot11 5ghz cleanair device cont-tx` `Device(config)#ap dot11 5ghz cleanair device dect-like` `Device(config)#ap dot11 5ghz cleanair device inv` `Device(config)#ap dot11 5ghz cleanair device jammer` `Device(config)#ap dot11 5ghz cleanair device nonstd` `Device(config)#ap dot11 5ghz cleanair device report` `Device(config)#ap dot11 5ghz cleanair device superag` `Device(config)#ap dot11 5ghz cleanair device tdd-tx` `Device(config)#ap dot11 5ghz cleanair device video` `Device(config)#ap dot11 5ghz cleanair device wimax-fixed` `Device(config)#ap dot11 5ghz cleanair device wimax-mobile`	deviceに報告するように 5 GHz 干渉デバイスを設定します。干渉デバイスのレポートを無効にするには、このコマンドの **no** 形式を実行します。 次に、キーワードの説明のリストを示します。 • **canopy**：Canopy デバイス • **cont-tx**：連続トランスミッタ • **dect-like**：Digital Enhanced Cordless Communication 方式の電話機 • **fh**：802.11 周波数ホッピング デバイス • **inv**：スペクトル反転 Wi-Fi 信号を使用するデバイス • **jammer**：電波妨害装 • **nonstd**：非標準 Wi-Fi チャネルを使用するデバイス • **report**：干渉デバイスのレポート • **superag**：802.11 SuperAG デバイス • **tdd-tx**：TDD トランスミッタ • **video**：ビデオ カメラ • **wimax-fixed**：WiMax 固定 • **wimax-mobile**：WiMax モバイル
ステップ 3	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config)# end`	ンフィギュレーション モードを終了できます。

CleanAir イベントのイベント駆動型 RRM の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Radio Configurations]** > **[RRM]** を選択します。
[Radio Resource Management] ページが表示されます。

ステップ 2 [DCA] タブをクリックします。

ステップ 3 [Event Driven RRM] セクションで、CleanAir 対応 AP が重大なレベルの干渉を検出したときに RRM を実行するには、[EDRRM] チェックボックスをオンにします。

ステップ 4 次のオプションから、RRM を起動する必要がある [Sensitivity Threshold] レベルを設定します。

- [Low]：環境の変化への感度が低いことを表します。値は 35 に設定されます。
- [Medium]：環境の変化への感度が中程度であることを表します。値は 50 に設定されます。
- [High]：環境の変化への感度が高いことを表します。値は 60 に設定されます。
- [Custom]：このオプションを選択した場合は、[Custom Threshold] ボックスでカスタム値を指定する必要があります。

ステップ 5 不正デューティ サイクルを設定するには、[Rogue Contribution] チェックボックスをオンにしてから、[Rogue Duty-Cycle] でパーセント値を指定します。不正デューティ サイクルのデフォルト値は 80 パーセントです。

ステップ 6 設定を保存します。

CleanAir イベントの EDRRM の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** 例： `Device(config)#ap dot11 24ghz rrm`	EDRRM の CleanAir イベントを有効にします。EDRRM を無効にするには、このコマンドの **no** 形式を実行します。

	コマンドまたはアクション	目的
	channel cleanair-event `Device(config)#`**no ap dot11 24ghz rrm channel cleanair-event**	
ステップ 3	**ap dot11** {**24ghz** | **5ghz**} **rrm channel cleanair-event** [**sensitivity** {**custom** | **high** | **low** | **medium**}] 例： `Device(config)#`**ap dot11 24ghz rrm channel cleanair-event sensitivity high**	CleanAir イベントの EDRRM 感度を設定します。 次に、キーワードの説明のリストを示します。 • [Custom]：AQ 値によって示される非 Wi-Fi 干渉に対するカスタム感度を指定します。 • [High]：AQ 値によって示される非 Wi-Fi 干渉に対する最も高い感度を指定します。 • [Low]：AQ 値によって示される非 Wi-Fi 干渉に対する最も低い感度を指定します。 • [Medium]：AQ 値によって示される非 Wi-Fi 干渉に対する中間の感度を指定します。
ステップ 4	**end** 例： `Device(config)#` **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

CleanAir パラメータの確認

次のコマンドを使用して CleanAir パラメータを確認できます。

表 *40 : CleanAir* の確認用コマンド

コマンド名	説明
show ap dot11 24ghz cleanair air-quality summary	2.4 GHz 帯域の CleanAir AQ データを表示します。
show ap dot11 24ghz cleanair air-quality worst	2.4 GHz 帯域の最も低い CleanAir AQ データを表示します。
show ap dot11 24ghz cleanair config	2.4 GHz 帯域の CleanAir 設定を表示します。

コマンド名	説明
show ap dot11 24ghz cleanair device type all	2.4 GHz 帯域のすべての CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type ble-beacon	2.4 GHz 帯域のすべての Bluetooth BLE ビーコンを表示します。
show ap dot11 24ghz cleanair device type bt-discovery	2.4 GHz 帯域の BT Discovery タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type bt-link	2.4 GHz 帯域の BT Link タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type canopy	2.4 GHz 帯域の Canopy タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type cont-tx	2.4 GHz 帯域の Continuous transmitter タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type dect-like	2.4 GHz 帯域の DECT Like タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type fh	2.4 GHz 帯域の 802.11FH タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type inv	2.4 GHz 帯域の Wi-Fi Inverted タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type jammer	2.4 GHz 帯域の Jammer タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type mw-oven	2.4 GHz 帯域の MW Oven タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type nonstd	2.4 GHz 帯域の Wi-Fi inverted channel タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type persistent	2.4 GHz 帯域の Persistent タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type superag	2.4 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type tdd-tx	2.4 GHz 帯域の TDD Transmit タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type video	2.4 GHz 帯域の Video Camera タイプの CleanAir 干渉源を表示します。

コマンド名	説明
show ap dot11 24ghz cleanair device type wimax-fixed	2.4 GHz 帯域の WiMax Fixed タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type wimax-mobile	2.4 GHz 帯域の WiMax Mobile タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type xbox	2.4 GHz 帯域の Xbox タイプの CleanAir 干渉源を表示します。
show ap dot11 24ghz cleanair device type zigbee	2.4 GHz 帯域の Zigbee タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair air-quality summary	5 GHz 帯域の CleanAir AQ データを表示します。
show ap dot11 5ghz cleanair air-quality worst	5 GHz 帯域の最も低い CleanAir AQ データを表示します。
show ap dot11 5ghz cleanair config	5 GHz 帯域の CleanAir 設定を表示します。
show ap dot11 5ghz cleanair device type all	5 GHz 帯域のすべての CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type canopy	5 GHz 帯域の Canopy タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type cont-tx	5 GHz 帯域の Continuous TX タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type dect-like	5 GHz 帯域の DECT Like タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type inv	5 GHz 帯域の WiFi Inverted タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type jammer	5 GHz 帯域の Jammer タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type nonstd	5 GHz 帯域の Wi-Fi inverted channel タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type persistent	5 GHz 帯域の Persistent タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type superag	5 GHz 帯域の SuperAG タイプの CleanAir 干渉源を表示します。

コマンド名	説明
show ap dot11 5ghz cleanair device type tdd-tx	5 GHz 帯域の TDD Transmit タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type video	5 GHz 帯域の Video Camera タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type wimax-fixed	5 GHz 帯域の WiMax Fixed タイプの CleanAir 干渉源を表示します。
show ap dot11 5ghz cleanair device type wimax-mobile	5 GHz 帯域の WiMax Mobile タイプの CleanAir 干渉源を表示します。

干渉デバイスのモニタリング

CleanAir対応のアクセス ポイントで干渉デバイスが検出されると、複数のセンサーによる同じデバイスの検出をマージして、クラスタが作成されます。各クラスタには一意の ID を割り当てます。一部のデバイスは、実際に必要になるまで送信時間を制限することによって電力を節約しますが、その結果、スペクトラム センサーでのそのデバイスの検出が一時的に停止します。その後、このデバイスはダウンとして適正にマークされます。このようなデバイスは、スペクトラムデータベースから適切に削除されます。特定のデバイスに対する干渉源検出がすべてレポートされる場合は、デバイス検出が増大しないように、クラスタ ID が長期間にわたって有効になります。同じデバイスが再度検出された場合は、元のクラスタ ID とマージして、そのデバイスの検出履歴を保持します。

たとえば、Bluetooth対応のヘッドフォンが電池を使用して動作している場合があります。このようなデバイスでは、実際に必要とされていない場合には送信機を停止するなど、電力消費を減らすための方法が採用されています。このようなデバイスは、分類処理の対象として現れたり、消えたりを繰り返すように見えます。CleanAirでは、このようなデバイスを管理するために、クラスタ ID をより長く保持し、検出時には同じ 1 つのレコードに再度マージされます。この処理によってユーザ レコードの処理が円滑になり、デバイスの履歴が正確に表現されるようになります。

（注） 干渉デバイスのモニタリングに関する前提条件は次のとおりです。

Cisco CleanAir は、CleanAir 対応のアクセス ポイントにのみ設定できます。

CleanAir の設定例

次に、チャネルで動作する 2.4 GHz 帯域の CleanAir とアクセス ポイントをイネーブルにする例を示します。

```
Device#configure terminal
Device(config)#ap dot11 24ghz cleanair
```

```
Device(config)#exit
Device#ap name TAP1 dot11 24ghz cleanair
Device#end
```

次に、2.4 GHz 帯域の EDRRM の CleanAir イベントを有効にして、非 Wi-Fi 干渉に対する高い感度を設定する例を示します。

```
Device#configure terminal
Device(config)#ap dot11 24ghz rrm channel cleanair-event
Device(config)#ap dot11 24ghz rrm channel cleanair-event sensitivity high
Device(config)#end
```

次に、モニタ モードでアクセス ポイントを有効にする例を示します。

```
Device#ap name <ap-name> mode monitor
```

CleanAir に関する FAQ

Q. 複数のアクセス ポイントが同じ干渉デバイスを検出します。ところが、deviceにはそれらが別個のクラスタ、または疑いのあるさまざまなデバイスがクラスタ化された状態で表示されます。このようになるのはなぜですか。

A. deviceがこれらのアクセス ポイントによって検出されたデバイスのマージを検討するためには、アクセス ポイントがRF ネイバーである必要があります。アクセス ポイントがネイバー関係を確立するためには時間がかかります。deviceが再起動してから数分後、またはRF グループの変更などのイベントの後は、クラスタリングがあまり正確ではありません。

Q. deviceを使用して 2 台のモニタ モード アクセス ポイントをマージできますか。

A. いいえ。deviceを使用して 2 台のモニタ モード アクセス ポイントをマージすることはできません。

Q. ネイバー アクセス ポイントを表示するにはどうすればよいですか。

A. ネイバー アクセス ポイントを表示するには、**show ap** *ap_name* **auto-rf dot11** {**24ghz** | **5ghz**} コマンドを使用します。

次に、ネイバー アクセス ポイントを表示する例を示します。

```
Device#show ap name AS-5508-5-AP3 auto-rf dot11 24ghz

<snippet>
Nearby APs
  AP 0C85.259E.C350 slot 0                          :  -12 dBm on   1 (10.10.0.5)

  AP 0C85.25AB.CCA0 slot 0                          :  -24 dBm on   6 (10.10.0.5)

  AP 0C85.25C7.B7A0 slot 0                          :  -26 dBm on  11 (10.10.0.5)

  AP 0C85.25DE.2C10 slot 0                          :  -24 dBm on   6 (10.10.0.5)

  AP 0C85.25DE.C8E0 slot 0                          :  -14 dBm on  11 (10.10.0.5)

  AP 0C85.25DF.3280 slot 0                          :  -31 dBm on   6 (10.10.0.5)

  AP 0CD9.96BA.5600 slot 0                          :  -44 dBm on   6 (10.0.0.2)
```

```
  AP 24B6.5734.C570 slot 0                          :  -48 dBm on  11 (10.0.0.2)
<snippet>
```

Q. CleanAir で利用可能なデバッグ コマンドはどれですか。

A. CleanAir のデバッグ コマンドは次のとおりです。

- **debug cleanair** {**bringup** | **event** | **logdebug** | **low** | **major** | **nsi** | **offchan**}
- **debug rrm** {**neighbor** | **off-channel** | **reports**}

第 91 章

Bluetooth Low Energy

Bluetooth Low Energy について

Bluetooth Low Energy（BLE）は、モバイル デバイスのロケーション サービスの向上を目的とした、ワイヤレス パーソナル エリア ネットワーク テクノロジーです。戦略的な場所に配置された小型の Bluetooth タグ デバイスは、汎用一意識別子（UUID）と、それらの ID としてメジャー フィールドおよびマイナー フィールドを送信します。これらの詳細は、bluetooth 対応のスマートフォンおよびデバイスで取り上げられています。これらのデバイスのロケーション情報は、対応するバックエンドサーバに送信されます。その後、関連するアドバタイズメントとその他の重要な情報が、このロケーション固有の情報を使用してデバイスにプッシュされます。

また、BLE 機能では、BLE ビーコン管理のサポートが提供され、Cisco WLAN システム内で使用される場合はその動作が指定されます。Cisco CleanAir を使用して、アクセス ポイントは iBeacon 信号を識別し、ペイロード コンテンツを復号化できます。抽出されたタグ デバイスの詳細は、デバイスのより良い管理のために使用されます。

干渉源としてタグ デバイスを扱い、干渉場所などの既存のシステム機能を使用して、タグ デバイスをワイヤレス LAN 展開のマップ ディスプレイ上に配置でき、その動作をモニタできます。この他、欠落しているタグの情報も取得できます。この機能を使用して、顧客から提供された所定のホワイトリストと対照して、各タグ（またはタグのファミリ）に関連付けられている固有識別子を使用している不正なタグおよび悪意のあるタグを確認できます。管理機能を使用して、不正なタグ、欠落したタグ、または移動したタグに基づいて、アラートを表示したり電子メールで送信したりできます。

BLE 機能の制限事項

- 無線インフラストラクチャは、Cisco CleanAir をサポートする必要があります。
- 最大 250 個の固有の BLE ビーコン（クラスタ エントリ）と 1000 個のデバイス エントリのみをサポートします。

- NTP を設定すると、Halo モジュールを搭載した Cisco Aironet 3700 シリーズ アクセス ポイントの BLE 機能が非アクティブ化されます（この動作は、Cisco CMX が存在しない場合も発生します）。したがって、Cisco CMX が存在する場合、または HyperLocation 用に設定されていない場合、従来の BLE は機能しません。

使用エリア

BLE 機能では、デバイス（スマートフォンまたは bluetooth 対応デバイス）のきめ細かな場所の詳細が提供されるので、状況依存アドバタイジングおよびその他の情報をユーザにプッシュできます。アプリケーションの使用可能エリアには、小売店、博物館、動物園、医療機関、フィットネス、セキュリティ、アドバタイジングなどがあります。

Bluetooth Low Energy ビーコンのイネーブル化

Bluetooth Low Energy（BLE）検出は、デフォルトでイネーブルになっています。無効になっている BLE を有効にするには、次に示す手順を使用します。

始める前に

- 無線インフラストラクチャは、Cisco CleanAir をサポートする必要があります。
- Cisco CleanAir 設定と show コマンドは、モビリティ コントローラ(MC)モードでのみ使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Controller# 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	**[no] ap dot11 24ghz cleanair device [ble-beacon]** 例： `Controller(config)# ap dot11 24ghz cleanair device ble-beacon`	802.11b ネットワークでの BLE 機能をイネーブルにします。802.11b ネットワークで BLE 機能を無効にするには、このコマンドの **no** 形式を使用します。
ステップ 3	**exit** 例： `Controller(config)# exit`	特権 EXEC モードに戻ります。
ステップ 4	**show ap dot11 24ghz cleanair config** 例： `Controller# show ap dot11 24ghz cleanair config`	（任意）BLE ビーコン設定を表示します。

	コマンドまたはアクション	目的
	Interference Device Settings: Interference Device Reporting..... : Enabled Bluetooth Link..... : Enabled Microwave Oven..... : Enabled BLE Beacon..... : Enabled	
ステップ 5	**show ap dot11 24ghz cleanair device type ble-beacon** 例： Controller# show ap dot11 24ghz cleanair device type ble-beacon DC = Duty Cycle (%) ISI = Interference Severity Index (1-Low Interference, 100-High Interference) RSSI = Received Signal Strength Index (dBm) DevID = Device ID No ClusterID DevID Type AP Name ISI RSSI DC Channel 1 2c:92:80:00:00:22 0xa001 BLE Beacon 5508_3_AP3600_f839 -- -74 0 unknown	（任意）BLE ビーコンのデバイス タイプ情報を表示します。

第 92 章

スペクトル インテリジェンス

スペクトル インテリジェンス

スペクトル インテリジェンス機能は、2.4 および 5 GHz 帯域で非 Wi-Fi 無線干渉をスキャンします。スペクトル インテリジェンスは、マイクロ波、連続波（ビデオ ブリッジやベビー モニタなど）、Wi-Fi および周波数ホッピング（Bluetooth および周波数ホッピング スペクトラム拡散（FHSS）コードレス電話）の 3 種類の干渉を検出する基本的な機能を提供します。

次の Cisco アクセス ポイント（AP）は、スペクトル インテリジェンス機能をサポートしています。

- Cisco Aironet 1852E/I AP
- Cisco Aironet 1832I AP
- Cisco Aironet 1815W/T/I/M AP
- Cisco Aironet 1810W/T AP
- Cisco Aironet 1800I/S AP
- Cisco Aironet 1542D/I AP

（注） Cisco DNA Center アシュアランス AP ヘルスでノイズ、電波品質、干渉、無線使用率などの無線の詳細情報を取得するには、Cisco Aironet 1832 および 1852 シリーズの AP でスペクトル インテリジェンス機能を有効にする必要があります。

制約事項

- SI AP は、ローカル モードで 1 つの干渉タイプのみを報告します。

- SI は、電波品質または干渉レポートのハイ アベイラビリティをサポートしていません。
- スペクトル インテリジェンスは、次の 3 タイプのデバイスのみを検出します。
  - マイクロ波
  - 連続波：ビデオ レコーダー、ベビー モニタ
  - SI-FHSS：Bluetooth、周波数ホッピング Digital European Cordless Telecommunication（DECT）電話機

スペクトル インテリジェンスの設定

スペクトル インテリジェンスを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11** {**24ghz** | **5ghz**} **SI** 例： `Device(config)# ap dot11 24ghz SI`	802.11a または 802.11b ネットワークで 2.4 GHz または 5 GHz スペクトル インテリジェンス機能を設定します。 802.11a または 802.11b ネットワークで SI を無効にするには、コマンドの **no** 形式を追加します。

スペクトル インテリジェンスの情報の確認

スペクトル インテリジェンスの情報を確認するには、次のコマンドを使用します。

2.4 GHz または 5 GHz 帯域の SI 情報を表示するには、次のコマンドを使用します。

```
Device# show ap dot11 24ghz SI config

SI Solution..................................... : Enabled
Interference Device Settings:
        SI_FHSS............................... : Enabled
    Interference Device Types Triggering Alarms:
        SI_FHSS............................... : Disabled
```

2.4 GHz 帯域の連続トランスミッタ タイプの SI 干渉源を表示するには、次のコマンドを使用します。

```
Device# show ap dot11 24ghz SI device type cont_tx

DC    = Duty Cycle (%)
ISI = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
AP type = CA, clean air, SI spectrum intelligence

No  ClusterID       DevID  Type     AP Type AP Name                 ISI  RSSI  DC
Channel
--- --------------- ------ -------- ------- ----------------- ---- ----- ----  ---
------
   xx:xx:xx:xx  0014  BT     CA    myAP1              --   -69 00  133
   xx:xx:xx:xx  0014  BT     SI    myAP1              --   -69 00  133
```

5 GHz の特定の AP に関する 802.11a 干渉デバイス情報を表示するには、次のコマンドを使用します。

```
Device# show ap dot11 5ghz SI device type ap

DC    = Duty Cycle (%)
ISI   = Interference Severity Index (1-Low Interference, 100-High Interference)
RSSI  = Received Signal Strength Index (dBm)
DevID = Device ID
AP type = CA, clean air, SI spectrum intelligence

No  ClusterID/BSSID    DevID  Type    AP Type AP Name                 ISI  RSSI  DC
Channel
--- ------------------ ------ ------- ------  ----------------------- ---- ----- ----
----------
```

2.4 GHz 帯域のすべての Cisco CleanAir 干渉源を表示するには、次のコマンドを使用します。

```
Device# show ap dot11 24ghz cleanair device type all
```

第 XII 部

メッシュ アクセス ポイント

第 93 章

メッシュ アクセス ポイント

メッシュの概要

メッシュ ネットワーキングでは、Cisco Aironet の屋外および屋内メッシュ アクセス ポイントと、シスコ ワイヤレス コントローラおよび Cisco Prime Infrastructure を組み合わせて、拡張性、集中管理、および屋内外の展開のモビリティが提供されます。Control and Provisioning of Wireless Access Points（CAPWAP）プロトコルは、ネットワークへのメッシュ アクセス ポイントの接続を管理します。

メッシュ ネットワーク内のエンドツーエンドのセキュリティは、ワイヤレス メッシュ アクセス ポイントと Wi-Fi Protected Access 2（WPA2）クライアントの間で Advanced Encryption Standard（AES）の暗号化を採用することでサポートされています。メッシュアクセスポイント（MAP）ワイヤレス クライアントへの接続（MAP 同士や MAP とルート アクセス ポイントなど）では、WPA2 が適用されます。

ワイヤレス メッシュは、有線ネットワークの 2 地点で終端します。1 つ目はルート アクセス ポイント（RAP）が有線ネットワークに接続される場所です。すべてのブリッジトラフィックがその場所で有線ネットワークに接続されます。2 つ目は CAPWAP コントローラが有線ネットワークに接続する場所です。ここでは、メッシュ ネットワークからの WLAN クライアント トラフィックが有線ネットワークに接続されます。CAPWAP からの WLAN クライアント トラフィックは、レイヤ 2 にトンネリングされます。一致する WLAN は、ワイヤレス コントローラが同じ場所に設置されている同じスイッチ VLAN で終端する必要があります。メッシュ上の各 WLAN のセキュリティとネットワークの設定は、ワイヤレス コントローラが接続されているネットワークのセキュリティ機能によって異なります。

新しい設定モデルでは、コントローラにデフォルトのメッシュプロファイルがあります。このプロファイルは、デフォルトの AP 接続プロファイルにマッピングされた後、サイト タグにマッピングされます。名前付きメッシュプロファイルを作成する場合は、これらのマッピングが行われていること、および該当する AP が対応するサイト タグに追加されていることを確認します。

機能制限

この機能は、次の AP プラットフォームでのみサポートされます。

- 屋外 AP
  - Cisco Aironet 1532 メッシュ アクセス ポイント
  - Cisco Aironet 1572 メッシュ アクセス ポイント
- 屋内 AP
  - Cisco Aironet 2700 メッシュ アクセス ポイント
  - Cisco Aironet 3700 メッシュ アクセス ポイント
- Cisco Wave 2 AP
  - Cisco Aironet 1542 メッシュ アクセス ポイント
  - Cisco Aironet 1562 メッシュ アクセス ポイント

次のメッシュ機能はサポートされていません。

- アップリンクとダウンリンク用に個別のバックホール無線を備えたシリアルバックホール AP のサポート
- Public Safety チャネル（4.9 GHz 帯域）のサポート
- パッシブ ビーコン（ストランディング防止）

（注） ルート AP のみが SSO をサポートしています。MAP は、SSO 後に接続が切断されて再参加します。

MAC 認証

MAP をコントローラに参加させるには、AP の MAC アドレスをコントローラに入力する必要があります。コントローラは、認証リストで使用可能な MAP からの CAPWAP 要求にのみ応答します。アクセス ポイントの背面に記載されている MAC アドレスを使用してください。

イーサネット経由でコントローラに接続された MAP の MAC 認証は、CAPWAP 接続プロセス中に行われます。無線でコントローラに接続する MAP の場合、対応する AP が親 MAP との WPP リンクを保護しようとすると、MAC 認証が行われます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラは、内部での MAC 認証と、外部 AAA サーバを使用した認証をサポートしています。

事前共有キーのプロビジョニング

メッシュ展開では、MAP がネットワークから移動して別のメッシュ ネットワークに接続することがあります。これは、両方のメッシュ展開がワイルドカードの MAC フィルタリングで AAA を使用して MAP のアソシエーションを許可する場合に発生します。MAP は EAP-FAST を使用する可能性があるので、この動作を制御することはできません。EAP セキュリティに AP の MAC アドレスとタイプの組み合わせが使用されて、制御設定を使用できないためです。デフォルトのパスフレーズを使用した事前共有キー（PSK）オプションには、セキュリティ リスクも存在します。

この問題は、MAP が移動車両（公共交通機関、フェリー、船など）で使用される場合に、2 つのサービス プロバイダーのオーバーラップ導入環境で顕著に現れます。この場合、サービス プロバイダーのメッシュ ネットワークに残る MAP に制限はなく、MAP がハイジャックされたり、別のサービス プロバイダーのネットワークで使用されたりして、導入環境で本来のサービス プロバイダーの対象顧客にサービスを提供できなくなる可能性があります。

PSK キープロビジョニング機能を使用すると、コントローラからプロビジョニング可能な PSK 機能が有効になります。これにより、メッシュ展開の制御が容易になり、デフォルトよりも MAP セキュリティが強化されます。この機能によってカスタム PSK が設定された MAP は、PSK キーを使用して RAP およびコントローラで認証を行います。

EAP 認証

ローカル EAP は、ユーザおよびワイヤレス クライアントのローカル認証をコントローラで可能にする認証方式です。バックエンド システムが妨害されたり、外部認証サーバがダウンした場合でも、ワイヤレス クライアントとの接続を維持する必要があるリモート オフィスでの使用を目的として設計されています。ローカル EAP を有効にすると、コントローラは認証サーバおよびローカル ユーザ データベースとして機能するため、外部認証サーバに依存する必要がなくなります。ローカル EAP は、ローカル ユーザ データベースまたは LDAP バックエンド データベースからユーザの資格情報を取得して、ユーザを認証します。ローカル EAP では、コントローラとワイヤレス クライアント間の MAP 認証で、EAP-FAST 認証方式のみがサポートされます。

ローカル EAP はバックエンド データベースとして LDAP サーバを使用し、コントローラとワイヤレス クライアント間の MAP 認証のユーザ ログイン情報を取得します。LDAP バックエンドデータベースを使用すると、コントローラで、特定のユーザの資格情報（ユーザ名およびパスワード）を LDAP サーバから検索できるようになります。これらの資格情報は、ユーザの認証に使用されます。

（注） コントローラ上で RADIUS サーバが設定されている場合、コントローラはまず RADIUS サーバを使用してワイヤレス クライアントを認証しようとします。ローカル EAP は、RADIUS サーバが見つからない、タイムアウトになっている、または設定されていない場合にのみ試行されます。

LSC による EAP 認証

ローカルで有効な証明書ベース（LSC ベース）の EAP 認証も MAP でサポートされています。この機能を使用するには、認証局の制御、生成された証明書のポリシー、有効期間、制限、および使用方法の定義、AP とコントローラでインストールされたこれらの証明書の取得を行うために、公開キー インフラストラクチャ（PKI）が必要です。

これらのユーザ生成証明書または LSC が AP とコントローラで使用可能になると、デバイスはこれらの LSC を使用して接続、認証、およびセッション キーの取得を開始できます。

LSC によって AP から既存の証明書が削除されることはありません。AP は LSC と製造元でインストールされる証明書（MIC）の両方を保持できます。ただし、AP が LSC でプロビジョニングされた後は、起動時に MIC 証明書が使用されなくなります。LSC から MIC に変更する場合は、該当する AP をリブートする必要があります。

次の目的で、コントローラは指定サーバに対する EAP 認証を使用したメッシュ セキュリティもサポートしています。

- メッシュ子 AP の認証
- パケット暗号化のためのマスター セッション キー（MSK）の生成

Bridge Group Names

ブリッジ グループ名（BGN）は、親メッシュ AP への MAP のアソシエーションを制御します。BGN を使用して無線を論理的にグループ分けしておくと、同じチャネルにある 2 つのネットワークが相互に通信することを防止できます。この設定はまた、同一セクター（領域）のネットワーク内に複数の RAP がある場合にも便利です。BGN は最大 10 文字から成る文字列です。

NULL VALUE という BGN が製造時にデフォルトで割り当てられます。このグループ名は表示されませんが、これにより、ネットワーク固有の BGN を割り当てる前に MAP をネットワークに参加させることができます。

同一セクターのネットワーク内に（より大きなキャパシティを得るために）RAP が 2 つある場合は、別々のチャネルで 2 つの RAP に同じ BGN を設定することをお勧めします。

完全一致 BGN を MAP で有効にすると、一致する BGN 親を見つけるためにスキャンが 10 回行われます。10 回スキャンしても一致する BGN 親を見つけられない場合、AP は一致しない BGN に接続して 15 分間接続を維持します。15 分後に AP は再び 10 回スキャンを行い、この

サイクルが繰り返されます。デフォルトのBGNの機能は完全一致BGNが有効な場合も同じです。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、メッシュ プロファイルに BGN が設定されています。MAPがコントローラに参加するたびに、コントローラはメッシュ プロファイルに設定されている BGN を AP にプッシュします。

優先される親（Preferred Parent）の選択

MAP の優先される親を使用すると、メッシュ環境で線形トポロジを適用できます。この機能を使用すると、Adaptive Wireless Path Protocol で定義された（AWPP 定義）親選択メカニズムをオーバーライドして、優先される親に MAP を強制的に移動できます。

Background Scanning

メッシュ バックグラウンド スキャンにより、コンバージェンス時間、および親選択の信頼性と安定性が向上します。バックグラウンド スキャン機能を使用すると、MAP はチャネル間でより適した親を見つけて接続し、適切な親とのアップリンクを常に維持することができます。

バックグラウンド スキャンが無効になっている場合、MAP は親の損失を検出した後に、新しい親を見つけて認証プロセスを進めるために規制ドメインのすべてのチャネルをスキャンする必要があります。したがって、メッシュ AP がコントローラに接続するまでにかかる時間が長くなります。

バックグラウンド スキャンが有効になっていれば、MAP は親の損失を検出した後で親を見つけるためにチャネル全体をスキャンしなくても、ネイバー リストから親を選択して AWPP リンクを確立できます。

2.4 GHz および 5 GHz でのメッシュ バックホール

バックホールは、MAP 間でワイヤレス接続のみを作成するために使用されます。バックホール インターフェイスは 802.11a/n/ac/g です（AP によって異なります）。デフォルトのバックホール インターフェイスは 802.11a です。利用可能な無線周波数スペクトラムを効果的に使用するには、レート選択が重要です。このレートは、クライアントデバイスのスループットにも影響を与える可能性があります（スループットはベンダーデバイスを評価するために業界出版物で使用される重要なメトリックです）。

メッシュ バックホールは、2.4 GHz および 5 GHz でサポートされています。ただし特定の国では、5 GHz のバックホール ネットワークでメッシュ ネットワークを使用することは許可されていません。2.4 GHz の無線周波数を使用すると、より大きなメッシュまたはブリッジ距離を実現できます。RAP はスロット変更設定を取得すると、すべての子 MAP に伝達します。すべての MAP は接続を解除し、新たに設定されたバックホール スロットに接続します。

Dynamic Frequency Selection（動的周波数選択）

既存のレーダーサービスを保護するため、規制当局は、新規に開放された周波数サブバンドを共有する必要があるデバイスに対して、動的周波数選択（DFS）プロトコルに従って動作することを求めています。DFSに準拠するために、無線デバイスがレーダー信号の存在を検出できることが義務付けられています。無線でレーダー信号が検出された場合、最低30分間は伝送を停止してそのサービスを保護する必要があります。その後、無線は別のチャネルを選択しますが、伝送する前にこのチャネルをモニタリングする必要があります。使用する予定のチャネルで1分間以上レーダーが検出されなかった場合は、新しい無線サービスデバイスがそのチャネルで伝送を開始できます。DFS機能により、メッシュAPはセクター内のいずれかのメッシュAPでレーダーイベントが検出されたときに、ただちにチャネルを切り替えることができます。

国コード

コントローラおよびAPは、法的な規制基準の異なるさまざまな国で使用できるように設計されています。AP内の無線は、製造時に特定の規制ドメイン（ヨーロッパの場合にはEなど）に割り当てられていますが、国コードを使用すると、稼働する特定の国を指定できます（フランスの場合にはFR、スペインの場合にはESなど）。国番号を設定すると、各無線のブロードキャスト周波数帯域、インターフェイス、チャネル、および送信電力レベルが国別の規制に準拠していることを確認できます。

国によっては、屋内と屋外のAPに次のような違いがあります。

- 規制ドメイン コード
- サポートされるチャネル セット
- 送信電力レベル

侵入検知システム

Cisco侵入検知システム/侵入防御システム（CIDS/CIPS）は、特定のクライアントに関わる攻撃がレイヤ3～レイヤ7で検出されたとき、これらのクライアントによるワイヤレス ネットワークへのアクセスをブロックするよう、コントローラに指示します。このシステムは、ワーム、スパイウェア/アドウェア、ネットワーク ウイルス、およびアプリケーション不正使用などの脅威を検出、分類、阻止することで、強力なネットワーク保護を提供します。

コントローラ間のメッシュ相互運用性

AireOSとCisco Catalyst 9800シリーズ ワイヤレス コントローラの間の相互運用性が維持され、次のサポートが提供されます。

- MAP は、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続された AP によって形成されたメッシュ ネットワークを介して AireOS コントローラに接続できます。
- MAP は、AireOS コントローラに接続された AP によって形成されたメッシュ ネットワークを介して Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに接続できます。
- AireOS に接続されている親メッシュ AP と Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの間で、PMK キャッシュを使用した MAP ローミングがサポートされます。

（注） シームレスな相互運用性を実現するためには、AireOS コントローラと Cisco Catalyst 9800 シリーズ ワイヤレス コントローラが同じモビリティ グループに属し、IRCM をサポートするイメージ バージョンを使用する必要があります。

メッシュ コンバージェンス

メッシュ コンバージェンスにより、MAPは現在の親とのバックホール接続が失われた場合に、コントローラとの接続を再確立できます。コンバージェンス時間を短縮するために、各メッシュ AP はチャネルのサブセットを維持して将来のスキャン/シークに使用し、ネイバー リストのサブセットで親を識別します。

次のコンバージェンス方式がサポートされています。

表 *41 :* メッシュ コンバージェンス

メッシュ コンバージェンス	親の損失検出/キープアライブタイマー
規格	21 / 3 秒
速い	7 / 3 秒
Very Fast	4 / 2 秒
ノイズトレラント高速	21 / 3 秒

ノイズトレラント高速

ノイズトレラント高速検出は、現在の親を 21 秒ごとに標準方式で評価する AWPP ネイバー要求に対する応答を取得できないことが前提になります。親への要求とともに、各ネイバーに 3 秒ごとにユニキャスト要求が送信されます。親からの応答を取得できないときは、ローミング（ネイバーが同じチャネルで使用可能な場合）または新しい親のフル スキャンが開始されます。

イーサネット ブリッジング

セキュリティ上の理由により、デフォルトではすべての MAP でイーサネット ポートが無効になっています。有効にするには、ルートおよび各 MAP でイーサネット ブリッジングを設定します。

タグ付きパケットとタグなしパケットの両方が、セカンダリ イーサネット インターフェイスでサポートされています。

ポイントツーポイント ブリッジング シナリオでは、バックホール無線を使用してスイッチドネットワークの 2 つのセグメントをブリッジ接続することにより、Cisco Aironet 1500 シリーズ MAP を使用してリモート ネットワークを拡張できます。これは基本的には、1 つの MAP があり、WLAN クライアントがないワイヤレス メッシュ ネットワークです。ポイントツーマルチポイント ネットワークと同様に、イーサネット ブリッジングを有効にすることでクライアント アクセスを提供できますが、建物間のブリッジングの場合、高い屋上からの MAP カバレッジはクライアントのアクセスに適していないことがあります。イーサネット ブリッジド アプリケーションを使用するには、RAP およびそのセクター内のすべての MAP でブリッジング機能を有効にする必要があります。

イーサネット ブリッジングは、次の場合に有効にする必要があります。

- メッシュ ノードをブリッジとして使用する。
- MAP でイーサネット ポートを使用してイーサネット デバイス（ビデオ カメラなど）を接続する。

（注） メッシュ AP からコントローラへのパスを取るすべての親メッシュ AP に対してイーサネット ブリッジングを有効にしてください。

イーサネット ブリッジング用の VLAN がサポートされたメッシュ環境では、**ap exec** コマンドを使用して MAP 上のセカンダリ イーサネット インターフェイスに VLAN を個別に割り当てます。すべてのバックホール ブリッジ リンク（有線とワイヤレスの両方）は、すべての VLAN が有効になっているトランク リンクです。非イーサネット ブリッジド トラフィック、およびタグなしイーサネット ブリッジド トラフィックは、メッシュ内の AP のネイティブ VLAN を使用してメッシュに沿って伝送されます。これは、AP がサービスを提供しているワイヤレス クライアントで送受信されるすべてのトラフィックで同様です。VLAN タグ付きパケットは、ワイヤレス バックホール リンクを介して AWPP でトンネリングされます。

MAP イーサネット クライアントの VLAN タギング

メッシュ AP のバックホール インターフェイスはプライマリ インターフェイスと呼ばれ、他のインターフェイスはセカンダリ インターフェイスと呼ばれます。

イーサネット VLAN タギングを使用すると、無線メッシュ ネットワーク内で特定のアプリケーション トラフィックをセグメント化して、有線 LAN に転送（ブリッジング）するか（アクセ

ス モード）、別の無線メッシュ ネットワークにブリッジングすることができます（トランク モード）。

メッシュを介したマルチキャスト

メッシュ マルチキャスト モードによって、ブリッジング対応 AP（MAP や RAP など）がメッシュ ネットワーク内のイーサネット LAN 間でマルチキャスト パケットを送信する方法が決まります。メッシュ マルチキャスト モードは非 CAPWAP マルチキャスト トラフィックのみを管理します。CAPWAP マルチキャスト トラフィックは異なるメカニズムで管理されます。

すべての MAP でビデオ カメラ ブロードキャストを管理するために、3 つの異なるメッシュ マルチキャスト モードを使用できます。イネーブルになっている場合、これらのモードは、メッシュ ネットワーク内の不要なマルチキャスト送信を減少させ、バックホール帯域幅を節約します。

3 つのツリー メッシュ マルチキャスト モードは次のとおりです。

- regular モード：データは、ブリッジング対応 RAP および MAP によってメッシュ ネットワーク全体とすべてのセグメントにマルチキャストされます。
- in-only モード：MAP がイーサネットから受信するマルチキャスト パケットは、対応する RAP のイーサネット ネットワークに転送されます。他の転送は行われないので、RAP が受信した非 CAPWAP マルチキャストはメッシュ ネットワーク内の MAP イーサネット ネットワーク（発信元）に返送されず、MAP から MAP へのマルチキャストはフィルタで除去されるため発生しません。
- in-out モード：RAP と MAP は別々の方法でマルチキャストを行います。
  - イーサネット経由で MAP が受信したマルチキャスト パケットは RAP に送信されますが、イーサネット経由で他の MAP に送信されることはありません。MAP から MAP へのパケットはマルチキャストからフィルタで除去されます。
  - マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。in-out モードで動作中の場合、1 台の RAP によって送信されるマルチキャストを同じイーサネット セグメント上の別の RAP が受信してネットワークに送り戻さないよう、ネットワークを適切に分割する必要があります。

メッシュでの無線リソース管理

Radio Resource Management（RRM）ソフトウェアはコントローラに組み込まれており、無線ネットワークのリアルタイムでの RF 管理を常時提供する組み込みの RF エンジニアとして機能します。RRM を使用すると、コントローラは関連する Lightweight AP を継続的にモニタリングして、トラフィック負荷、干渉、ノイズ、カバレッジ、およびその他の隣接 AP に関する情報を取得できます。

メッシュ AP バックホールの RRM 測定は、次の条件に基づいて有効になります。

- メッシュ AP にルート AP ロールがある。
- ルート AP がイーサネット リンクを使用して接続している。
- ルート AP が子 AP にサービスを提供していない。

メッシュの Air Time Fairness

メッシュの Air Time Fairness（ATF）機能は、ローカル アクセス ポイント（AP）の ATF 機能と概念的に似ています。ATF は、ダウンリンク通信時間（出力帯域幅ではない）を調整するワイヤレス Quality of Service（QoS）の形式です。フレームが送信される前に、フレームを送信するのに十分な通信時間量があることを確認するために、その SSID 用の ATF 量がチェックされます。各 SSID は、トークン バケット（1 つのトークン = 通信時間の 1 マイクロ秒）を持つと見なされます。フレームを送信するために十分な通信時間がトークンバケットに含まれている場合は、無線で送信されます。それ以外は、フレームをドロップまたは保留できます。フレームの保留とは、フレームがアクセス カテゴリ キュー（ACQ）に許可されないことを意味します。代わりにクライアント プライオリティ キュー（CPQ）に残り、対応するトークン バケットに十分な数のトークンが確保された時点で送信されます（CPQ の容量がいっぱいになってフレームがドロップされた場合を除く）。ATF に関連する作業の大部分は AP で行われます。ワイヤレス コントローラは、メッシュでの ATF の設定と結果の表示に使用されます。

メッシュ アーキテクチャでは、メッシュ ツリー内のメッシュ AP（親および子 MAP）は、親 MAP と子 MAP 間のメッシュ接続用バックホール無線の同じチャネルにアクセスします。ルート AP はコントローラに有線接続され、MAP はコントローラにワイヤレス接続されます。そのため、すべての CAPWAP および Wi-Fi トラフィックは、ワイヤレス バックホール無線および RAP によってコントローラにブリッジされます。物理的な配置については、一般に RAP はルーフ トップに配置され、複数のホップにある MAP はメッシュ ネットワークのセグメント化ガイドラインに基づいて互いに間隔を置いて配置されます。したがって、メッシュ ツリー内の各 MAP は同じメディアにアクセスするにも関わらず、自身の無線通信時間ダウンストリームの 100 % をユーザに提供できます。これに対してメッシュ以外のシナリオでは、アリーナ内の異なる部屋に設置された隣接するローカル モードのユニファイド AP が、同じチャネル上のそれぞれのクライアントに 100 % の無線通信時間ダウンストリームを提供します。ATF は、同じメディアにアクセスする異なる 2 つの隣接 AP でクライアントを制御できません。これはメッシュ ツリー内の MAP についても同様です。

屋外または屋内メッシュ AP の場合、クライアントにサービスを提供する非メッシュのユニファイド ローカル モード AP の ATF でサポートされているのと同様に、通常のクライアントにサービスを提供するクライアント アクセス無線で ATF がサポートされている必要があります。さらに、クライアント アクセス無線のクライアント間のトラフィックを RAP にブリッジする（1 ホップ）、または MAP を経由して RAP にブリッジする（複数のホップ）バックホール無線でもサポートされている必要があります。同じ SSID/ポリシー/ウェイト/クライアントの Fair Sharing モデルを使用してバックホール無線の ATF をサポートする方法は、多少複雑になります。バックホール無線には SSID がなく、常にトラフィックは隠れたバックホール ノードを通じてブリッジされます。そのため、RAP または MAP のバックホール無線では、バック

ホール ノード数に基づいて無線通信時間ダウンストリームが公平に共有されます。この方法により、2 番目のホップ MAP が 1 番目のホップ MAP にバックホール無線を通じてワイヤレス接続されている状況で、2 番目のホップ MAP に関連付けられているクライアントが 1 番目のホップ MAP に関連付けられているクライアントを失速させた場合に、MAP の Wi-Fi ユーザが物理的に離れていても、ワイヤレス メッシュ ネットワーク全体のユーザが公平に扱われます。バックホール無線でユニバーサル クライアント アクセス機能を通じて通常のクライアントにサービスを提供できる場合、ATF は通常のクライアントを単一ノードに配置してグループ化します。また、ノードの数（バックホール ノード + 通常のクライアント用の単一ノード）に基づいて、無線通信時間ダウンストリームを均等に共有して通信時間を適用します。

メッシュのスペクトル インテリジェンス

スペクトル インテリジェンス機能は、2.4 および 5 GHz 帯域で非 Wi-Fi 無線干渉をスキャンします。この機能は、クライアント サービス モードおよびモニタ モードをサポートします。メッシュ バックホールおよびアクセス無線の Cisco CleanAir テクノロジーは、干渉デバイス レポート（IDR）と電波品質の指標（AQI）を提供します。CleanAir には、イベント駆動型無線リソース管理（EDRRM）と永続型デバイス回避（PDA）という 2 つの主要な緩和機能があります。両機能とも CleanAir によってのみ収集可能な情報を直接利用します。クライアントアクセス無線帯域では、バックホール無線帯域の非メッシュ ネットワークの場合と同じようにメッシュ ネットワークで動作し、CleanAir レポートはコントローラにのみ表示されます。ED-RRM で実行されるアクションはありません。

MAP の CleanAir を有効または無効にするために使用できる特定の設定オプションはありません。

屋内メッシュと屋外メッシュの相互運用性

屋外 AP と屋内 MAP の相互運用性がサポートされます。これは、屋外から屋内にカバレッジを広げるのに役立ちます。ただし、屋内 MAP は屋内専用で使用することを推奨します。屋外への配置は、屋内 WLAN から駐車場の入り口までのごく短い距離を延長する場合など、限られた状況のみに限定してください。

モビリティ グループは、屋外メッシュ ネットワークと屋内 WLAN ネットワークの間で共有できます。1 台のコントローラで、屋内と屋外の MAP を同時に制御することもできます。同じ WLAN が屋内と屋外の両方の MAP からブロードキャストされる点に注意してください。

ワークグループ ブリッジ

ワークグループ ブリッジ（WGB）は、対応する MAP に、WGB の有線セグメントにあるすべてのクライアントを IAPP メッセージで通知することにより、単一ワイヤレス セグメントを介して有線ネットワークに接続するために使用されます。IAPP 制御メッセージの他にも、WGB クライアントのデータ パケットでは 802.11 ヘッダー内に追加 MAC アドレスが含まれます（通常は 3 つの MAC データ ヘッダーであるのに対し、4 つの MAC ヘッダーがあります）。ヘッ

ダー内の追加 MAC は、ワークグループ ブリッジ自体のアドレスです。この追加 MAC アドレスは、該当するクライアントと送受信するパケットのルーティングに使用されます。

自律 AP はワークグループ ブリッジとして機能します。コントローラ接続に唯一の無線インターフェイス、有線クライアント接続にイーサネット インターフェイス、ワイヤレス クライアント接続に他の無線インターフェイスが使用されます。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでは、WGB はクライアント関連付けとして機能し、WGB の背後にある有線クライアントがメッシュ ネットワーク上のデータ トラフィックに対してサポートされます。WGB の背後にあるさまざまな VLAN の有線クライアントもサポートされます。

リンク テスト

リンクテストを使用して、2つのデバイス間の無線リンクの質を決定します。リンク テストの際には、要求と応答の 2 種類のリンク テスト パケットを送信します。リンク テストの要求パケットを受信した無線は、適切なテキスト ボックスを記入して、応答タイプ セットを使用して送信者にパケットを返信します。

クライアントからアクセス ポイント方向への無線リンクの質は、アクセス ポイントからクライアント方向へのものと異なることがあり、それは双方の送信電力と受信感度が非対称であることによるものです。2 種類のリンク テスト（ping テストおよび CCX リンク テスト）を実行できます。

ping リンク テストでは、コントローラはクライアントからアクセス ポイント方向でのみリンクの質をテストできます。アクセス ポイントで受信された ping パケットの RF パラメータは、クライアントからアクセス ポイント方向のリンクの質を決定するためにコントローラによりポーリングされます。

CCX リンク テストでは、コントローラはアクセス ポイントからクライアント方向でもリンクの質をテストできます。コントローラはクライアントにリンクテスト要求を発行し、クライアントは、応答パケットで受信した要求パケットの RF パラメータを記録します（受信信号強度インジケータ [RSSI]、信号対雑音比 [SNR] など）。リンク テストの要求ロールと応答ロールの両方を、アクセス ポイントとコントローラに実装します。アクセス ポイントまたはコントローラが CCX v4 クライアントまたは v5 クライアントに対してリンク テストを開始でき、同様に CCX v4 クライアントまたは v5 クライアントもアクセス ポイントまたはコントローラに対してリンク テストを開始できます。

メッシュ デイジー チェーン接続

Cisco Aironet 1530 シリーズ アクセス ポイントには、MAP として機能する AP をデイジー チェーン接続する機能があります。デイジー チェーン接続された MAP では、AP をシリアル バックホールとして運用する（アップリンク アクセスとダウンリンク アクセスに別々のチャネルを使用できるためバックホール帯域幅が向上する）ことも、ユニバーサル アクセスを拡張することもできます。ユニバーサル アクセスの拡張により、ローカル モードまたは FlexConnect モー

ドの Cisco Aironet 1530 シリーズ アクセス ポイントを MAP のイーサネット ポートに接続できるため、ネットワークが拡張されてより適切なクライアント アクセスを提供できます。

デイジー チェーン接続された AP は、AP の電源供給方法に応じて異なる方法でケーブル接続する必要があります。AP への電力が DC 電源を使用して供給されている場合は、イーサネット ケーブルをマスター AP の LAN ポートからスレーブ AP の PoE 入力ポートに直接接続する必要があります。

デイジー チェーン接続モードに関するガイドラインは次のとおりです。

- マスター MAP は、メッシュ AP として設定する必要があります。
- スレーブ MAP はルート AP として設定する必要があります。
- マスター MAP とスレーブ MAP の両方でデイジー チェーン接続を有効にする必要があります。
- ブリッジ モードのすべての AP でイーサネット ブリッジングを有効にする必要があります。メッシュ プロファイルでイーサネット ブリッジングを有効にして、セクター内のすべてのブリッジ モード AP を同じメッシュ プロファイルにマッピングします。
- VLAN サポートは、適切なネイティブ VLAN 設定とともに、有線ルート AP、スレーブ MAP、およびマスター MAP で有効にする必要があります。

メッシュ リーフ ノード

リーフ ノードとしてのみ動作するパフォーマンスの低い MAP を設定できます。メッシュ ネットワークが形成および統合されると、リーフ ノードは子 MAP としてのみ動作でき、他の MAP が親 MAP として選択することはできなくなります。したがって、ワイヤレス バックホール パフォーマンスはダウングレードされません。

フレックス + ブリッジ モード

フレックス + ブリッジ モードは、メッシュ（ブリッジ モード）AP 上で FlexConnect の機能を有効にするために使用されます。メッシュ AP は接続先のルート AP から VLAN を継承します。

次のいずれかのモードの各 AP で、VLAN トランキングを有効または無効にしたり、ネイティブ VLAN ID を設定したりできます。

- FlexConnect
- Flex + ブリッジ（FlexConnect + メッシュ）

バックホール クライアント アクセス

バックホール クライアント アクセスが有効な場合は、無線バックホールを介したワイヤレス クライアント アソシエーションが許可されます。バックホール無線は 2.4 または 5 GHz 無線です。つまり、バックホール無線は、バックホール トラフィックとクライアント トラフィックの両方を伝送できます。

バックホール クライアント アクセスが無効な場合は、バックホール トラフィックのみがバックホール無線を介して送信され、クライアント関連付けはアクセス無線でのみ実行されます。

（注） バックホール クライアント アクセスはデフォルトで無効になっています。バックホール クライアント アクセスを有効にすると、デイジーチェーン接続展開のスレーブ AP と子 AP を除くすべての MAP が再起動します。

屋外 AP の GPS サポート

拡張ネットワークで屋外 AP の場所を追跡することは、オペレータにとって大変な作業です。この問題の解決策として、一部の Cisco Aironet AP には GPS のレシーバとアンテナが付属しています。AP の GPS 座標は、コントローラまたは管理システムがマップ上で各デバイスを見つけるために使用されます。AP の場所に関する情報を取得するには、**show** コマンドを使用します。

メッシュ AP のバッテリ ステータス

一部のシスコ屋外 AP（Cisco Aironet 1532 など）には、バッテリ バックアップのオプションが付属しています。AP には、ビデオ監視カメラに電力を供給できる PoE 出力もあります。外部電源が使用できないとき、内部バッテリを一時的にバックアップ電源として使用できます。

MAC 認証の設定

ブリッジ モード AP の MAC アドレスをコントローラに追加するには、次の手順に従います。

始める前に

- コントローラでは、ブリッジ モード AP の MAC フィルタリングがデフォルトで有効になっています。したがって、設定する必要があるのは MAC アドレスだけです。使用する MAC アドレスは、該当する AP の背面に記載されています。
- MAC 認証は内部での認証と、外部 AAA サーバを使用した認証がサポートされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**username** *user-name* **mac** 例： `Device(config)# username 11:22:33:44:55:66 mac`	ユーザ名が MAC アドレスである MAC フィルタリングのユーザ名認証を設定します。
ステップ 3	**aaa authorization credential-download** *method-name* **local** 例： `Device(config)# aaa authorization credential-download list1 local`	ローカル データベースから EAP クレデンシャルをダウンロードするための名前付き許可リストを設定します。
ステップ 4	**aaa authorization dot1x** *method-name* **local** 例： `Device(config)# aaa authentication dot1x auth1 local`	ローカル ユーザ名認証として IEEE 802.1x の認証リストを設定します。
ステップ 5	**aaa authorization dot1x** *method-name* **radius group** *server-group-name* 例： `Device(config)# aaa authentication dot1x auth1 radius group radius-server-1`	RADIUS サーバ グループを使用した認証用に IEEE 802.1x の認証リストを設定します。
ステップ 6	**aaa authorization credential-download** *method-name* **radius group** *server-group-name* 例： `Device(config)# aaa authorization credential-download auth1 radius group radius-server-1`	サーバグループを使用した認証用に、RADIUS サーバから EAP クレデンシャルをダウンロードします。
ステップ 7	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュプロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 8	**security eap** 例： `Device(config-wireless-mesh-profile)# security eap`	メッシュ AP のメッシュ セキュリティ EAP を設定します。

	コマンドまたはアクション	目的
ステップ 9	**method authentication** *method-name* 例： `Device(config-wireless-mesh-profile)# method authentication auth1`	メッシュ AP 認証の認証方式を設定します。
ステップ 10	**method authorization** *method-name* 例： `Device(config-wireless-mesh-profile)# method authorization auth1`	メッシュ AP 認証の認証方式を設定します。

PSK プロビジョニングの設定

PSK プロビジョニングが有効になっている場合、AP は最初にデフォルト PSK を使用して接続します。PSK プロビジョニング キーが設定された後は、新しく接続した AP に設定済みのキーがプッシュされます。

PSK を設定するには、以下の手順に従います。

始める前に

プロビジョニングされた PSK は、メッシュ セキュリティとして PSK が設定されているすべての AP にプッシュされます。

- PSK は、コントローラおよび対応するメッシュ AP のリブート後も保存されます。
- コントローラは、合計 5 つの PSK と 1 つのデフォルト PSK を保持できます。
- メッシュ AP は、初期設定へのリセット時にのみプロビジョニング済み PSK を削除します。
- メッシュ AP は、最初のプロビジョニング済み PSK を受信した後はデフォルトの PSK を使用しません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless mesh security psk provisioning** 例：	ワイヤレスのセキュリティ方式を PSK として設定します。

	コマンドまたはアクション	目的
	`Device(config)# wireless mesh security psk provisioning`	（注） プロビジョニングされた PSK は、メッシュ セキュリティ方式として PSK が設定されている AP にのみプッシュされます。
ステップ 3	**wireless mesh security psk provisioning key** *index* {**0** | **8**} *pre-shared-key description* 例： `Device(config)# wireless mesh security psk provisioning key 1 0 secret secret-key`	メッシュ AP の新しい PSK を設定します。
ステップ 4	**wireless mesh security psk provisioning default-psk** 例： `Device(config)# wireless mesh security psk provisioning default-psk`	デフォルトの PSK ベースの認証を有効にします。
ステップ 5	**wireless mesh security psk provisioning inuse** *index* 例： `Device(config)# wireless mesh security psk provisioning inuse 1`	アクティブに使用する PSK を指定します。 （注） PSK インデックスを指すグローバル設定で、使用中のキー インデックスを明示的に設定する必要があります。

ブリッジ グループ名の設定

始める前に

- ブリッジ グループ名（BGN）がメッシュ プロファイルに設定されている場合、MAP がコントローラに接続するたびに、メッシュ プロファイルに設定されている BGN が AP にプッシュされます。
- メッシュ AP が AireOS コントローラから Cisco Catalyst 9800 シリーズ ワイヤレス コントローラに移動するたびに、メッシュ プロファイルに設定されている BGN がその AP にプッシュされて保存されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**bridge-group name** *bridge-grp-name* 例： `Device(config-wireless-mesh-profile)# bridge-group name bgn1`	ブリッジ グループ名を設定します。

バックグラウンド スキャンの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**background-scanning** 例： `Device(config-wireless-mesh-profile)# background-scanning`	メッシュ展開でバックグラウンドスキャンを設定します。

バックホール クライアント アクセスの設定

メッシュ プロファイルでバックホール クライアント アクセスを有効にするには、次の手順に従います。

始める前に

バックホール クライアント アクセスはデフォルトで無効になっています。有効にすると、デイジーチェーン接続展開のスレーブ AP と子 AP を除くすべての MAP がリブートします。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**client-access** 例： `Device(config-wireless-mesh-profile)# client-access`	クライアント アクセス AP を使用してバックホールを設定します。

無線バックホールのデータ レートの設定

バックホールは、AP 間でワイヤレス接続を作成するために使用されます。AP に応じて 802.11bg/a/n/ac のバックホール インターフェイスを使用できます。レート選択によって、利用可能な RF スペクトラムを効果的に使用できます。データ レートは、RF カバレッジとネットワーク パフォーマンスにも影響を与えます。低データ レート（6 Mbps など）のほうが、高データ レート（1300 Mbps など）よりも AP からの距離を延長できます。結果として、データ レートはセル カバレッジ、および必要な AP の数に影響を与えます。

特権 EXEC モードまたはメッシュ プロファイル コンフィギュレーション モードでワイヤレス バックホール データ レートを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **mesh backhaul rate** {**auto** | **dot11abg** | **dot11ac** |**dot11n**} 例：	バックホール転送速度を設定します。

	コマンドまたはアクション	目的
	`Device# #ap name ap1 mesh backhaul rate auto`	
ステップ 3	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**backhaul rate dot11 {24ghz | 5ghz}dot11n RATE_6M** 例： `Device(config-wireless-mesh-profile)# backhaul rate dot11 5ghz dot11n RATE_6M`	バックホール転送速度を設定します。

動的周波数選択の設定

DFSは、DFSチャネルでライセンスを必要としない操作の特定のタイマーとともに検出されるレーダー波形のタイプを指定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**full-sector-dfs** 例： `Device(config-wireless-mesh-profile)# full-sector-dfs`	DFS を有効にします。

侵入検知システムの設定

侵入検知システムを有効にすると、クライアントアクセスのすべてのトラフィックに関するレポートが生成されます。ただし、バックホール トラフィックは対象になりません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**ids** 例： `Device(config-wireless-mesh-profile)# ids`	屋外メッシュ AP の侵入検知システム レポートを設定します。

イーサネット ブリッジングの設定

MAP のイーサネット ポートはデフォルトで無効になっています。有効にするには、ルート AP と他の各 MAP でイーサネット ブリッジングを設定する必要があります。

イーサネット ブリッジングは、次の場合に有効にできます。

- メッシュ ノードをブリッジとして使用する。
- MAP のイーサネット ポートを使用してイーサネット デバイス（ビデオ カメラなど）を接続する。

始める前に

イーサネット ブリッジングを有効にするには、メッシュ プロファイル設定で次のコマンドを設定してください。

- **ethernet-bridging**：AP でイーサネット ブリッジング機能を有効にします。
- **no ethernet-vlan-transparent**：ブリッジ VLAN を認識させます。VLAN トランスペアレントが無効になっていることを確認します。
- イーサネットブリッジングが機能するように、ルート AP が接続されているスイッチ ポートをトランク ポートとして設定する必要があります。
- ブリッジ モード AP の場合は、**ap name** *name-of-rap* **mesh vlan-trunking native** *vlan-id* コマンドを使用して対応する RAP でトランク VLAN を設定します。イーサネット ブリッジング機能は、このコマンドが設定されていない AP では有効になりません。
- フレックス + ブリッジ AP の場合は、対応する flex プロファイルでネイティブ VLAN ID を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device# enable`	特権 EXEC モードを有効にします。 プロンプトが表示されたらパスワードを入力します。
ステップ 2	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode access** *vlan-id* 例： `Device# ap name ap1 mesh ethernet 1 mode access 21`	AP のイーサネットポートを設定し、モードをトランクとして設定します。
ステップ 3	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan** *vlan-id* 例： `Device# ap name ap1 mesh ethernet 1 mode trunk vlan native 21`	ネイティブ VLAN をトランク ポート用に設定します。
ステップ 4	**ap name** *ap-name* **mesh ethernet** {**0** | **1** | **2** | **3**}**mode trunk vlan allowed** *vlan-id* 例： `Device# ap name ap1 mesh ethernet 1 mode trunk vlan allowed 21`	トランク ポートの許可 VLAN を設定します。

メッシュを介したマルチキャストの設定

始める前に

- マルチキャスト パケットがイーサネット経由で MAP で受信された場合は、RAP に送信されます。ただし、他の MAP には送信されません。MAP から MAP へのパケットは、マルチキャストからフィルタで除去されます。
- マルチキャスト パケットがイーサネット経由で RAP で受信された場合、すべての MAP およびその個々のイーサネットワークに送信されます。
- in-out モードがデフォルトのモードです。in-out モードで動作中の場合、1 台の RAP によって送信されたマルチキャストを同じイーサネットセグメント上の別の RAP が受信してネットワークに戻さないよう、ネットワークを適切に分割する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**multicast** {**in-only** | **in-out** | **regular**} 例： `Device(config-wireless-mesh-profile)# multicast regular`	メッシュ マルチキャスト モードを設定します。

メッシュ バックホールの RRM の設定

メッシュ バックホールで RRM を有効にするには、次の手順に従います。

始める前に

メッシュ AP バックホールの RRM 測定は、次の条件に基づいて有効になります。

- メッシュ AP にルート AP ロールがある。
- ルート AP がイーサネット リンクを使用して接続している。
- ルート AP が子 AP にサービスを提供していない。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless mesh backhaul rrm** 例： `Device(config)# wireless mesh backhaul rrm`	メッシュ バックホールの RRM を設定します。

優先される親の選択

MAP の優先される親を設定するには、次の手順に従います。

このメカニズムを使用すると、AWPP で定義された親選択メカニズムをオーバーライドして、優先される親にメッシュ AP を強制的に移動できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **mesh parent preferred** *mac-address* **例：** `Device# ap name ap1 mesh parent preferred 00:0d:ed:dd:25:82`	AP のメッシュ パラメータを設定し、メッシュで優先される親の MAC アドレスを設定します。 （注） 優先される親の無線 MAC アドレスを使用してください。

AP のロールの変更

AP を RAP（または RAP を AP）に変更するには、次の手順に従います。

デフォルトでは、AP はメッシュ AP ロールでコントローラに参加します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **role** {**mesh-ap** | **root-ap**} **例：** `Device# #ap name ap1 root-ap`	ブリッジ モードの Cisco AP のロールを変更します。

メッシュ リーフ ノードの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name***mesh block-child** 例： `Device# #ap name ap1 mesh block-child`	リーフ ノードとしてのみ動作するように AP を設定します。他の MAP がこの AP を親 MAP として選択することはできません。 （注） 通常の AP に変更するには、このコマンドの **no** 形式を使用します。

サブセットチャネルの同期の設定

コントローラ内のすべてのRAPで使用されるすべてのチャネルが、以降の検索とコンバージェンスのためにすべてのMAPに送信されます。コントローラは、各ブリッジグループ名（BGN）のサブセット チャネルのリストを保持します。また、サブセット チャネルのリストはモビリティ グループ内のすべてのコントローラで共有されます。

モビリティ グループのサブセット チャネルの同期を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless mesh subset-channel-sync mac** 例： `Device(config)# wireless mesh subset-channel-sync`	モビリティ グループのサブセット チャネルの同期を設定します。

ブリッジモードおよびメッシュAP用のLSCのプロビジョニング

ブリッジモードおよびメッシュ AP の LSC を設定するには、次の手順に従います。

始める前に

- ローカルで有効な証明書（LSC）を設定しても、AP から既存の証明書が削除されることはありません。
- AP は、LSC とメッセージ整合性チェック（MIC）の両方の証明書を保持できます。ただし、AP が LSC でプロビジョニングされると、起動時に MIC 証明書は使用されません。LSC から MIC に変更する場合は、AP をリブートする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap lsc-provision** 例： `Device(config)# ap lsc-provision`	AP で LSC プロビジョニングを設定します。 （注） この手順は、メッシュ AP にのみ適用されます。
ステップ 3	**ap lsc-provision provision-list** 例： `Device(config)# ap lsc-provision provision-list`	（任意）プロビジョン リスト内のすべての AP に対して LSC プロビジョニングを設定します。
ステップ 4	**aaa authentication dot1x** *auth-list* **radius group** *radius-server-grp* 例： `Device(config)# aaa authentication dot1x list1 radius group sg1`	Radius グループ サーバから EAP クレデンシャルをダウンロードするための名前付き許可リストを設定します。
ステップ 5	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 6	**lsc-only-auth** 例： `Device(config-wireless-mesh-profile)# lsc-only-auth`	メッシュ セキュリティを LSC 専用 MAP 認証に設定します。 このコマンドを実行すると、すべてのメッシュ AP がリブートします。
ステップ 7	**method authorization** ローカル 例： `Device(config-wireless-mesh-profile)# method authorization list1`	メッシュ AP 認証の認証方式を設定します。

ルート AP のバックホール スロットの指定

メッシュ バックホール レートを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **mesh backhaul rate**{**auto** | **dot11abg**| **dot11ac** | **dot11n**} 例： `Device# ap name ap1 mesh backhaul rate auto`	メッシュ バックホール レートを auto に設定します。

メッシュ バックホールでのリンク テストの使用

ネイバー メッシュ AP 間のリンクテストをトリガーするには、次の手順に従います。

（注） AP からリンクテストを実行するには、**test mesh linktest mac-address** *neighbor-ap-mac* **rate** *data-rate* **fps** *frames-per-second* **frame-size** *frame-size* コマンドを使用します。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを開始します。
ステップ 2	**ap name** *ap-name* **mesh linktest** *dest-ap-mac data-rate packet-per-sec packet-size test-duration* 例： `Device# #ap name ap1 mesh linktest F866.F267.7DFB 24 234 1200 200`	リンク テスト パラメータを設定します。

メッシュ AP のバッテリ状態の設定

一部のシスコ屋外 AP には、バッテリ バックアップのオプションが付属しています。ビデオ監視カメラに電力を供給できる PoE 出力も用意されています。外部電源が使用できないとき、内部バッテリを一時的にバックアップ電源として使用できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile mesh** *profile-name* 例： `Device(config)# wireless profile mesh mesh1`	メッシュ プロファイルを設定し、メッシュ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**battery-state** 例： `Device(config-wireless-mesh-profile)# battery-state`	AP のバッテリ状態を設定します。

メッシュ設定の確認

次の **show** コマンドを使用して、メッシュ設定のさまざまな要素を確認します。

これらのコマンドの詳細については、『Cisco Catalyst 9800 Series Wireless Controller Command Reference』ドキュメントを参照してください。

- **show wireless mesh stats** *ap-name*
- **show wireless mesh security-stats** {*all* | *ap-name*}
- **show wireless mesh queue-stats** {*all* | *ap-name*}
- **show wireless mesh per-stats summary** {*all* | *ap-name*}
- **show wireless mesh neighbor summary** {*all* | *ap-name*}
- **show wireless mesh neighbor detail** *ap-name*
- **show wireless mesh ap summary**
- **show wireless mesh ap tree**
- **show wireless mesh ap backhaul**
- **show wireless mesh config**
- **show wireless mesh convergence detail** *bridge-group-name*
- **show wireless mesh convergence subset-channels**
- **show wireless mesh neighbor**
- **show wireless profile mesh detailed** *mesh-profile-name*
- **show wireless stats mesh security**
- **show wireless stats mesh queue**
- **show wireless stats mesh packet error**
- **show wireless mesh ap summary**
- **show ap name** *ap-name* **mesh backhaul**
- **show ap name** *ap-name* **mesh neighbor detail**
- **show ap name** *ap-name* **mesh path**
- **show ap name** *ap-name* **mesh stats packet error**
- **show ap name** *ap-name* **mesh stats queue**
- **show ap name** *ap-name* **mesh stats security**
- **show ap name** *ap-name* **mesh stats**
- **show ap name** *ap-name* **mesh bhrate**
- **show ap name** *ap-name* **config ethernet**
- **show ap name** *ap-name* **cablemodem**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **gps location**
- **show ap name** *ap-name* **environment**
- **show ap name** *ap-name* **mesh linktest data** *dest-mac*

- **show ap environment**
- **show ap gps location**

第 XIII 部

VideoStream

第 94 章

VideoStream

VideoStream について

IEEE 802.11 ワイヤレス マルチキャスト配信メカニズムには、パケットの消失や破損を認識するための、信頼できる方法がありません。結果として、無線配信中にマルチキャスト パケットが消失しても再送されないため、IP マルチキャスト ストリームが表示できなくなることがあります。

VideoStream 機能は、無線でマルチキャスト フレームをユニキャスト フレームに変換することで、IP マルチキャスト ストリームの無線配信を信頼できるものにします。VideoStream クライアントは、それぞれビデオ IP マルチキャスト ストリームの受信を認識します。

VideoStream の前提条件

- マルチキャスト機能が有効であることを確認します。コントローラ上の IP マルチキャストはマルチキャスト-マルチキャスト モードで設定することを推奨します。
- クライアント マシン上の IP アドレスを確認します。マシンには、それぞれの VLAN の IP アドレスが必要です。

• アクセス ポイントがコントローラに join していることを確認します。

VideoStream の設定方法

メディア ストリームのマルチキャストダイレクトのグローバル設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless multicast** 例： `Device(config)# wireless multicast`	ワイヤレス転送のマルチキャストをイネーブルにします。
ステップ 3	**ip igmp snooping** 例： `Device(config)# ip igmp snooping`	VLAN ごとに IGMP スヌーピングをイネーブルにします。グローバル設定が無効になっている場合、すべての VLAN は、有効かどうかに関係なく無効として扱われます。
ステップ 4	**ip igmp snooping querier** 例： `Device(config)# ip igmp snooping querier`	クエリーを生成するマルチキャスト ルータが VLAN 内に存在しない場合に、インターフェイスのスヌーピング クエリアを設定します。
ステップ 5	**wireless media-stream multicast-direct** 例： `(config)#wireless media-stream multicast-direct`	コントローラでグローバル マルチキャスト ダイレクトを設定します。
ステップ 6	**wireless media-stream message** 例： `(config)#wireless media-stream message ?` `Email Configure Session Announcement Email` `Notes Configure Session Announcement notes` `URL Configure Session Announcement URL` `phone Configure Session Announcement`	電話、URL、電子メール、メモなどのさまざまなメッセージ設定パラメータを設定します。つまり、メディア ストリームが（帯域幅制約が原因で）拒否された場合に、該当するユーザにメッセージを送信できます。これらのパラメータは、IT サポートの電子メール アドレスに送信するメッセージ、メモ（ストリームが拒否された理由を説明する画面メッセー

	コマンドまたはアクション	目的
	Phone number <cr>	ジ）、ユーザがリダイレクトされるURL、および拒否されたストリームについてユーザが問い合わせられる電話番号を設定します。
ステップ 7	**wireless media-stream group** *name startIp endIp* 例： (config)#**wireless media-stream group grp1 231.1.1.1 239.1.1.3** avg-packet-size Configures average packet size default Set a command to its defaults exit Exit sub-mode max-bandwidth Configures maximum Expected Stream Bandwidth in Kbps no Negate a command or set its defaults policy Configure media stream admission policy qos Configure Over the AIR QoS class, <'video'> ONLY	各メディア ストリームとそのパラメータ（予想されるマルチキャスト宛先アドレス、ストリームの帯域幅使用量、およびストリーム優先順位のパラメータなど）を設定します。
ステップ 8	**end** 例： Device(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11 帯域のメディア ストリームの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： Device# **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	**ap dot11 {24ghz | 5ghz} media-stream multicast-direct** 例： Device(config)#**ap dot11 24ghz media-stream multicast-direct**	802.11 帯域でメディア ストリーム（mc2uc）を使用可能かどうかを設定します

	コマンドまたはアクション	目的
ステップ 3	**ap dot11 {24ghz | 5ghz} media-stream video-redirect** 例： `Device(config)#ap dot11 24ghz media-stream video-redirect`	ユニキャスト ビデオ トラフィックのベストエフォート キューへのリダイレクトを設定します。
ステップ 4	**ap dot11 {24ghz | 5ghz} media-stream multicast-direct admission-besteffort** 例： `Device(config)#ap dot11 24ghz media-stream multicast-direct admission-besteffort`	帯域幅の可用性の制約によってメディア ストリームを優先できない場合に、ベスト エフォート キューを介してメディア ストリームが送信されるように設定します。帯域幅の可用性の制約によってメディア ストリームを優先できない場合にストリームをドロップするには、このコマンドの **no** 形式を実行します。
ステップ 5	**ap dot11 {24ghz | 5ghz} media-stream multicast-direct client-maximum** [*value*] 例： `Device(config)#ap dot11 24ghz media-stream multicast-direct client-max 15`	個々のクライアントごとに許可されるメディア ストリームの最大数を設定します。最大値は 15 で、デフォルトは 0 です。値 0 は、無制限のストリームを意味します。
ステップ 6	**ap dot11 {24ghz | 5ghz} media-stream multicast-direct radio-maximum** [*value*] 例： `Device(config)#ap dot11 24ghz media-stream multicast-direct radio-maximum 20`	無線ストリームの最大数を設定します。有効な範囲は、1 ～ 20 です。デフォルトは 0 です。値 0 は、無制限のストリームを意味します。
ステップ 7	**ap dot11 {24ghz | 5ghz} cac multimedia max-bandwidth** [*bandwidth*] 例： `Device(config)#ap dot11 24ghz cac multimedia max-bandwidth 60`	最大メディア（音声およびビデオ）帯域幅をパーセント単位で設定します。範囲は 5 ～ 85% です。
ステップ 8	**ap dot11 {24ghz | 5ghz} cac media-stream multicast-direct min_client_rate** [*dot11_rate*] 例： `Device(config)#ap dot11 24ghz cac media-stream multicast-direct min_client_rate`	クライアントがユニキャストとしてメディア ストリームを送信するために必要な最小 PHY レートを設定します。これよりも低いレートで通信するクライアントは、メディア ストリームをユニキャスト フローとして受信しません。通常、この PHY レートは、マルチキャスト フレームが送信されるレートと同じかそれ以上です。

	コマンドまたはアクション	目的
ステップ 9	**ap dot11 5ghz cac media-stream** 例： `Device(config)#ap dot11 5ghz cac media-stream`	メディア ストリーム アクセス カテゴリのコール アドミッション制御（CAC）パラメータを設定します。
ステップ 10	**ap dot11 5ghz cac multimedia** 例： `Device(config)#ap dot11 5ghz cac multimedia`	音声およびビデオに使用される、メディア アクセス カテゴリの CAC パラメータを設定します。
ステップ 11	**ap dot11 5ghz cac video** 例： `Device(config)#ap dot11 5ghz cac video`	音声シグナリングに使用される、ビデオ アクセス カテゴリの CAC パラメータを設定します。
ステップ 12	**ap dot11 5ghz cac voice** 例： `Device(config)#ap dot11 5ghz cac voice`	音声アクセスカテゴリのCACパラメータを設定します。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ビデオ ストリーミング用の WLAN 設定（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [WLANs] > [Wireless Networks] の順に選択します。
ステップ 2 [WLAN] を選択して、[Edit WLAN] ウィンドウを表示します。
ステップ 3 [Advanced] タブをクリックします。
ステップ 4 [Media Stream Multicast-Direct] チェック ボックスをオンにして、この機能を有効にします。
ステップ 5 [Update & Apply to Device] をクリックします。

ビデオ ストリーミング用の WLAN 設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *wlan_name* 例： `(config)#wlan wlan50`	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**shutdown** 例： `(config-wlan)#shutdown`	パラメータを設定するために、WLAN を無効にします。
ステップ 4	**media-stream multicast-direct** 例： `(config)#media-stream multicast-direct`	WLAN のメディア ストリームでマルチキャストダイレクトを設定します。
ステップ 5	**no shutdown** 例： `(config-wlan)#no shutdown`	WLAN をイネーブルにします。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

メディア ストリームの削除（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Media Stream]** を選択します。

ステップ 2 [Streams] タブをクリックします。

ステップ 3 削除するストリーム名の横にあるチェックボックスをオンにします。

複数のストリームを削除するには、複数のストリーム名のチェックボックスをオンにします。

ステップ 4 [削除（Delete）] をクリックします。

ステップ 5 確認ウィンドウで [Yes] をクリックして VLAN を削除します。

メディア ストリームの削除

始める前に

メディアス トリームを削除するには、メディア ストリームが有効化および設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**no wireless media-stream group** *media_stream_name* 例： `Device(config)#no wireless media-stream grp1`	コマンドで指定された名前を持つメディア ストリームを削除します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

メディア ストリームの監視

表 *42:* メディア ストリームの監視用のコマンド

コマンド	説明
show wireless media-stream client detail *group name*	特定のグループのメディア ストリーム クライアントの詳細を表示します。
show wireless media-stream client summary	すべてのクライアントのメディア ストリーム情報を表示します。
show wireless media-stream group detail *group name*	特定のグループのメディア ストリーム設定の詳細を表示します。

コマンド	説明
show wireless media-stream group summary	すべてのグループのメディア ストリーム設定の詳細を表示します。
show wireless media-stream message details	セッション通知メッセージの詳細を表示します。
show wireless multicast	マルチキャストダイレクト設定の状態を表示します。
show ap dot11 24ghz | 5ghz media-stream rrc	802.11 メディアのリソース予約コントロールの設定を表示します。

メディア ストリームの追加（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Media Stream] を選択します。

ステップ 2 [General] タブで [Multicast Direct Enable] チェック ボックスをオンにします。

ステップ 3 [Session Message Config] セクションで、[Session Announcement State] チェック ボックスをオンにしてセッション通知メカニズムを有効にします。セッション通知の状態が有効になっている場合、コントローラがクライアントにマルチキャスト ダイレクト データを提供できない場合は常にクライアントに通知されます。

ステップ 4 [Session Announcement URL] フィールドに、マルチキャスト メディア ストリーム伝送中にエラーが発生した場合にクライアントが詳細情報を参照できる URL を入力します。

ステップ 5 [Session Announcement Email] フィールドに、連絡可能な電子メール アドレスを入力します。

ステップ 6 [Session Announcement Phone] フィールドに、連絡可能な電話番号を入力します。

ステップ 7 [Session Announcement Note] フィールドに、特定のクライアントにマルチキャスト メディアを提供できない理由を入力します。

ステップ 8 [Apply] をクリックします。

メディア ストリームの追加（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless media-stream group** *groupName startIpAddr endIpAddr* 例：	各メディア ストリームとそのパラメータ（予想されるマルチキャスト宛先アドレス、ストリームの帯域幅使用量、およ

	コマンドまたはアクション	目的
	`Device(config)# wireless media-stream group group1 224.0.0.0 224.0.0.223`	びストリーム優先順位のパラメータなど）を設定します。
ステップ 2	**avg-packet-size** *packetsize* 例： `Device(media-stream)# avg-packet-size 100`	平均パケット サイズを設定します。
ステップ 3	**max-bandwidth** *bandwidth* 例： `Device(media-stream)# max-bandwidth 80`	予想されるストリームの最大帯域幅を Kbps 単位で設定します。
ステップ 4	**policy** {**admit** | **deny** } 例： `Device(media-stream)# policy admit`	メディア ストリームのアドミッション ポリシーを設定します。
ステップ 5	**qos video** 例： `Device(media-stream)# qos video`	無線 QoS クラスを「video」に設定します。
ステップ 6	**violation** {**drop** | **fallback** } 例： `Device(media-stream)# violation drop`	違反モードを設定します。
ステップ 7	**rrc-evaluation** {**initial** | **periodic** } 例： `Device(media-stream)# rrc-evaluation initial`	最初または定期的なアドミッション評価を提供するリソース予約コントロール（RRC）再評価アドミッションを設定します。
ステップ 8	**priority** *priority-value* 例： `Device(media-stream)# priority 6`	プライオリティ値を設定します。有効な範囲は 1 ～ 8 で、1 が最低です。

WLAN ごとのメディア ストリームの有効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [WLANs] ページで、**WLAN** の名前をクリックするか、[Add] をクリックして新規に作成します。

ステップ 3 表示される [Add/Edit WLAN] ウィンドウで [Advanced] タブをクリックします。

ステップ 4 [Enabling a Media Stream for each WLAN] チェック ボックスをオンにして、WLAN でメディア ストリームを有効にします。

ステップ 5 設定を保存します。

WLAN ごとのメディア ストリームの有効化

各 WLAN のメディア ストリームを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *wlan_name* 例： `Device(config)# wlan wlan5`	WLAN コンフィギュレーション モードを開始します。
ステップ 3	**shutdown** 例： `Device(config-wlan)# shutdown`	パラメータを設定するために、WLAN を無効にします。
ステップ 4	**media-stream multicast-direct** 例： `Device(config-wlan)# media-stream multicast-direct`	WLAN のマルチキャストダイレクトを設定します。
ステップ 5	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。

メディア ストリームの一般パラメータの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Media Stream]** を選択します。

ステップ 2 [Multicast Direct Enable] チェック ボックスをオンにして、ローカル モードでグローバルにマルチキャスト ダイレクトを有効にします。

ステップ 3 [Session Message Config] セクションで、次のパラメータの値を入力します。

- Session Announcement URL
- Session Announcement Email
- Session Announcement Phone
- Session Announcement Note

ステップ 4 設定を保存します。

メディア ストリームの一般パラメータの設定

メディア ストリームの一般パラメータを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# 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	**wireless media-stream message** {**URL** *url* | **email** *email-address* | **phone** *phone-no* | **notes** *notes* } **例：** `Device(config)# wireless media-stream message url www.xyz.com`	電話、URL、電子メール、メモなどのさまざまなメッセージ設定パラメータを設定します。
ステップ 3	**wireless media-stream multicast-direct** **例：** `Device(config)# wireless media-stream multicast-direct`	ローカル モードのマルチキャスト ダイレクトをグローバルに有効にします。 （注） この設定は、フレックスおよびファブリック メディア ストリームの設定には影響しません。
ステップ 4	**exit** **例：** `Device(config)# exit`	特権 EXEC モードに戻ります。

マルチキャスト ダイレクト アドミッション コントロールの設定

マルチキャスト ダイレクト アドミッション コントロールを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap dot11 {24ghz | 5ghz} shutdown** 例： `Device(config)# ap dot11 24ghz shutdown`	802.11b ネットワークを無効にします。
ステップ 3	**ap dot11 {24ghz | 5ghz} media-stream video-redirect** 例： `Device(config)# ap dot11 24ghz media-stream video-redirect`	ユニキャスト ビデオ トラフィックのベストエフォート キューへのリダイレクトを設定します。
ステップ 4	**ap dot11 {24ghz | 5ghz} cac media-stream acm** 例： `Device(config)# ap dot11 24ghz cac media-stream acm`	メディア ストリーム アクセス カテゴリのアドミッション コントロールを有効にします。
ステップ 5	**ap dot11 {24ghz | 5ghz} cac media-stream max-bandwidth** *bandwidth* 例： `Device(config)# ap dot11 24ghz cac media-stream max-bandwidth 65`	最大メディア帯域幅をパーセント単位で設定します。範囲は 5 ～ 85% です。
ステップ 6	**ap dot11 {24ghz | 5ghz} cac multimedia max-bandwidth** *bandwidth* 例： `Device(config)# ap dot11 24ghz cac multimedia max-bandwidth 65`	メディアの Wi-Fi マルチメディア（WMM）クライアントに割り当てられる最大帯域幅を設定します。範囲は 5 ～ 85% です。

	コマンドまたはアクション	目的
ステップ 7	**ap dot11 {24ghz | 5ghz} cac media-stream multicast-direct min-client-rate** *dot11Rate* 例： `Device(config)# ap dot11 24ghz cac media-stream multicast-direct min-client-rate 800`	クライアントがユニキャストとしてメディアストリームを受信するために必要な最小PHY レートを設定します。これよりも低いレートで通信するクライアントは、メディアストリームをユニキャストフローとして受信しません。通常、このPHY レートは、マルチキャストフレームが送信されるレートと同じかそれ以上です。
ステップ 8	**ap dot11 {24ghz | 5ghz} cac media-stream multicast-direct max-retry-percent** *retryPercent* 例： `Device(config)# ap dot11 24ghz cac media-stream multicast-direct max-retry-percent 50`	マルチキャストダイレクトストリームのCACパラメータ最大再試行パーセントを設定します。
ステップ 9	**ap dot11 {24ghz | 5ghz} media-stream multicast-direct radio-maximum** *value* 例： `Device(config)# ap dot11 24ghz media-stream multicast-direct radio-maximum 10`	無線ストリームの最大数を設定します。有効な範囲は1～20です。デフォルトは0です。値0は、無制限のストリームを意味します。
ステップ 10	**ap dot11 {24ghz | 5ghz} media-stream multicast-direct client-maximum** *value* 例： `Device(config)# ap dot11 24ghz media-stream multicast-direct client-maximum 12`	個々のクライアントごとに許可されるメディアストリームの最大数を設定します。最大値は15で、デフォルトは0です。値0は、無制限のストリームを意味します。
ステップ 11	**ap dot11 {24ghz | 5ghz} media-stream multicast-direct admission-besteffort** 例： `Device(config)# ap dot11 24ghz media-stream multicast-direct admission-besteffort`	帯域幅のアベイラビリティの制約によりメディアストリームを優先できない場合でも、メディアストリームがベストエフォートキューを介して送信されるように設定します。帯域幅のアベイラビリティの制約によりメディアストリームを優先できない場合、**no** をコマンドに追加して、ストリームをドロップします。
ステップ 12	**no ap dot11 {24ghz | 5ghz} shutdown** 例： `Device(config)# no ap dot11 24ghz shutdown`	802.11b ネットワークを有効にします。

メディア ストリーム情報の表示

メディア ストリーム情報を表示するには、次の **show** コマンドを使用します。

メディア ストリームの一般情報とステータスを表示するには、次のコマンドを使用します。

```
Device# show wireless media-stream multicast-direct state

Multicast-direct State..... : enabled
Allowed WLANs:
WLAN-Name                                          WLAN-ID
-------------------------------------------------------------
zsetup_mc                                          1
vwlc-mc_mo                                         3
mcuc_test1                                         4
mcuc_test2                                         5
```

```
Device# show wireless media-stream group summary


Number of Groups:: 4

Stream Name          Start IP                                  End IP
               Status
-------------------------------------------------------------------------------------------------------
new2                 231.2.2.3                                 231.2.4.4
               Enabled
my234                234.0.0.0                                 234.10.10.10
               Enabled
uttest2              235.1.1.20                                235.1.1.25
               Enabled
uttest3              235.1.1.40                                235.1.1.200
               Enabled
```

特定のメディア ストリームの詳細情報を表示するには、**show wireless media-stream client detail** *media_stream_name* コマンドを使用します。

```
Device# show wireless media-stream group detail uttest2


Media Stream Name         : uttest2
Start IP Address          : 235.1.1.20
End IP Address            : 235.1.1.25
RRC Parameters:
 Avg Packet Size(Bytes)   : 1200
 Expected Bandwidth(Kbps) : 1000
 Policy                   : Admitted
 RRC re-evaluation        : Initial
 QoS                      : video
 Status                   : Multicast-direct
 Usage Priority           : 4
 Violation                : Drop
```

dot11 帯域の RRC 情報を表示するには、**show ap dot11 {24ghz | 5ghz} mediastream rrc** コマンドを使用します。

```
Device# show  ap dot11 5ghz media-stream rrc

Multicast-direct                 : Enabled
Best Effort                      : Disabled
Video Re-Direct                  : Disabled
Max Allowed Streams Per Radio    : Auto
Max Allowed Streams Per Client   : 5
Max Media-Stream Bandwidth       : 5
Max Voice Bandwidth              : 50
Max Media Bandwidth              : 43
Min PHY Rate (Kbps)              : 6000
Max Retry Percentage             : 5
```

セッション アナウンス メッセージの詳細を表示するには、**show wireless media-stream message details** コマンドを使用します。

```
Device# show wireless media-stream message details
URL          :
Email        : abc@cisc
Phone        :
Note         :
State        : Disabled
```

データベース内のブラックリスト登録クライアントのリストを表示するには、**show ip igmp snooping igmpv2-tracking** コマンドを使用します。

```
Device# show ip igmp snooping igmpv2-tracking

Client to SGV mappings
----------------------
Client: 10.10.10.215 Port: Ca1
 Group: 239.255.255.250 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 234.5.6.7 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 234.5.6.8 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 234.5.6.9 Vlan: 10 Source: 0.0.0.0 blacklisted: no

Client: 10.10.101.177 Port: Ca2
 Group: 235.1.1.14 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 235.1.1.16 Vlan: 10 Source: 0.0.0.0 blacklisted: no
 Group: 235.1.1.18 Vlan: 10 Source: 0.0.0.0 blacklisted: no

SGV to Client mappings
----------------------
Group: 234.5.6.7 Source: 0.0.0.0 Vlan: 10
 Client: 10.10.10.215 Port: Ca1 Blacklisted: no
```

第 XIV 部

SD-Access ワイヤレス

第 95 章

SD-Access ワイヤレス

SD-Access ワイヤレスについて

エンタープライズファブリックは、エンドツーエンドのエンタープライズ全体のセグメンテーション、フレキシブルなサブネットアドレッシング、およびコントローラベースのネットワーキングにエンタープライズ全体にわたって統一されたポリシーとモビリティを提供します。これにより、エンタープライズネットワークは、サイト内およびサイト間のフレキシブルなレイヤ 2 拡張機能とともに、現在の VLAN 中心のアーキテクチャからユーザ グループベースのエンタープライズ アーキテクチャへと移行します。

エンタープライズファブリックは、相互接続されたスイッチを介してトラフィックを転送するネットワーク トポロジであり、単一レイヤ2またはレイヤ3のデバイスの抽象化を行います。これにより、ファブリックのエッジでポリシーを適用し、強制することで、シームレスな接続が実現します。ファブリックは IP オーバーレイを使用します。これにより、クラスタリング テクノロジーを使用せずにネットワークが単一の仮想エンティティとして表示されます。

ファブリック ノードに使用される定義は次のとおりです。

- **エンタープライズ ファブリック**：相互接続スイッチを通じてトラフィックが渡され、単一レイヤ 2 またはレイヤ 3 のデバイスの抽象化を実行するネットワーク トポロジ。
- **ファブリック ドメイン**：ネットワークの独立した操作部。他のファブリック ドメインとは別に管理されます。
- **エンドポイント**：ファブリック エッジ ノードに接続されたホストまたはデバイスをエンドポイント（EP）といいます。エンドポイントはファブリック エッジ ノードに直接接続するかまたはレイヤ 2 ネットワークを通じて接続します。

SD-Access ソリューションは、Cisco DNA Center ソフトウェアとファブリック ワイヤレス コントローラの機能を兼ね備えています。SD-Access ソリューションでは、ファブリック コント

ロール プレーン ノード、エッジ ノード、中間（トランスポート専用）ノード、ボーダー ノードの独立したセットによってファブリック サイトが構成されます。

次に、通常の SD-Access ワイヤレスのコンポーネントの図を示します。これは、ファブリック ボーダーノード（BN）、ファブリック中間ノード（IN）、ファブリックエッジノード（EN）、ワイヤレス コントローラ、Cisco DNA Center、およびホスト トラッキング データベース（HDB）で構成されています。

この図には、次の概念が含まれています。

- **Cisco DNA Center**：Cisco Catalyst 9800 シリーズ ワイヤレス コントローラの設定と管理を目的に、一連の設計原則に基づいて構築されたオープンなソフトウェア主導型アーキテクチャです。
- **ホスト ID トラッキング データベース（LISP のマップサーバとマップリゾルバ）**：このデータベースにより、ネットワークでデバイスまたはユーザの場所を特定できます。ホストの EP ID を学習すると、他のエンドポイントがホストの場所に関してデータベースにクエリを実行できます。トラッキング サブネットの柔軟性により、ドメイン間での集約が助長され、データベースのスケーラビリティが向上します。
- **ワイヤレス コントローラ（WLC）**：コントローラは AP イメージと設定管理、クライアント セッション管理およびモビリティを提供します。さらに、ワイヤレス クライアントの MAC アドレスをクライアント接続時にホスト トラッキング データベースに登録するとともに、クライアントのローミング時に場所を更新します。
- **共有サービスの分散（VSS）**：一般的に WLC はアンダーレイの一部である共有サービスの分散ブロックに接続されます。優先分散ブロックではシャーシが冗長化され、WLC に対するリンクとプラットフォームの冗長性も確保するために、L2 マルチシャーシ EtherChannel 接続がサポートされています。
- **アンダーレイ ネットワーク**：アンダーレイ ネットワークは、SD-Access ネットワークの導入に使用される物理スイッチによって定義されます。SD-Access のアンダーレイの実装では、キャンパス エッジ スイッチを含む、適切に設計されたレイヤ 3 基盤が使用され、ネットワークのパフォーマンス、拡張性、高可用性が確保されます。
- **オーバーレイ ネットワーク**：オーバーレイ ネットワークは、仮想ネットワークを構築するためにアンダーレイの上に作成されます。複数のオーバーレイ ネットワークを同じアンダーレイ ネットワークで実行して、仮想化によるマルチテナントをサポートできます。各オーバーレイ ネットワークは、外部ネットワークへの接続の仮想ルーティングおよび転送（VRF）インスタンスとして表示されます。
- **ボーダー ノードまたはコントロール プレーン ノード**：これらのノードは、従来のレイヤ 3 ネットワークまたはさまざまなファブリック ドメインをエンタープライズ ファブリック ドメインに接続します。複数のファブリック ドメインがある場合、これらのノードは 1 つのファブリック ドメインを 1 つ以上のファブリック ドメインに接続しますが、それらのドメインのタイプは同じであることも、異なることもあります。これらのノードは、1 つのファブリック ドメインから別のドメインへのコンテキストの変換を担います。カプセル化が異なるファブリック ドメイン間で同じである場合、ファブリック コンテキストの変

換は通常 1 対 1 となります。2 つのドメインのファブリック コントロール プレーンはこのデバイスを介した到達可能性とポリシー情報を交換します。

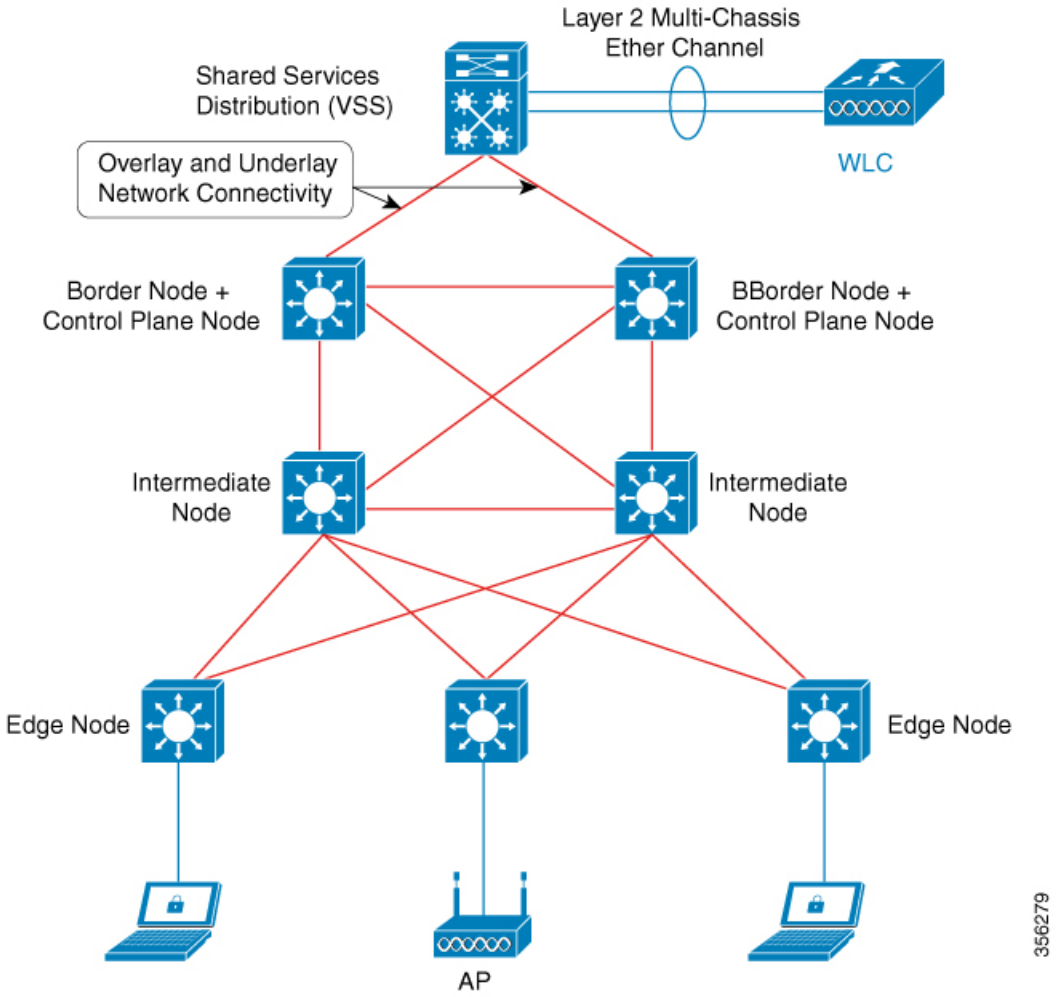
- **中間ノード**：エッジ ノードとボーダー ノードの相互接続に使用されるレイヤ 3 ネットワークの一部です。中間ノードはファブリック内の IP トラフィックをルーティングおよび転送します。
- **エッジ ノード**：これらのノードは EP からのトラフィックの承認、カプセル化またはカプセル化解除、および転送を担います。これらはファブリックを囲む境界にあり、ポリシーが適用される最初のポイントです。EP は、ファブリック ドメインの外側にある中間レイヤ 2 ネットワークを使用してファブリック エッジ ノードに直接または間接的に接続されることがあります。従来のレイヤ 2 ネットワーク、ワイヤレス アクセス ポイント、またはエンド ホストがファブリック エッジ ノードに接続されます。
- **アクセス ポイント**：AP はすべてのワイヤレス メディアの固有の機能を適用します。たとえば、無線ポリシー、SSID ポリシー、WebAuth パント、ピアツーピア ブロッキングなどがあります。CAPWAP 制御、およびコントローラへのデータ トンネルを確立します。ワイヤレス クライアントからの 802.11 データ トラフィックを 802.3 に変換し、VXLAN カプセル化を使用してアクセス スイッチに送信します。

この導入シナリオでは、ワイヤレス コントローラが共有サービスの分散（VSS）を使用してボーダー ノードに接続されます。ここで、VSS はモジュラ構成スイッチを指します。ファブリック展開には、ボーダー ノード、中間ノード、およびエッジ ノードが含まれています。すべてのノードがレイヤ 3 接続を使用して相互接続されます。ラップトップとアクセス ポイントは、レイヤ 2 接続を使用してデータ トラフィック（IP 接続）を受信します。

（注） 赤色の線はすべてレイヤ 3 接続です。

ラップトップとアクセス ポイントにつながっている青色の線は、レイヤ 2 接続です。

図 *25 : SD–Access* ワイヤレス



SDA では次を簡素化できます。

- ワイヤレス ネットワーク内でのアドレッシング
- ワイヤレス ネットワーク内でのモビリティ
- ゲスト アクセスとマルチ テナントに向けての移行
- ワイヤレス ネットワーク内でのサブネット拡張機能（拡張サブネット）の活用
- 一貫性のあるワイヤレス ポリシーの提供

AP 起動プロセス

次に、AP を起動する手順を示します。

- スイッチが AP に電源を投入します（PoE または UPoE）。

- AP は DHCP サーバから IP アドレスを取得します。
- スイッチは AP の IP アドレスをマップ サーバに登録します。
- AP は CAPWAP 検出によってコントローラを検出します。
- Datagram Transport Layer Security（DTLS）のハンドシェイク後、制御パケット用に CAPWAP 制御トンネルが AP とコントローラの間に作成されます。CAPWAP データ トンネルが IEEE 802.11 管理フレーム用に作成されます。AP イメージがダウンロードされ、設定がコントローラから AP にプッシュされます。
- コントローラは、登録された AP が背後にあるスイッチのマップ サーバ（RLOC IP）を照会します。
- コントローラは、マップ サーバにダミーの MAC アドレスを登録します。
- マップ サーバは、AP に VXLAN トンネルを作成するスイッチにダミーの MAC アドレス通知を送信します。
- AP はクライアントを受け入れる準備が整います。

ワイヤレス クライアントのオンボーディング

次に、クライアントをオンボーディングする手順を示します。

- ワイヤレス クライアントがそれ自体を AP に関連付けます。
- クライアントは、CAPWAP データ トンネルを使用してコントローラで IEEE 802.1x 認証を開始します（設定されている場合）。
- レイヤ 2 認証が完了すると、コントローラはクライアントの MAC アドレスをマップ サーバに登録します。
- マップ サーバはクライアントの詳細を示した通知メッセージをスイッチに送信します。
- スイッチはクライアントの MAC をレイヤ 2 転送テーブルに追加します。
- コントローラはクライアントを RUN 状態に移行し、クライアントはトラフィックの送信を開始できるようになります。
- スイッチはクライアントの IP アドレスをマップ サーバに登録します。
- スイッチは VXLAN パケットのカプセル化を解除します。
- スイッチは DHCP パケットを DHCP サーバに転送するか、またはリレーします。
- スイッチはワイヤレス クライアントの DHCP ACK を受信します。スイッチはクライアントの IP アドレスを学習し、更新をマップ サーバに送信します。
- スイッチは DHCP ACK を AP 側 VXLAN トンネルを含めて、VLAN 内のすべてのポートにブロードキャストします。
- DHCP 確認応答が AP に到達し、AP によってクライアントに転送されます。

- AP はクライアントの IP アドレスをコントローラに送信します。
- コントローラはクライアントを RUN 状態に移行します。

プラットフォーム サポート

表 *43 : SD-Access* ワイヤレスでサポートされるプラットフォーム

プラットフォーム	サポート
Catalyst 9300	はい
クラウド向け Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ	はい
Cisco Catalyst 9800-40 シリーズ ワイヤレス コントローラ	はい

表 *44 :* マルチインスタンスのサポート

マルチインスタンス	サポート
複数の LISP セッション	はい
エミュレート データベースのサポート	はい
WNCd インスタンス間のクライアント ローミング	はい

表 *45 :* 機能サポート

機能	サポート
IRCM の WLC 間ローミング	VLANがファブリック全体に拡張されるため、L2 モビリティのみがサポートされます。
DNS-IPv4-ACL	• ACL は AP で適用されます。 • コントローラは DNS-ACL 情報を AP にプッシュする必要があります。
クライアントの IPv6 ACL	可。オープン、802.11x、WebAuth、PSK WLAN、IPv6 アドレスの可視性もサポートされています。
ロケーション トラッキング/Hyperlocation	はい
マルチキャスト ビデオストリーム（IPv4）	はい

機能	サポート
スマート ライセンス	はい

表 *46 :* 屋外用アクセス ポイントのサポート

AP	サポート
1542	はい
1560	対応

SD-Access ワイヤレスの設定

SD-Access ワイヤレスをグローバルに有効にするには、次のコンフィギュレーション コマンドを実行する必要があります。

wireless fabric

デフォルト マップ サーバの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless Plus]** > **[Fabric]** > **[Fabric Configuration]** をクリックします。
ステップ 2 [Map Server] セクションで、サーバ 1 の IP アドレスと事前共有キーの詳細を指定します。
ステップ 3 必要に応じて、サーバ 2 の IP アドレスと事前共有キーの詳細を指定できます。
ステップ 4 [Apply] をクリックします。

デフォルト マップ サーバの設定（CLI）

デフォルト マップ サーバを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless fabric control-plane** *map-server-name* 例： `Device(config)# wireless fabric control-plane map-server-name`	デフォルト マップ サーバを設定します。 *map-server-name* はマップ サーバのペアを定義します。
ステップ 3	**ip address** *ip-address* **key** *user_password reenter_password* 例： `Device(config-wireless-cp)# ip address 200.0.0.0 key user-password user-password`	デフォルト マップ サーバの IP アドレスを設定します。
ステップ 4	**end** 例： `Device(config-wireless-cp)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

SD-Access ワイヤレス プロファイルの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Fabric]** を選択します。

ステップ 2 [Fabric] ページで [Profiles] タブ、[Add] の順にクリックします。

ステップ 3 表示された [Add New Profile] ウィンドウで、以下のパラメータを設定します。

- プロファイル名
- 説明
- [L2 VNID]：有効な範囲は 0 ～ 16777215 です。
- [SGT tag]：有効な範囲は 2 ～ 65519 です。

ステップ 4 [Save & Apply to Device] をクリックします。

SD-Access ワイヤレス プロファイルの設定（CLI）

SD-Access ワイヤレス プロファイルを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile fabric** *fabric-profile-name* 例： `Device(config)# wireless profile fabric fabric-profile-name`	SD-Access ワイヤレス プロファイルのパラメータを設定します。
ステップ 3	**sgt-tag** *sgt* 例： `Device(config-wireless-fabric)# sgt-tag 2`	SGT タグを設定します。 *sgt* は sgt タグ値を指します。有効な範囲は 2 ～ 65519 です。デフォルト値は 0 です。
ステップ 4	**client-l2-vnid** *client-l2-vnid* 例： `Device(config-wireless-fabric)# client-l2-vnid client-l2-vnid`	クライアントの L2-VNID を設定します。 *client-l2-vnid* は、クライアントの L2-VNID 値を指します。有効な範囲は 0 ～ 16777215 です。
ステップ 5	**end** 例： `Device(config-wireless-fabric)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

サイト タグでのマップ サーバの設定（GUI）

始める前に

ワイヤレス ファブリックの設定時にコントロール プレーンが設定されていることを確認します。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] > > を選択します。

ステップ 2 [Manage Tags] ページで、[Site] タブをクリックします。

ステップ 3 サイト タグの名前をクリックします。

ステップ 4 [Edit Site Tag] ウィンドウで、[Control Plane Name] ドロップダウンリストからファブリック コントロール プレーンの名前を選択します。

ステップ 5 設定を保存します。

サイト タグでのマップ サーバの設定（CLI）

サイト タグにマップ サーバを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag site** *site-tag* 例： `Device(config)# wireless tag site default-site-tag`	サイト タグを設定します。 *site-tag* はサイト タグ名を指します。
ステップ 3	**fabric control-plane** *map-server-name* 例： `Device(config-site-tag)# fabric control-plane map-server-name`	ファブリック コントロール プレーンの詳細を設定します。 *map-server-name* は、サイト タグに関連付けられているファブリック コントロール プレーン名を指します。
ステップ 4	**end** 例： `Device(config-site-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

L2-VNID ごとのマップ サーバの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Fabric]** を選択します。

ステップ 2 [Fabric Configuration] ページの [Fabric VNID Mapping] セクションで、[Add] をクリックします。

ステップ 3 [Add Client and AP VNID] ウィンドウで、ファブリックの名前、L2 VNID 値（有効な範囲は 0 ～ 4294967295）、コントロール プレーン名を指定します。

ステップ 4 設定を保存します。

L2-VNID ごとのマップ サーバの設定（CLI）

サイト タグにマップ サーバを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless fabric name** *name* **l2-vnid** *l2-vnid-value* **l3-vnid** *l3-vnid-value* **ip** *network-ip subnet-mask* **control-plane-name** *control-plane-name* 例： `Device(config)# wireless fabric name fabric_name l2-vnid 2 l3-vnid 2 ip 122.220.234.0 255.255.0.0 control-plane-name sample-control-plane`	VNID マップ テーブルにマップ サーバを設定します。 ここで、各変数は次のように定義されます。 • *name* はファブリック名を指します。 • *l2-vnid-value* は L2 VNID 値を指します。有効な範囲は 0 ～ 16777215 です。 • *L3-vnid-value* は L3 VNID 値を指します。有効な範囲は 0 ～ 16777215 です。 • *control-plane-name* はコントロール プレーン名を指します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

SD–Access ワイヤレスの確認

SD-Access ワイヤレス設定を確認するには、次のコマンドを使用します。

表 *47 : SD-Access* ワイヤレスを確認するためのコマンド

コマンド	説明
show wireless fabric summary	ファブリック ステータスを表示します。
show wireless fabric vnid mapping	VNID マッピングの詳細をすべて表示します。

コマンド	説明
show wireless profile fabric detailed *fabric_profile_name*	特定のファブリック プロファイル名の詳細を表示します。
show ap name *AP_name***config general**	Cisco AP の一般的な詳細情報を表示します。
show wireless client mac *MAC_addr* **detail**	クライアントの詳細情報を MAC アドレス別に表示します。
show wireless tag site detailed *site_tag*	サイト タグの詳細パラメータを表示します。

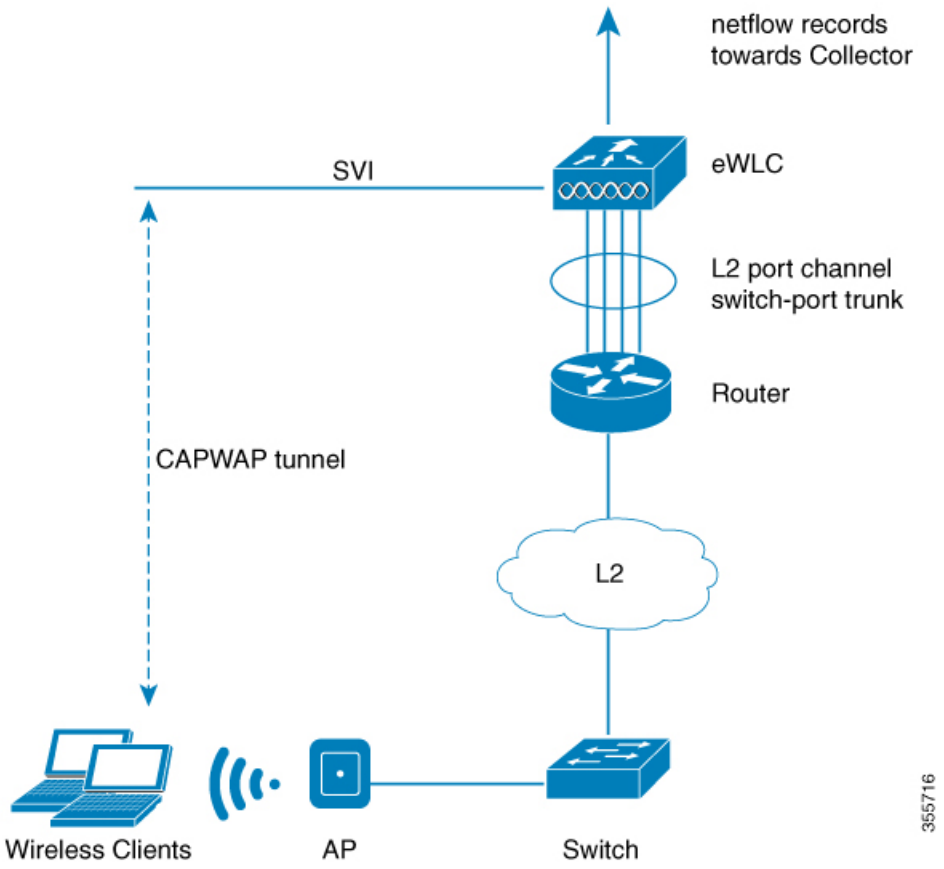
第 96 章

SD-Access（SDA ワイヤレス）での暗号化トラフィック分析の設定

暗号化トラフィック分析について

暗号化トラフィック分析（ETA）は、Flexible Netflow（FNF）テクノロジーを利用してフローに関する有用な情報をコレクタにエクスポートし、ネットワークの可視化を実現します。

図 *26 :* ローカル モードの *Cisco Catalyst 9800* シリーズ ワイヤレス コントローラに導入された暗号化トラフィック分析



ワイヤレス クライアントはデータ パケットをアクセス ポイントに送信します。次にパケットは CAPWAP によってカプセル化され、コントローラに送信されます。つまり、実際のクライアント データは CAPWAP ペイロードに含まれています。ETA をクライアント データに適用するには、パケットを ETA モジュールに渡す前に CAPWAP ヘッダーを除去する必要があります。

ETA には、次のような利点があります。

- 強化されたテレメトリ ベースの脅威分析。
- 分析によるマルウェアの特定。

ETA のグローバルな有効化

ETA の有効化

暗号化トラフィック分析を有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**et-analytics** 例： `Device(config)# et-analytics`	暗号化トラフィック分析を設定します。
ステップ 3	**end** 例： `Device(config-et-analytics)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ETA フロー エクスポートの宛先の設定

ETA フロー エクスポートの宛先を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**et-analytics** 例： `Device(config)# et-analytics`	暗号化トラフィック分析を設定します。
ステップ 3	**ip flow-export destination** *ip_address port_number* 例： `Device(config-et-analytics)# ip flow-export destination 120.0.0.1 2055`	NetFlow レコードのエクスポートを設定します。 ここで、各変数は次のように定義されます。 *port_number* の範囲は 1 ～ 65535 です。
ステップ 4	**end** 例： `Device(config-et-analytics)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ETA フロー エクスポートの宛先の設定（GUI）

手順

ステップ 1 [Configuration] > [Services] > [NetFlow] を選択します。

ステップ 2 [Add] ボタンをクリックします。[Create NetFlow] ダイアログ ボックスが表示されます。

ステップ 3 [Netflow Template] ドロップダウンリストから、使用可能なテンプレートのいずれかを選択します。

ステップ 4 [Collector Address] フィールドに IP アドレスを入力します。

ステップ 5 [Exporter Port] フィールドにポート番号を入力します。1 ～ 65535 の範囲で値を指定する必要があります。

ステップ 6 [Export Interface IP] ドロップダウンリストから必要なオプションを選択します。

ステップ 7 [Sampling Method] ドロップダウンリストから、いずれかのサンプリング方式を選択します。使用可能なオプションは、[Deterministic]、[Random]、および [Full Netflow] です。

ステップ 8 サンプルの範囲を入力します。32 ～ 1032 の値を指定する必要があります。

ステップ 9 [Available] ペインから必要なインターフェイスを選択して [Selected] ペインに移動します。

ステップ 10 [Save & Apply to Device] ボタンをクリックします。

非アクティブ タイマーの有効化

非アクティブ タイマーを有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**et-analytics** 例： `Device(config)# et-analytics`	暗号化トラフィック分析を設定します。
ステップ 3	**inactive-timeout** *timeout-in-seconds* 例： `Device(config-et-analytics)# inactive-timeout 15`	非アクティブ フローのタイムアウト値を指定します。 *timeout-in-seconds* の範囲は 1 ～ 604800 です。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config-et-analytics)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN ポリシー プロファイルでの ETA の有効化

WLAN ポリシー プロファイルで ETA を有効にするには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**et-analytics enable** 例： `Device(config-wireless-policy)# et-analytics enable`	ポリシーで暗号化トラフィック分析を有効にします。
ステップ 4	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

VLAN へのポリシー プロファイルの適用（GUI）

VLAN にポリシー プロファイルを適用するには、次の手順を実行します。

手順

ステップ 1 [RADIUS Profilling] チェックボックスをオンにします。

ステップ 2 [Local Subscriber Policy Name] から必要なポリシー名を選択します。

ステップ 3 [WLAN Local Profiling] セクションで [Global State of Device Classification] を有効または無効にして、[HTTP TLV Caching] と [DHCL TLV Caching] のチェックボックスをオンにします。

ステップ 4 [VLAN] セクションで、ドロップダウンリストから [VLAN/VLAN Group] を選択します。マルチキャスト VLAN を入力します。

ステップ 5 [WLAN ACL] セクションで、ドロップダウンリストから [IPv4 ACL] と [IPv6 ACL] を選択します。

ステップ 6 [URL Filters] セクションで、ドロップダウンリストから [Pre Auth] と [Post Auth] を選択します。

ステップ 7 [Save & Apply to Device] をクリックします。

VLAN へのポリシー プロファイルの適用

VLAN にポリシー プロファイルを適用するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *profile-name* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN のポリシー プロファイルを作成します。 *profile-name* はポリシー プロファイルのプロファイル名です。
ステップ 3	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan vlan-name`	ポリシー プロファイルを VLAN に割り当てます。
ステップ 4	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ワイヤレス ポリシー プロファイルを有効にします。

ETA 設定の確認

ETA のグローバルな確認

ETA グローバルおよびインターフェイスの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform software utd chassis active F0 et-analytics global

ET Analytics Global Configuration
ID: 1
All Interfaces: Off
IP address and port and vrf: 192.168.5.2:2055:0
```

ETA グローバル設定を表示するには、次のコマンドを使用します。

```
Device# show platform software et-analytics global

ET-Analytics Global state
=========================
 All Interfaces   : Off
 IP Flow-record Destination: 192.168.5.2 : 2055
 Inactive timer: 15
```

（注） **show platform software et-analytics global** コマンドでは、ETA が有効になっているワイヤレス クライアント インターフェイスは表示されません。

データパスの ETA グローバル状態を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature et-analytics datapath runtime

ET-Analytics run-time information:

   Feature state: initialized (0x00000004)
   Inactive timeout      : 15 secs (default 15 secs)
   WhiteList information :
       flag: False
       cgacl w0 :  n/a
       cgacl w1 :  n/a
   Flow CFG information  :
       instance ID       : 0x0
       feature ID        : 0x1
       feature object ID : 0x1
       chunk ID : 0xC
```

ETA メモリの詳細を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature et-analytics datapath memory

ET-Analytics memory information:

   Size of FO            : 3200 bytes
   No. of FO allocs      : 0
   No. of FO frees       : 0
```

データパスの ETA フロー エクスポートを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats
export

ET-Analytics 192.168.5.2:2055 vrf 0 Stats:
    Export statistics:
      Total records exported     : 5179231
      Total packets exported     : 3124873
      Total bytes exported       : 3783900196
      Total dropped records      : 0
      Total dropped packets      : 0
      Total dropped bytes        : 0
```

```
      Total IDP records exported :
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SPLT records exported:
            initiator->responder : 1285146
            responder->initiator : 979284
      Total SALT records exported:
            initiator->responder : 0
            responder->initiator : 0
      Total BD records exported  :
            initiator->responder : 0
            responder->initiator : 0
      Total TLS records exported :
            initiator->responder : 309937
            responder->initiator : 329469
```

ETA フローの統計情報を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature et-analytics datapath stats
flow

ET-Analytics Stats:
    Flow statistics:
      feature object allocs : 0
      feature object frees  : 0
      flow create requests  : 0
      flow create matching  : 0
      flow create successful: 0
      flow create failed, CFT handle: 0
      flow create failed, getting FO: 0
      flow create failed, malloc FO : 0
      flow create failed, attach FO : 0
      flow create failed, match flow: 0
      flow create, aging already set: 0
      flow ageout requests          : 0
      flow ageout failed, freeing FO: 0
      flow ipv4 ageout requests     : 0
      flow ipv6 ageout requests     : 0
      flow whitelist traffic match  : 0
```

ワイヤレス クライアント インターフェイス上の ETA の確認

ポリシーに ETA が設定されているかどうかを確認するには、次のコマンドを使用します。

```
Device# show wireless profile policy detailed default-policy-profile

Policy Profile Name           : default-policy-profile
Description                   : default policy profile
Status                        : ENABLED
VLAN                          : 160
Multicast VLAN                : 0
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
WLAN Switching Policy
  Central Switching           : ENABLED
  Central Authentication      : ENABLED
  Central DHCP                : ENABLED
  Flex NAT PAT            : DISABLED
  Central Assoc               : ENABLED
```

ワイヤレス クライアントの詳細で ETA ステータスを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature wireless wlclient datapath
<client_mac>

Wlclient Details for Client mac: 0026.c635.ebf8
  ---------------------------------
    Input VlanId  :  160
    Point of Presence      :  0
    Wlclient Input flags   :  9
    Instance ID   :  3
    ETA enabled   :  True
    client_mac_addr        :  0026.c635.ebf8

    bssid_mac_addr:  58ac.7843.037f
    Point of Attachment    :  65497
    Output vlanId :  160
    wlan_output_uidb       :  -1
    Wlclient Output flags  :  9
    Radio ID :  1
    cgacl w0 :  0x0
    cgacl w1 :  0x0
    IPv6 addr number       :  0
    IPv6 addr learning     :  0
```

ETA 保留ワイヤレス クライアント ツリー内のクライアントを表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature wireless et-analytics
eta-pending-client-tree

CPP IF_H     DPIDX      MAC Address    VLAN  AS  MS WLAN          POA
------------------------------------------------------------------------------
   0X2A     0XA0000001  2c33.7a5b.827b  160   RN  LC xyz_ssid     0x90000003
   0X2B     0XA0000002  2c33.7a5b.80fb  160   RN  LC xyz_ssid     0x90000003
```

QFP インターフェイス ハンドルを表示するには、次のコマンドを使用します。

```
Device#
show platform hardware chassis active qfp interface if-handle <qfp_interface_handle>

show platform hardware chassis active qfp interface if-handle 0X29
FIA handle - CP:0x27f3ce8  DP:0xd7142000
  LAYER2_IPV4_INPUT_ARL_SANITY
  WLCLIENT_INGRESS_IPV4_FWD
  IPV4_TVI_INPUT_FIA         >>> ETA FIA Enabled
  SWPORT_VLAN_BRIDGING
  IPV4_INPUT_GOTO_OUTPUT_FEATURE (M)
Protocol 1 - ipv4_output
FIA handle - CP:0x27f3d30  DP:0xd7141780
  IPV4_VFR_REFRAG (M)
  IPV4_TVI_OUTPUT_FIA        >>> ETA FIA Enabled
  WLCLIENT_EGRESS_IPV4_FWD
  IPV4_OUTPUT_DROP_POLICY (M)
  DEF_IF_DROP_FIA (M)
```

（注） *qfp_interface_handle* の範囲は 1 ～ 4294967295 です。

ETA 保留ワイヤレス クライアント ツリーの統計情報を表示するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature wireless et-analytics statistics

Wireless ETA cpp-client plumbing statistics
Number of ETA pending clients : 2
Counter                                          Value
-----------------------------------------------------------------
Enable ETA on wireless client called             0
Delete ETA on wireless client called             0
ETA global cfg init cb TVI FIA enable error      0
ETA global cfg init cb output SB read error      0
ETA global cfg init cb output SB write error     0
ETA global cfg init cb input SB read error       0
ETA global cfg init cb input SB write error      0
ETA global cfg init cb TVI FIA enable success    0
ETA global cfg uninit cb ingress feat disable    0
ETA global cfg uninit cb ingress cfg delete e    0
ETA global cfg uninit cb egress feat disable     0
ETA global cfg uninit cb egress cfg delete er    0
ETA pending list insert entry called             4
ETA pending list insert invalid arg error        0
ETA pending list insert entry exists error       0
ETA pending list insert no memory error          0
ETA pending list insert entry failed             0
ETA pending list insert entry success            4
ETA pending list delete entry called             2
ETA pending list delete invalid arg error        0
ETA pending list delete entry missing            0
ETA pending list delete entry remove error       0
ETA pending list delete entry success            2
```

第 XV 部

VLAN

第 97 章

VLAN

VLAN の前提条件

VLAN 設定時の前提条件と考慮事項を次に示します。

- VLANを作成する前に、VLANトランキングプロトコル（VTP）を使用してネットワークのグローバルな VLAN 設定を維持するかどうかを決定する必要があります。
- deviceで多数のVLANを設定し、ルーティングをイネーブルにしない予定の場合は、Switch Database Management（SDM）機能を VLAN テンプレートに設定します。これにより、最大数のユニキャストMACアドレスをサポートするようにシステムリソースが設定されます。
- VLAN グループに VLAN を追加できるようにするため、VLAN がdeviceに存在している必要があります。

VLAN の制約事項

次に、VLAN の制約事項を示します。

- 関連付けられている VLAN インターフェイスがすでに削除されている場合、ワイヤレス管理インターフェイスを削除することはできません。このシナリオを回避するには、VLAN インターフェイスを削除する前に、ワイヤレス管理インターフェイスを削除する必要があります。
- Per-VLAN Spanning Tree（PVST）または Rapid PVST のデバイス数は、スイッチ上のトランクの数にトランク上のアクティブ VLAN の数を掛けて、スイッチ上の非トランキング

インターフェイスの数を足したもの（トランク * VLAN + 非トランク ポート）に基づいています。MSTP の場合、サポートされる MST インスタンスの最大数は 4094 です。

- デバイスは、イーサネット ポート経由の VLAN トラフィック送信方式として IEEE 802.1Q トランキングをサポートします。
- クライアント VLAN が WLAN に設定されていない場合は、AP のネイティブ VLAN が使用されます。

VLAN について

論理ネットワーク

VLANは、ユーザの物理的な位置に関係なく、機能、プロジェクトチーム、またはアプリケーションなどで論理的に分割されたスイッチド ネットワークです。VLAN は、物理 LAN と同じ属性をすべて備えていますが、同じ LAN セグメントに物理的に配置されていないエンド ステーションもグループ化できます。どのようなdeviceポートでもVLANに属することができ、ユニキャスト、ブロードキャスト、マルチキャストのパケットは、その VLAN 内のエンド ステーションだけに転送またはフラッディングされます。各 VLAN は 1 つの論理ネットワークと見なされ、VLAN に属さないステーション宛のパケットは、ルータまたはフォールバック ブリッジングをサポートするdeviceを経由して伝送しなければなりません。VLAN はそれぞれが独立した論理ネットワークと見なされるので、VLANごとに独自のブリッジ管理情報ベース（MIB）情報があり、スパニングツリーの独自の実装をサポートできます。

VLAN は通常、IP サブネットワークに対応付けられます。たとえば、特定の IP サブネットに含まれるエンドステーションはすべて同じVLANに属します。device上のインターフェイスのVLAN メンバーシップは、インターフェイスごとに手動で割り当てます。この方法でdeviceインターフェイスを VLAN に割り当てた場合、これをインターフェイス ベース（またはスタティック）VLAN メンバーシップと呼びます。

VLAN 間のトラフィックは、ルーティングする必要があります。

deviceは、device仮想インターフェイス（SVI）を使用して、VLAN 間でトラフィックをルーティングできます。VLAN 間でトラフィックをルーティングするには、SVI を明示的に設定して IP アドレスを割り当てる必要があります。

サポートされる VLAN

deviceは、VTP クライアント、サーバ、およびトランスペアレントの各モードで VLAN をサポートしています。VLAN は、1 ～ 4094 の番号で識別します。VLAN 1 はデフォルト VLAN で、システム初期化中に作成されます。VLAN ID 1002 ～ 1005 は、トークンリングおよびファイバ分散データ インターフェイス（FDDI）VLAN 専用です。1002 ～ 1005 を除くすべての VLAN がユーザ設定のために使用できます。

VLAN ポート メンバーシップ モード

VLANに所属するポートは、メンバーシップ モードを割り当てることで設定します。メンバーシップ モードは、各ポートが伝送できるトラフィックの種類、および所属できる VLAN の数を指定します。

ポートが VLAN に所属すると、deviceは VLAN 単位で、ポートに対応するアドレスを学習して管理します。

表 *48 :* ポートのメンバーシップ モードとその特性

メンバーシップ モード	VLAN メンバーシップの特性	VTP の特性
スタティック アクセス	スタティック アクセス ポートは、手動で割り当てられ、1つの VLAN だけに所属します。	VTP は必須ではありません。VTP にグローバルに情報を伝播させないようにする場合は、VTP モードをトランスペアレント モードに設定します。VTP に加入するには、別のdeviceのトランク ポートに接続されているdevice少なくとも 1 つのトランク ポートが必要です。
トランク（IEEE 802.1Q） • IEEE 802.1Q：業界標準のトランキング カプセル化方式です。	デフォルトで、トランク ポートは拡張範囲 VLAN を含むすべての VLAN のメンバです。ただし、メンバーシップは許可 VLAN リストを設定して制限できます。また、プルーニング適格リストを変更して、リストに指定したトランク ポート上の VLAN へのフラッディング トラフィックを阻止することもできます。	VTP を推奨しますが、必須ではありません。VTP は、ネットワーク全体にわたって VLAN の追加、削除、名前変更を管理することにより、VLAN 設定の整合性を維持します。VTP はトランク リンクを通じて他のdevicesと VLAN コンフィギュレーション メッセージを交換します。
音声 VLAN	音声 VLAN ポートは、Cisco IP Phoneに接続し、電話に接続されたデバイスからの音声トラフィックに 1 つの VLAN を、データ トラフィックに別の VLAN を使用するように設定されたアクセス ポートです。	VTP は不要です。VTP は音声 VLAN に対して無効です。

VLAN コンフィギュレーション ファイル

VLAN ID 1 ～ 1005 の設定は vlan.dat ファイル（VLAN データベース）に書き込まれます。この設定を表示するには、**show vlan** 特権 EXEC コマンドを入力します。vlan.dat ファイルはフラッシュ メモリに格納されます。VTP モードがトランスペアレント モードの場合、それらの設定もdeviceの実行コンフィギュレーション ファイルに保存されます。

さらに、インターフェイス コンフィギュレーション モードを使用して、ポートのメンバーシップ モードの定義、VLAN に対するポートの追加および削除を行います。これらのコマンドの実行結果は、実行コンフィギュレーション ファイルに書き込まれます。このファイルを表示するには、**show running-config** 特権 EXEC コマンドを入力します。

VLAN および VTP 情報（拡張範囲 VLAN 設定情報を含む）をスタートアップ コンフィギュレーション ファイルに保存して、deviceを再起動すると、deviceの設定は次のように選択されます。

- スタートアップ コンフィギュレーションおよび VLAN データベース内の VTP モードがトランスペアレントで、VLANデータベースとスタートアップ コンフィギュレーション ファイルの VTP ドメイン名が一致する場合は、VLAN データベースが無視され（クリアされ）、スタートアップ コンフィギュレーション ファイル内の VTP および VLAN 設定が使用されます。VLAN データベース内の VLAN データベース リビジョン番号は変更されません。
- スタートアップ コンフィギュレーション内の VTP モードまたはドメイン名が VLAN データベースと一致しない場合、VLAN ID 1 ～ 1005 のドメイン名、VTP モード、および VTP 設定には VLAN データベース情報が使用されます。
- VTP バージョン 1 および 2 では、VTP モードがサーバである場合、VLAN ID 1 ～ 1005 のドメイン名と VLAN 設定で VLAN データベース情報が使用されます。VTP バージョン 3 は、VLAN 1006 ～ 4094 もサポートします。

（注） スイッチの設定をリセットする前に、**write erase** コマンドを使用して、必ずコンフィギュレーション ファイルと一緒に vlan.dat ファイルを削除してください。これにより、リセット時にスイッチが正しく再起動します。

標準範囲 VLAN 設定時の注意事項

標準範囲 VLAN は、ID が 1 ～ 1005 の VLAN です。

ネットワーク内で標準範囲 VLAN を作成または変更する場合には、次の注意事項に従ってください。

- 標準範囲 VLAN は、1 ～ 1001 の番号で識別します。VLAN 番号 1002 ～ 1005 は、トークンリングおよび FDDI VLAN 専用です。

- VLAN 1 ～ 1005 の VLAN 設定は、常に VLAN データベースに格納されます。VTP モードがトランスペアレント モードの場合、VTP と VLAN の設定もdeviceの実行コンフィギュレーション ファイルに保存されます。
- deviceが VTP サーバ モードまたは VTP トランスペアレント モードの場合は、VLAN データベース内の VLAN 2 ～ 1001 の設定を追加、変更、または削除できます（VLAN ID 1 および 1002 ～ 1005 は自動作成され、削除できません）。
- VTP トランスペアレント モードで作成された拡張範囲 VLAN は、VLAN データベースに保存されず、伝播されません。VTP バージョン 3 では、VTP サーバ モードでの拡張範囲 VLAN（VLAN 1006～4094）データベース伝播をサポートします。
- VLAN を作成する前に、deviceを VTP サーバ モードまたは VTP トランスペアレント モードにする必要があります。deviceが VTP サーバである場合には、VTP ドメインを定義する必要があります。VTP ドメインを定義しないと、VTP は機能しません。
- deviceは、トークンリングまたは FDDI メディアをサポートしません。deviceは FDDI、FDDI-Net、TrCRF、または TrBRF トラフィックを転送しませんが、VTP を介して VLAN 設定を伝播します。
- device は 128 スパニングツリー インスタンスをサポートします。deviceのアクティブな VLAN 数が、サポートされているスパニングツリー インスタンス数よりも多い場合、スパニングツリーは 128 の VLAN で有効にできます。残りの VLAN で、スパニングツリーは無効になります。

  device上の使用可能なスパニングツリー インスタンスをすべて使い切ってしまった後に、VTP ドメインの中にさらに別の VLAN を追加すると、そのdevice上にスパニングツリーが稼働しない VLAN が生成されます。そのdeviceのトランク ポート上でデフォルトの許可リスト（すべての VLAN を許可するリスト）が設定されていると、すべてのトランク ポート上に新しい VLAN が割り当てられます。ネットワーク トポロジによっては、新しい VLAN 上で、切断されないループが生成されることがあります。特に、複数の隣接devicesでスパニングツリー インスタンスをすべて使用してしまっている場合には注意が必要です。スパニングツリー インスタンスの割り当てを使い果たしたdevicesのトランク ポートに許可リストを設定することにより、このような可能性を防ぐことができます。

  device上の VLAN の数がサポートされているスパニングツリーインスタンスの最大数を超える場合、device上に IEEE 802.1s Multiple STP（MSTP）を設定して、複数の VLAN を単一のスパニングツリー インスタンスにマッピングすることを推奨します。

拡張範囲 VLAN 設定時の注意事項

拡張範囲 VLAN は、ID が 1006 ～ 4094 の VLAN です。

拡張範囲 VLAN を作成するときは次の注意事項に従ってください。

- 拡張範囲の VLAN ID は、deviceが VTP バージョン 3 を実行していない場合は VLAN データベースに保存されず、VTP で認識されません。
- プルーニング適格範囲に拡張範囲 VLAN を含めることはできません。

- VTP バージョン 1 または 2 では、グローバル コンフィギュレーション モードで、VTP モードをトランスペアレントに設定できます。VTP トランスペアレント モードでdeviceが始動するように、この設定をスタートアップ コンフィギュレーションに保存する必要があります。このようにしないと、deviceをリセットした場合に、拡張範囲 VLAN 設定が失われます。VTP バージョン 3 で拡張範囲 VLAN を作成する場合は、VTP バージョン 1 または 2 に変更できません。

VLAN の設定方法

標準範囲 VLAN の設定方法

VLAN データベースに新しい標準範囲 VLAN を作成したり、VLAN データベース内の既存の VLAN を変更したりする場合、次のパラメータを設定できます。

- VLAN ID
- VLAN 名
- VLAN タイプ
  - イーサネット
  - Fiber Distributed Data Interface [FDDI]
  - FDDI ネットワーク エンティティ タイトル [NET]
  - TrBRF または TrCRF
  - Token Ring
  - トークンリング Net
- VLAN ステート（アクティブまたは中断）
- Security Association Identifier（SAID）
- TrBRF VLAN のブリッジ識別番号
- FDDI および TrCRF VLAN のリング番号
- TrCRF VLAN の親 VLAN 番号
- TrCRF VLAN のスパニングツリー プロトコル（STP）タイプ
- ある VLAN タイプから別の VLAN タイプに変換するときに使用する VLAN 番号

vlan.dat ファイルを手動で削除しようとすると、VLAN データベースに不整合が生じる可能性があります。VLAN 設定を変更する場合は、この項の手順に従ってください。

イーサネット VLAN の作成または変更

始める前に

VTP バージョン 1 および 2 でdeviceが VTP トランスペアレント モードの場合は、1006 を超える VLAN ID を割り当てることができますが、それらを VLAN データベースに追加できません。

deviceは、イーサネット インターフェイスだけをサポートしています。FDDI およびトークンリング VLAN は、ローカルではサポートされないので、FDDI およびトークンリング メディア固有の特性は、他のdevicesに対する VTP グローバル アドバタイズにのみ設定します。

このdeviceはトークン リング接続をサポートしませんが、トークン リング接続を行っているリモート デバイスを、いずれかのサポート対象devicesから管理できます。VTP バージョン 2 を実行しているDevicesは、次のトークン リング VLAN に関する情報をアドバタイズします。

- トークンリング TrBRF VLAN
- トークンリング TrCRF VLAN

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**vlan** *vlan-id* 例： `Device(config)# vlan 20`	VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。新規の VLAN ID を入力して VLAN を作成するか、または既存の VLAN ID を入力してその VLAN を変更します。 （注） このコマンドで指定できる VLAN ID 範囲は 1 ～ 4094 です。
ステップ 3	**name** *vlan-name* 例： `Device(config-vlan)# name test20`	（任意）VLAN の名前を入力します。VLAN名を指定しなかった場合には、デフォルトとして、VLANという語の後ろに先行ゼロを含めた *vlan-id* 値が付加されます。たとえば、VLAN 4 のデフォルトの VLAN 名は VLAN0004 になります。

	コマンドまたはアクション	目的
ステップ 4	**media** { **ethernet** | **fd-net** | **fddi** | **tokenring** | **trn-net** } 例： `Device(config-vlan)# media ethernet`	VLANのメディアタイプを設定します。コマンドオプションは次のとおりです。 • **ethernet**：VLANのメディアタイプをイーサネットに設定します。 • **fd-net**：VLANのメディアタイプをFDDI-netに設定します。 • **fddi**：VLANのメディアタイプをFDDIに設定します。 • **tokenring**：VLANメディアタイプをトークンリングに設定します。 • **trn-net**：VLANメディアタイプをトークンリングネットに設定します。
ステップ 5	**remote-span** 例： `Device(config-vlan)# remote-span`	
ステップ 6	**end** 例： `Device(config)# end`	特権EXECモードに戻ります。
ステップ 7	**show vlan** { **name** *vlan-name* | **id** *vlan-id*} 例： `Device# show vlan name test20 id 20`	入力を確認します。

VLAN の削除（GUI）

手順

ステップ 1 **[Configuration]** > **[Layer2]** > **[VLAN]** を選択します。

ステップ 2 [VLAN] タブを選択します。

ステップ 3 削除する VLAN の横にあるチェックボックスをオンにします。

複数の VLAN を削除するには、複数の VLAN のチェックボックスをオンにします。

ステップ 4 [削除（Delete）] をクリックします。

ステップ 5 確認ウィンドウで [Yes] をクリックして VLAN を削除します。

VLAN の削除

VTP サーバ モードのdeviceから VLAN を削除すると、VTP ドメイン内のすべてのdevicesの VLAN データベースから、その VLAN が削除されます。VTP トランスペアレント モードの deviceから VLAN を削除した場合、その特定のdeviceスイッチ上に限り VLAN が削除されます。

イーサネット VLAN 1 および FDDI、またはトークンリング VLAN 1002 ～ 1005 の、メディア タイプ別のデフォルト VLAN は削除できません。

⚠

注意 VLAN を削除すると、その VLAN に割り当てられていたすべてのポートが非アクティブになります。これらのポートは、新しいVLANに割り当てられるまで、元のVLANに（非アクティブで）対応付けられたままです。

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** **例：** `Device# 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 3	**no vlan** *vlan-id* **例：** `Device(config)# no vlan 4`	VLAN ID を入力して、VLAN を削除します。
ステップ 4	**end** **例：** `Device(config)# end`	特権 EXEC モードに戻ります。

	コマンドまたはアクション	目的
ステップ 5	**show vlan brief** 例： `Device# show vlan brief`	VLANが削除されたことを確認します。
ステップ 6	**copy running-config startup-config** 例： `Device# 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。

VLAN へのスタティック アクセス ポートの割り当て

VTP をディセーブルにすることによって（VTP トランスペアレント モード）、VTP に VLAN 設定情報をグローバルに伝播させずに、スタティック アクセス ポートを VLAN に割り当てることができます。

Cisco Catalyst 9500 シリーズ スイッチで、クラスタ メンバ deviceのポートを VLAN に割り当てる場合は、最初に **rcommand** 特権 EXEC コマンドを使用してそのクラスタ メンバ スイッチにログインします。

存在しない VLAN にインターフェイスを割り当てると、新しい VLAN が作成されます

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**interface** *interface-id* 例： `Device(config)# interface gigabitethernet2/0/1`	VLANに追加するインターフェイスを入力します。

	コマンドまたはアクション	目的
ステップ 4	**switchport mode access** 例： `Device(config-if)# switchport mode access`	ポート（レイヤ 2 アクセス ポート）の VLAN メンバーシップ モードを定義します。
ステップ 5	**switchport access vlan** *vlan-id* 例： `Device(config-if)# switchport access vlan 2`	VLANにポートを割り当てます。指定できる VLAN ID の範囲は 1 ～ 4094 です。
ステップ 6	**end** 例： `Device(config-if)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show running-config interface** *interface-id* 例： `Device# show running-config interface gigabitethernet2/0/1`	インターフェイスのVLANメンバーシップ モードを確認します。
ステップ 8	**show interfaces** *interface-id* **switchport** 例： `Device# show interfaces gigabitethernet2/0/1 switchport`	表示された [Administrative Mode] フィールドおよび [Access Mode VLAN] フィールドの設定を確認します。
ステップ 9	**copy running-config startup-config** 例： `Device# 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。

拡張範囲 VLAN の設定方法

サービス プロバイダーは拡張範囲 VLAN を使用することにより、インフラストラクチャを拡張して、多数の顧客に対応できます。拡張範囲 VLAN ID は、VLAN ID が許可されている **switchport** コマンドで使用できます。

VTP バージョン 1 または 2 での拡張範囲 VLAN の設定は VLAN データベースに格納されません。ただし、VTPモードがトランスペアレントであるため、deviceの実行コンフィギュレーション ファイルに格納されます。また、設定をスタートアップ コンフィギュレーション ファイルに保存できます。VTP バージョン 3 で作成された拡張範囲 VLAN は、VLAN データベースに保存されます。

拡張範囲 VLAN については MTU サイズおよびリモート SPAN 設定ステートしか変更できません。残りのすべての特性はデフォルト状態のままでなければなりません。

拡張範囲 VLAN の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Layer2]** > **[VLAN]** を選択します。

ステップ 2 [VLAN] ページで [ADD] をクリックします。

ステップ 3 [VLAN ID] フィールドに拡張範囲 VLAN ID を入力します。

拡張範囲は 1006 ～ 4094 です。

ステップ 4 [Name] フィールドに VLAN 名を入力します。

ステップ 5 設定を保存します。

拡張範囲 VLAN の作成

手順

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# 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 3	**vlan** *vlan-id* 例： `Device(config)# vlan 2000` `Device(config-vlan)#`	拡張範囲 VLAN ID を入力して、VLAN コンフィギュレーション モードを開始します。指定できる範囲は 1006 ～ 4094 です。

	コマンドまたはアクション	目的
ステップ 4	**remote-span** 例： `Device(config-vlan)# remote-span`	（任意）RSPAN VLAN として VLAN を設定します。
ステップ 5	**exit** 例： `Device(config-vlan)# exit` `Device(config)#`	コンフィギュレーション モードに戻ります。
ステップ 6	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 7	**show vlan id** *vlan-id* 例： `Device# show vlan id 2000`	VLANが作成されたことを確認します。
ステップ 8	**copy running-config startup-config** 例： `Device# 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。

VLAN のモニタリング

表 *49 :* 特権 *EXEC* 表示コマンド

コマンド	目的
show interfaces [**vlan** *vlan-id*]	device上に設定されたすべてのインターフェイスまたは特定のVLAN の特性を表示します。

コマンド	目的
show vlan [**access-map** *name* | **brief** | **dot1q** { **tag native** } | **filter** [**access-map** | **vlan**] | **group** [**group-name** *name*] | **id** *vlan-id* | **ifindex** | **mtu** | **name** *name* | **remote-span** | **summary**]	device上のすべての VLAN または特定の VLAN のパラメータを表示します。次のコマンド オプションが使用可能です。 • **access-map**：VLAN アクセスマップを表示します。 • **brief**：VTP VLAN のステータス概要を表示します。 • **dot1q**：dot1q パラメータを表示します。 • **filter**：VLAN フィルタ情報を表示します。 • **group**：VLAN グループをグループ名と使用可能な接続済みの VLAN と一緒に表示します。 • **id**：識別番号別に VTP VLAN ステータスを表示します。 • **ifindex**：SNMP ifIndex を表示します。 • **mtu**：VLAN MTU 情報を表示します。 • **name**：指定された名前の VTP VLAN 情報を表示します。 • **remote-span**：リモート SPAN VLAN を表示します。 • **summary**：VLAN 情報の要約を表示します。

第 98 章

VLAN グループ

VLAN グループについて

クライアントがワイヤレス ネットワーク（WLAN）に接続するたびに、WLAN にマッピングされたポリシー プロファイルに関連付けられている VLAN にクライアントが配置されます。講堂、競技場、会議場などといった大規模な会場では、大量のワイヤレス クラインアントが使用されており、1 つの WLAN だけで多数のクライアントに対応することは困難な場合があります。

VLAN グループ機能は、複数の VLAN に対応できる 1 つのポリシー プロファイルを使用します。クライアントは、設定されている VLAN の 1 つに割り当てることができます。この機能は、VLAN グループを使用してポリシー プロファイルを 1 つまたは複数の VLAN にマッピングします。ワイヤレス クライアントが WLAN に関連付けられると、ワイヤレス クライアントの MAC アドレスに基づいてアルゴリズムにより VLAN が生成されます。VLAN がクライアントに割り当てられ、クライアントが割り当てられた VLAN から IP アドレスを取得します。またこの機能は、現行の AP グループ アーキテクチャおよび AAA オーバーライド アーキテクチャを拡張します。これらのアーキテクチャでは AP グループと AAA オーバーライドが、WLAN がマップされている 1 つの VLAN または VLAN グループをオーバーライドできます。

クライアントが DHCP を使用して IP アドレスを受信できない場合、VLAN は 30 分間にわたり「ダーティ」としてマークされます。30 分経過しても、VLAN グループの VLAN から「ダーティ」フラグがクリアされないことがあります。30 分後に VLAN がダーティではないとマークされたら、プール内の空き IP が使用可能で、かつ DHCP スコープが正しく定義されている場合は、IP 学習状態の新しいクライアントに VLAN からの IP アドレスを割り当てることができます。グローバル タイマーが期限切れになるまでに 5 分の遅延があり、各インターフェイスのタイムスタンプを調べて 30 分よりも大きいかどうかを確認する必要があるため、これは想定されている動作です。

VLAN グループの前提条件

- VLAN グループに VLAN を追加するには、VLAN がdeviceに存在している必要があります。
- VLAN グループが適切に機能するように、DHCP スヌーピングをグローバルに有効化したうえで、DHCP スヌーピングがすべての VLAN で有効になっていることを確認する必要があります。

VLAN グループの制約事項

- 1 つの VLAN グループにマッピングされる VLAN の数は、Cisco IOS XE ソフトウェア リリースによる制限を受けません。ただし、VLAN グループの VLAN の数が推奨値である 32 を超えた場合、モビリティが想定どおりに機能しなくなる可能性があり、VLAN グループ内の一部の VLAN で L2 マルチキャストが中断します。したがって、ネットワーク管理者は VLAN グループに適切な数の VLAN を設定する必要があります。

  VLAN グループ機能が想定どおりに動作するには、グループにマッピングされた VLAN がdeviceに存在している必要があります。スタティック IP クライアント動作はサポートされません。
- VLAN グループ機能はローカル モードでのみ動作します。

VLAN グループの設定

ここでは、VLAN グループのさまざまな設定作業について説明します。

VLAN グループの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Layer2]** > **[VLAN]** を選択します。

ステップ 2 **[VLAN]** > **[VLAN]** ページで [Add] をクリックします。

ステップ 3 [VLAN ID] フィールドに VLAN ID を入力します。

有効な範囲は 2 ～ 4094 です。

ステップ 4 [Name] フィールドに VLAN 名を入力します。

必要に応じてその他のパラメータを設定します。

ステップ 5 [Update & Apply to Device] をクリックします。

VLAN グループの作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**vlan group** *WORD* **vlan-list** *vlan-ID* 例： `Device(config)#vlan group vlangrp1 vlan-list 91-95`	所定のグループ名（vlangrp1）で VLAN グループを作成し、コマンドに一覧表示されているすべての VLAN を追加します。VLAN リストの範囲は 1 ～ 4096 で、1 つのグループの VLAN 数として推奨される数は 64 です。
ステップ 3	**end** 例： `Device(config)#end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。また、**CTRL-Z** を押して、グローバル コンフィギュレーション モードを終了します。

VLAN グループの削除（GUI）

手順

ステップ 1 **[Configuration]** > **[Layer2]** > **[VLAN]** を選択します。

ステップ 2 **[VLAN]** > **[VLAN Group]** ページで、削除する VLAN グループの横にあるチェックボックスをオンにします。

複数の VLAN グループを削除するには、複数の VLAN グループのチェックボックスをオンにします。

ステップ 3 [削除（Delete）] をクリックします。

ステップ 4 確認ウィンドウで [Yes] をクリックして VLAN グループを削除します。

VLAN グループの削除（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**vlan group** *WORD* **vlan-list** *vlan-ID* 例： `Device(config)#vlan group vlangrp1 vlan-list 91-95`	所定のグループ名（vlangrp1）で VLAN グループを作成し、コマンドに一覧表示されているすべての VLAN を追加します。VLAN リストの範囲は 1 ～ 4096 で、1 つのグループの VLAN 数として推奨される数は 64 です。
ステップ 3	**no vlan group** *WORD* **vlan-list** *vlan-ID* 例： `Device(config)#no vlan group vlangrp1 vlan-list 91-95`	所定のグループ名（vlangrp1）の VLAN グループが削除されます。
ステップ 4	**end** 例： `Device(config)#end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。または、Ctrl+Z を押してグローバル コンフィギュレーション モードを終了します。

WLAN への VLAN グループの追加（GUI）

ポリシー プロファイルは、広義にはネットワーク ポリシーとスイッチング ポリシーで構成されます。ポリシー プロファイルはタグ全体にわたって再利用可能なエンティティです。AP またはコントローラに適用されたクライアント向けのポリシーはすべて、ポリシープロファイルに移動されます。たとえば、VLAN、ACL、QOS、セッション タイムアウト、アイドル タイムアウト、AVC プロファイル、Bonjour プロファイル、ローカル プロファイリング、デバイス分類、BSSID QoS などが該当します。ただし、WLAN のワイヤレス関連のセキュリティ属性と機能はすべて、WLAN プロファイルにグループ化されます。

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] ＞ ＞を選択します。

ステップ 2 [Policy Profile] ページで [Add] をクリックし、次の設定を行います。

- 一般

- Access Policies
- QOS and AVC
- モビリティ
- Advanced

ステップ 3 [General] タブで、次の手順を実行します。

a) ポリシー プロファイルの名前および説明を入力します。
b) ポリシー プロファイルを有効にするには、[Status] を [Enabled] に設定します。
c) スライダを使用して、[Passive Client] と [Encrypted Traffic Analytics] を有効または無効にします。
d) [CTS Policy] セクションで、次について適切なステータスを選択します。
   - インライン タギング
   - SGACL Enforcement
e) デフォルトの SGT を指定します。有効な範囲は 2 ～ 65519 です。
f) [WLAN Switching Policy] セクションで、次について適切なステータスを選択します。
   - [Central Switching]
   - Central Authentication（中央認証）
   - Central DHCP
   - Central Association Enable
   - Flex NAT/PAT
g) [Save & Apply to Device] をクリックします。

ステップ 4 [Access Policies] タブで次の手順を実行します。

a) 次について適切なステータスを選択します。
   - HTTP TLV Caching
   - RADIUS Profiling
   - DHCP TLV Caching
b) [Local Subscriber Policy Name] を選択します。
c) 必要な [VLAN/VLAN Group] を選択します。
d) マルチキャスト VLAN を指定します。
e) 必要な [IPv4 ACL] と [IPv6 ACL] を選択します。
f) 必要な [Pre Auth] および [Post Auth] URL フィルタを選択します。
g) [Save & Apply to Device] をクリックします。

ステップ 5 [QoS and AVC] タブで次の手順を実行します。

a) 必要な [Auto QoS] を選択します。

b) 次について [Egress] と [Ingress] の詳細を指定します。

- **QoS SSID Policy**
- **QoS Client Policy**
- **Flow Monitor IPv4**
- **Flow Monitor IPv6**

c) [SIP-CAC] セクションで、次について適切なステータスを選択します。

- コール スヌーピング
- Send Disassociate
- Send 486 Busy

d) [Save & Apply to Device] をクリックします。

ステップ 6 [Mobility] タブで次の手順を実行します。

a) 必要に応じて、[Export Anchor] チェック ボックスをオンにしてエクスポート アンカーを有効にします。
b) スライダを使用して [Static IP Mobility] を有効または無効にします。
c) [Available] アンカーのリストから必要なアンカーを選択し、[Selected] アンカーのリストに移動します。
d) [Save & Apply to Device] をクリックします。

ステップ 7 [Advanced] タブで次の手順を実行します。

a) 次の [WLAN Timeout] の詳細を指定します。

- セッション タイムアウト
- アイドル タイムアウト
- Idle Threshold
- Client Exclusion Timeout

b) [DHCP] セクションで [DHCP Enable] チェック ボックスをオンにして、DHCP サーバの IP アドレスを入力します。
c) 次について適切なステータスを選択します。

- DHCP Option 82 Enable
- DHCP Option 82 ASCII
- DHCP Option 82 RID
- DHCP Option 82 Format
- DHCP AP MAC
- DHCP SSID
- DHCP AP ETH MAC

- DHCP AP NAME
- DHCP Policy Tag
- DHCP AP Location
- DHCP VLAN ID

d) [AAA Policy] セクションで、次について適切なステータスを選択します。
- Allow AAA Override
- NAC State

e) ポリシー名とアカウンティング リストを選択します。
f) 必要に応じて [Fabric Profile] を有効にして、使用可能なプロファイルのリストから選択します。
g) [Umbrella Parameter Map] から適切なパラメータ マップを選択します。
h) [WLAN Flex Policy] セクションで、次について適切なステータスを選択します。
- VLAN Central Switching
- Split MAC ACL

i) [Air Time Fairness Policies] セクションで、次について適切なステータスを選択します。
- 2.4 GHz Policy
- 5 GHz Policy

j) [Save & Apply to Device] をクリックします。

WLAN への VLAN グループの追加（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# 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	**wireless profile policy** *wlan-policy-profile-name* **例：** `Device(config)#wireless profile policy my-wlan-policy`	WLAN ポリシー プロファイルを設定します。

	コマンドまたはアクション	目的
ステップ 3	**vlan** *vlan-group1* 例： `Device(config-wireless-policy)#vlan myvlan-group`	グループ名を入力して、VLANグループを WLAN にマッピングします。
ステップ 4	**end** 例： `Device(config-wlan)#end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。または、Ctrl+Z を押してグローバル コンフィギュレーション モードを終了します。

VLAN グループの VLAN の表示（CLI）

コマンド	説明
show vlan group	VLAN グループの名前と使用可能な VLAN のリストを表示します。
show vlan group group-name *group_name*	指定された VLAN グループの詳細を表示します。
show wireless client mac-address *client-mac-addr* **detail**	クライアントに割り当てられている VLAN グループを表示します。
show wireless vlan details	VLAN の詳細を表示します。

第 XVI 部

WLAN

第 99 章

WLAN

WLAN について

この機能により、Lightweight アクセス ポイント全体に対して、最大 の WLAN を制御できます。各 WLAN には識別子である WLAN ID、プロファイル名、および WLAN SSID があります。すべてのdevicesは接続している各アクセス ポイントに対して最大 16 の WLAN を公開しますが、管理しやすくするため、サポートされる最大数の WLAN を作成し、これらの WLAN を異なるアクセス ポイントに選択的に公開する（アクセス ポイント グループを使用）ことができます。

異なる SSID または同じ SSID で WLAN を設定できます。SSID は、deviceがアクセスする必要がある特定の無線ネットワークを識別します。

（注） **no configure max-user-identity response** コマンドが設定されている場合でも、**wireless client max-user-login concurrent** コマンドは意図したとおりに機能します。

バンドの選択

帯域選択によって、デュアルバンド（2.4 GHz および 5 GHz）動作が可能なクライアントの無線を、輻輳の少ない 5 GHz アクセス ポイントに移動できます。2.4 GHz 帯域は、混雑していることがあります。この帯域のクライアントは一般に、Bluetooth デバイス、電子レンジ、およびコードレス電話機からの干渉を受けるだけでなく、他のアクセス ポイントからの同一チャネル干渉も受けます。これは、802.11b/g では、重複しないチャネルの数が 3 つに制限されているためです。このような干渉源を防ぎ、ネットワーク全体のパフォーマンスを向上させるには、deviceで帯域選択を設定します。

オフチャネル スキャンの保留

通常の動作状態では、Lightweightアクセス ポイントは定期的にオフ チャネルになり、別のチャネルをスキャンします。これは、次のような RRM 動作を実行するためのものです。

- 他の AP を使用した NDP パケットの送受信
- 不正 AP とクライアントの検出
- ノイズと干渉の測定

オフ チャネル期間は通常は約 70 ミリ秒で、この期間は AP は対応するチャネル上でデータの送受信ができません。したがって、パフォーマンスに若干の影響が及び、一部のクライアント送信がドロップされることがあります。

重要なデータをAPが送受信している間はオフチャネル スキャンを保留するように設定して、APがオフチャネルにならず、通常動作に影響を与えないようにすることができます。オフチャネル スキャンの保留は、指定した時間しきい値（ミリ秒単位）でWMM UPクラス単位でWLANごとに設定できます。AP が指定されたしきい値内の所定の UP クラスでマークされたデータ フレームを特定の WLAN 上で送受信している場合、その AP は次の RRM オフチャネル スキャンを保留します。たとえば、デフォルトでは、オフチャネル スキャンの保留は UP クラス 4、5、および 6 に対して 100 ミリ秒の時間しきい値で有効になります。したがって、RRM がオフチャネル スキャンを実行しようとしているときに直近の 100 ミリ秒内に UP 4、5、または 6 でマークされたデータ フレームを受信すると、RRM はオフチャネルになるのを保留します。音声サンプルを送受信し、UP 6 としてマークされている音声コールが 20 ミリ秒ごとにアクティブになる場合は、AP 無線はオフチャネルになりません。

オフチャネル スキャンの保留ではトレードオフが生じます。オフチャネル スキャンは、設定やトラフィック パターンなどに応じて2%以上の影響をスループットに与える可能性があります。すべてのトラフィック クラスに対してオフチャネル スキャンの保留を有効にし、時間しきい値を引き上げると、スループットが若干改善する可能性があります。ただし、オフチャネルにならないようにすることによって、RRM は AP ネイバーや不正を識別できず、セキュリティ、DCA、TPC、および 802.11k メッセージに悪影響が及びます。

デフォルトのオフチャネル スキャンの保留設定を変更しないことを推奨します。

DTIM 期間

802.11 ネットワークでは、Lightweight アクセス ポイントは、Delivery Traffic Indication Map (DTIM) と一致するビーコンを定期的に送信します。アクセス ポイントでビーコンがブロードキャストされると、DTIM期間で設定した値に基づいて、バッファされたブロードキャスト フレームおよびマルチキャスト フレームが送信されます。この機能により、ブロードキャスト データやマルチキャストデータが予想されると、適切なタイミングで省電力クライアントを再起動できます。

通常、DTIM の値は 1（ブロードキャスト フレームおよびマルチキャスト フレームはビーコンのたびに送信）または 2（ビーコン 1 回おきに送信）のいずれかに設定されます。たとえば、802.11 ネットワークのビーコン間隔が 100 ミリ秒で DTIM 値が 1 に設定されている場合、アク

セス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒 10 回送信します。ビーコン期間が 100ms で DTIM 値が 2 に設定されていると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを毎秒5回送信します。これらの設定はいずれも、ブロードキャスト フレームおよびマルチキャスト フレームの頻度を想定する、Voice over IP（VoIP）を含むアプリケーションに適しています。

ただし、DTIM 値は、802.11 のすべてのクライアントで省電力モードがイネーブルである場合、255 まで設定できます（255 回のビーコンごとにブロードキャスト フレームおよびマルチキャスト フレームを送信します）。クライアントは DTIM 期間に達したときのみリッスンする必要があるため、ブロードキャストとマルチキャストをリッスンする頻度を少なく設定することで、結果的にバッテリー寿命を長くできます。たとえば、ビーコン期間が 100 ms、DTIM 値を 100 に設定すると、アクセス ポイントは、バッファされたブロードキャスト フレームおよびマルチキャスト フレームを 10 秒ごとに 1 回送信します。このレートにより省電力クライアントで、ブロードキャストとマルチキャストをリッスンし、ウェイク アップするまでのスリープ状態が長くなり、バッテリ寿命を長くできます。

（注） ビーコン期間は、deviceでミリ秒単位で指定され、ソフトウェアによって、802.11 の時間単位（TU）（1 TU = 1.024 ミリ秒）に、内部的に変換されます。Cisco の 802.11n アクセス ポイントでは、この値は直近の 17 TU の倍数に丸められます。たとえば、100 ミリ秒に設定されたビーコン間隔は 104 ミリ秒の実際のビーコン間隔の結果です。

多くのアプリケーションでは、ブロードキャスト メッセージとマルチキャスト メッセージとの間隔を長くすると、プロトコルとアプリケーションのパフォーマンスが低下します。このようなクライアントをサポートする 802.11 ネットワークでは、低い DTIM 値を推奨します。

セッション タイムアウト

WLAN にセッション タイムアウトを設定できます。セッション タイムアウトとは、クライアント セッションが再認証を要求することなくアクティブである最大時間を指します。

Cisco Client Extensions

Cisco Client Extensions（CCX）ソフトウェアは、サードパーティ製クライアント デバイスの製造業者およびベンダーに対してライセンスされます。これらのクライアント上の CCX コードにより、サードパーティ製クライアント デバイスは、シスコ製のアクセス ポイントと無線で通信できるようになり、セキュリティの強化、パフォーマンスの向上、高速ローミング、電源管理などの、他のクライアントデバイスがサポートしていないシスコの機能もサポートできるようになります。

- ソフトウェアは、CCX バージョン 1 ～ 5 をサポートします。これによって、devicesとそのアクセス ポイントは、CCX をサポートするサードパーティ製クライアント デバイスと無線で通信できます。CCX サポートは、device上の各 WLAN に対して自動的に有効にな

り、無効にすることはできません。ただし、Aironet Information Element（IE）を設定できます。

- Aironet IE のサポートが有効になっている場合、アクセス ポイントは、Aironet IE 0x85（アクセス ポイント名、ロード、アソシエートされたクライアントの数などを含む）をこの WLAN のビーコンやプローブ応答に格納して送信します。また、アクセス ポイントが再アソシエーション要求内の Aironet IE 0x85 を受信する場合、deviceは、Aironet IEs 0x85 および 0x95（deviceの管理 IP アドレスおよびアクセス ポイントの IP アドレスを含む）を再アソシエーション応答に格納して送信します。

ピアツーピア ブロッキング

ピアツーピアブロッキングは個別のWLANに対して適用され、各クライアントが、アソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。ピア ツー ピアにより、トラフィックをリダイレクトする方法を制御できます。たとえば、トラフィックがdevice内でローカルにブリッジされたり、deviceによってドロップされたり、またはアップストリーム VLAN に転送されるように選択することができます。

ローカル スイッチングの WLAN にアソシエートしたクライアントに対して、ピアツーピアブロッキングはサポートされています。

診断チャネル

クライアントの WLAN による通信で問題が生じる理由についてトラブルシューティングする診断チャネルを選択できます。クライアントで発生している問題を識別し、ネットワーク上でクライアントを動作させるための修正措置を講じるために、クライアントとアクセスポイントをテストできます。診断チャネルを有効にするには、deviceの GUI または CLI を使用します。また、診断テストを実行するには、deviceの CLI を使用します。

（注） 診断チャネル機能は、管理インターフェイスを使用するアンカーされていない SSID に対してのみ有効にすることをお勧めします。CCX 診断機能は Cisco ADU カードを持つクライアントでのみテストされています。

WLAN の前提条件

- 最大 16 個の WLAN を各アクセス ポイント グループにアソシエートし、各グループに個々のアクセス ポイントを割り当てることができます。各アクセス ポイントは、有効化されている WLAN のうち、そのアクセス ポイント グループに属する WLAN だけをアドバタイズします。アクセス ポイント グループで無効化されている WLAN または別のグループに属する WLAN はアドバタイズしません。

- devicesがVLANトラフィックを正常にルーティングできるように、WLANと管理インターフェイスにはそれぞれ別の VLAN を割り当てることをお勧めします。

（注） Cisco IOS XE Fuji 16.8.x リリース以降、BSSID は対応するすべての WLAN ID と AP 無線に対して動的に生成されます。

WLAN の制約事項

- WLAN のプロファイル名を変更すると、FlexConnect AP（AP 固有の VLAN マッピングを使用する）が WLAN 固有になります。FlexConnect グループが適切に設定されている場合、VLAN マッピングはグループ固有になります。
- Flex ローカル認証が有効にされている WLAN では、Fast Transition 802.1X キー管理でクライアント関連付けがサポートされないため、IEEE 802.1X Fast Transition を有効にしないでください。
- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- WLAN 名と SSID は 32 文字以内にする必要があります。
- WLAN 名で特殊文字は使えません。
- WLAN 名はキーワードにはできません。たとえば、**wlan s** コマンドを入力して、「s」という名前で WLAN を作成しようとすると、「s」はシャットダウン用のキーワードとして使用されているため、すべての WLAN がシャットダウンします。
- WLAN から VLAN0 へのマッピング、VLAN 1002～1006 のマッピングはできません。
- 固定 IPv4 アドレスのデュアル スタック クライアントはサポートされません。
- 同じ SSID を持つ WLAN を作成するときには、各 WLAN に対して一意のプロファイル名を作成する必要があります。
- 同じ SSID を持つ複数の WLAN を同じ AP 無線に割り当てる場合は、クライアントがその中から安全に選択できるように、一意のレイヤ2セキュリティ ポリシーを使用している必要があります。
- WLAN がローカル スイッチングの場合、AVC が有効化されているローカル スイッチング WLAN にクライアントを関連付けます。AVC の統計 90 秒後を確認した時、クライアントからトラフィックを送信します。Cisco WLC はトップアプリケーション下では表示されますが、クライアントには表示されません。タイマーの問題があるため、最初のスロットの Cisco WLC ではクライアントの統計が表示されない可能性があります。AP と WLC でのタイマーが 89 秒間オフであった場合、その前のわずか 1 秒間のクライアントの統計情報が表示されます。現在では統計の削除は 180 秒後であるため、91 秒から 179 秒までのクライアントの統計情報が表示されます。これは、各クライアントあたり 2 つのコピーの統計がメモリの制約で Cisco 5508 WLC に保持することができないために起こります。

- ユーザ プロファイルの一部として送信される SSID は、**aaa override** コマンドが設定されている場合にのみ機能します。
- WLAN ごとの RADIUS サーバ上書きインターフェイス機能はサポートされていません。ただし、次の設定を使用して同じ結果を得ることができます。
  - RADIUS 認証サーバの設定
  - RADIUS 認証サーバ グループの設定
  - 802.1x WLAN の作成
  - ワイヤレス プロファイル ポリシーの設定と VLAN への適用

RADIUS 認証サーバの設定

- Device (config)# **radius server** *server-name*
- Device (config-radius-server)# **address ipv4** *address* **auth-port** *auth_port_number* **acct-port** *acct_port_number*
- Device (config-radius-server)# **key** *key*

RADIUS 認証サーバ グループの設定

- Device(config)# **aaa group server radius** *server-name*
- Device(config)# **server name** *server-name*
- Device(config)# **ip radius source-interface vlan** *vlan-name*
- Device(config)# **aaa authentication dot1x** *dot1x_name* **group** *server-name*

802.1x WLAN の作成

- Device(config)# **wlan** *wlan-name id ssid*
- Device(config-wlan)# **security dot1x authentication-list** *list-name*
- Device(config-wlan)# **no shutdown**

ワイヤレス プロファイル ポリシーの設定と VLAN への適用

- Device(config)# **wireless profile policy** *profile-name*
- Device(config-wireless-policy)# **vlan** *vlan-name*
- Device(config-wireless-policy)# **no shutdown**

シスコ ワイヤレス コントローラでの設定例を次に示します。

```
radius server RAD_EXT_3

 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813

 key cisco


aaa group server radius AAA_EXT_3
```

```
server name RAD_EXT_3
ip radius source-interface vlan 50

aaa authentication dot1x test_ext group AAA_EXT_3

wlan test_wpa2_dot1x 2 test_wpa2_dot1x
security dot1x authentication-list test_ext
no shutdown


wireless profile policy pp-1
vlan 50
no shutdown


radius server RAD_EXT_3

 address ipv4 9.2.62.56 auth-port 1812 acct-port 1813

 key cisco


aaa group server radius AAA_EXT_2
server name RAD_EXT_3
ip radius source-interface vlan 51

aaa authentication dot1x test_ext_2 group AAA_EXT_2

wlan test_wpa2 3 test_wpa3
security dot1x authentication-list test_ext_2
no shutdown


wireless profile policy pp-1
vlan 51
no shutdown
```

注意 一部のクライアントが複数のセキュリティ ポリシーで同じ SSID を検出すると WLAN に正しく接続できない場合があります。この機能を使用する際は、十分注意してください。

WLAN の設定方法

WLAN の作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックします。

[Add WLAN] ペインが表示されます。

ステップ 3 表示される [General] タブで、[Profile Name] フィールドに WLAN の名前を入力します。
ステップ 4 [Save & Apply to Device] をクリックします。

WLAN の作成（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name wlan-id* [*ssid*] 例： `Device(config)# wlan mywlan 34 mywlan-ssid`	WLAN の名前と ID を指定します。 • *profile-name* に、プロファイル名を入力します。入力できる範囲は英数字で 1 ～ 32 文字です。 • *wlan-id*に、WLAN ID を入力します。範囲は 1 ～ 512 です。 • *ssid* では、この WLAN に対する Service Set Identifier (SSID) を入力します。SSID を指定しない場合、WLANプロファイル名はSSIDとして設定されます。 （注） WLAN はデフォルトでディセーブルにされています。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN の削除（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 削除する WLAN の横にあるチェックボックスをオンにします。

複数の WLAN を削除するには、複数の WLAN のチェックボックスをオンにします。

ステップ 3 [削除（Delete）] をクリックします。

ステップ 4 確認ウィンドウで [Yes] をクリックして WLAN を削除します。

WLAN の削除

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**no wlan** *wlan-name wlan-id ssid* 例： `Device(config)# no wlan test2`	WLAN を削除します。引数は次のとおりです。 • *wlan-name*はWLANプロファイル名です。 • *wlan-id*は、WLAN ID です。 • *ssid* は WLAN に設定された WLAN SSID 名前です。 （注） AP グループに属する WLAN を削除すると、WLAN は AP グループと AP の無線から削除されます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN の検索

手順

	コマンドまたはアクション	目的
ステップ 1	**show wlan summary** 例： `Device# show wlan summary`	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

例

```
Device# show wlan summary
Number of WLANs: 4

WLAN Profile Name                     SSID                              VLAN Status
------------------------------------------------------------------------------------
1    test1                             test1-ssid                        137  UP
3    test2                             test2-ssid                        136  UP
2    test3                             test3-ssid                        1    UP
45   test4                             test4-ssid                        1    DOWN
```

WLAN を検索するときにワイルドカードを使用できます。たとえば、**show wlan summary include** *|variable* などです。variable は、出力内の検索文字列です。

```
Device# show wlan summary | include test-wlan-ssid
1    test-wlan                        test-wlan-ssid                     137   UP
```

WLAN の有効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [WLANs] ページで、WLAN 名をクリックします。

ステップ 3 [Edit WLAN] ウィンドウで、[Status] ボタンを [ENABLED] に切り替えます。

ステップ 4 [Update & Apply to Device] をクリックします。

WLAN のイネーブル化（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WLAN の無効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 [WLANs] ページで、WLAN 名をクリックします。
ステップ 3 [Edit WLAN] ウィンドウで、[Status] ボタンを [DISABLED] に切り替えます。
ステップ 4 [Update & Apply to Device] をクリックします。

WLAN のディセーブル（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 5	**show wlan summary** 例： `Device# show wlan summary`	デバイスに設定されているすべての WLAN のリストを表示します。出力内で WLAN を検索できます。

汎用 WLAN プロパティの設定（CLI）

次のパラメータを設定できます。

- メディア ストリーム
- ブロードキャスト SSID
- コール スヌーピング
- Radio
- インターフェイス
- ステータス

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name* 例：	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設

	コマンドまたはアクション	目的
	`Device# wlan test4`	定されているWLANのプロファイル名です。
ステップ 3	**shutdown** 例： `Device# shutdown`	パラメータを設定する前に、WLANをディセーブルにします。
ステップ 4	**broadcast-ssid** 例： `Device(config-wlan)# broadcast-ssid`	このWLANのSSIDをブロードキャストします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**radio** {**all** | **dot11a** | **dot11ag** | **dot11bg** | **dot11g**} 例： `Device# radio all`	WLANで無線をイネーブルにします。キーワードは次のとおりです。 • **all**：の無線帯域でWLANを設定します。 • **dot1a**：802.11aの無線帯域だけにWLANを設定します。 • **dot11g**：802.11agの無線帯域でのみWLANを設定します。 • **dot11bg**：802.11b/gの無線帯域でのみWLANを設定します（802.11gが無効の場合、802.11bのみ）。 • **dot11ag**：802.11gの無線帯域だけに無線LANを設定します。
ステップ 6	**client vlan** *vlan-identifier* 例： `Device# client vlan test-vlan`	WLANのインターフェイス グループをイネーブルにします。 *vlan-identifier*：VLAN IDを指定します。次に、VLAN名、VLAN ID、またはVLANグループ名を指定できます。
ステップ 7	**ip multicast vlan** *vlan-name* 例： `Device(config-wlan)# ip multicast vlan test`	WLANのマルチキャストをイネーブルにします。キーワードは次のとおりです。 • **vlan**：VLAN IDを指定します。 • *vlan-name*：VLAN名を指定します。

	コマンドまたはアクション	目的
ステップ 8	**media-stream multicast-direct** 例： `Device(config-wlan)# media-stream multicast-direct`	この WLAN でマルチキャスト VLAN をイネーブルにします。
ステップ 9	**call-snoop** 例： `Device(config-wlan)# call-snoop`	コール スヌーピング サポートをイネーブルにします。
ステップ 10	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 11	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

高度な WLAN プロパティの設定（CLI）

次の高度なプロパティを設定できます。

- AAA オーバーライド
- カバレッジ ホールの検出
- セッション タイムアウト
- Cisco Client Extensions
- 診断チャネル
- インターフェイス オーバーライド ACL
- P2P ブロッキング
- Client Exclusion
- WLAN ごとの最大クライアント数
- オフ チャネル スキャンの延期

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例：	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。

	コマンドまたはアクション	目的
	`Device# configure terminal`	
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**aaa-override** 例： `Device(config-wlan)# aaa-override`	AAA オーバーライドをイネーブルにします。
ステップ 4	**chd** 例： `Device(config-wlan)# chd`	この WLAN のカバレッジ ホールの検出をイネーブルにします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 5	**session-timeout** *time-in-seconds* 例： `Device(config-wlan)# session-timeout 450`	セッション タイムアウトを秒単位で設定します。範囲とデフォルト値は、セキュリティ設定によって異なります。WLAN セキュリティが dot1x に設定されている場合、範囲は 300～86400 秒で、デフォルト値は 1800 秒です。他のすべての WLAN セキュリティ設定では、有効範囲は 1～65535 秒であり、デフォルト値は 0 秒です。値 0 は、セッション タイムアウトなしを示します。
ステップ 6	**ccx aironet-iesupport** 例： `Device(config-wlan)# ccx aironet-iesupport`	この WLAN の Aironet IE のサポートをイネーブルにします。このフィールドは、デフォルトでイネーブルにされています。
ステップ 7	**diag-channel** 例： `Device(config-wlan)# diag-channel`	WLAN でクライアントの通信の問題を修復するための診断チャネルのサポートをイネーブルにします。
ステップ 8	**ip access-group** [web] *acl-name* 例： `Device(config)# ip access-group test-acl-name`	WLAN ACL グループを設定します。可変 *acl* 名前はユーザ定義する IPv4 ACL の名前を指定します。キーワード **web** は、IPv4 Web ACL を指定します。
ステップ 9	**peer-blocking** ［**drop** | **forward-upstream**］ 例：	ピアツーピア ブロッキング パラメータを設定します。キーワードは次のとおりです。

	コマンドまたはアクション	目的
	`Device(config)# peer-blocking drop`	• **drop**：ドロップアクションのピアツーピアブロッキングをイネーブルにします。 • **forward-upstream**：アップストリーム転送処理のピアツーピアブロッキングをイネーブルにします。
ステップ 10	**exclusionlist** *time-in-seconds* 例： `Device(config)# exclusionlist 10`	タイムアウトを秒単位で指定します。0 ～ 2147483647 の範囲の値を指定できます。タイムアウトなしでは、0 を入力します。ゼロ（0）タイムアウトは、クライアントが除外リストに追加されたことを示しています。
ステップ 11	**client association limit** *max-number-of-clients* 例： `Device(config)# client association limit 200`	WLAN で設定できる最大クライアント数を設定します。
ステップ 12	**channel-scan defer-priority** {**defer-priority** {**0-7**} | **defer-time** {**0 - 6000**}} 例： `Device(config)# channel-scan defer-priority 6`	チャネル スキャンの延期プライオリティと延期時間を設定します。引数は次のとおりです。 • **defer-priority**：オフチャネル スキャンを延期できるパケットのプライオリティ マーキングを指定します。範囲は 0 ～ 7 です。デフォルト値は 3 です。 • **defer-time**：延期時間（ミリ秒単位）。範囲は 0 ～ 6000 です。デフォルトは 100 です。
ステップ 13	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

高度な WLAN プロパティの設定（GUI）

始める前に

プライマリ コントローラとバックアップ コントローラを設定する前に、AP 参加プロファイルがすでに設定済みであることを確認します。

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[WLANs]** > **[Wireless Networks]** の順に選択します。

ステップ 2 [Wireless Networks] ページで [Add] をクリックします。

ステップ 3 [Advanced] タブで [Coverage Hole Detection] チェック ボックスをオンにします。

ステップ 4 [Aironet IE] チェック ボックスをオンにして、WLAN で Aironet IE を有効にします。

ステップ 5 [Diagnostic Channel] チェック ボックスをオンにして、WLAN で診断チャネルを有効にします。

ステップ 6 ドロップダウンリストから、必要な [P2P Blocking Action] 値を選択します。

ステップ 7 スライダを使用して、[Multicast Buffer] を有効または無効にします。

ステップ 8 [Media Stream Multicast-Direct] チェック ボックスをオンにして、この機能を有効にします。

ステップ 9 [Max Client Connections] セクションで、次のクライアント接続の最大数を指定します。

- WLAN 単位
- Per AP Per WLAN
- Per AP Radio Per WLAN

ステップ 10 [11v BSS Transition Support] セクションで次の設定タスクを実行します。

a) [BSS Transition] チェック ボックスをオンにして、802.11v BSS 移行サポートを有効にします。

b) [Disassociation Imminent] の値を入力します。

c) [Optimized Roaming Disassociation Timer] の値を入力します。

d) チェック ボックスをオンにして以下の項目を有効にします。

- BSS Max Idle Service
- BSS Max Idle Protected
- Disassociation Imminent Service
- Directed Multicast Service
- Universal Admin
- Load Balance
- 帯域選択
- IP ソース ガード

ステップ 11 [WMM Policy] で [Allowed]、[Disabled]、または [Required] を選択します。デフォルトでは、WMM ポリシーが許可されています。

ステップ 12 [Off Channel Scanning Defer] セクションで適切な延期プライオリティ値を選択し、必要なスキャン延期時間の値をミリ秒単位で指定します。

ステップ 13 [Assisted Roaming (11k)] セクションで、次について適切なステータスを選択します。

- Prediction Optimization
- ネイバー リスト
- Dual-Band Neighbor List

ステップ 14 [DTIM Period (in beacon intervals)] セクションで、802.11a/n 無線と 802.11b/g/n 無線の値を指定します。有効な範囲は 1 ～ 255 です。

ステップ 15 [Save & Apply to Device] をクリックします。

WLAN プロパティの監視（CLI）

コマンド	説明
show wlan id *wlan-id*	WLAN ID に基づいて WLAN プロパティを表示します。
show wlan name *wlan-name*	WLAN 名に基づいて WLAN プロパティを表示します。
show wlan all	設定されているすべての WLAN の WLAN プロパティを表示します。
show wlan summary	すべての WLAN の要約を表示します。サマリー詳細には、次の情報が含まれます。 • WLAN ID • プロファイル名 • SSID • VLAN • Status（ステータス）
show running-config wlan *wlan-name*	WLAN の名前に基づいて WLAN の実行コンフィギュレーションを表示します。
show running-config *wlan*	すべての WLAN の実行コンフィギュレーションを表示します。

第 100 章

リモート LAN

リモート LAN について

リモート LAN（RLAN）は、コントローラを使用する有線クライアントの認証に使用されます。有線クライアントがコントローラに正常に接続すると、LAN ポートは中央スイッチング モードとローカル スイッチング モードの間でトラフィックをスイッチングします。有線クライアントからのトラフィックは、ワイヤレス クライアント トラフィックとして扱われます。

アクセス ポイント（AP）の RLAN は、有線クライアントを認証するための認証要求を送信します。RLAN での有線クライアントの認証は、ワイヤレス クライアントの中央認証に似ています。

（注） RLAN は、複数のイーサネット ポートを備えた AP でサポートされています。

サポートされる AP モデルは次のとおりです。

- Cisco Aironet OEAP 1810 および 1815T シリーズ
- Cisco Aironet 1810w および 1815w シリーズ
- Cisco Aironet 702w シリーズ

（注） Cisco Aironet 702w シリーズ AP に接続されているオープン認証 RLAN クライアントは、有線クライアントとして機能します。したがって、次の show コマンドを実行しても、これらのクライアントの IP アドレスと統計情報は表示されません。

- show wireless client summary
- show wireless client mac *mac_address* detail

イーサネット（AUX）ポートについて

Cisco Aironet 1850、2800、および 3800 シリーズ AP では、2 番目のイーサネット ポートがデフォルトでリンク集約（LAG）ポートとして使用されます。この LAG ポートは LAG が無効になっている場合に RLAN ポートとして使用できます。

次の AP は、LAG ポートを RLAN ポートとして使用します。

- 1852E
- 1852I
- 2802E
- 2802I
- 3802E
- 3802I
- 3802P

Cisco 2700 アクセス ポイントでの AUX ポートの使用に関する制限事項

- RLAN は、このポートの AUX ポートおよび非ネイティブ VLAN をサポートしています。
- ローカル モードでは、中央スイッチの有線クライアント トラフィックがサポートされます。一方、Flexconnect モードでは中央スイッチはサポートされません。
- Flexconnect モードでは、ローカル スイッチの有線クライアント トラフィックはサポートされますが、中央スイッチについてはサポートされません。
- AUX ポートをトランク ポートとして使用することはできません。ポートの背後にスイッチまたはブリッジを追加することもできません。
- AUX ポートは dot1x をサポートしていません。

コントローラの役割

- コントローラはオーセンティケータとして機能し、有線クライアントからの Extensible Authentication Protocol（EAP）over LAN（EAPOL）メッセージは AP 経由でコントローラに到達します。
- コントローラは、設定された認証、認可、およびアカウンティング（AAA）サーバと通信します。
- コントローラは AP 用の LAN ポートを設定し、対応する AP にプッシュします。

リモート LAN（RLAN）の設定

すべての RLAN の有効化または無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**[no] ap remote-lan shutdown** 例： `Device(config)# [no] ap remote-lan shutdown`	すべての RLAN を有効または無効にします。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RLAN プロファイルの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap remote-lan profile-name** *remote-lan-profile-name rlan-id* 例： `Device(config)# ap remote-lan profile-name rlan_profile_name 3`	リモート LAN プロファイルを設定します。 • *remote-lan-profile*：リモート LAN プロファイル名です。範囲は英数字で 1 ～ 32 文字です。 • *rlan-id*：リモート LAN の識別子です。範囲は 1 ～ 128 です。

	コマンドまたはアクション	目的
		（注） 最大 128 の RLAN を作成できます。既存の RLAN の *rlan id* を別の RLAN の作成時に使用することはできません。 RLAN と WLAN の両方のプロファイルに同じ名前を付けることはできません。同様に、RLAN と WLAN のポリシープロファイルに同じ名前を付けることはできません。

RLAN プロファイル パラメータの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Remote LAN]** を選択します。

ステップ 2 [RLAN Profile] タブで [Add] をクリックします。

[Add RLAN Profile] ウィンドウが表示されます。

ステップ 3 [General] タブで次の手順を実行します。

a) RLAN プロファイルの [Name] と [RLAN ID] を入力します。

b) [Client Association Limit] フィールドで RLAN ごとのクライアント接続数を設定します。

範囲は 0 ～ 10000 です。0 は無制限のクライアント接続を意味します。

c) プロファイルを有効にするには、ステータスを [Enable] に設定します。

ステップ 4 **[Security]** > **[Layer2]** タブで次の手順を実行します。

a) RLAN の 802.1x を有効にするには、[802.1x] ステータスを [Enabled] に設定します。

（注） Web 認証リストまたは 802.1x 認証リストを同時にアクティブにできます。

b) [MAC Filtering] ドロップダウンリストから、許可リスト名を選択します。

c) [Authentication List] ドロップダウンリストから RLAN 認証リスト名に対して 802.1x を選択します。

ステップ 5 **[Security]** > **[Layer3]** タブで次の手順を実行します。

a) RLAN の Web 認証を有効にするには、[Web Auth] ステータスを [Enabled] に設定します。

（注） Web 認証リストまたは 802.1x 認証リストを同時にアクティブにできます。

b) [Webauth Parameter Map] ドロップダウンリストから、Web 認証パラメータ マップを選択します。

c) [Authentication List] ドロップダウンリストから Web 認証リスト名を選択します。

ステップ 6 **[Security]** > **[AAA]** タブで次の手順を実行します。

a) [Local EAP Authentication] を [enabled] に設定します。また、必要な [EAP Profile Name] をドロップダウンリストから選択します。

ステップ 7 設定を保存します。

RLAN プロファイル パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**client association limit** *client-connections* 例： `Device(config-remote-lan)# client association limit 1`	RLAN ごとのクライアント接続数を設定します。 *client-connections*：RLAN ごとの最大クライアント接続数。範囲は 0 ～ 10000 です。0 は無制限を意味します。
ステップ 2	**ip access-group web** *IPv4-acl-name* 例： `Device(config-remote-lan)# ip access-group web acl_name`	RLAN IP コンフィギュレーション コマンドを設定します。 *IPv4-acl-name*：IPv4 ACL の名前または ID を指します。
ステップ 3	**local-auth** *profile name* 例： `Device(config-remote-lan)# local-auth profile_name`	RLAN で EAP プロファイルを設定します。 *profile name*：RLAN 上の EAP プロファイルです。
ステップ 4	**mac-filtering** *mac-filter-name* 例： `Device(config-remote-lan)# mac-filtering mac_filter`	RLAN で MAC フィルタリング サポートを設定します。 *mac-filter-name*：許可リスト名です。
ステップ 5	**security dot1x authentication-list** *list-name* 例： `Device(config-remote-lan)# security dot1x authentication-list dot1_auth_list`	RLAN の 802.1X を設定します。 *list-name*：認証リスト名です。
ステップ 6	**security web-auth authentication-list** *list-name* 例：	RLAN の Web 認証を設定します。 *list-name*：認証リスト名です。

	コマンドまたはアクション	目的
	`Device(config-remote-lan)# security web-auth authentication-list web_auth_list`	（注） Web 認証リストまたは dot1x 認証リストを同時にアクティブにできます。
ステップ 7	**[no] shutdown** 例： `Device(config-remote-lan)# shutdown`	RLANプロファイルを有効または無効にします。
ステップ 8	**end** 例： `Device(config-remote-lan)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。 （注） この項の設定は、RLAN プロファイルに必須ではありません。 中央スイッチング モードの場合は、中央スイッチングと中央 DHCP の両方を設定する必要があります。

RLAN ポリシー プロファイルの作成

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap remote-lan-policy policy-name** *profile name* 例： `Device(config)# ap remote-lan-policy policy-name rlan_policy_prof_name`	RLANポリシープロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。

RLAN ポリシー プロファイル パラメータの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Wireless]** > **[Remote LAN]** を選択します。

ステップ 2 [Remote LAN] ページで [RLAN Policy] タブをクリックします。

ステップ 3 [RLAN Policy] ページで、[Policy] の名前をクリックするか、[Add] をクリックして新しいポリシーを作成します。

[Add/Edit RLAN Policy] ウィンドウが表示されます。

ステップ 4 [General] タブで次の手順を実行します。

a) ポリシー プロファイルの [Name] と [Description] を入力します。
b) [Central Authentication] を [Enabled] 状態に設定します。
c) [Central DHCP] を [Enabled] 状態に設定します。
d) [PoE] チェック ボックスを有効または無効の状態に設定します。
e) ポリシーを有効にするには、ステータスを [Enable] に設定します。

ステップ 5 [Access Policies] タブで、[VLAN] ドロップダウンリストから VLAN 名または番号を選択します。

ステップ 6 [Host Mode] ドロップダウンリストで、次のオプションからリモート LAN 802.1x の [Host Mode] を選択します。

- [Single-Host Mode]：デフォルトのホスト モードです。このモードでは、スイッチ ポートは 1 つのホストだけを認証し、トラフィックを 1 つずつ通過させます。
- [Multi-Host Mode]：最初に認証するデバイスがスイッチ ポートを開き、他のすべてのデバイスがそのポートを使用できます。他のデバイスを個別に認証する必要はありません。認証されたデバイスが承認済み状態になると、スイッチ ポートは閉じられます。
- [Multi-Domain Mode]：オーセンティケータは、データ ドメインの 1 つのホストと、音声ドメインの別のホストを許可します。これは、IP フォンが接続されているスイッチ ポートの一般的な設定です。

ステップ 7 IPv6 ACL または Flexible Netflow を設定します。

- **[Access Policies]** > **[Remote LAN ACL]** セクションで、ドロップダウンリストから [IPv6 ACL] を選択します。
- **[Access Policies]** > **[AVC]** > **[Flow Monitor IPv6]** セクションで、[Egress Status] と [Ingress Status] のチェック ボックスをオンにしてドロップダウンリストからポリシーを選択します。

ステップ 8 [Advanced] タブをクリックします。

a) [Violation Mode] ドロップダウンリストから、リモート LAN 802.1x の違反モードを設定し、次のオプションから違反モード タイプを選択します。

- [Shutdown]：ポートを無効にします。
- [Replace]：現在のセッションを削除し、新しいホストの認証を開始します。これはデフォルトの動作です。
- [Protect]：システム メッセージを生成せずに、予期しない MAC アドレスを使用するパケットをドロップします。

b) [Session Timeout (sec)] の値を入力して、クライアントのセッション期間を定義します。

範囲は 20 ～ 86400 秒です。

c) [AAA Policy Params] セクションで、[AAA Override] チェック ボックスをオンにして AAA オーバーライドを有効にします。

d) [Exclusionlist Params] セクションで、[Exclusionlist] チェック ボックスをオンにして [Exclusionlist Timeout] の値を入力します。

これにより、クライアントの除外時間が設定されます。範囲は 0 ～ 2147483647 秒です。0 はタイムアウトしないことを意味します。

ステップ 9 設定を保存します。

RLAN ポリシー プロファイル パラメータの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**central switching** 例： `Device(config-remote-lan-policy)# central switching`	中央スイッチングを設定します。
ステップ 2	**central dhcp** 例： `Device(config-remote-lan-policy)# central dhcp`	中央 DHCP を設定します。
ステップ 3	**exclusionlist timeout** *timeout* 例： `Device(config-remote-lan-policy)# exclusionlist timeout 200`	RLAN で除外リストを設定します。 *timeout*：クライアントが除外状態になるまでの時間を設定します。範囲は 0 ～ 2147483647 秒です。0 はタイムアウトしないことを意味します。
ステップ 4	**vlan** *vlan* 例：	VLAN 名または ID を設定します。 - *vlan*：VLAN 名です。

	コマンドまたはアクション	目的
	`Device(config-remote-lan-policy)# vlan vlan1`	
ステップ 5	例： `Device(config-remote-lan-policy)# ipv6 acl ipv6_acl`	
ステップ 6	**aaa-override** 例： `Device(config-remote-lan-policy)# aaa-override`	AAA ポリシーのオーバーライドを設定します。
ステップ 7	**session-timeout** *timeout in seconds* 例： `Device(config-remote-lan-policy)# session-timeout 21`	クライアントのセッション タイムアウトを設定します。 *timeout in seconds*：セッション期間を定義します。範囲は 20 ～ 86400 秒です。
ステップ 8	**host-mode** {**multidomain** *voice domain* | **multihost** |**singlehost**} 例： `Device(config-remote-lan-policy)# host-mode multidomain`	リモート LAN 802.1x のホスト モードを設定します。 *voice domain*：RLAN 音声ドメインの VLAN ID です。範囲は 0 ～ 65535 です。 次の IEEE 802.1X 認証モードを設定できます。 • [Multi-Domain Mode]：オーセンティケータは、データ ドメインの 1 つのホストと、音声ドメインの別のホストを許可します。これは、IP フォンが接続されているスイッチ ポートの一般的な設定です。 • [Multi-Host Mode]：最初に認証するデバイスがスイッチ ポートを開き、他のすべてのデバイスがそのポートを使用できます。他のデバイスを個別に認証する必要はありません。認証されたデバイスが承認済み状態になると、スイッチ ポートは閉じられます。 • [Single-Host Mode]：デフォルトのホスト モードです。このモードでは、スイッチ ポートは 1 つのホス

	コマンドまたはアクション	目的
		トだけを認証し、トラフィックを 1 つずつ通過させます。
ステップ 9	**violation-mode** {**protect** | **replace** | **shutdown**} 例： `Device(config-remote-lan-policy)# violation-mode protect`	リモート LAN 802.1x の違反モードを設定します。 セキュリティ違反が発生すると、ポートは、次のような設定済みの違反アクションに基づいて保護されます。 • [Shutdown]：ポートを無効にします。 • [Replace]：現在のセッションを削除し、新しいホストの認証を開始します。これはデフォルトの動作です。 • [Protect]：システム メッセージを生成せずに、予期しない MAC アドレスを使用するパケットをドロップします。シングルホスト認証モードでは、データ VLAN で複数のデバイスが検出された場合に違反がトリガーされます。マルチホスト認証モードでは、データ VLAN または音声 VLAN で複数のデバイスが検出された場合に違反がトリガーされます。
ステップ 10	[**no**] **poe** 例： `Device(config-remote-lan-policy)# poe`	PoE を有効または無効にします。
ステップ 11	[**no**] **shutdown** 例： `Device(config-remote-lan-policy)# shutdown`	RLAN ポリシー プロファイルを有効または無効にします。
ステップ 12	**end** 例： `Device(config-remote-lan-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ポリシー タグの設定と RLAN ポリシー プロファイルの RLAN プロファイルへのマッピング

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy remote-lan-policy-tag`	ポリシー タグを設定し、ポリシー タグ コンフィギュレーション モードを開始します。
ステップ 3	**remote-lan** *remote-lan-profile-name* **policy** *rlan-policy-profile-name* **port-id** *port-id* 例： `Device(config-policy-tag)# remote-lan rlan_profile_name policy rlan_policy_profile port-id 2`	RLAN ポリシー プロファイルを RLAN プロファイルにマッピングします。 • *remote-lan-profile-name*：RLAN プロファイルの名前です。 • *rlan-policy-profile-name*：ポリシー プロファイルの名前です。 • *port-id*：アクセス ポイントの LAN ポート番号です。指定できる値の範囲は 1 ～ 4 です。
ステップ 4	**end** 例： `Device(config-policy-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

LAN ポートの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**ap name** *ap name* **lan port-id** *lan port id* {**disable** | **enable**} 例： `Device# ap name L2_1810w_2 lan port-id 1 enable`	LAN ポートを設定します。 • enable：LAN ポートを有効にします。

	コマンドまたはアクション	目的
		• disable：LAN ポートを無効にします。

アクセス ポイントへのポリシー タグの付加（GUI）

手順

ステップ 1 [Configuration] > [Wireless] > [Access Points] の順に選択します。

ステップ 2 ポリシー タグを付加する AP を選択します。

ステップ 3 [Tags] セクションで、[Policy] ドロップダウンを使用してポリシー タグを選択します。

ステップ 4 [Update & Apply to Device] をクリックします。

アクセス ポイントへのポリシー タグの付加（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap** *ap-ethernet-mac* 例： `Device(config)# ap 00a2.891c.21e0`	AP のマップ アドレスを設定し、AP コンフィギュレーション モードを開始します。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device(config-ap-tag)# policy-tag remote-lan-policy-tag`	アクセス ポイントにポリシータグを付加します。 *policy-tag-name*：以前に定義したポリシー タグの名前です。
ステップ 4	**end** 例： `Device(config-ap-tag)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

RLAN 設定の確認

すべての RLAN の概要を表示するには、次のコマンドを使用します。

```
Device# show remote-lan summary

Number of RLANs: 1

RLAN        Profile Name                      Status
------------------------------------------------------------------
1            rlan_test_1                       Enabled
```

ID 別に RLAN 設定を表示するには、次のコマンドを使用します。

```
Device# show remote-lan id <id>

Remote-LAN Profile Name              : rlan_test_1
=================================================
Identifier                                  : 1
Status                                      : Enabled
Mac-filtering                               : Not Configured
Number of Active Clients                    : 1
Security_8021X                              : Disabled
8021.x Authentication list name             : Not Configured
Local Auth eap Profile Name                 : Not Configured
Web Auth Security                           : Disabled
Webauth Authentication list name            : Not Configured
Web Auth Parameter Map                      : Not Configured
Client association limit                    : 0
Ipv4 Web Pre Auth Acl                       : Not Configured
Ipv6 Web Pre Auth Acl                       : Not Configured
```

プロファイル名別に RLAN 設定を表示するには、次のコマンドを使用します。

```
Device# show remote-lan name <profile-name>

Remote-LAN Profile Name                     : rlan_test_1
=========================================================
Identifier                                  : 1
Status                                      : Enabled
Mac-filtering                               : Not Configured
Number of Active Clients                    : 1
Security_8021X                              : Disabled
8021.x Authentication list name             : Not Configured
Local Auth eap Profile Name                 : Not Configured
Web Auth Security                           : Disabled
Webauth Authentication list name            : Not Configured
Web Auth Parameter Map                      : Not Configured
Client association limit                    : 0
Ipv4 Web Pre Auth Acl                       : Not Configured
Ipv6 Web Pre Auth Acl                       : Not Configured
```

すべての RLAN の詳細な出力を表示するには、次のコマンドを使用します。

```
Device# show remote-lan all

Remote-LAN Profile Name            : rlan_test_1
================================================
Identifier                         : 1
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
```

```
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured

Remote-LAN Profile Name            : rlan_test_2
================================================
Identifier                         : 2
Status                             : Enabled
Mac-filtering                      : Not Configured
Number of Active Clients           : 1
Security_8021X                     : Disabled
8021.x Authentication list name    : Not Configured
Local Auth eap Profile Name        : Not Configured
Web Auth Security                  : Disabled
Webauth Authentication list name   : Not Configured
Web Auth Parameter Map             : Not Configured
Client association limit           : 0
Ipv4 Web Pre Auth Acl              : Not Configured
Ipv6 Web Pre Auth Acl              : Not Configured
```

```
Device# show remote-lan policy summary
Number of Policy Profiles: 1

Profile Name                      Description                              Status

-------------------------------------------------------------------------------------------
rlan_named_pp1                Testing RLAN policy profile              Enabled
```

Cisco AP の LAN ポート設定を表示するには、次のコマンドを使用します。

```
Device# show ap name <ap_name> lan port summary
LAN Port status for AP L2_1815w_1
Port ID      status       vlanId      poe
---------------------------------------------
LAN1         Enabled       20          Disabled
LAN2         Enabled       20          NA
LAN3         Disabled      0           NA
```

すべてのクライアントの概要を表示するには、次のコマンドを使用します。

```
Device# show wireless client summary
Number of Local Clients: 1

MAC Address       AP Name         WLAN         State    Protocol    Method     Role
-------------------------------------------------------------------------------------------
d8eb.97b6.fcc6    L2_1815w_1      1            * Run     Ethernet    None      Local
```

ユーザ名を指定してクライアントの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless client username cisco
MAC Address        AP Name          Status      WLAN      Auth Protocol
-------------------------------------------------------------------------------------------
0014.d1da.a977    L2_1815w_1        Run 1 *      Yes        Ethernet
d8eb.97b6.fcc6    L2_1815w_1        Run 1 *      Yes        Ethernet
```

MAC アドレス別にクライアントの詳細情報を表示するには、次のコマンドを使用します。

```
Device# show wireless client mac-address <mac_address> detail
Client MAC Address : d8eb.97b6.fcc6
Client IPv4 Address : 9.2.20.78
Client IPv6 Addresses : fe80::1863:292f:feaa:2cf
```

```
Client Username: N/A
AP MAC Address : 707d.b99e.c2e0
AP Name: L2_1815w_1
AP slot : 2
Client State : Associated
Policy Profile : rlan_named_pp1
Flex Profile : rlan-flex-profile
Remote LAN Id : 1
Remote LAN Name: rlan_test_1
BSSID : 707d.b99e.c2e1
Connected For : 1159 seconds
Protocol : Ethernet
Channel : 0
Port ID: 2
Client IIF-ID : 0xa0000001
Association Id : 1
Authentication Algorithm : Open System
Client CCX version : No CCX support
Session Timeout : 1800 sec (Remaining time: 641 sec)
Input Policy Name  : None
Input Policy State : None
Input Policy Source : None
Output Policy Name  : None
Output Policy State : None
Output Policy Source : None
WMM Support : Disabled
Fastlane Support : Disabled
Power Save : OFF
Current Rate : 0.0
Mobility:
  Move Count                  : 0
  Mobility Role               : Local
  Mobility Roam Type          : None
  Mobility Complete Timestamp : 07/06/2018 11:25:26 IST
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 1159 seconds
Policy Type : N/A
Encryption Cipher : None
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : No
EAP Type : Not Applicable
VLAN : 20
Access VLAN : 20
Anchor VLAN : 0
WFD capable : No
Managed WFD capable : No
Cross Connection capable : No
Support Concurrent Operation : No
Session Manager:
  Interface        : capwap_90000008
  IIF ID           : 0x90000008
  Authorized       : TRUE
  Session timeout  : 1800
  Common Session ID: 32130209000000136C48A29D
  Acct Session ID  : 0x00000000
  Aaa Server Details
  Server IP        :
  Auth Method Status List
   Method : None
  Local Policies:
   Service Template : wlan_svc_rlan_named_pp1_local (priority 254)
```

```
    Absolute-Timer   : 1800
    VLAN             : 20
  Server Policies:
  Resultant Policies:
    VLAN             : 20
    Absolute-Timer   : 1800
DNS Snooped IPv4 Addresses : None
DNS Snooped IPv6 Addresses : None
Client Capabilities
  CF Pollable : Not implemented
  CF Poll Request : Not implemented
  Short Preamble : Not implemented
  PBCC : Not implemented
  Channel Agility : Not implemented
  Listen Interval : 0
Fast BSS Transition Details :
  Reassociation Timeout : 0
11v BSS Transition : Not implemented
FlexConnect Data Switching : Central
FlexConnect Dhcp Status : Central
FlexConnect Authentication : Central
FlexConnect Central Association : No
Client Statistics:
  Number of Bytes Received : 6855
  Number of Bytes Sent : 1640
  Number of Packets Received : 105
  Number of Packets Sent : 27
  Number of Policy Errors : 0
  Radio Signal Strength Indicator : 0 dBm
  Signal to Noise Ratio : 0 dB
Fabric status : Disabled
Client Scan Reports
Assisted Roaming Neighbor List
```

すべての AP タグの概要を表示するには、次のコマンドを使用します。

```
Device# show ap tag summary
Number of APs: 2

AP Name             AP Mac               Site Tag Name         Policy Tag Name
RF Tag Name              Misconfigured     Tag Source
------------------------------------------------------------------------------------------
L2_1810d_1        0008.3296.24c0       default-site-tag        default-policy-tag
  default-rf-tag             No              Default
L2_1810w_2        00b0.e18c.5880       rlan-site-tag              rlan_pt_1
  default-rf-tag             No              Static
```

すべてのポリシー タグの概要を表示するには、次のコマンドを使用します。

```
Device# show wireless tag policy summary
Number of Policy Tags: 2

Policy Tag Name                  Description
------------------------------------------------------------------------
rlan_pt_1
default-policy-tag               default policy-tag
```

特定のポリシー タグの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless tag policy detailed <rlan_policy_tag_name>
Policy Tag Name : rlan_pt_1
Description     :

Number of WLAN-POLICY maps: 0
```

```
Number of RLAN-POLICY maps: 2
REMOTE-LAN Profile Name           Policy Name                              Port Id

-------------------------------------------------------------------------------------------
rlan_test_1                       rlan_named_pp1                             1

rlan_test_1                       rlan_named_pp1                             2
```

第 101 章

ネットワーク アクセス サーバ識別子

ネットワーク アクセス サーバ識別子について

ネットワーク アクセス サーバ識別子（NAS-ID）は、送信元に RADIUS アクセス要求を通知するために使用されます。これにより、RADIUS サーバはその要求のポリシーを選択できます。各 WLAN プロファイル、VLAN インターフェイス、またはアクセス ポイント グループで設定できます。NAS-ID は、ユーザをさまざまなグループに分類する認証要求を使用してコントローラによって RADIUS サーバに送信されます。これにより、RADIUS サーバはカスタマイズした認証応答を送信できるようになります。

AP グループに対して NAS-ID を設定すると、WLAN プロファイルまたは VLAN インターフェイスに対して設定されている NAS-ID がオーバーライドされます。同様に、WLAN プロファイルに対して NAS-ID を設定すると、VLAN インターフェイスに対して設定されている NAS-ID がオーバーライドされます。

NAS ID には、次のオプションを設定できます。

- sys-name（システム名）
- sys-ip（システム IP アドレス）
- sys-mac（システム MAC アドレス）
- ap-ip（AP の IP アドレス）
- ap-name（AP の名前）
- ap-mac（AP の MAC アドレス）
- ap-eth-mac（AP のイーサネット MAC アドレス）

- ap-policy-tag（AP のポリシー タグ名）
- ap-site-tag（AP のサイト タグ名）
- ssid（SSID 名）
- ap-location（AP の場所）

NAS ID ポリシーの作成（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Wireless AAA Policy]** の順に選択します。

ステップ 2 [Wireless AAA Policy] ページで、[Policy] の名前をクリックするか、[Add] をクリックして新しいポリシーを作成します。

ステップ 3 表示される [Add/Edit Wireless AAA Policy] ウィンドウで、[Policy Name] フィールドにポリシーの名前を入力します。

ステップ 4 [Option 1] ドロップダウンリストから、いずれかの NAS ID オプションを選択します。

ステップ 5 [Option 2] ドロップダウンリストから、いずれかの NAS ID オプションを選択します。

ステップ 6 [Option 3] ドロップダウンリストから、いずれかの NAS ID オプションを選択します。

ステップ 7 設定を保存します。

NAS ID ポリシーの作成

NAS ID ポリシーを作成するには、次の手順に従います。

始める前に

- NAS ID には、複数の NAS ID オプションの組み合わせ（3 個まで）を使用できます。
- NAS ID 属性の最大長は 253 です。新しい属性を追加する前に属性バッファがチェックされ、十分なスペースがない場合は新しい属性が無視されます。
- デフォルトでは、ワイヤレス AAA ポリシー default-aaa-policy がデフォルト設定（sys-name）で作成されます。このポリシーをさまざまな NAS ID オプションを使用して更新できます。ただし、default-aaa-policy を削除することはできません。
- NAS ID が設定されていない場合、デフォルトの sys-name が、コントローラから送信されるすべてのワイヤレス固有 RADIUS パケット（認証およびアカウンティング）の NAS ID と見なされます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless aaa policy** *policy-name* 例： `Device(config)# wireless aaa policy test`	新しい AAA ポリシーを設定します。
ステップ 3	**nas-id option1 sys-name** 例： `Device(config-aaa-policy)# nas-id option1 sys-name`	option1 の NAS ID を設定します。
ステップ 4	**nas-id option2 sys-ip** 例： `Device(config-aaa-policy)# nas-id option2 sys-ip`	option2 の NAS ID を設定します。
ステップ 5	**nas-id option3 sys-mac** 例： `Device(config-aaa-policy)# nas-id option3 sys-mac`	option3 の NAS ID を設定します。

タグへのポリシーの付加（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Tags] ページを選択し、[Policy] タブをクリックします。

ステップ 2 [Add] をクリックして、[Add Policy Tag] ウィンドウを表示します。

ステップ 3 ポリシー タグの名前と説明を入力します。

ステップ 4 [Add] をクリックして、WLAN プロファイルとポリシー プロファイルをマッピングします。

ステップ 5 適切な [Policy Profile] を使用してマッピングする [WLAN Profile] を選択し 、チェック アイコンをクリックします。

ステップ 6 [Save & Apply to Device] をクリックします。

タグへのポリシーの適用（CLI）

NAS ID ポリシーをタグに適用するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-name* 例： `Device(config)# wireless profile policy test1`	WLAN ポリシー プロファイルを設定します。
ステップ 3	**aaa-policy** *aaa-policy-name* 例： `Device(config-wireless-policy)# aaa-policy policy-aaa`	AAA ポリシー プロファイルを設定します。
ステップ 4	**exit** 例： `Device(config-wireless-policy)# exit`	グローバル コンフィギュレーション モードに戻ります。
ステップ 5	**wireless tag policy** *policy-tag* 例： `Device(config)# wireless tag policy policy-tag1`	ワイヤレス ポリシー タグを設定します。
ステップ 6	**wlan wlan1 policy** *policy-name* 例： `Device(config)# wlan wlan1 policy test1`	WLAN プロファイルをポリシー プロファイルにマッピングします。 （注） **ap-tag** オプションを使用して AP グループに NAS-ID を設定することもできます。この場合、WLAN プロファイルまたは VLAN インターフェイスに対して設定されている NAS ID がオーバーライドされます。

NAS ID 設定の確認

NAS ID 設定を確認するには、次の **show** コマンドを使用します。

```
Device# show wireless profile policy detailed test1

Policy Profile Name           : test1
Description                   :
Status                        : ENABLED
VLAN                          : 1
Client count                  : 0

:
:
AAA Policy Params
  AAA Override                : DISABLED
  NAC                         : DISABLED
  AAA Policy name             : test
```

第 102 章

WLAN の DHCP

Dynamic Host Configuration Protocol について

WLAN では、同じ Dynamic Host Configuration Protocol（DHCP）サーバまたは異なる DHCP サーバを使用するか、または DHCP サーバを使用しないように設定できます。DHCP サーバには、内部 DHCP サーバと外部 DHCP サーバの 2 つのタイプがあります。

内部 DHCP サーバ

devicesは、内部 DHCP サーバを持っています。このサーバは、一般的に、DHCP サーバを持たないブランチ オフィスで使用されます。通常、ワイヤレス ネットワークにはdeviceと同じ IP サブネット上にある AP が最大で 10 台含まれます。内部サーバは、ワイヤレス クライアント、ダイレクトコネクト AP、および AP からリレーされる DHCP 要求に対して DHCP アドレスを提供します。Lightweight アクセス ポイントのみサポートされています。内部 DHCP サーバを使用する場合は、deviceの管理インターフェイスの IP アドレスを DHCP サーバの IP アドレスとして設定する必要があります。

内部サーバでは、DHCP オプション 43 はサポートされていません。したがって、アクセス ポイントは、ローカル サブネット ブロードキャスト、ドメイン ネーム システム（DNS）、またはプライミングなどの別の方法を使用してdeviceの管理インターフェイスの IP アドレスを見つける必要があります。

内部 DHCP サーバ プールは、そのdeviceの無線クライアントだけをサポートし、他のdevicesのクライアントはサポートしません。また、内部 DHCP サーバは、無線クライアントだけをサポートし、有線クライアントをサポートしません。

クライアントがdeviceの内部 DHCP サーバを使用する場合、IP アドレスは、再起動後には保持されません。その結果、複数のクライアントに同じ IP アドレスが割り当てられることがあり

ます。IP アドレスの競合を解決するには、クライアントは既存の IP アドレスを解放し、新しいアドレスを要求する必要があります。有線ゲストクライアントは常に、ローカルまたは外部 deviceに接続されたレイヤ 2 ネットワークにあります。

（注）
- VRF は内部 DHCP サーバではサポートされません。
- DHCPv6 は内部 DHCP サーバではサポートされません。

一般的な注意事項

- 内部 DHCP サーバはワイヤレス クライアントと有線クライアントの両方にサービスを提供します（有線クライアントには AP が含まれます）。
- 内部 DHCP サーバでワイヤレス クライアントにサービスを提供するには、そのワイヤレス クライアントのユニキャスト DHCP サーバの IP アドレスを設定する必要があります。内部 DHCP サーバの IP アドレスは、インターフェイス（ループバック インターフェイス、SVI インターフェイス、または L3 物理インターフェイス）に面しているサーバで設定する必要があります。
- ワイヤレスおよび有線クライアント VLAN の両方で内部 DHCP サーバを使用するには、クライアント VLAN SVI インターフェイスで IP アドレスを設定する必要があります。
- ワイヤレス クライアントの場合、DHCP ヘルパー アドレス設定では、内部 DHCP サーバの IP アドレスとワイヤレス クライアント VLAN SVI インターフェイスのアドレスは異なっている必要があります。
- 内部DHCPサーバのサポートがあるワイヤレスクライアントの場合、クライアントVLAN SVI インターフェイスまたはワイヤレス ポリシー プロファイルで、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内部 DHCP サーバを設定できます。
- 内部 DHCP サーバ プールは、その他のコントローラのクライアントにもサービスを提供できます。

外部 DHCP サーバ

オペレーティング システムは、DHCP リレーをサポートする業界標準の外部 DHCP サーバを使用することにより、ネットワークに対してはDHCPリレーとして機能し、クライアントに対してはDHCPサーバとして機能するように設計されています。これは、各deviceは、DHCP サーバに対しては DHCP リレー エージェントとして機能し、無線クライアントに対しては仮想 IP アドレスでの DHCP サーバとして機能することを意味します。

deviceは DHCP サーバから取得したクライアント IP アドレスをキャプチャするため、device 内、device間、およびサブネット間でのクライアント ローミング時に、各クライアントに対して同じ IP アドレスが保持されます。

（注） 外部 DHCP サーバは DHCPv6 をサポートします。

DHCP 割り当て

DHCP はインターフェイスごとに、または WLAN ごとに設定できます。特定のインターフェイスに割り当てられたプライマリ DHCP サーバのアドレスを使用することをお勧めします。

個々のインターフェイスにDHCPサーバを割り当てることができます。プライマリおよびセカンダリ DHCP サーバの管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスの設定、DHCPサーバをイネーブルまたはディセーブルするためのサービス ポート インターフェイスの設定を行うことができます。WLAN で DHCP サーバを定義することもできます。この場合、サーバは、WLAN に割り当てられたインターフェイスの DHCP サーバアドレスを上書きします。

セキュリティに関する注意事項

高度なセキュリティが必要な場合は、すべてのクライアントが DHCP サーバから IP アドレスを取得するように設定してください。この要件を適用するために、DHCPアドレスですべての WLAN を設定できます。Assignment Required 設定で設定して、クライアントの固定 IP アドレスが禁止されるようにします。DHCP Addr. Assignment Required が選択されている場合、クライアントはDHCP を使って IP アドレスを取得する必要があります。固定 IP アドレスを持つクライアントはすべて、ネットワーク上で許可されなくなります。クライアントのDHCPプロキシとして動作するdeviceが、DHCP トラフィックを監視します。

（注）
- 無線による管理をサポートする WLAN では、管理（デバイスサービシング）クライアントが DHCP サーバから IP アドレスを取得できるようにする必要があります。

セキュリティが多少劣ってもかまわない場合は、DHCP Addr. Assignment Required を無効に設定して WLAN を作成できます。その後クライアントは、固定 IP アドレスを使用するか、指定された DHCP サーバの IP アドレスを取得するかを選択できます。

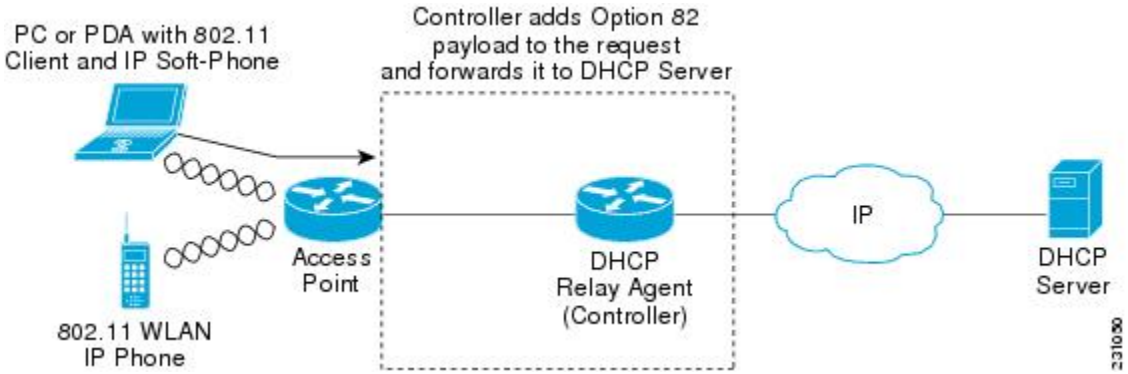
（注） DHCP アドレス有線ゲスト LAN に対する Assignment Required は、サポートされていません。

個別の WLAN は、[DHCP Address Assignment Required] を無効にして作成できます。これは、deviceの DHCP プロキシがイネーブルの場合だけです。DHCP プロキシをディセーブルにする必要があるプライマリ/セカンダリ コンフィギュレーションの DHCP サーバを定義しないでください。このような WLAN では、すべての DHCP 要求がドロップするため、クライアントは固定 IP アドレスを使用しなければなりません。これらの WLAN は、無線接続による管理をサポートしていません。

DHCP オプション 82 について

DHCP オプション 82 では、DHCP を使用してネットワーク アドレスを割り当てる場合のセキュリティが強化されます。deviceが DHCP リレー エージェントとして動作して、信頼できないソースからの DHCP クライアント要求を阻止できるようにします。DHCP サーバに転送するようにクライアントからの DHCP 要求にオプション 82 情報を追加するようにdeviceを設定できます。

図 *27 : DHCP* オプション *82*



アクセス ポイントは、クライアントからのすべての DHCP 要求をdeviceに転送します。deviceは、DHCP オプション 82 ペイロードを追加してから要求を DHCP サーバに転送します。このオプションの設定方法によって、ペイロードには MAC アドレス、または MAC アドレスとアクセス ポイントの SSID が含まれます。

（注） すでにリレー エージェント オプションが含まれている DHCP パケットは、deviceでドロップされます。

DHCP オプション 82 が正しく動作するには、DHCP プロキシが有効でなければなりません。

DHCP スコープの設定

内部 DHCP サーバに関する情報

Devicesには組み込みの DHCP リレー エージェントがあります。ただし、別個の DHCP サーバを持たないネットワーク セグメントが必要な場合、devicesに、IP アドレスとサブネット マスクを無線クライアントに割り当てる組み込みの内部 DHCP サーバを設定できます。一般に、1つのdeviceには、それぞれある範囲の IP アドレスを指定する 1 つ以上の内部 DHCP サーバを設定できます。

内部 DHCP サーバは内部 DHCP が機能するために必要となります。deviceで DHCP が定義されると、管理インターフェイス、AP マネージャ インターフェイス、動的インターフェイスのプライマリ DHCP サーバの IP アドレスをdeviceの管理インターフェイスにポイントすることができます。

（注） コントローラには、内部 DHCP サーバを提供する機能があります。この機能は非常に限定的で、多くの場合はラボ環境などでの単純なデモンストレーションや概念実証に有用であると見なされています。企業の実稼動ネットワークではこの機能を使用しないことを推奨します。

詳細については、以下を参照してください。 http://www.cisco.com/c/en/us/support/docs/wireless/4400-series-wireless-lan-controllers/110865-dhcp-wlc.html#anc16

DHCP for WLANs を設定するための前提条件

- DHCP オプション 82 を使用するには、Cisco IOS ソフトウェアで DHCP を設定します。デフォルトでは、DHCP オプション 82 は、すべてのクライアントに対してイネーブルにされます。WLAN サブオプションを使用して無線クライアントの動作を制御できます。
- 大規模なエンタープライズクラスのネットワークを構築する一般的な導入ガイドラインとして、外部 DHCP サーバを使用してワイヤレス クライアントにダイナミック IP アドレスを提供することをお勧めします。このような分散機能は、ネットワーク デバイスにかかる処理および設定の負荷を低減し、大規模環境で効率的に動作させることができます。
- DHCP スヌーピング設定：DHCP スヌーピング設定は、の迅速なクライアント接続機能に必要なベスト プラクティス設定です。DHCP スヌーピングは各クライアント VLAN 上で有効にする必要があります。WLAN でオーバーライドが適用される場合は、オーバライド VLAN も対象となります。

DHCP スヌーピング設定の例

1. グローバル DHCP スヌーピングの設定：
   1. `Device(config)#ip dhcp snooping`

      `Device(config)#ip dhcp snooping vlan 100`
   2. `Bootp-broadcast` コマンドを有効にします。これは、ブロードキャスト アドレスを使用して DHCP メッセージを送信するクライアントに必要で、ブロードキャスト ビットが DHCP メッセージに設定されます。

      `Device(config)#ip dhcp snooping wireless bootp-broadcast enable`
   3. DHCP オプション情報を付加しないためには、次のコマンドを入力します。

      `Device(config)#no ip dhcp snooping information option`
2. インターフェイス上で、次のように設定します。

（注） IP DHCP snooping trust は、ポート チャネル インターフェイスのメンバ リンクおよびポート チャネル インターフェイスで必要です。

```
Device(config)#interface range TenGigabitEthernet 1/0/1 - 2
Device(config-if)#switchport mode trunk
Device(config-if)#switchport trunk allowed vlan 100
Device(config-if)#ip dhcp snooping trust

Device(config)#interface port-channel 1
Device(config-if)#switchport mode trunk
Device(config-if)#switchport trunk allowed vlan 100
Device(config-if)#ip dhcp snooping trust
```

（注） DHCP スヌーピングは、上記の設定と同様に、ゲスト アクセス用のゲスト アンカーで設定する必要があります。

DHCP for WLANs の設定に関する制約事項

- WLAN で DHCP サーバをオーバーライドすると、DHCP サーバが到達可能であることを確認するために、基盤となる Cisco IOS 設定を行う必要があります。
- DHCP WLAN オーバーライドは DHCP サービスがdevice上で有効な場合にだけ動作します。

  次のいずれかの方法で、DHCP サービスを設定できます。

  - deviceで DHCP プールを設定します。
  - SVI で DHCP リレー エージェントを設定します。注: SVI の VLAN は DHCP のオーバーライドが設定された WLAN にマッピングする必要があります。

DHCP for WLANs の設定方法

WLAN の DHCP の設定（GUI）

手順

ステップ 1 [Configuration] > [Tags & Profiles] > [Policy] を選択します。

ステップ 2 [General] タブで [Multicast Direct Enable] チェック ボックスをオンにします。

ステップ 3 [Policy Profile Name] を選択して、[Edit Policy Profile] ウィンドウをアクティブにします。
ステップ 4 [Advanced] タブをクリックします。
ステップ 5 [DHCP] セクションで、[IPv4 DHCP Required] チェックボックスをオンにします。
ステップ 6 [DHCP Server IP Address] フィールドに、DHCP サーバの IP アドレスを入力します。
ステップ 7 [Update & Apply to Device] をクリックします。

WLAN 用の DHCP 設定（CLI）

WLAN で次の DHCP パラメータを設定するには、次の手順に従います。

- DHCP オプション 82 ペイロード
- DHCP（必須）
- DHCP オーバーライド

始める前に

- WLAN を設定するには admin 権限がなければなりません。
- DHCP のオーバーライドを設定するには、DHCP サーバの IP アドレスが必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**shutdown** 例： `Device(config)# shutdown`	WLAN をシャットダウンします。
ステップ 3	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 4	**ip dhcp opt82** {**ascii** | **format** {*add-ssid* | *ap-ethmac*} | **rid**} 例： `Device(config)# ip dhcp opt82 format add-ssid`	WLAN で DHCP82 ペイロードを指定します。キーワードおよび引数は、次のとおりです。 • **ascii**：DHCP オプション 82 の ASCII を設定します。これが設定されてい

	コマンドまたはアクション	目的
		ない場合、オプション 82 の形式は ASCII 形式に設定されます。 • **format**：DHCP オプション 82 の形式を指定します。次のオプションを使用できます。 • *add-ssid*：AP 無線の MAC アドレスおよび SSID である RemoteID 形式を設定します。 • *ap-ethmac*：AP Ethernet MAC アドレスである RemoteID 形式を設定します。 （注） フォーマット オプションが設定されていない場合、AP 無線の MAC アドレスだけが使用されます。 • **rid**：DHCP オプション 82 に Cisco 2 バイト RID を追加します。
ステップ 5	**ip dhcp required** 例： `Device(config-wlan)# ip dhcp required`	DHCP サーバから IP アドレスをクライアントが取得することを必須にします。スタティック クライアントは許可されません。
ステップ 6	**ip dhcp server** *ip-address* 例： `Device(config-wlan)# ip dhcp server 200.1.1.2`	WLAN に割り当てられたインターフェイスの DHCP サーバ アドレスを上書きする WLAN 上の DHCP サーバを定義します。
ステップ 7	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN を再起動します。
ステップ 8	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 9	**show wlan** *wlan-name* 例：	DHCP の設定を確認します。

	コマンドまたはアクション	目的
	`Device(config-wlan)# show wlan test-wlan`	

DHCP スコープの設定（GUI）

手順

ステップ 1 [Administration] > [DHCP Pools] を選択します。

ステップ 2 [Pools] セクションで、[Add] をクリックして新しい DHCP プールを追加します。[Create DHCP Pool] ダイアログボックスが表示されます。

ステップ 3 [DHCP Pool Name] フィールドに、新しい DHCP プールの名前を入力します。

ステップ 4 [IP Type] ドロップダウンリストから、IP アドレス タイプとして [IPv4] または [IPv6] を選択します。

ステップ 5 [Network] フィールドに、この DHCP スコープの対象となるネットワークを入力します。この IP アドレスは、[Interfaces] ページで設定されている、ネットマスクが適用された管理インターフェイスによって使用されます。

ステップ 6 [Subnet Mask] フィールドに、すべての無線クライアントに割り当てられるサブネット マスクを入力します。

ステップ 7 [Starting ip] フィールドに、開始 IP アドレスを入力します。

ステップ 8 [Ending ip] フィールドに、最後の IP アドレスを入力します。

ステップ 9 [Reserved Only] で [enabled] または [disabled] を選択します。

ステップ 10 [Lease] ドロップダウンリストから、[User Defined] または [Never Expires] のいずれかのリース タイプを選択します。[User Defined] を選択した場合は、IP アドレスがクライアントに付与される期間を入力できます。

ステップ 11 DHCP スコープの詳細設定を行うには、[Advanced] をクリックして次のタスクを実行します。

ステップ 12 [Enable DNS Proxy] チェック ボックスをオンにして、DNS プロキシを有効にします。

ステップ 13 [Default Router(s)] フィールドに、デバイスに接続するオプションのルータ（複数可）の IP アドレスを入力し、[+] アイコンをクリックしてリストに追加します。各ルータには、1 台のデバイスで複数のデバイスのクライアントを処理できる DHCP フォワーディング エージェントを含める必要があります。

ステップ 14 [DNS Server(s)] フィールドにオプションの DNS サーバの IP アドレスを入力し、[+] アイコンをクリックしてリストに追加します。各 DNS サーバは、この DHCP スコープで割り当てられた IP アドレスと一致するように、クライアントの DNS エントリを更新できる必要があります。

ステップ 15 [NetBios Name Server(s)] フィールドにオプションの Microsoft NetBIOS ネーム サーバ（Microsoft Windows Internet Naming Service（WINS）サーバなど）の IP アドレスを入力し、[+] アイコンをクリックしてリストに追加します。

ステップ 16 [Domain] フィールドに、1 つまたは複数の DNS サーバで使用する、この DHCP スコープのオプションのドメイン ネームを入力します。

ステップ 17 [DHCP] オプションを追加するには、[DHCP Options List] セクションで [Add] をクリックします。DHCP は、設定パラメータなどの制御情報を DHCP オプションとしてネットワーク上のクライアントに渡すための内部フレームワークを提供します。DHCP オプションでは、DHCP サーバとそのクライアントの間でやり取りされるプロトコル メッセージ内に格納されたタグ付きデータとしてパラメータが伝送されます。

ステップ 18 追加する [DHCP] オプションを入力します。

ステップ 19 [Save & Apply to Device] をクリックします。

DHCP スコープの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ip dhcp pool** *pool-name* 例： `Device(config)#ip dhcp pool test-pool`	DHCP プール アドレスを設定します。
ステップ 3	**network** *network-name mask-address* 例： `Device(dhcp-config)#network 209.165.200.224 255.255.255.0`	ドット付き 10 進表記とマスク アドレスでネットワーク番号を指定します。
ステップ 4	**dns-server** *hostname* 例： `Device(dhcp-config)#dns-server example.com`	DNS ネーム サーバを指定します。IP アドレスまたはホスト名を指定できます。
ステップ 5	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

内部 DHCP サーバの設定

クライアント VLAN SVI での内部 DHCP サーバの設定

始める前に

- ワイヤレスおよび有線クライアント VLAN の両方で内部 DHCP サーバを使用するには、クライアント VLAN スイッチ仮想インターフェイス（SVI）で IP アドレスを設定する必要があります。
- ワイヤレス クライアントの場合、内部 DHCP サーバの IP アドレスとワイヤレス クライアント VLAN SVI インターフェイスのアドレスが異なっている必要があります（DHCP ヘルパー アドレス設定）。
- ワイヤレス クライアントの場合、クライアント VLAN SVI インターフェイスまたはワイヤレス ポリシー プロファイルで内部 DHCP サーバを設定できます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 loopback** *interface-number* 例： `Device(config)# interface Loopback0`	ループバック インターフェイスを作成し、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。
ステップ 3	**ip address** *ip-address* 例： `Device(config-if)# ip address 10.10.10.1 255.255.255.255`	インターフェイスの IP アドレスを設定します。
ステップ 4	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 32`	VLAN ID を設定します。
ステップ 6	**ip address** *ip-address* 例：	インターフェイスの IP アドレスを設定します。

	コマンドまたはアクション	目的
	`Device(config-if)# ip address 192.168.32.100 255.255.255.0`	
ステップ 7	**ip helper-address** *ip-address* 例： `Device(config-if)# ip helper-address 10.10.10.1`	UDP ブロードキャストの宛先アドレスを設定します。 （注） **ip helper-address** コマンドで使用されている IP アドレスがコントローラの内部アドレスである場合は、内部 DHCP サーバが使用されます。内部アドレス以外の場合は、外部 DHCP サーバが使用されます。
ステップ 8	**no mop enabled** 例： `Device(config-if)# no mop enabled`	インターフェイスのメンテナンス オペレーション プロトコル（MOP）を無効にします。
ステップ 9	**no mop sysid** 例： `Device(config-if)# no mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。
ステップ 10	**end** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 11	**ip dhcp excluded-address** *ip-address* 例： `Device(config)# ip dhcp excluded-address 192.168.32.1`	DHCP サーバが DHCP クライアントに割り当てられない IP アドレスを指定します。
ステップ 12	**ip dhcp excluded-address** *ip-address* 例： `Device(config)# ip dhcp excluded-address 192.168.32.100`	DHCP サーバが DHCP クライアントに割り当てない IP アドレスを指定します。
ステップ 13	**ip dhcp pool** *pool-name* 例： `Device(config)# ip dhcp pool pool-vlan32`	DHCP プール アドレスを設定します。
ステップ 14	**network** *network-name mask-address* 例： `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	ドット付き 10 進表記のネットワーク番号とマスク アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 15	**default-router** *ip-address* 例： `Device(dhcp-config)# default-router 192.168.32.1`	DHCP クライアントのデフォルト ルータの IPアドレスを指定します。
ステップ 16	**exit** 例： `Device(dhcp-config)# exit`	DHCP コンフィギュレーション モードを終了します。
ステップ 17	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN ポリシー プロファイルを設定し、ワイヤレスポリシー コンフィギュレーション モードを開始します。
ステップ 18	**central association** 例： `Device(config-wireless-policy)# central association`	ローカルにスイッチされるクライアントの中央アソシエーションを設定します。
ステップ 19	**central dhcp** 例： `Device(config-wireless-policy)# central dhcp`	ローカルにスイッチされるクライアントの中央 DHCP を設定します。
ステップ 20	**central switching** 例： `Device(config-wireless-policy)# central switching`	WLANを中央スイッチング用に設定します。
ステップ 21	**description** *policy-proile-name* 例： `Device(config-wireless-policy)# description "default policy profile"`	ポリシープロファイルの説明を追加します。
ステップ 22	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 32`	プロファイル ポリシーを VLAN に割り当てます。
ステップ 23	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

ワイヤレス ポリシー プロファイルでの内部 DHCP サーバの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 loopback** *interface-number* 例： `Device(config)# interface Loopback0`	ループバック インターフェイスを作成し、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。
ステップ 3	**ip address** *ip-address* 例： `Device(config-if)# ip address 10.10.10.1 255.255.255.255`	インターフェイスの IP アドレスを設定します。
ステップ 4	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	**interface vlan** *vlan-id* 例： `Device(config)# interface vlan 32`	VLAN ID を設定します。
ステップ 6	**ip address** *ip-address* 例： `Device(config-if)# ip address 192.168.32.100 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 7	**no mop enabled** 例： `Device(config-if)# no mop enabled`	インターフェイスのメンテナンス オペレーション プロトコル（MOP）を無効にします。
ステップ 8	**no mop sysid** 例： `Device(config-if)# no mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**ip dhcp excluded-address** *ip-address* 例： `Device(config)# ip dhcp excluded-address 192.168.32.1`	DHCP サーバが DHCP クライアントに割り当てない IP アドレスを指定します。
ステップ 11	**ip dhcp excluded-address** *ip-address* 例： `Device(config)# ip dhcp excluded-address 192.168.32.100`	DHCP サーバが DHCP クライアントに割り当てられない IP アドレスを指定します。
ステップ 12	**ip dhcp pool** *pool-name* 例： `Device(config)# ip dhcp pool pool-vlan32`	DHCP プール アドレスを設定します。
ステップ 13	**network** *network-name mask-address* 例： `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	ドット付き 10 進表記のネットワーク番号とマスク アドレスを指定します。
ステップ 14	**default-router** *ip-address* 例： `Device(dhcp-config)# default-router 192.168.32.1`	DHCP クライアントのデフォルト ルータの IP アドレスを指定します。
ステップ 15	**exit** 例： `Device(dhcp-config)# exit`	DHCP コンフィギュレーション モードを終了します。
ステップ 16	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 17	**central association** 例： `Device(config-wireless-policy)# central association`	ローカルにスイッチされるクライアントの中央アソシエーションを設定します。
ステップ 18	**central switching** 例： `Device(config-wireless-policy)# central switching`	ローカル スイッチングを設定します。

	コマンドまたはアクション	目的
ステップ 19	**description** *policy-proile-name* 例： `Device(config-wireless-policy)# description "default policy profile"`	ポリシープロファイルの説明を追加します。
ステップ 20	**ipv4 dhcp opt82** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82`	ワイヤレス クライアントの DHCP オプション 82 を有効にします。
ステップ 21	**ipv4 dhcp opt82 ascii** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 ascii`	DHCP オプション 82 の ASCII を有効にします。
ステップ 22	**ipv4 dhcp opt82 format vlan_id** 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 format vlan32`	VLAN ID を有効にします。
ステップ 23	**ipv4 dhcp opt82 rid** *vlan_id* 例： `Device(config-wireless-policy)# ipv4 dhcp opt82 rid`	DHCP オプション 82 に対するシスコ 2 バイト リモート ID（RID）の追加をサポートします。
ステップ 24	**ipv4 dhcp server** *ip-address* 例： `Device(config-wireless-policy)#  ipv4 dhcp server 10.10.10.1`	WLAN の IPv4 DHCP サーバを設定します。
ステップ 25	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 32`	プロファイル ポリシーを VLAN に割り当てます。
ステップ 26	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイル ポリシーを有効にします。

内部 DHCP サーバのグローバル設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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 loopback** *interface-num* 例： `Device(config)# interface Loopback0`	ループバック インターフェイスを作成し、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。
ステップ 3	**ip address** *ip-address* 例： `Device(config-if)# ip address 10.10.10.1 255.255.255.255`	インターフェイスの IP アドレスを設定します。
ステップ 4	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	**interface vlan***vlan-id* 例： `Device(config)# interface vlan 32`	VLAN ID を設定します。
ステップ 6	**ip address** *ip-address* 例： `Device(config-if)# ip address 192.168.32.100 255.255.255.0`	インターフェイスの IP アドレスを設定します。
ステップ 7	**no mop enabled** 例： `Device(config-if)# no mop enabled`	インターフェイスのメンテナンス オペレーション プロトコル（MOP）を無効にします。
ステップ 8	**no mop sysid** 例： `Device(config-if)# no mop sysid`	MOP 定期システム ID メッセージを送信するタスクを無効にします。
ステップ 9	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 10	**ip dhcp-server** *ip-address* 例： `Device(config)# ip dhcp-server 10.10.10.1`	ターゲット DHCP サーバのパラメータを指定します。
ステップ 11	**ip dhcp excluded-address** *ip-address* 例： `Device(config)# ip dhcp excluded-address 192.168.32.1`	DHCP サーバが DHCP クライアントに割り当てられないIPアドレスを指定します。
ステップ 12	**ip dhcp excluded-address** *ip-address* 例： `Device(config)# ip dhcp excluded-address 192.168.32.100`	DHCP サーバが DHCP クライアントに割り当てられないIPアドレスを指定します。
ステップ 13	**ip dhcp pool** *pool-name* 例： `Device(config)# ip dhcp pool pool-vlan32`	DHCP プール アドレスを設定します。
ステップ 14	**network** *network-name mask-address* 例： `Device(dhcp-config)# network 192.168.32.0 255.255.255.0`	ドット付き10進表記のネットワーク番号とマスク アドレスを指定します。
ステップ 15	**default-router** *ip-address* 例： `Device(dhcp-config)# default-router 192.168.32.1`	DHCP クライアントのデフォルト ルータの IPアドレスを指定します。
ステップ 16	**exit** 例： `Device(dhcp-config)# exit`	DHCP コンフィギュレーション モードを終了します。
ステップ 17	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy default-policy-profile`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 18	**central association** 例： `Device(config-wireless-policy)# central association`	ローカルにスイッチされるクライアントの中央アソシエーションを設定します。

	コマンドまたはアクション	目的
ステップ 19	**central dhcp** 例： `Device(config-wireless-policy)# central dhcp`	ローカルにスイッチされるクライアントの中央 DHCP を設定します。
ステップ 20	**central switching** 例： `Device(config-wireless-policy)# central switching`	ローカルスイッチングを設定します。
ステップ 21	**description** *policy-proile-name* 例： `Device(config-wireless-policy)# description "default policy profile"`	ポリシープロファイルの説明を追加します。
ステップ 22	**vlan** *vlan-name* 例： `Device(config-wireless-policy)# vlan 32`	プロファイルポリシーを VLAN に割り当てます。
ステップ 23	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	プロファイルポリシーを有効にします。

内部 DHCP 設定の確認

クライアント バインディングを確認するには、次のコマンドを使用します。

```
Device# show ip dhcp binding

Bindings from all pools not associated with VRF:
IP address      Client-ID/              Lease expiration        Type       State
Interface
                Hardware address/
                User name
192.168.32.3    0130.b49e.491a.53       Mar 23 2018 06:42 PM    Automatic  Active
Loopback0
```

ワイヤレス クライアントの DHCP リレー統計情報を確認するには、次のコマンドを使用します。

```
Device# show wireless dhcp relay statistics

DHCP Relay Statistics
---------------------

DHCP Server IP :   10.10.10.1

Message              Count
```

```
--------------------------
DHCPDISCOVER      :  1
BOOTP FORWARD     :  137
BOOTP REPLY       :  0
DHCPOFFER         :  0
DHCPREQUEST       :  54
DHCPACK           :  0
DHCPNAK           :  0
DHCPDECLINE       :  0
DHCPRELEASE       :  0
DHCPINFORM        :  82

Tx/Rx Time :
------------
LastTxTime : 18:42:18
LastRxTime : 00:00:00

Drop Counter :
-------------
TxDropCount : 0
```

CPP の DHCP パケット パント統計情報を確認するには、次のコマンドを使用します。

```
Device# show platform hardware chassis active qfp feature wireless punt statistics

CPP Wireless Punt stats:

                                App Tag     Packet Count
                                -------     ------------
          CAPWAP_PKT_TYPE_DOT11_PROBE_REQ           14442
               CAPWAP_PKT_TYPE_DOT11_MGMT              50
               CAPWAP_PKT_TYPE_DOT11_IAPP            9447
               CAPWAP_PKT_TYPE_DOT11_RFID               0
                CAPWAP_PKT_TYPE_DOT11_RRM               0
              CAPWAP_PKT_TYPE_DOT11_DOT1X               0
        CAPWAP_PKT_TYPE_CAPWAP_KEEPALIVE            2191
     CAPWAP_PKT_TYPE_MOBILITY_KEEPALIVE               0
           CAPWAP_PKT_TYPE_CAPWAP_CNTRL            7034
            CAPWAP_PKT_TYPE_CAPWAP_DATA               0
         CAPWAP_PKT_TYPE_MOBILITY_CNTRL               0
                       WLS_SMD_WEBAUTH                0
                     SISF_PKT_TYPE_ARP             5292
                    SISF_PKT_TYPE_DHCP              140
                   SISF_PKT_TYPE_DHCP6             1213
                 SISF_PKT_TYPE_IPV6_ND              350
              SISF_PKT_TYPE_DATA_GLEAN               44
           SISF_PKT_TYPE_DATA_GLEAN_V6               51
              SISF_PKT_TYPE_DHCP_RELAY              122
          CAPWAP_PKT_TYPE_CAPWAP_RESERVED               0
```

第 103 章

WLAN セキュリティ

WPA1 および WPA2 について

Wi-Fi 保護アクセス（WPA または WPA1）および WPA2 は、無線 LAN システム用のデータ保護とアクセス コントロールを提供する Wi-Fi Alliance の規格ベースのセキュリティ ソリューションです。WPA1 は、IEEE 802.11i 規格に準拠していますが、規格の承認前に実装されたものです。これに対して、WPA2 は、承認された IEEE 802.11i 規格が Wi-Fi Alliance によって実装されています。

デフォルトで、WPA1 ではデータの保護に Temporal Key Integrity Protocol（TKIP）およびメッセージ整合性チェック（MIC）が使用されますが、WPA2 では Counter Mode with Cipher Block Chaining Message Authentication Code Protocol を使用したより強力な Advanced Encryption Standard 暗号化アルゴリズム（AES-CCMP）が使用されます。デフォルトでは、WPA1 および WPA2 のどちらも 802.1X を使用して認証キー管理を行います。ただし、次の方法も使用できます。

- 802.1X：IEEE によって定義された無線 LAN セキュリティの規格。802.1X for 802.11、または単に 802.1X と呼ばれます。802.1X をサポートするアクセス ポイントは、無線ネットワークを介して通信を行う相手となるワイヤレス クライアントと認証サーバ（RADIUS サーバなど）の間のインターフェイスとして機能します。[802.1X] が選択されている場合は、802.1X クライアントのみがサポートされます。802.1X は、Cisco 2700 シリーズの AP の AUX ポートではサポートされていません。
- PSK：PSK（WPA 事前共有キーまたは WPA パスフレーズとも呼ばれます）を選択した場合は、事前共有キー（またはパスフレーズ）を設定する必要があります。このキーは、クライアントと認証サーバの間でペアワイズ マスター キー（PMK）として使用されます。
- CCKM：Cisco Centralized Key Management（CCKM）では、迅速なキーの再生成技術を使用しています。この技術を使用すると、クライアントは、通常 150 ミリ秒（ms）以下で、コントローラを経由せずにあるアクセス ポイントから別のアクセス ポイントにローミン

グできます。CCKM により、クライアントが新しいアクセス ポイントと相互に認証を行い、再アソシエーション時に新しいセッション キーを取得するために必要な時間が短縮されます。CCKM の迅速かつ安全なローミングにより、ワイヤレス VoIP（Voice over IP）、エンタープライズ リソース プランニング（ERP）、Citrix ベースのソリューションなどの時間依存型アプリケーションで認識できるほどの遅延は発生しません。CCKMは、CCXv4に準拠する機能です。CCKMが選択されている場合は、CCKMクライアントのみがサポートされます。

CCKM を有効にすると、アクセス ポイントの動作は、高速ローミングのコントローラと次の点で異なります。

- クライアントから送信されるアソシエーション要求の Robust Secure Network Information Element（RSN IE）で CCKM が有効になっているものの、CCKM IE がエンコードされておらず、PMKID だけが RSN IE でエンコードされている場合、コントローラは完全な認証を行いません。代わりに、コントローラは PMKID を検証し、フォーウェイ ハンドシェイクをします。
- クライアントから送信されるアソシエーション要求の RSN IE で CCKM が有効になっているものの、CCKM IE がエンコードされておらず、PMKID だけが RSN IE でエンコードされている場合でも、AP は完全な認証を行います。CCKM が RSN IE で有効になっている場合、このアクセス ポイントではアソシエーション要求と一緒に送信される PMKID は使用されません。

- 802.1X+CCKM：通常の動作状態の間、802.1X が有効になっているクライアントは、主要な RADIUS サーバとの通信を含む完全な 802.1X 認証を実行することにより、新しいアクセス ポイントとの相互認証を行います。ただし、802.1X および CCKM の迅速で安全なローミング用に WLAN を設定した場合、CCKM が有効になっているクライアントは、RADIUS サーバに対して再認証せずに、あるアクセス ポイントから別のアクセス ポイントに安全にローミングを行います。このオプションが選択されている場合、CCKMクライアントと非CCKMクライアントの両方がサポートされるため、802.1X+CCKMはオプションの CCKM と見なされます。

単一の WLAN では、WPA1、WPA2、および 802.1X/PSK/CCKM/802.1X+CCKM のクライアントに接続を許可できます。このような WLAN のアクセス ポイントはいずれも、ビーコンとプローブ応答で WPA1、WPA2、および 802.1X/PSK/CCKM/ 802.1X+CCKM 情報要素をアドバタイズします。WPA1 または WPA2、あるいは両方を有効にした場合は、データ トラフィックを保護するために設計された 1 つまたは 2 つの暗号方式（暗号化アルゴリズム）を有効にすることもできます。具体的には、WPA1 または WPA2、あるいはその両方に対して、AES または TKIP、またはその両方を有効にすることができます。TKIP は WPA1 のデフォルト値で、AES は WPA2 のデフォルト値です。

AAA Override について

WLAN の AAA Override オプションを使用すると、WLAN で Identity ネットワーキングを設定できます。これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライア

ントに VLAN タギング、Quality Of Service (QoS)、およびアクセス コントロール リスト (ACL) を適用することができます。

レイヤ 2 セキュリティの前提条件

同じ SSID を持つ WLAN には、ビーコン応答とプローブ応答でアドバタイズされる情報に基づいてクライアントが WLAN を選択できるように、一意のレイヤ 2 セキュリティ ポリシーが設定されている必要があります。使用可能なレイヤ 2 セキュリティ ポリシーは、次のとおりです。

- なし（オープン WLAN）
-

（注）
- Static WEP と 802.1x はどちらも、ビーコン応答とプローブ応答でアドバタイズされるため、クライアントはこれらを区別できません。したがって、同じ SSID を持つ複数の WLAN では、 それらの両方を使用できません。
- 802.1x WEP はサポートされていません。
- Static WEP は、1810、1830、1850、2800、および 3802 アクセス ポイントではサポートされていません。

- CKIP
- WPA+WPA2

（注）
- 同じ SSID を持つ複数の WLAN で WPA と WPA2 を使用することはできませんが、同じ SSID を持つ 2 つの WLAN は、PSK を使用する WPA/TKIP と 802.1X を使用する Wi-Fi Protected Access（WPA）/Temporal Key Integrity Protocol（TKIP）で設定するか、802.1X を使用する WPA/TKIP または 802.1X を使用する WPA/AES で設定することができます。
- TKIP サポートが設定された WLAN は RM3000AC モジュールでは有効になりません。

- WPA2+WPA3
- 拡張オープン

WLAN セキュリティの設定方法

静的 WEP レイヤ 2 セキュリティ パラメータの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [WLANs] ページで、WLAN の名前をクリックします。

ステップ 3 [Edit WLAN] ウィンドウで [Security] タブをクリックします。

ステップ 4 [Layer 2 Security Mode] ドロップダウンリストから [Static WEP] オプションを選択します。

ステップ 5 （任意）[Shared Key Authentication] チェック ボックスをオンにして、認証タイプを共有に設定します。このチェック ボックスをオフのままにすると、認証タイプはオープンに設定されます。

ステップ 6 [Key Size] を [40 bits] または [104 bits] に設定します。

- [40 bits]：40 ビット暗号化を使用したキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。
- [104 bits]：104 ビット暗号化を使用したキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。

ステップ 7 適切な [Key Index] を設定します。1 ～ 4 の範囲で選択できます。

ステップ 8 [Key Format] を [ASCII] または [Hex] のいずれかに設定します。

ステップ 9 有効な [Encryption Key] を入力します。

- [40 bits]：40 ビット暗号化を使用したキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。
- [104 bits]：104 ビット暗号化を使用したキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。

ステップ 10 [Update & Apply to Device] をクリックします。

静的 WEP レイヤ 2 セキュリティ パラメータの設定（CLI）

始める前に

管理者特権が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name wlan-id SSID_Name* 例： `Device# wlan test4 1 test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は設定する WLAN のプロファイル名です。 *wlan-id* はワイヤレス LAN の ID です。指定できる範囲は 1 ～ 512 です。 *SSID_Name* は、最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *profile-name* コマンドを入力します。
ステップ 3	**disable ft** 例： `Device(config-wlan)# disable ft`	高速移行を無効にします。
ステップ 4	**no security ft over-the-ds** 例： `Device(config-wlan)# no security ft over-the-ds`	WLAN のデータ ソース経由の高速移行を無効にします。
ステップ 5	**no security ft** 例： `Device(config-wlan)# no security ft`	WLAN の 802.11r 高速移行をディセーブルにします。
ステップ 6	**no security wpa**{**akm** | **wpa1** | **wpa2**} 例： `Device(config-wlan)# no security wpa wpa1 ciphers tkip`	WLAN の WPA/WPA2 サポートを無効にします。
ステップ 7	**security static-wep-key** ［**authentication** {**open** | **shared**}］ 例： `Device(config-wlan)# security static-wep-key authentication open`	キーワードは次のとおりです。 • **static-wep-key**：静的な WEP キー認証を設定します。

	コマンドまたはアクション	目的
		• **authentication**：設定する認証タイプを指定します。値は、open および shared です。
ステップ 8	**security static-wep-key** ［**encryption** {**104** | **40**} {**ascii** | **hex**} [**0** | **8**]] 例： `Device(config-wlan)# security static-wep-key encryption 104 ascii 0 1234567890123 1`	キーワードは次のとおりです。 • **static-wep-key**：静的な WEP キー認証を設定します。 • **encryption**：設定する暗号化タイプを指定します。有効な値は 104 と 40 です。40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。104 ビットキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。 • **ascii**：キー形式を ASCII に指定します。 • **hex**：キー形式を HEX に指定します。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** をクリックします。

ステップ 2 [Add] をクリックして新しい WLAN プロファイルを追加するか、編集するプロファイルをクリックします。

ステップ 3 [Edit WLAN] ウィンドウで **[Security]** > **[Layer2]** をクリックします。

ステップ 4 [Layer 2 Security Mode] ドロップダウン メニューから [WPA + WPA2] を選択します。

ステップ 5 セキュリティ パラメータを設定して [Save and Apply to Device] をクリックします。

WPA + WPA2 レイヤ 2 セキュリティ パラメータの設定（CLI）

（注） セキュリティ ポリシー WPA2 のデフォルト値は次のとおりです。

- 暗号化は AES です。
- 認証キー管理（AKM）は dot1x です。

始める前に

管理者特権が必要です。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name wlan-id SSID_Name* 例： `Device# wlan test4 1 test4`	WLAN コンフィギュレーション サブモードを開始します。 *profile-name* は設定する WLAN のプロファイル名です。 *wlan-id* はワイヤレス LAN の ID です。指定できる範囲は 1 ～ 512 です。 *SSID_Name* は、最大 32 文字の英数字からなる SSID です。 （注） すでにこのコマンドを設定している場合は、**wlan** *profile-name* コマンドを入力します。
ステップ 3	**security wpa {akm | wpa1 | wpa2}** 例： `Device(config-wlan)# security wpa`	WLAN の WPA または WPA2 サポートを有効にします。
ステップ 4	**security wpa wpa1** 例： `Device(config-wlan)# security wpa wpa1`	WPA を有効にします。

	コマンドまたはアクション	目的
ステップ 5	**security wpa wpa1 ciphers**［**aes**	**tkip**］ 例： `Device(config-wlan)# security wpa wpa1 ciphers aes`	WPA1 暗号を指定します。次のいずれかの暗号化タイプを選択します。 • **aes**：WPA/AES のサポートを指定します。 • **tkip**：WPA/TKIP のサポートを指定します。 WPA1 および WPA2 のデフォルト値は、それぞれ TKIP および AES です。 （注） CLI を使用してのみ TKIP 暗号化を有効または無効にできます。GUI での TKIP 暗号化の設定はサポートされていません。 WGB に VLAN 設定がある場合、**encryption vlan 80 mode ciphers tkip** など、特定の VLAN に対して暗号化モードとキーを設定する必要があります。次に、コマンド **encryption mode ciphers tkip** を入力して、マルチキャストインターフェイスで暗号化モードをグローバルに設定する必要があります。
ステップ 6	**security wpa akm** {**cckm**| **dot1x**	**ft**	**pmf** |**psk**}	CCKM、802.1x、Fast Transition、Protected Management Frame、または PSK を有効または無効にします。
ステップ 7	**security wpa akm psk set-key** {**ascii**	**hex**} **psk-key**	PSK を有効にしている場合は、このコマンドを入力して事前共有キーを指定します。 WPA の事前共有キーには、8 ～ 63 文字の ASCII テキスト、または 64 桁の 16進数文字が含まれている必要があります。
ステップ 8	**security wpa akm ft** {**dot1x**	**psk**}	高速移行に対して認証キー管理スイートを有効または無効にします。 （注） AKM スイートとして PSK または高速移行 PSK を選択できます。

	コマンドまたはアクション	目的
ステップ 9	**security wpa wpa2** 例： `Device(config-wlan)# security wpa`	WPA2 を有効にします。
ステップ 10	**security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# security wpa wpa2 ciphers aes`	WPA2 暗号化を設定します。 **aes**：WPA/AES のサポートを指定します。
ステップ 11	**show wireless pmk-cache**	PMK キャッシュの有効期間タイマーの期限が切れるまでの残りの時間を表示します。 802.1X 認証キー管理で WPA2、または CCKM 認証キー管理で WPA1 または WPA2 を有効にした場合、必要に応じて、PMK キャッシュ ライフタイム タイマーを使用して、クライアントでの再認証をトリガーします。タイマーは、AAA サーバから受信したタイムアウト値または WLAN のセッション タイムアウト設定に基づきます。 802.1X 認証キー管理で WPA2 を有効にした場合、コントローラは opportunistic PMKID キャッシュと sticky（non-opportunistic）PMKID キャッシュの両方をサポートします。sticky PMKID キャッシュ（SKC）では、クライアントは複数の PMKID（アソシエートする AP ごとに異なる）を保存します。opportunistic PMKID キャッシュ（OKC）は、クライアントあたり 1 つの PMKID だけを保存します。デフォルトで、コントローラは OKC をサポートします。 （注） このコマンドは、VLAN オーバーライド フィールドに VLAN プーリング機能を含む VLAN ID を表示します。
ステップ 12	**end** 例：	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コ

	コマンドまたはアクション	目的
	`Device(config)# end`	ンフィギュレーションモードを終了できます。

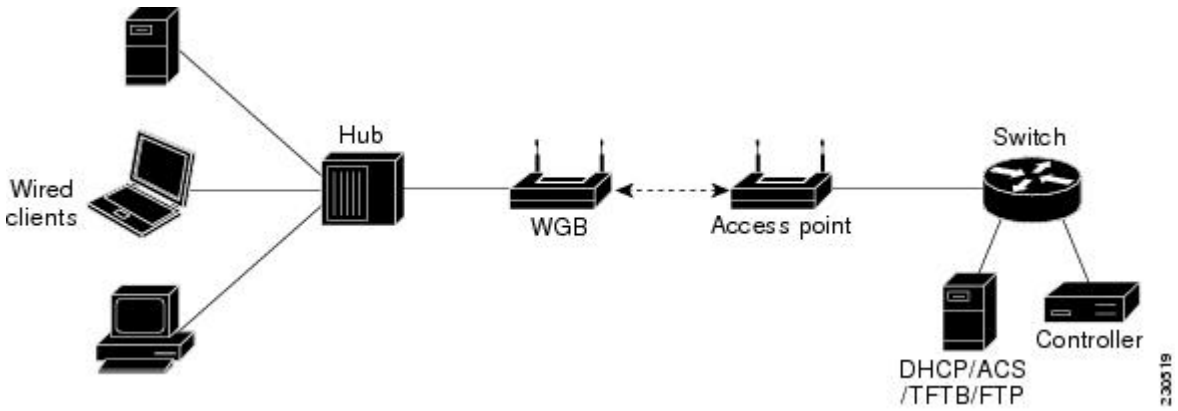
第 104 章

ワークグループ ブリッジ

Cisco ワークグループ ブリッジについて

ワークグループ ブリッジ（WGB）は、自律 Cisco IOS アクセス ポイント（AP）で設定できるモードで、イーサネットで WGB アクセス ポイントに接続されるクライアントの代わりに Lightweight AP へのワイヤレス接続を提供します。WGB はイーサネット インターフェイス上の有線クライアントの MAC アドレスを学習し、Internet Access Point Protocol（IAPP）メッセージングを使用して Lightweight AP に報告することで、1 つのワイヤレス セグメントを介して有線ネットワークに接続します。WGB は Lightweight AP への単一のワイヤレス接続を確立して、有線クライアントへのワイヤレス アクセス接続を提供します（Lightweight AP は、WGB をワイヤレス クライアントとして扱います）。

図 *28 : WGB* の例



WGB でサポートされるモードは次のとおりです。

- ローカル モード：中央認証、中央スイッチング。
- フレックス モード：中央認証、Cisco Wave 2 AP でのローカル スイッチング。

次の表に、サポートされる AP とサポートされない AP を示します。

表 *50 : AP* での *WGB* サポート

WGB の WLAN サポート	Cisco Wave 1 AP	Cisco Wave 2 AP
Central Authentication（中央認証）	サポート対象	サポート対象
中央スイッチング	サポート対象	サポート対象
ローカル認証	サポート対象	未サポート
ローカル スイッチング	未サポート	サポート対象

制約事項

- コントローラまたは AP 上の WGB 有線クライアントでは、中央認証およびローカル認証はサポートされません。
- MAC フィルタリングは、有線クライアントではサポートされていません。
- アイドル タイムアウトは、WGB と有線のどちらのクライアントでもサポートされません。
- セッション タイムアウトは、有線クライアントには適用されません。
- Web 認証はサポートされていません。
- WGB は最大 20 のクライアントのみをサポートします。

関連トピック

無線ゲスト アクセス （1119 ページ）

WLAN でのワークグループ ブリッジの設定

WLAN で WGB を設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy test-wgb`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA ポリシーのオーバーライドを設定します。
ステップ 4	**no central authentication** 例： `Device(config-wireless-policy)# no central authentication`	WLAN を ローカル認証用に設定します。
ステップ 5	**description** 説明 例： `Device(config-wireless-policy)# description "test-wgb"`	ポリシープロファイルの説明を追加します。
ステップ 6	**idle-timeout** *value* 例： `Device(config-wireless-policy)# idle-timeout 3600`	アイドル タイムアウト値を設定します。
ステップ 7	**session-timeout** *value* 例： `Device(config-wireless-policy)# session-timeout 300`	セッション タイムアウト値を設定します。
ステップ 8	**vlan** *vlan-no* 例： `Device(config-wireless-policy)# vlan 48`	プロファイル ポリシーを VLAN に割り当てます。
ステップ 9	**wgb vlan** 例： `Device(config-wireless-policy)# wgb vlan`	WGB VLAN クライアントのサポートを設定します。
ステップ 10	**wgb broadcast-tagging** 例： `Device(config-wireless-policy)# wgb broadcast-tagging`	WLAN で WGB ブロードキャスト タギングを設定します。

	コマンドまたはアクション	目的
ステップ 11	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	WLAN を再起動します。

ワークグループ ブリッジのステータスの確認

WGB のステータスを確認するには、次のコマンドを使用します。

アクティブなクライアントのワイヤレス固有設定を表示するには、次のコマンドを使用します。

```
Device# show wireless client summary
```

ネットワーク上の WGB を表示するには、次のコマンドを使用します。

```
Device# show wireless wgb summary
```

特定の WGB に接続された有線クライアントの詳細を表示するには、次のコマンドを使用します。

```
Device# show wireless wgb mac-address 00:0d:ed:dd:25:82 detail
```

第 105 章

ピアツーピア クライアント サポート

ピアツーピア クライアント サポートについて

ピアツーピア クライアント サポートは個別の WLAN に適用でき、各クライアントがアソシエート先の WLAN のピアツーピア ブロッキング設定を継承します。ピアツーピア クライアント サポート機能を使用すると、トラフィックの送信方法を細かく制御できます。たとえば、トラフィックをデバイス内でローカルにブリッジしたり、デバイスによってドロップしたり、アップストリーム VLAN に転送したりするように指定できます。

ローカル スイッチングの WLAN にアソシエートしたクライアントに対して、ピアツーピアブロッキングはサポートされています。

制約事項

- ピアツーピア ブロッキングは、マルチキャスト トラフィックには適用されません。
- ピアツーピア ブロッキングは、デフォルトでは有効になっていません。
- FlexConnect では、特定の FlexConnect AP または一部の AP のみにピアツーピア ブロッキング設定を適用することはできません。SSID をブロードキャストするすべての FlexConnect AP に適用されます。
- 中央スイッチングのクライアントに対応する統合ソリューションではピアツーピア アップストリーム転送がサポートされます。ただし、FlexConnect ソリューションではサポートされておらず、ピアツーピア ドロップとして処理されてクライアント パケットがドロップされます。

ピアツーピア クライアント サポートの設定

ピアツーピア クライアント サポートを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name* 例： `Device(config)# wlan wlan1`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**peer-blocking** [**drop** | **forward-upstream**] 例： `Device(config-wlan)# peer-blocking drop`	ピアツーピア ブロッキング パラメータを設定します。 **drop**：ドロップ アクションのピアツーピア ブロッキングをイネーブルにします。 **forward-upstream**：アップストリーム転送処理のピアツーピア ブロッキングをイネーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。
ステップ 5	**show wlan id** *wlan-id* 例： `Device# show wlan id 12`	選択した WLAN の詳細を表示します。

第 106 章

無線ゲスト アクセス

無線ゲスト アクセス

ワイヤレス ゲスト アクセス機能は、安全かつ信頼できる方法でゲストにインターネット アクセスを提供するニーズに対処します。ワイヤレス ゲスト ネットワークの実装では、企業の既存のワイヤレスおよび有線インフラストラクチャが最大限に使用されます。これにより、物理オーバーレイ ネットワークを構築する際のコストと複雑さが軽減されます。ワイヤレス ゲスト アクセス ソリューションは、ゲスト フォーリンとゲスト アンカーの 2 台のコントローラで構成されます。管理者は帯域幅を制限してゲスト トラフィックをシェーピングし、内部ネットワークのパフォーマンスに影響しないようにすることができます。

ワイヤレス ゲスト アクセス機能は、次の機能で構成されています。

- ゲスト アンカー コントローラは、クライアントの Point of Presence です。

- ゲスト アンカー コントローラは、ゲスト クライアントからのトラフィックをアンカー コントローラを介して Demilitarized Zone（DMZ）ネットワーク内のシスコ ワイヤレス コントローラに転送することで、内部セキュリティを確保します。
- ゲスト フォーリン コントローラは、クライアントの接続ポイントです。
- ゲスト フォーリン コントローラでは、ゲスト アクセスを必要とするあらゆる場所にキャンパス ワイヤレス ネットワークを介して専用のゲスト WLAN または SSID が実装されます。モビリティ アンカー（ゲスト コントローラ）が設定された WLAN でゲスト WLAN が識別されます。
- ゲスト トラフィックの分離により、キャンパス ネットワーク全体にレイヤ 2 またはレイヤ 3 手法が実装され、ゲストがアクセスできる場所が制限されます。
- ゲスト ユーザレベルの QoS は、レート制限およびシェーピングに使用されますが、ゲスト ユーザの帯域幅の使用を制限するために広く実装されています。
- アクセス制御では、キャンパス ネットワーク内に組み込まれたアクセス制御機能が使用されるか、企業ネットワークからインターネットへのゲストアクセスを制御する外部プラットフォームが実装されます。
- 日付、期間、帯域幅などの変数に基づく、ゲストの認証および承認。
- ネットワークを使用中または使用したことのあるユーザをトラックする監査メカニズム。
- ロビーや共有施設など、有線によるネットワーク接続もなかったエリアを含めて、より広範なカバレッジを提供します。
- ゲスト アクセス用のエリアや部屋を特別に用意する必要がなくなります。

（注） ネットワーク内で AireOS で IRCM を使用するには、Cisco TAC に連絡してサポートを受けてください。

表 *51 :* サポートされるコントローラ

Controller Name	ゲスト アンカーとしてのサポート	ゲスト フォーリンとしてのサポート
Cisco Catalyst 9800-40 ワイヤレス コントローラ	対応	対応
Cisco Catalyst 9800-80 ワイヤレス コントローラ	対応	対応
Cisco Catalyst 9800-CL ワイヤレス コントローラ	対応	対応

Controller Name	ゲスト アンカーとしてのサポート	ゲスト フォーリンとしてのサポート
スイッチ用 Cisco Catalyst 9800 組み込みワイヤレス コントローラ	なし	なし

Cisco ゲスト アクセスでサポートされている機能のリストを次に示します。

Supported Features

- スリープ状態のクライアント
- FQDN
- AVC（AP アップストリームおよびダウンストリーム）
- ネイティブ プロファイリング
- オープン認証
- OpenDNS
- サポートされているセキュリティ方式：
  - MAB CWA
  - LWA（ローカル Web 認証）
  - Dot1x + CWA（中央 Web 認証）
  - MAB エラー時の LWA
- SSID QoS アップストリームおよびダウンストリーム（外部）
- AP/クライアント SSO
- スタティック IP ローミング
- クライアント IPv6
- コントローラ間でのローミング
- RADIUS Accounting

（注） ゲストアクセスのシナリオでは、すべての認証方式を対象にアカウンティングは常にフォーリン コントローラで実行されます。

- QoS：クライアントレベルのレート制限
- ゲスト アンカー ロード バランシング
- ワークグループ ブリッジ （WGB）

（注） WLC が WGB からの複数の VLAN をサポートできるようにするには、**wgb vlan** コマンドを使用します。

関連トピック

スリープ状態にあるクライアントの認証について （602 ページ）
Application Visibility and Control について （337 ページ）
ネイティブ プロファイリングについて （845 ページ）
ローカル Web 認証の概要 （561 ページ）
中央 Web 認証について （591 ページ）
ワイヤレス QoS の概要 （817 ページ）
ハイ アベイラビリティについて （801 ページ）
スタティック IP クライアント モビリティについて （795 ページ）
IPv6 クライアント アドレス ラーニングについて （871 ページ）
モビリティの概要 （779 ページ）
複数のゲスト コントローラ間のロード バランシング （1122 ページ）
Cisco ワークグループ ブリッジについて （1113 ページ）

複数のゲスト コントローラ間のロード バランシング

大量のゲスト クライアント ボリュームをロード バランシングするようにエクスポート アンカーを設定できます。1 つのエクスポート フォーリン ゲスト WLAN 設定で、最大 72 のコントローラが許可されます。モビリティ ゲスト コントローラを設定するには、**mobility anchor** *ip address* を使用します。

プライマリ アンカーにプライオリティ（1、3）を指定し、障害が発生した場合のバックアップとして別のアンカーを選択できます。

関連トピック

無線ゲスト アクセス （1119 ページ）

ワイヤレス ゲスト アクセスに関する制限事項

- この機能は、Cisco AireOS 8.8.111.0 以降でサポートされています。
- ゲスト フォーリンとゲスト アンカーの両方で WLAN のセキュリティ プロファイルを一致させてください。
- ゲスト フォーリンとゲスト アンカーの両方のコントローラで、NAC や AAA オーバーライドなどのポリシー プロファイル属性を一致させてください。

- エクスポート アンカーでは、クライアントが実行時に接続する際に WLAN プロファイル名とポリシー プロファイル名が選択されます。これらはゲスト フォーリン コントローラで使用されているものと同じである必要があります。

IPv6 の制約事項

ゲスト エクスポート クライアントが、SLAAC を介してルーティング可能な IPv6 アドレスを取得できない場合、または IPv6 アドレスが学習されたときに DHCPv6 を介してトラフィックを渡せない場合は、次の回避策を使用できます。

- IPv6 ルータでの回避策：IPv6 ゲートウェイ上の動作を変更して、RA マルチキャストからユニキャストへの変換を回避できます。製品によって、これがデフォルトの動作である場合と、設定が必要な場合があります。
  - Cisco IPv6 ルータでの回避策
    - Nexus プラットフォーム：ワイヤレス展開に役立つ送信要求ユニキャスト RA がデフォルトで有効になっています。
    - IOS-XE プラットフォーム：次の設定ノブを使用して、ワイヤレス展開に役立つユニキャスト RA をオンにします。

      ipv6 nd ra solicited unicast

  - Cisco IPv6 ルータ以外での回避策：シスコ以外のネットワーク デバイスが送信要求ユニキャスト RA を有効にする設定ノブをサポートしていない場合、回避策はありません。

ゲスト アクセス用モビリティ トンネルの設定（GUI）

手順

ステップ 1 **[Configure]** > **[Tags and Profiles]** > **[WLANs]** をクリックします。

ステップ 2 [Wireless Networks] 領域で関連する WLAN または RLAN をクリックし、[Mobility Anchor] をクリックします。

ステップ 3 [Wireless Network Details] セクションで、[Switch IP Address] ドロップダウンリストからデバイスを選択します。

ステップ 4 [Apply] をクリックします。

ゲスト アクセス用モビリティ トンネルの設定

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラでモビリティ トンネルを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**wireless mobility group name** *group name*	独自のグループを設定します。
ステップ 2	**wireless mobility mac** *mac address*	独自の MAC アドレスを設定します。
ステップ 3	**wireless mobility group member mac** *mac address* **ip** *ip address* **group** *group name*	ピアを設定します。

ゲスト アクセス ポリシーの設定

ゲスト アクセス プロファイル ポリシーを作成して設定するには、次の手順に従います。または、モビリティ アンカーを設定した既存のデフォルト ポリシー プロファイルを使用することもできます。

ピアになっているアンカーのみを設定できます。使用されている IP アドレスがモビリティ ピアであり、モビリティ グループに含まれていることを確認します。他の IP アドレスが使用されている場合は、無効なアンカー IP アドレスのエラー メッセージが表示されます。

モビリティ グループを削除するには、モビリティ アンカーでもあるモビリティ ピアがポリシー プロファイルから削除されていることを確認します。

（注）

- VLAN を表示するために、ゲスト フォーリンにペイロードが送信されることはありません。
- VLAN が原因でクライアント除外が発生しないように、9800 シリーズ コントローラでは、ISE からプッシュされる関連名とともに VLAN を定義する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless profile policy** *wlan_policy_profile* 例： `Device (config)# wireless profile policy guest-test-policy`	ポリシープロファイルを設定し、ワイヤレス プロファイル コンフィギュレーション モードを開始します。 （注） • **default-policy-profile** を使用してプロファイル ポリシーを設定できます。 • プロファイル ポリシーでは、デフォルトのポリシー タグを使用できます。
ステップ 3	**shutdown** 例： `Device (config-wireless-policy)# shutdown`	ポリシーが存在する場合は、アンカーを設定する前にシャットダウンします。
ステップ 4	**central switching** 例： `Device (config-wireless-policy)# central switching`	（任意）中央スイッチングを設定します。
ステップ 5	最初のオプションを使用してゲスト フォーリンを設定するか、2 番目のオプションを使用してゲスト アンカーを設定します。 • **mobility anchor** *anchor-ip-address* • **mobility anchor** 例： ゲスト フォーリンの場合： `Device (config-wireless-policy)# mobility anchor 19.0.2.1` ゲスト アンカーの場合： `Device (config-wireless-policy)# mobility anchor`	ゲスト フォーリンまたはゲスト アンカーを設定します。
ステップ 6	**idle-timeout** *timeout* 例： `Device (config-wireless-policy)# idle-timeout 1000`	（任意）アイドル タイムアウト時間を秒単位で設定します。

	コマンドまたはアクション	目的
ステップ 7	**vlan** *vlan-id* 例： `Device (config-wireless-policy)# vlan 2`	VLAN 名または VLAN ID を設定します。 （注） ゲスト フォーリン コントローラでは VLAN は任意です。
ステップ 8	**no shutdown** 例： `Device (config-wireless-policy)# no shutdown`	ポリシー プロファイルを有効にします。
ステップ 9	**end** 例： `Device (config-wireless-policy)# end`	コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。
ステップ 10	**show wireless profile policy summary** 例： `Device# show wireless profile policy summary`	（任意）設定されたプロファイルを表示します。
ステップ 11	**show wireless profile policy detailed** *policy-profile-name* 例： `Device# show wireless profile policy detailed guest-test-policy`	（任意）ポリシープロファイルの詳細情報を表示します。

ゲスト アクセスのデバッグ情報の表示（CLI）

- このコマンドは、モビリティの状態に関するクライアント レベルの詳細情報とアンカー IP アドレスを表示します。

  show wireless client mac-add *mac-address***detail**

- このコマンドはクライアント モビリティの統計情報を表示します。

  show wireless client mac-address *mac-address***mobility statistics**

- このコマンドは、サブドメイン内のアクティブなクライアントに関するクライアント レベルのローミング履歴を表示します。

  show wireless client mac-address *mac-address* **mobility history**

- このコマンドは、特定のプロファイル ポリシーの詳細なパラメータを表示します。

  show wireless profile policy detailed *policy-name*

- このコマンドは、すべてのモビリティ メッセージに関するグローバル レベルのサマリーを表示します。

  show wireless mobility summary

- このコマンドはモビリティ マネージャの統計情報を表示します。

  show wireless stats mobility

サイト タグの設定

サイト タグを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag site** *site-tag-name* 例： `Device (config)# wireless tag site site-tag-name`	サイト タグを設定し、サイト タグ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**ap profile** *ap-profile* 例： `Device (config-site-tag)# ap profile temp-ap-profile`	AP プロファイルをサイトにマッピングします。
ステップ 4	**description** *site-tag-name* 例： `Device (config-site-tag)# description "description-of-site-tag"`	サイト タグに説明を追加します。
ステップ 5	**end** 例： `Device (config-site-tag)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show wireless tag site summary** 例： `Device# show wireless tag site summary`	サイト タグの数を表示します。
ステップ 7	**show wireless tag site detailed** *site-tag-name* 例：	サイト タグの詳細情報を表示します。

	コマンドまたはアクション	目的
	`Device# show wireless tag site detailed site-tag-name`	

ポリシー タグの設定

ポリシー タグを設定するには、次の手順に従います。

（注） AVC とともに使用されていない場合は、アンカーにポリシー タグを設定する必要はありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless tag policy** *policy-tag-name* 例： `Device (config)# wireless tag policy guest-tag-policy`	ポリシー タグを設定し、ポリシー タグ プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device (config-policy-tag)# wlan test-wlan policy guest-test-policy`	ポリシー プロファイルを WLAN プロファイルにマッピングします。
ステップ 4	**end** 例： `Device (config-policy-tag)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 5	**show wireless tag policy summary** 例： `Device# show wireless tag policy summary`	設定されたポリシータグを表示します。
ステップ 6	**show wireless tag policy detailed** *policy-profile-name* 例： `Device# show wireless tag policy detailed guest-test-policy`	ポリシータグの詳細情報を表示します。

AP へのポリシー タグの関連付け

（注） デフォルトのポリシー プロファイルにモビリティ アンカーを含めることもできます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap filter name** *filter-name* 例： `Device(config)# ap filter name guest-ap-filter` `Device(config-ap-filter)# ap name-regex ap-name`	AP フィルタを設定します。
ステップ 3	**tag policy** *policy-tag-name* 例： `Device(config-ap-filter)# tag policy policy-tag-name`	フィルタのポリシータグを設定します。
ステップ 4	**wlan** *wlan-name* **policy** *profile-policy-name* 例： `Device (config-policy-tag)# wlan test-wlan policy guest-test-policy`	ポリシー プロファイルを WLAN プロファイルにマッピングします。
ステップ 5	**end** 例： `Device (config-policy-tag)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show wireless tag policy summary** 例： `Device# show wireless tag policy summary`	設定されたポリシータグを表示します。
ステップ 7	**show wireless tag policy detailed** *policy-profile-name* 例： `Device# show wireless tag policy detailed guest-test-policy`	ポリシータグの詳細情報を表示します。

AP へのサイト タグとポリシー タグの付加

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**ap** *mac-address* 例： `Device (config)# ap e2:d0:f3:d3:c0:8e`	APを設定し、APタグ コンフィギュレーション モードを開始します。 （注） イーサネット MAC アドレスを使用します。
ステップ 3	**policy-tag** *policy-tag-name* 例： `Device (config-ap-tag)# policy-tag guest-tag-policy`	ポリシー タグを AP にマッピングします。
ステップ 4	**site-tag** *site-tag-name* 例： `Device (config-ap-tag)# site-tag site-tag-name`	サイト タグをAPにマッピングします。
ステップ 5	**end** 例： `Device (config-ap-tag)# end`	コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。
ステップ 6	**show ap tag summary** 例： `Device# show wireless tag policy summary`	AP の詳細と AP に関連付けられているタグを表示します。

さまざまなセキュリティ方式を使用したゲストアクセスの設定

オープン認証を使用したゲスト アクセスの設定

ポリシー プロファイルの設定

オープン認証を使用するゲスト アンカーを設定するには、次の手順に従います。

（注） AVC が有効になっていない場合は、タグは必要ありません。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *wlan-policy-profile* 例： `Device(config)# wireless profile policy open_it`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	最初のオプションを使用してゲスト フォーリンを設定するか、2番目のオプションを使用してゲスト アンカーを設定します。 • **mobility anchor** *anchor-ip-address* • **mobility anchor** 例： ゲスト フォーリンの場合： `Device (config-wireless-policy)# mobility anchor 19.0.2.1` ゲスト アンカーの場合： `Device (config-wireless-policy)# mobility anchor`	ゲスト フォーリンまたはゲスト アンカーを設定します。
ステップ 4	**central switching**を使用して無効にすることができます。	中央スイッチングを有効にします。

	コマンドまたはアクション	目的
	例： `Device(config-wireless-policy)# central switching`	
ステップ 5	**vlan** *id* 例： `Device(config-wireless-policy)# vlan 16`	VLAN 名または VLAN ID を設定します。 （注） ゲストフォーリンコントローラでは VLAN は任意です。
ステップ 6	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ポリシープロファイルを有効にします。

WLAN プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name wlan-id ssid-name.* 例： `Device(config)# wlan mywlan 34 mywlan-ssid`	WLAN と SSID を設定します。
ステップ 3	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 4	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 6	**no security wpa wpa2 ciphers aes** 例：	AES の WPA2 暗号化をディセーブルにします。

	コマンドまたはアクション	目的
	`Device(config-wlan)# no security wpa wpa2 ciphers aes`	
ステップ 7	**no shutdown** 例： `Device(config-wlan)# no shutdown`	設定を保存します。

ローカル Web 認証を使用したゲスト アクセスの設定

パラメータ マップの設定

ローカル Web 認証を使用するゲスト アンカーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**parameter-map type webauth global** 例： `Device(config)# parameter-map type webauth global`	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。
ステップ 3	**type webauth** 例： `Device(config-params-parameter-map)#type webauth`	webauth タイプ パラメータを設定します。
ステップ 4	**timeout init-state sec** *timeout-seconds* 例： `Device(config-params-parameter-map)# timeout inti-state sec 3600`	WEBAUTH のタイムアウトを秒単位で設定します。 タイムアウト（秒単位）パラメータの有効な範囲は 60 ～ 3932100 秒です。
ステップ 5	**virtual-ip ipv4** *virtual_IP_address* 例： `Device(config-params-parameter-map)#virtual-ip ipv4 209.165.201.1`	VLAN 名または VLAN ID を設定します。

ポリシー プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *policy-profile-name* 例： `Device(config)# wireless profile policy policy1`	ポリシー プロファイルを設定します。
ステップ 3	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 4	最初のオプションを使用してゲスト フォーリンを設定するか、2番目のオプションを使用してゲスト アンカーを設定します。 • **mobility anchor** *anchor-ip-address* • **mobility anchor** 例： ゲスト フォーリンの場合： `Device (config-wireless-policy)# mobility anchor 19.0.2.1` ゲスト アンカーの場合： `Device (config-wireless-policy)# mobility anchor`	ゲスト フォーリンまたはゲスト アンカーを設定します。
ステップ 5	**vlan** *name* 例： `Device(config-wireless-policy)# vlan 16`	VLAN 名または VLAN ID を設定します。 （注） ゲスト フォーリン コントローラでは VLAN は任意です。
ステップ 6	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ポリシープロファイルを有効にします。

WLAN プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *wlan-id ssid-name* 例： `Device# Device(config)# wlan mywlan 38 mywlan-ssid1`	WLAN と SSID を設定します。
ステップ 3	**security web-auth** 例： `Device(config-wlan)# security web-auth`	WLAN の Web 認証を有効にします。
ステップ 4	**security web-auth parameter-map** デフォルト 例： `Device(config-wlan)# security web-auth parameter-map default`	デフォルトのパラメータ マップを設定します。 （注） **security web-auth** が有効になっている場合、**default authentication-list** とグローバルの **parameter-map** がマッピングされます。これは、明示的に記述されていない認証リストとパラメータマップに適用されます。
ステップ 5	**security web-auth parameter-map** *global* 例： `Device(config-wlan)# security web-auth parameter-map global`	グローバル パラメータ マップを設定します。
ステップ 6	**security web-auth authentication-list** *LWA-AUTHENTICATION* 例： `Device(config-wlan)# security web-auth authentication-list LWA-AUTHENTICATION`	IEEE 802.1x の認証リストを設定します。

AAA サーバ設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**aaa authentication login** *LWA-AUTHENTICATION* **local** 例： `Device(config)#aaa authentication login lwa-authentication local`	ログイン時の認証方法を定義します。
ステップ 3	**aaa authorization network default local if-authenticated** 例： `Device(config)#aaa authorization network default local if-authenticated`	ユーザが認証済みの場合は、認証方法をローカルに設定します。

グローバル コンフィギュレーション

グローバル設定については、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**username** *name* **password 0** *clear-text-passowrd* 例： `Device(config)# #username base password 0 pass1`	ユーザのクリア テキスト パスワードを設定します。
ステップ 3	**ip http server** 例： `Device(config)#ip http server`	HTTP サーバをイネーブルにします。
ステップ 4	**ip http authentication local** 例：	HTTP サーバの認証方式をローカルに設定します。

	コマンドまたはアクション	目的
	`Device(config)#ip http authentication local`	

中央 Web 認証を使用したゲスト アクセスの設定

ポリシー プロファイルの設定

中央 Web 認証を使用するゲスト アンカーを設定するには、次の手順に従います。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wireless profile policy** *cwa* 例： `Device(config)# wireless profile policy cwa`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**aaa-override** 例： `Device(config-wireless-policy)# aaa-override`	AAA サーバまたは ISE サーバから受信したポリシーを適用するように AAA オーバーライドを設定します。
ステップ 4	**central switching** 例： `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 5	最初のオプションを使用してゲスト フォーリンを設定するか、2 番目のオプションを使用してゲスト アンカーを設定します。 • **mobility anchor** *anchor-ip-address* • **mobility anchor** 例： ゲスト フォーリンの場合： `Device (config-wireless-policy)# mobility anchor 19.0.2.1` ゲスト アンカーの場合：	ゲスト フォーリンまたはゲスト アンカーを設定します。

	コマンドまたはアクション	目的
	`Device (config-wireless-policy)# mobility anchor`	
ステップ 6	**nac** 例： `Device(config-wireless-policy)# nac`	ポリシープロファイルにNACを設定します。
ステップ 7	**session-timeout** *seconds* 例： `Device(config-wireless-policy)# session-timeout 300`	セッション タイムアウト値を秒単位で設定します。範囲は 20 ～ 86400 です。
ステップ 8	**vlan** *name* 例： `Device(config-wireless-policy)# vlan 16`	VLAN 名または VLAN ID を設定します。 （注） ゲストフォーリンコントローラでは VLAN は任意です。
ステップ 9	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ポリシープロファイルを有効にします。

WLAN プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *wlan-id ssid-name* 例： `Device# Device(config)# wlan mywlan 38 mywlan-ssid1`	WLAN と SSID を設定します。
ステップ 3	**mac-filtering** *remote_authorization_list_name* 例： `Device(config-wlan)# mac-filtering auth-list`	リモートRADIUSサーバのMAB認証を有効にします。
ステップ 4	**no security wpa** 例：	WPA セキュリティを無効にします。

	コマンドまたはアクション	目的
	`Device(config-wlan)# no security wpa`	
ステップ 5	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 6	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 7	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 8	**no shutdown** 例： `Device(config-wlan)# no shutdown`	設定を保存します。

AAA サーバ設定

（注） ゲスト フォーリン専用の AAA サーバを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**aaa authorization network** *authorization-list***local group** *Server-group-name* 例： `Device(config)#aaa authorization network cwa local group ise`	許可の方法をローカルに設定します。
ステップ 3	**aaa group server radius** *server-group-name* 例： `Device(config)#aaa group server radius ise`	RADIUS サーバ グループの定義を設定します。

	コマンドまたはアクション	目的
ステップ 4	**server name** *radius-server-name* 例： `Device(config-sg-radius)#server name ise1`	RADIUS サーバ名を設定します。
ステップ 5	**subscriber mac-filtering security-mode mac** 例： `Device(config-sg-radius)#$mac-filtering security-mode mac`	パスワードとしてMACアドレスを設定します。
ステップ 6	**mac-delimiter colon** 例： `Device(config-sg-radius)#mac-delimiter colon`	MAC アドレスの区切り文字をコロンに設定します。
ステップ 7	**end** 例： `Device(config-sg-radius)#end`	設定を保存し、コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。
ステップ 8	**radius server** *name* 例： `Device(config)#radius server ISE1`	RADIUS サーバ名を設定します。
ステップ 9	**address ipv4** *radius-server-ipaddress* **auth-port** *port-number* **acct-port** *port-number* 例： `Device(config-radius-server)#address ipv4 209.165.201.1 auth-port 1635 acct-port 33`	RADIUSサーバのIPアドレス、認証ポート、アカウンティング ポートを設定します。

MAC 障害時の Web 認証の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags and Profiles]** > **[WLANs]** をクリックします。

ステップ 2 [Add] をクリックして新しい WLAN プロファイルを追加するか、編集するプロファイルをクリックします。

ステップ 3 [Edit WLAN] ウィンドウで **[Security]** > **[Layer3]** をクリックします。

ステップ 4 [Show Advanced Settings] をクリックして [On MAC Filter Failure] チェックボックスをオンにします。

MAC 障害時の Web 認証の設定

クライアントが WLAN への接続試行時に MAC フィルタ（ローカルまたは RADIUS）を使用して認証できない場合、Web 認証にフォールバックするように設定できます。この機能を有効にするには、デバイスで MAC フィルタリングと Web 認証の両方を設定します。これにより、MAC フィルタ認証の失敗のみを理由に発生するアソシエーション解除も回避できます。この機能を設定するには、次の手順を実行します。

ポリシー プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# 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	**wireless profile policy** *cwa* **例：** `Device(config)# wireless profile policy cwa`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**central switching** **例：** `Device(config-wireless-policy)# central switching`	中央スイッチングを有効にします。
ステップ 4	最初のオプションを使用してゲスト フォーリンを設定するか、2 番目のオプションを使用してゲスト アンカーを設定します。 • **mobility anchor** *anchor-ip-address* • **mobility anchor** **例：** ゲスト フォーリンの場合： `Device (config-wireless-policy)# mobility anchor 19.0.2.1` ゲスト アンカーの場合：	ゲスト フォーリンまたはゲスト アンカーを設定します。

	コマンドまたはアクション	目的
	`Device (config-wireless-policy)# mobility anchor`	
ステップ 5	**vlan** *name* 例： `Device(config-wireless-policy)# vlan 16`	VLAN 名または VLAN ID を設定します。 （注） ゲストフォーリンコントローラでは VLAN は任意です。
ステップ 6	**no shutdown** 例： `Device(config-wireless-policy)# no shutdown`	ポリシープロファイルを有効にします。

WLAN プロファイルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**wlan** *guest-wlan-name wlan-id ssid* 例： `config# wlan test-wlan-guest 10 wlan-ssid`	ゲスト WLAN を設定します。
ステップ 2	**security web-auth** 例： `config-wlan# security web-auth`	Web 認証を有効にします。
ステップ 3	**security web-auth on-macfilter-failure** 例： `config-wlan# security web-auth on-macfilter-failure`	MAC フィルタ認証が失敗した場合に Web 認証を有効にします。

外部マップの概要

ゲストアクセスは、Cisco Catalyst 9800 シリーズ ワイヤレス コントローラのポリシープロファイルと WLAN プロファイルの設定モデルを使用した外部マップをサポートしています。

Cisco Catalyst 9800 シリーズ ワイヤレス コントローラで外部マップがサポートされるのは、次のポリシー プロファイルと WLAN プロファイルの設定モデルを使用した場合です。

- ゲスト フォーリン
  - **Foreign1**：**wlanProf1 PolicyProf1**

- **Foreign2**：**wlanProf2 PolicyProf2**

- ゲスト アンカー
  - **wlanProf1**、**wlanProf2**
  - **PolicyProf1**：**Vlan100 - subnet1**
  - **PolicyProf2**：**Vlan200 - subnet2**

外部マップ ローミング

2 つのゲスト フォーリンで 2 つの異なる WLAN プロファイルを設定した場合、それらの間でシームレス ローミングを実行することはできません。これは予期される設定です。ただし、2 つのゲスト フォーリンで同じ WLAN プロファイルが設定されている場合はシームレス ローミングが許可されますが、外部マップ機能は動作しません。

ワイヤレス ゲスト アクセス：使用例

この機能は、ゲストアクセス機能として実行した場合にさまざまな要件を満たすために使用できます。ここでは、考えられるいくつかの例を紹介します。

シナリオ 1：企業の合併時にセキュリティで保護されたネットワーク アクセスを提供する

会社 B にアクセスする**会社 A** の社員が会社 B のネットワークで会社 A のリソースに安全にアクセスできるように、この機能を設定できます。

シナリオ 2：既存の設定を介したサービスの共有

この機能を使用すると、既存のネットワークにピギーバッキングする複数のベンダーを使用して複数のサービスを提供できます。会社は、既存のコントローラにアンカーされている SSID でサービスを提供できます。これは、既存のサービスが同じコントローラとネットワーク上で機能している間継続されます。

第 107 章

802.11r BSS Fast Transition

802.11R 高速移行について

高速ローミングの IEEE 標準である 802.11r では、対応するクライアントがターゲット アクセス ポイントにローミングする前でも、新しい AP との最初のハンドシェイクが実行される、ローミングの新しい概念が導入されています。この概念は高速移行と呼ばれます。最初のハンドシェイクによって、クライアントとアクセス ポイントは Pairwise Transient Key（PTK）を事前に計算できます。これらの PTK キーは、クライアントが再アソシエーション要求に応答するか、新しいターゲット アクセス ポイントとの交換に応答した後で、クライアントと AP に適用されます。

FT キー階層は、クライアントが各 AP での再認証なしで、AP 間の高速 BSS 移行ができるように設計されています。WLAN 設定には、FT（高速移行）と呼ばれる、新しい認証キー管理（AKM）タイプが含まれています。

クライアント ローミング

クライアントが FT プロトコルを使用して現在の AP からターゲット AP に移動する場合、メッセージ交換は次のいずれかの方法を使用して実行されます。

- 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。

- Over-the-Distribution System（DS）：クライアントは、現在の AP を介してターゲット AP と通信します。クライアントとターゲット AP との通信は、クライアントと現在の AP の間の FT アクション フレームで実行されてから、デバイスによって送信されます。

図 *29 : Over–the–Air* クライアント ローミングが設定されている場合のメッセージ交換

この図は、Over–the–Air クライアント ローミングが設定されている場合に実行されるメッセージ交換のシーケンスを示しています。

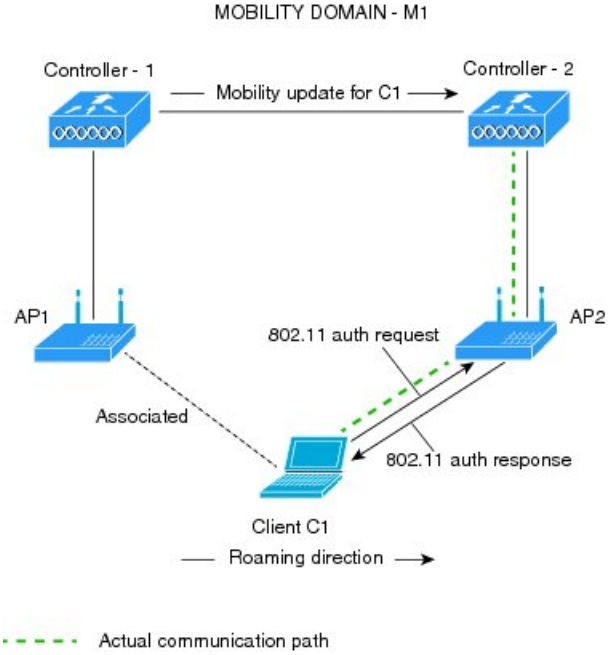
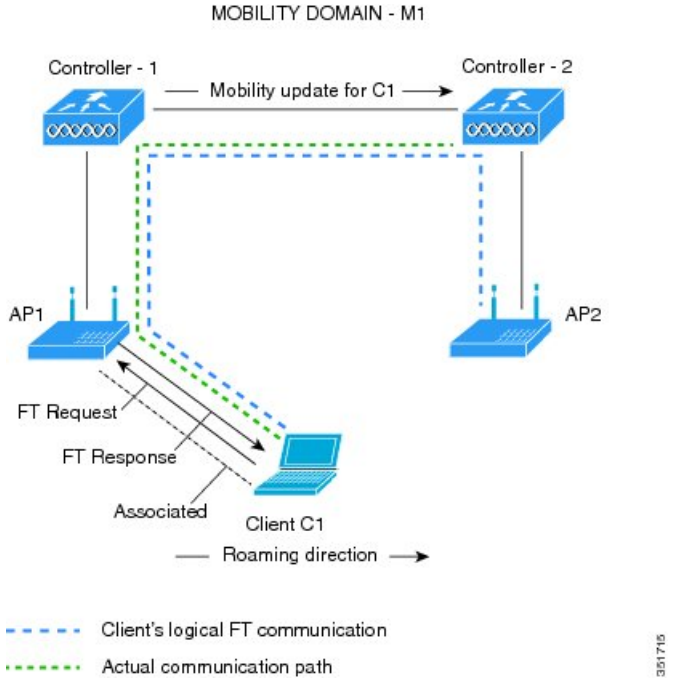


図 *30 : Over–the–DS* クライアント ローミングが設定されている場合のメッセージ交換

この図は、Over–the–DS クライアント ローミングが設定されている場合に実行されるメッセージ交換のシーケンスを示しています。



802.11R 高速移行の制約事項

- EAP LEAP 方式はサポートされません。
- トラフィック仕様（TSPEC）は802.11r高速ローミングではサポートされません。したがって、RIC IE の処理はサポートされません。
- WAN リンク遅延がある場合、高速ローミングも遅延します。音声またはデータの最大遅延を確認する必要があります。Cisco WLC は、Over-the-Air と Over-the-DS のどちらの方式でもローミング時に 802.11r 高速移行の認証要求を処理します。
- この機能は、オープンおよび WPA2 が設定された WLAN でサポートされます。
- レガシー クライアントは、Robust Security Network Information Exchange（RSN IE）の解析を担当するサプリカントのドライバが古く、IE 内の追加 AKM を認識しない場合、802.11r が有効にされている WLAN にアソシエートできません。この制限のため、クライアントは、WLAN にアソシエーション要求を送信できません。ただし、これらのクライアントは、非 802.11r WLAN とアソシエートできます。802.11r 対応クライアントは、802.11i と 802.11r の両方の認証キー管理スイートが有効になっている WLAN で 802.11i クライアントとしてアソシエートできます。

  回避策は、レガシー クライアントのドライバを新しい 802.11r AKM で動作できるようにするか、アップグレードすることです。これにより、レガシー クライアントは 802.11r 対応 WLAN と正常にアソシエートできます。

もう 1 つの回避策は、同じ名前で異なるセキュリティ設定（FT および非 FT）の 2 つの SSID を持つことです。

- 高速移行のリソース要求プロトコルは、クライアントがこのプロトコルをサポートしていないため、サポートされません。また、リソース要求プロトコルはオプションのプロトコルです。
- サービス不能（DoS）攻撃を回避するため、Cisco WLC では、異なる AP と最大 3 つの高速移行ハンドシェイクが可能です。
- 非 802.11r 対応デバイスは FT 対応 WLAN にアソシエートできなくなります。
- 802.11r FT + PMF は推奨されません。
- FlexConnect 導入には 802.11r FT Over-the-Air ローミングをお勧めします。
- WLAN がコントローラで作成されると、デフォルトで 802.11r FT Over DS が有効になります。Cisco Wave 2 AP では、802.11r を使用したローカル スイッチング ローカル認証はサポートされません。Cisco Wave 2 AP でローカル スイッチング ローカル認証を機能させるには、WLAN で 802.11r を明示的に無効にします。設定例を次に示します。

```
wlan local-dot1x 24 local-dot1x
no security ft over-the-ds
no security ft adaptive
security dot1x authentication-list spwifi_dot1x
no shutdown
```

802.11r 高速移行の確認（CLI）

次のコマンドを使用して、802.11r 高速移行を確認できます。

コマンド	説明
show wlan name *wlan-name*	WLAN に設定されているパラメータの要約を表示します。

コマンド	説明
show wireless client mac-address *mac-address*	クライアントの 802.11r 認証キー管理の設定の概要を表示します。 . . . . . . Client Capabilities CF Pollable : Not implemented CF Poll Request : Not implemented Short Preamble : Not implemented PBCC : Not implemented Channel Agility : Not implemented Listen Interval : 15 Fast BSS Transition : Implemented Fast BSS Transition Details : Client Statistics: Number of Bytes Received : 9019 Number of Bytes Sent : 3765 Number of Packets Received : 130 Number of Packets Sent : 36 Number of EAP Id Request Msg Timeouts : 0 Number of EAP Request Msg Timeouts : 0 Number of EAP Key Msg Timeouts : 0 Number of Data Retries : 1 Number of RTS Retries : 0 Number of Duplicate Received Packets : 1 Number of Decrypt Failed Packets : 0 Number of Mic Failured Packets : 0 Number of Mic Missing Packets : 0 Number of Policy Errors : 0 Radio Signal Strength Indicator : -48 dBm Signal to Noise Ratio : 40 dB . . . . . .

Dot1x セキュリティ対応 WLAN での 802.11r BSS 高速移行の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name* 例：	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設

	コマンドまたはアクション	目的
	`Device# wlan test4`	定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： `Device(config-wlan)# client vlan 0120`	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**local-auth** *local-auth-profile-eap* 例： `Device(config-wlan)# local-auth`	ローカル認証 EAP プロファイルを有効にします。
ステップ 5	**security dot1x authentication-list default** 例： `Device(config-wlan)# security dot1x authentication-list default`	dot1x セキュリティ用のセキュリティ認証リストを有効にします。この設定は、すべての dot1x セキュリティ WLAN で類似しています。
ステップ 6	**security ft** 例： `Device(config-wlan)# security ft`	WLAN で 802.11r 高速移行を有効にします。
ステップ 7	**security wpa akm ft dot1x** 例： `Device(config-wlan)# security wpa akm ft dot1x`	WLAN 上で 802.1x セキュリティをイネーブルにします。
ステップ 8	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

オープン WLAN での 802.11r 高速移行の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

ステップ 3 **[Security]** > **[Layer2]** タブで、AP 間の [Fast Transition] の適切なステータスを選択します。
ステップ 4 [Save & Apply to Device] をクリックします。

オープン WLAN での 802.11r 高速移行の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-id* 例： `Device(config-wlan)# client vlan 0120`	WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa** 例： `Device(config-wlan)# no security wpa`	WPA セキュリティを無効にします。
ステップ 5	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 6	**no security wpa wpa2** 例： `Device(config-wlan)# no security wpa wpa2`	WPA2 セキュリティを無効にします。
ステップ 7	**no wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化をディセーブルにします。
ステップ 8	**security ft** 例：	802.11r 高速移行パラメータを指定します。

	コマンドまたはアクション	目的
	`Device(config-wlan)# security ft`	
ステップ 9	**no shutdown** 例： `Device(config-wlan)# shutdown`	WLAN をシャット ダウンします。
ステップ 10	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

PSK セキュリティ対応 WLAN での 802.11r 高速移行の設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**client vlan** *vlan-name* 例： `Device(config-wlan)# client vlan 0120`	この WLAN にクライアント VLAN を関連付けます。
ステップ 4	**no security wpa akm dot1x** 例： `Device(config-wlan)# no security wpa akm dot1x`	dot1x に対するセキュリティの AKM をディセーブルにします。
ステップ 5	**security wpa akm ft psk** 例： `Device(config-wlan)# security wpa akm ft psk`	高速移行 PSK サポートを設定します。
ステップ 6	**security wpa akm psk set-key** {**ascii** {**0** | **8**} | **hex** {**0** | **8**}}	PSK AKM の共有キーを設定します。

	コマンドまたはアクション	目的
	例： `Device(config-wlan)# security wpa akm psk set-key ascii 0 test`	
ステップ 7	**security ft** 例： `Device(config-wlan)# security ft`	802.11r 高速移行を設定します。
ステップ 8	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、**Ctrl+Z** キーを押しても、グローバル コンフィギュレーション モードを終了できます。

802.11r 高速移行の無効化（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。
ステップ 2 [WLANs] ページで、WLAN 名をクリックします。
ステップ 3 [Edit WLAN] ウィンドウで **[Security]** > **[Layer2]** タブをクリックします。
ステップ 4 [Fast Transition] ドロップダウンリストから [Disabled] を選択します。
ステップ 5 [Update & Apply to Device] をクリックします。

802.11r 高速移行のディセーブル（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *profile-name* 例： `Device# wlan test4`	WLAN コンフィギュレーション サブモードを開始します。*profile-name* は設定されている WLAN のプロファイル名です。
ステップ 3	**no security ft** [**over-the-ds** | **reassociation-timeout** *timeout-in-seconds*] 例： `Device(config-wlan)# no security ft over-the-ds`	WLAN の 802.11r 高速移行をディセーブルにします。
ステップ 4	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

第 108 章

経由ローミング

経由ローミングについて

802.11k 標準では、クライアントがサービス セットの移行の候補となる既知のネイバー アクセス ポイントに関する情報を含むネイバー レポートを要求することができます。802.11k ネイバー リストを使用すると、アクティブおよびパッシブ スキャンを軽減できます。

経由ローミング機能は、インテリジェントでクライアントによって最適化されたネイバー リストに基づいています。

Cisco Client Extension（CCX）ネイバー リストとは異なり、802.11k ネイバー リストは動的かつオンデマンドで生成されます。device上では維持されません。802.11k ネイバー リストは、クライアントのロケーションに基づくもので、Mobility Services Engine (MSE) を必要としません。同じdevice上であっても異なる AP の 2 クライアントが、周囲の AP の個々の関係に応じて提供される異なるネイバー リストを設定できます。

デフォルトでは、ネイバー リストには、クライアントがアソシエートされている同じ帯域のネイバーだけが含まれます。ただし、両方の帯域のネイバーを返すために、802.11k を可能にするスイッチが存在します。

クライアントは、ビーコン内の RRM（無線リソース管理）機能の情報要素（IE）をアドバタイズする AP に関連付けた後でのみ、ネイバー リストの要求を送信します。ネイバー リストには、隣接する無線の BSSID、チャネル、および処理の詳細についての情報が含まれます。

ネイバー リストの作成と最適化

802.11k ネイバー リスト要求をdeviceが受信すると、次の処理が実行されます。

1. deviceは、クライアントが現在関連付けられている AP と同じ帯域で、ネイバー リストについて RRM ネイバー テーブルを検索します。

2. deviceは、帯域ごとにネイバー リストを 6 つに削減するために、AP 間の RSSI（Received Signal Strength Indication）、現在の AP の現在のロケーション、Cisco Prime インフラストラクチャからのネイバー AP のフロア情報、device上でのローミング履歴情報に従ってネイバーをチェックします。このリストは、同じフロアの AP に対して最適化されています。

非 802.11k クライアントの経由ローミング

非 802.11k クライアントのローミングを最適化することもできます。クライアントが 802.11k ネイバー リスト要求を送信する必要なく、各クライアントの予測ネイバー リストを生成できます。成功した各クライアント アソシエーション/再アソシエーションの後、WLAN でこれが有効である場合、ネイバー リストを生成し、モバイル ステーションのソフトウェア データ構造にリストを格納するために、同じネイバー リストの最適化を非 802.11k クライアントに適用する必要があります。クライアント プローブが異なるネイバーによって異なる RSSI 値により認識されるため、異なるロケーションのクライアントが異なるリストを持ちます。クライアントは、通常はアソシエーションまたは再アソシエーションの前にプローブするため、このリストは、更新されたほとんどのプローブ データによって構築され、クライアントがローミングする可能性が高い次の AP を予測します。

AP へのアソシエーション要求が保存された予測ネイバー リストのエントリに一致しない場合に、アソシエーションを拒否することによって、あまり望ましくないネイバーへのクライアントのローミングを抑止します。

アグレッシブ ロード バランシングに加えて、経由ローミング機能を毎 WLAN ごとおよびグローバルにオンにするスイッチがあります。次のオプションを使用できます。

- Denial count：クライアントでアソシエーションが拒否される最大回数です。
- Prediction threshold：経由ローミング機能をアクティブにするために、予測リスト内で必要なエントリの最小数です。

ロードバランシングおよび経由ローミングの両方で、クライアントがアソシエートする AP に影響を与えるように設計されているため、WLAN で両オプションを同時にイネーブルにすることはできません。

経由ローミングの制約事項

- この機能は、802.11n 対応の屋内アクセス ポイントでのみサポートされています。 1 つの帯域構成の場合、最大 6 のネイバーがネイバー リストに表示されます。デュアル バンド構成の場合、最大 12 のネイバーが表示されます。
- device CLI をのみを使用して経由ローミングを設定できます。

経由ローミングの設定方法

経由ローミングの設定（GUI）

始める前に

プライマリ コントローラとバックアップ コントローラを設定する前に、AP参加プロファイルがすでに設定済みであることを確認します。

手順

ステップ1 **[Configuration]** > **[Wireless Advanced]** > **[Optimized Roam]** を選択します。

ステップ2 [5 GHz Band] または [2.4 GHz Band] ページで、[Optimized Roaming Mode] チェック ボックスをオンにします。

ステップ3 [Optimized Roaming Data Rate Threshold] フィールドに、クライアントのしきい値データ レートの値を入力します。次のデータ レートが使用可能です。

- 802.11a：6、9、12、18、24、36、48、および54。
- 802.11b：1、2、5、6、9、11、12、18、24、36、48、および54。

ローミングの最適化は、クライアントのデータ パケットおよびデータ レートのRSSIに基づいてクライアントのアソシエートを解除します。クライアントの現在のデータ レートが、[Optimized Roaming Data Rate Threshold] よりも小さい値の場合は、クライアントはアソシエート解除されます。

ステップ4 [Apply] をクリックします。

経由ローミングの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wireless assisted-roaming floor-bias** *dBm* 例： `Device(config)# wireless assisted-roaming floor-bias 20`	ネイバー フロア ラベル バイアスを設定します。有効な範囲は –5 ～ 25 dBm で、デフォルト値は –15 dBm です。
ステップ 3	**wlan** *wlan-id* 例： `Device(config)# wlan wlan1`	WLAN コンフィギュレーション サブモードを開始します。*wlan-name* は設定されている WLAN のプロファイル名です。
ステップ 4	**assisted-roaming neighbor-list** 例： `Device(wlan)# assisted-roaming neighbor-list`	WLAN の 802.11k ネイバー リストを設定します。WLANを作成すると、デフォルトで assisted roaming がネイバー リストで有効になります。コマンドの **no** 形式を実行すると、経由ローミングのネイバー リストが無効になります。
ステップ 5	**assisted-roaming dual-list** 例： `Device(wlan)# assisted-roaming dual-list`	WLAN のデュアル バンド 802.11k デュアル リストを設定します。WLAN を作成すると、デフォルトで assisted roaming がデュアル リストで有効になります。コマンドの **no** 形式を実行すると、経由ローミングのデュアル リストが無効になります。
ステップ 6	**assisted-roaming prediction** 例： `Device(wlan)# assisted-roaming prediction`	WLAN の経由ローミング予測リスト機能を設定します。デフォルトでは、経由ローミング予測リストはディセーブルです。 （注） ロードバランシングが WLAN に対してすでにイネーブルである場合、警告メッセージが表示され、ロード バランシングが WLANに対してディセーブルになります。

	コマンドまたはアクション	目的
ステップ 7	**wireless assisted-roaming prediction-minimum** *count* 例： `Device# wireless assisted-roaming prediction-minimum`	予測リスト機能が動作するために必要な予測 AP の最小数を設定します。デフォルト値は 3 です。 （注） クライアントに割り当てられた Forecast、AP が指定した数よりもこの値が小さい場合、経由ローミング機能はこのルールに適用されません。
ステップ 8	**wireless assisted-roaming denial-maximum** *count* 例： `Device# wireless assisted-roaming denial-maximum 8`	AP に送信されたアソシエーション要求が予測の AP に一致しない場合に、クライアントでアソシエーションを拒否できる最大回数を設定します。有効な範囲は 1 ～ 10 で、デフォルト値は 5 です。
ステップ 9	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

経由ローミングの確認

次のコマンドを使用して、WLAN に設定された経由ローミングを確認できます。

コマンド	説明
show wlan id *wlan-id*	WLAN の WLAN パラメータを表示します。

経由ローミングの設定例

次に、ネイバー フロア ラベル バイアスを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless assisted-roaming floor-bias 10
Device(config)# end
Device# show wlan id 23
```

次に、特定の WLAN のネイバー リストをディセーブルにする例を示します。

```
Device# configure terminal
Device(config)# wlan test1
Device(config (wlan)# no assisted-roaming neighbor-list
```

```
Device(config)(wlan)# end
Device# show wlan id 23
```

次に、特定の WLAN の予測リストを設定する例を示します。

```
Device# configure terminal
Device(config)# wlan test1
Device(config)(wlan)# assisted-roaming prediction
Device(config)(wlan)# end
Device# show wlan id 23
```

次に、特定の WLAN の経由ローミングの予測しきい値および最大の拒否数に基づいて予測リストを設定する例を示します。

```
Device# configure terminal
Device(config)# wireless assisted-roaming prediction-minimum 4
Device(config)# wireless assisted-roaming denial-maximum 4
Device(config)(wlan)# end
Device# show wlan id 23
```

第 109 章

802.11v

802.11v に関する情報

コントローラはワイヤレス ネットワークに関する 802.11v 改訂をサポートします。これには、ワイヤレス ネットワーク管理に対するさまざまな機能拡張について記載されています。

このような機能拡張の 1 つに、クライアントでスリープ時間を延ばしてバッテリ寿命を改善できるようにするネットワーク支援型電力節約があります。たとえば、多くのモバイルデバイスは、特定のアイドル期間を利用してアクセス ポイントとの接続を維持するため、ワイヤレス ネットワークで以降のタスクを実行するときにより多くの電力を消費します。

もう 1 つの機能拡張は、WLAN 上で関連するクライアントに要求を送信して、クライアントにアソシエートするより適切な AP をアドバタイズ可能なネットワーク支援型ローミングです。これは、ロード バランシングと、接続が不安定なクライアントの管理の両方に役立ちます。

802.11v ネットワーク支援型電力節約の有効化

ワイヤレスデバイスはクライアントへの接続を維持するためにさまざまな方法でバッテリを消費します。

- 定期的にスリープ解除し、DTIM を含むアクセス ポイント ビーコンをリッスンします。DTIM は、アクセス ポイントがクライアントに送信する、ブロードキャストまたはマルチキャスト トラフィックがバッファされていることを示します。
- アクセス ポイントとの接続を維持するために、null フレームをキープアライブ メッセージの形式でアクセス ポイントに送信します。

- デバイスは、定期的に、ビーコンをリッスン（DTIM フィールドがない場合も）して、対応するアクセス ポイントとクロックを同期させます。

このすべてのプロセスがバッテリを消費し、その消費は特にデバイス（Apple など）に影響します。これは、これらのデバイスが保守的なセッション タイムアウト推定を使用しているために、頻繁にスリープ解除してキープアライブ メッセージを送信するためです。802.11 標準は、802.11v なしのローカル クライアントのセッション タイムアウトの無線クライアントと通信するため、コントローラまたはアクセス ポイントの機能は含まれていません。

ワイヤレス ネットワーク上の上記タスクによるクライアントの電力を節約するために、802.11v 標準の次の機能が使用されます。

- Directed Multicast Service
- Base Station Subsystem（BSS）最大アイドル期間

Directed Multicast Service

Directed Multicast Service（DMS）を使用して、クライアントは、必要なマルチキャスト パケットをユニキャスト フレームとして送信するようにアクセス ポイントに要求します。これにより、クライアントは、スリープ モードでは無視していたマルチキャスト パケットを受信でき、レイヤ 2 の信頼性も保証されます。また、ユニキャスト フレームができるだけ高いワイヤレス リンク レートでクライアントに送信されるため、クライアントは無線の持続期間を短縮してパケットをすばやく受信できるようになり、バッテリの電力が節約されます。ワイヤレス クライアントはマルチキャスト トラフィックを受信するために DTIM 間隔ごとにスリープ解除する必要がないため、スリープ間隔を延ばすことができます。

BSS の最大アイドル時間

BSS 最大アイドル期間は、アクセス ポイント（AP）が接続先のクライアントからフレームが受信されないという理由でそのクライアントをアソシエート解除しないタイムフレームです。これにより、クライアント デバイスがキープアライブ メッセージを頻繁に送信しないことが保証されます。アイドル期間タイマー値は、アクセス ポイントからクライアントへのアソシエーションおよび再アソシエーション応答フレームを使用して送信されます。このアイドル時間値は、クライアントがアクセス ポイントにフレームを送信せずにアイドル状態を維持できる最大時間を示します。したがって、クライアントは、キープアライブ メッセージを頻繁に送信することなく、より長い間スリープ モードを維持します。これがバッテリの電力の節約につながります。

802.11v の実装の前提条件

- Apple iOS バージョン 7 以降で動作する Apple iPad や iPhone などの Apple クライアントに適用されます。
- ローカル モードをサポートしています。中央認証モードだけ FlexConnect のアクセス ポイントをサポートします。

802.11v に関する制約事項

クライアントは 802.11v BSS 移行をサポートする必要があります。

802.11v BSS 移行管理の有効化

802.11v BSS 移行は次の 3 つのシナリオに適用されます。

- 要請された要求：クライアントは、再度関連付ける AP のより適切なオプションをローミングする前に、802.11v 基本サービス セット（BSS）移行管理クエリを送信できます。
- 要請されないロード バランシング要求：AP は負荷が高い場合、関連付けられたクライアントに 802.11v BSS 移行管理要求を送信します。
- 要請されない最適化ローミング要求：クライアントの RSSI とレートが要件を満たしていない場合は、対応する AP はこのクライアントに 802.11v BSS 移行管理要求を送信します。

（注） 802.11v BSS 移行管理要求は、クライアントが従うか無視するか選択できる、クライアントに与えられた提案事項（つまりアドバイス）です。クライアントの関連付け解除を強制するには、関連付け解除イミネント機能をオンにします。これにより、クライアントは別の AP に再アソシエートしないと一定時間後にアソシエート解除されます。

802.11v BSS 移行管理の設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

ステップ 3 [Advanced] タブおよび [11v BSS Transition Support] セクションで、[BSS Transition] チェック ボックスをオンにして WLAN ごとの BSS 移行を有効にします。

ステップ 4 [Disassociation Imminent] の値を入力します。有効な範囲は 0 ～ 3000 TBTT です。

ステップ 5 [Save & Apply to Device] をクリックします。

802.11v BSS 移行管理の設定（CLI）

802.11v BSS 移行は次の 3 つのシナリオに適用されます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name* 例： `Device(config)# wlan test-wlan`	WLAN プロファイルを設定し、WLAN プロファイル コンフィギュレーション モードを開始します。
ステップ 3	**shut** 例： `Device(config-wlan)# shut`	WLAN プロファイルをシャットダウンします。
ステップ 4	**bss-transition** 例： `Device(config-wlan)# bss-transition`	WLAN ごとの BSS 移行を設定します。
ステップ 5	**bss-transition disassociation-imminent** 例： `Device(config-wlan)# bss-transition disassociation-imminent`	WLAN ごとの BSS 移行関連付け解除イミネントを設定します。
ステップ 6	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN プロファイルを有効にします。
ステップ 7	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。または、Ctrl+Z キーを押してグローバル コンフィギュレーション モードを終了できます。

第 110 章

802.11W

802.11w に関する情報

Wi-Fi は、正規のデバイスまたは不法なデバイスのいずれであっても、あらゆるデバイスで傍受または参加が可能なブロードキャストメディアです。認証、認証解除、アソシエーション、アソシエーション解除、ビーコン、プローブなどの管理フレームは、ワイヤレスクライアントがネットワーク サービスのセッションを開始および切断するために使用します。暗号化により、一定レベルの機密保持を実現できるデータ トラフィックとは異なり、これらのフレームはすべてのクライアントによって受信および解釈される必要があるため、オープンまたは非暗号化形式で送信されます。これらのフレームは暗号化できませんが、攻撃から無線メディアを保護するために偽造を防止することが必要になります。たとえば、攻撃者は AP にアソシエートされたクライアントを攻撃するために、AP からの管理フレームをスプーフィングする可能性があります。

802.11w プロトコルは、保護管理フレーム（PMF）サービスによって保護された一連の堅牢な管理フレームにのみ適用されます。これには、アソシエーション解除フレーム、認証解除フレーム、ロバスト アクション フレームなどが含まれます。

したがって、ロバストアクションであり、保護されているものと見なされる管理フレームは次のとおりです。

- スペクトル管理
- QoS
- DLS
- ブロック ACK

- 無線測定
- 高速 BSS 移行
- SA クエリ
- 保護されたデュアル パブリック アクション
- ベンダー固有保護

802.11w が無線メディアで実行されると、次のことが行われます。

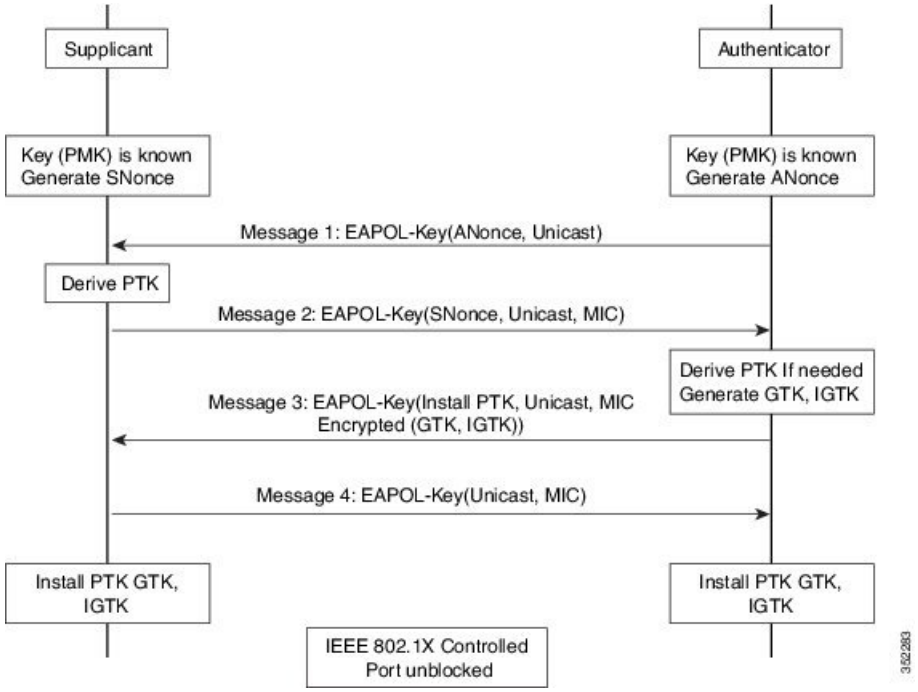
- AP が認証解除フレームと関連付け解除フレームに暗号保護を追加することでクライアント保護が追加され、DoS 攻撃でのスプーフィングを阻止します。
- アソシエーション復帰期間とセキュリティ アソシエーション（SA）クエリの手順で構成される SA ティアダウン保護メカニズムを追加することでインフラストラクチャ保護が追加され、スプーフィングされたアソシエーション要求によって接続済みのクライアントが切断されることを阻止します。

802.11w で新たに導入された IGTK キーは、ブロードキャスト/マルチキャストの堅牢な管理フレームを保護するために使用されます。

- IGTK はオーセンティケータ STA（WLC）によって割り当てられるランダムな値で、ソース STA からの MAC 管理プロトコル データ ユニット（MMPDU）を保護するために使用されます。

管理フレーム保護のネゴシエーション時に、AP は 4 ウェイ ハンドシェイクのメッセージ 3 で送信される EAPOL キー フレーム内の GTK 値と IGTK 値を暗号化します。

図 *31 : 4* ウェイ ハンドシェイクでの *IGTK* 交換

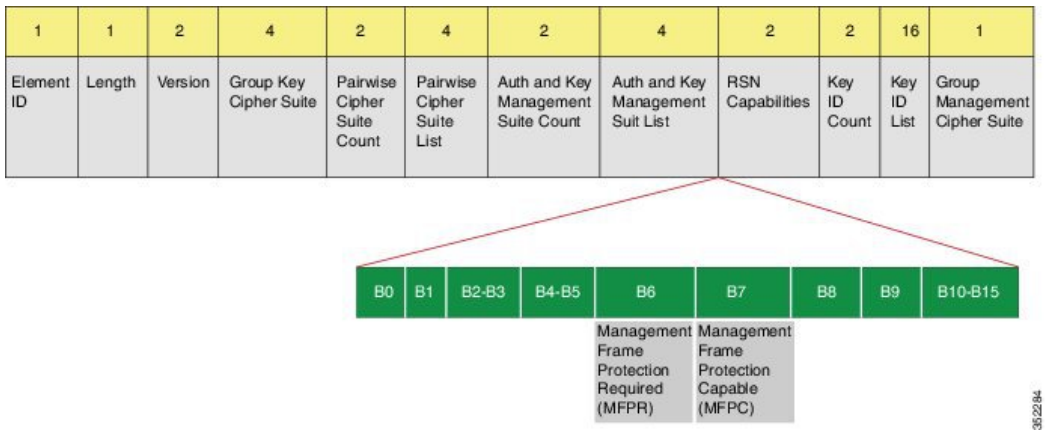


- AP は後で GTK を変更した場合には、グループ キー ハンドシェイクを使用して新しい GTK と IGTK をクライアントに送信します。

802.11w では、新たに Broadcast/Multicast Integrity Protocol（BIP）が定義されています。このプロトコルは、IGTKSA が正常に確立された後、ブロードキャスト/マルチキャストの堅牢な管理フレームにおけるデータの整合性、およびリプレイ保護を提供し、共有 IGTK キーを使用して計算される MIC を追加します。

802.11w の情報要素（IE）

図 *32 : 802.11w* の情報要素



1. RSNIE の RSN 機能フィールドに変更が加えられています。

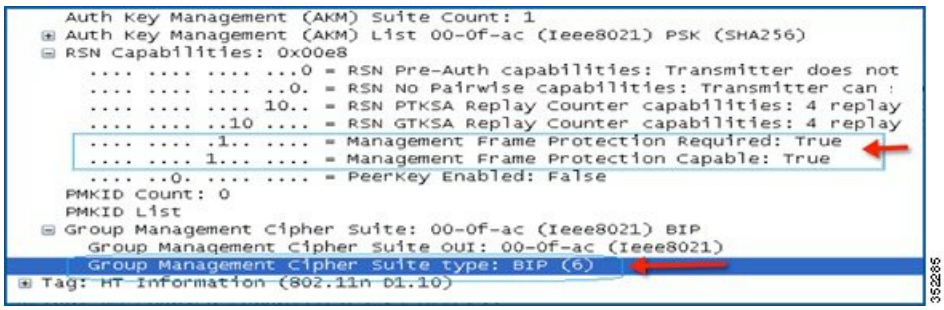
1. ビット 6：Management Frame Protection Required（MFPR）
2. ビット 7：Management Frame Protection Capable（MFPC）

2. 2 つの新しい AKM スイート 5 および 6 が AKM スイート セレクタ用に追加されています。
3. BIP に対応するため、タイプ 6 の新たな暗号スイートが追加されました。

この変更された RSNIE を WLC はアソシエーション応答と再アソシエーション応答に追加し、AP はビーコン応答とプローブ応答に追加します。

次の Wireshark キャプチャ画面は、RSNIE 機能とグループ管理暗号スイートの要素を示します。

図 *33 : 802.11w* の情報要素



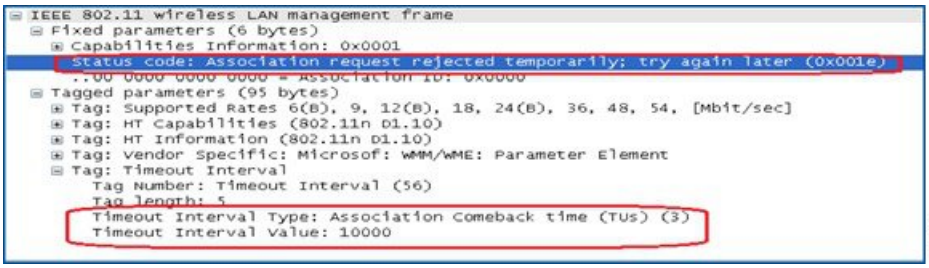
セキュリティ アソシエーション（SA）ティアダウン保護

SA ティアダウン保護は、リプレイ攻撃によって既存のクライアントのセッションが切断されるのを防止するメカニズムです。アソシエーションの復帰期間と SA クエリの手順を組み合わせることで、スプーフィングされたアソシエーション要求により、接続済みのクライアントが切断されることを防止します。

クライアントが有効なセキュリティ アソシエーションを有し、802.11w をネゴシエートしている場合は、AP はステータス コード 30 を使用して、新たなアソシエーション要求を拒否します。このステータス コードは、「アソシエーション要求が一時的に拒否されました。後でやり直してください」ということを意味します。AP は、SA クエリ手順によって元の SA が無効であると判断されない限り、既存アソシエーションを切断したり、その状態を変更したりすることはできません。また、APのアソシエーション応答には、APがこのクライアントとのアソシエーションを受け入れる準備が整うまでの時間を指定したアソシエーション復帰期間の情報要素が含められます。

次の図は、ステータス コード 0x1e（30）のアソシエーション拒否メッセージと、10 秒に設定されたアソシエーション復帰期間を示しています。

図 *34* : アソシエーション拒否と復帰期間



クライアントとの SA クエリがまだ実行されていない場合、AP は一致する SA クエリ応答を受信するか、アソシエーション復帰期間が経過するまで、SA クエリを発行します。AP は有効な保護フレームを受信すると、SA クエリが正常に完了したと解釈します。

一致するトランザクション識別子を含む SA クエリ応答が期間内に行われると、AP は追加の SA クエリ手順を開始せずに、アソシエーション プロセスの開始を許可します。

802.11w の前提条件

- 任意および必須の 802.11w 機能を設定するには、WPA および AKM を設定する必要があります。

（注） Robust Secure Network（RNS）IE は AES 暗号化とともにイネーブルにする必要があります。

- 必須として 802.11w を設定するには、WPA AKM に加えて PMF AKM を有効にします。

802.11w の制約事項

- 802.11w はオープン WLAN、 WEP 暗号化 WLAN、または TKIP 暗号化 WLAN に適用されていません。
- Cisco Catalyst 9800 シリーズ ワイヤレス コントローラ Apple 以外のクライアントに対しては、802.11w + PMF の組み合わせがサポートされています。ただし、Apple iOS バージョン 11 以前で関連の問題を解決するには、Apple iOS 側からの修正が必要です。

802.11w の設定方法

802.11w の設定（GUI）

始める前に

WPA および AKM を設定する必要があります。

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

ステップ 3 **[Security]** > **[Layer2]** タブで、[Protected Management Frame] セクションに移動します。

ステップ 4 [PMF] で [Disabled]、[Optional]、または [Required] を選択します。デフォルトでは、PMF は無効になっています。

[PMF] で [Optional]、または [Required] を選択した場合は、次のフィールドが表示されます。

- [Association Comeback Timer]：1 ～ 10 秒の値を入力して、802.11w のアソシエーション復帰期間を設定します。
- [SA Query Time]：100 ～ 500（ミリ秒）の値を入力します。これは、クライアントが WLAN の 802.11w PMF 保護をネゴシエートするために必要です。

ステップ 5 [Save & Apply to Device] をクリックします。

802.11w の設定（CLI）

始める前に

WPA および AKM を設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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。

	コマンドまたはアクション	目的
ステップ 2	**wlan** *profile-name wlan-id ssid* 例： `Device(config)# wlan wlan-test 12 alpha`	WLANを設定し、コンフィギュレーション モードを開始します。
ステップ 3	**security wpa akm pmf dot1x** 例： `Device(config-wlan)#security wpa akm pmf dot1x`	802.1x のサポートを設定します。
ステップ 4	**security pmf association-comeback** *comeback-interval* 例： `Device(config-wlan)# security pmf association-comeback 10`	802.11wアソシエーション復帰時間を設定します。
ステップ 5	**security pmf mandatory** 例： `Device(config-wlan)# security pmf mandatory`	クライアントが WLAN の 802.11w PMF 保護をネゴシエートすることを要求します。
ステップ 6	**security pmf saquery-retry-time** *timeout* 例： `Device(config-wlan)# security pmf saquery-retry-time 100`	SA クエリ応答を受け取るまでの時間（ミリ秒単位）です。デバイスが応答を受け取らなかった場合、別の SQ クエリが試行されます。

802.11w の無効化

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# 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	**wlan** *profile-name wlan-id ssid* 例： `Device(config)# wlan wlan-test 12 alpha`	WLANを設定し、コンフィギュレーション モードを開始します。
ステップ 3	**no security wpa akm pmf dot1x** 例： `Device(config-wlan)# no security wpa akm pmf dot1x`	802.1x サポートを無効にします。

	コマンドまたはアクション	目的
ステップ 4	**no security pmf association-comeback** *comeback-interval* 例： `Device(config-wlan)# no security pmf association-comeback 10`	802.11wのアソシエーション復帰期間を無効にします。
ステップ 5	**no security pmf mandatory** 例： `Device(config-wlan)# no security pmf mandatory`	クライアントによる WLAN の 802.11w PMF 保護のネゴシエートを無効にします。
ステップ 6	**no security pmf saquery-retry-time** *timeout* 例： `Device(config-wlan)# no security pmf saquery-retry-time 100`	SQ クエリの再試行を無効にします。

802.11w のモニタリング

802.11w をモニタリングするには、次のコマンドを使用します。

手順

ステップ 1 **show wlan name** *wlan-name*

WLAN の WLAN パラメータを表示します。PMF パラメータが表示されます。

```
. . . .
. . . .
Auth Key Management
            802.1x                              : Disabled
            PSK                                 : Disabled
            CCKM                                : Disabled
            FT dot1x                            : Disabled
            FT PSK                              : Disabled
            FT SAE                              : Disabled
            Dot1x-SHA256                        : Enabled
            PSK-SHA256                          : Disabled
            SAE                                 : Disabled
            OWE                                 : Disabled
            SUITEB-1X                           : Disabled
            SUITEB192-1X                        : Disabled
    CCKM TSF Tolerance                          : 1000
    FT Support                                  : Adaptive
        FT Reassociation Timeout                : 20
        FT Over-The-DS mode                     : Enabled
    PMF Support                                 : Required
        PMF Association Comeback Timeout        : 1
        PMF SA Query Time                       : 500
```

```
. . . .
. . . .
```

ステップ 2 **show wireless client mac-address** *mac-address***detail**

クライアントの 802.11w 認証キー管理設定の概要を表示します。

```
. . . .
. . . .
Policy Manager State: Run
NPU Fast Fast Notified : No
Last Policy Manager State : IP Learn Complete
Client Entry Create Time : 497 seconds
Policy Type : WPA2
Encryption Cipher : CCMP (AES)
Authentication Key Management : 802.1x-SHA256
Encrypted Traffic Analytics : No
Management Frame Protection : No
Protected Management Frame - 802.11w : Yes
EAP Type : LEAP
VLAN : 39
Multicast VLAN : 0
Access VLAN : 39
Anchor VLAN : 0
WFD capable : No
Manged WFD capable : No
. . . .
. . . .
```