NEC

GVT-153323-001-00 1.24

QX-W1000/W1100 シリーズ アクセスポイント

Anchor-AC オペレーションマニュアル

改版履歴

版数	日付	改版内容
1.0	2020/11	初版発行
1.1	2020/12	・表紙の「本マニュアルについて」の記載を変更しました。 ・誤記訂正
1.2	2021/02	・誤記訂正 ・「5 章 WLAN セキュリティ」の下記コマンドについてメモを追加しました。 - **wpa3** - **pmf** ・「15 章 スペクトル管理の設定」の章を追加しました。 ・「21 章 WLAN メッシュ」の章を追加しました。
1.3	2021/05	・「3 章 無線管理の設定」の「概要」に下記機能の概要を追加しました。 - OFDMA - MU-MIMO - Spatial reuse ・「3 章 無線管理の設定」の「802.11ac/ax 機能の設定」の「TxBF の設定」のデフォルト状態を変更しました。 ・「3 章 無線管理の設定」の「802.11ac/ax 機能の設定」に「OFDMA の設定」、「BSS カラーリングの設定」、「TWT ネゴシエーションの設定」を追加しました。 ・「5 章 WLAN セキュリティ」の「WPA3 エンタープライズ(192bit セキュリティなし)設定例」の設定方法を修正しました。 ・「7 章 WLAN 認証の設定」の「失敗許可機能の有効化」のメモにバックアップ用サービステンプレートに関する内容を追加しました。 ・「9 章 WLAN QoS の設定」の「概要」の「U-APSD 節電方法」に説明を追加しました。 ・「9 章 WLAN QoS の設定」に「U-APSD の設定」を追加しました。

版数	日付	改版内容
1.4	2021/07	・「2 章 AP 管理」の「リモート設定の割り当て設定」に **remote-configuration synchronize** コマンドに関する説明を追記しました。 ・「3 章 無線管理の設定」の「無線モードの指定」に QX-W1100 シリーズの Radio3 に関するメモ書きと QX-W1120 に関するメモ書きを追加しました。 ・「13 章 チャネルスキャンの設定」の「最大サービス期間の設定」の **scan max-service-time** コマンドの補足説明を変更しました。 ・「17 章 WLAN RRM の設定」の **wlan rrm calibration-channel interval** コマンドの補足説明を変更しました。 ・「21 章 WLAN メッシュの設定」の「WLAN メッシュ設定の制限とガイドライン」にレーダ検出時に関するメモ書きを追加しました。 ・誤記訂正
1.5	2021/09	・「2 章 AP 管理」の「AP に対する制御トンネルの keepalive 時間の設定」に、CAPWAP トンネルダウンの判断時間に関するメモ書きを追加しました。 ・「10 章 WLAN ローミングの設定」の「設定の制限とガイドライン」の内容を一部修正しました。 ・誤記訂正
1.6	2021/10	・「2 章 AP 管理」の「リモート設定の割り当て設定」と「AP の VLAN 設定」のメモ書きの内容を見直しました。 ・「4 章 WLAN アクセスの設定」の「AP へのコンフィグレーションファイルの設定」のメモ書きを見直しました。 ・「7 章 WLAN 認証の設定」の「失敗許可機能の設定」に「keep-online」パラメータを追加しました。 ・「7 章 WLAN 認証の設定」に「MAC アドレス認証クライアントのための AC 内ローミング高速接続有効化」を追加しました。 ・「9 章 WLAN QoS の設定」に「Air Time Fairness の設定」および「Air Time Fairness の設定例」を追加しました。
1.7	2021/11	・「1 章 Anchor-AC の設定」に、QX-W1100 シリーズで QX-W1000 シリーズの FIT を管理できる旨の説明および注意事項を追加しました。 ・「7 章 WLAN 認証の設定」に「Web 認証(ポータル認証)の設定」を追加しました。
1.8	2021/12	・「1 章 Anchor-AC の設定」の「QX-W1100 シリーズでの QX-W1000 シリーズの管理設定」の設定手順に、**display wlan ap name files** コマンドを追加しました。 ・「7 章 WLAN 認証の設定」の「定期的なオンラインユーザ再認証機能の有効化」の説明を修正しました。 ・「21 章 WLAN メッシュの設定」の誤記を訂正しました。
1.9	2022/02	・「15 章 WLAN 最適化」に「ブロードキャストおよびマルチキャストのパケットレート制限の設定」を追加しました。 ・「21 章 WLAN メッシュの設定」に、QX-W1100 シリーズでの WLAN メッシュ機能サポートに関するメモ書きを追加しました。

版数	日付	改版内容
1.10	2022/03	・「2 章 AP 管理」の「CAPWAP トンネル」の AC 選択基準の記載内容を見直しました。 ・「5 章 WLAN セキュリティ」の **domain default enable** コマンドが使用されている設定例のドメイン指定方法を見直しました。 ・「5 章 WLAN セキュリティ」の「管理フレーム保護の設定」に KDF の設定に関する記述を追記しました。また、pmf を使用している設定例に KDF の設定手順を追加しました。 ・「7 章 WLAN 認証の設定」の **domain default enable** コマンドが使用されている設定例のドメイン指定方法を見直しました。 ・「10 章 WLAN ローミングの設定」に「802.11r の設定」と「802.11v の設定」を追加しました。 ・「12 章 WLAN 無線リソースの計測の設定」に「802.11k 計測」を追記しました。 ・「15 章 WLAN 最適化」に「ブロードキャストおよびマルチキャストパケット制御の設定」を追加しました。 ・「19 章 デュアルリンクバックアップ」を追加しました ・誤記訂正
1.11	2022/05	・「1 章 Anchor-AC の設定」の「Anchor-AC の概要」に QX-W1110 Anchor-AC および Anchor-FIT の情報を追加しました。 ・「1 章 Anchor-AC の設定」の「Anchor-FIT モードからの AC 選出」に、QX-W1110 Anchor-AC の情報を追記しました。 ・「5 章 WLAN セキュリティ」の「暗号化方式の設定」に QX-W1100 シリーズの gcmp パラメータサポートに関する記述を追記しました。 ・「5 章 WLAN セキュリティ」の「WPA3 の設定」に QX-W1100 シリーズの WPA3 エンタープライズ 192bit セキュリティモードサポートに関する記述を追記しました。 ・「7 章 WLAN 認証の設定」に「 MAC アドレス認証の認証方式の設定」を追加しました。 ・「7 章 WLAN 認証の設定」の「802.1X 認証クライアントの最大同時接続数の設定」に接続制限の動作に関するメモ書きを追加しました。 ・「7 章 WLAN 認証の設定」の「MAC アドレス認証クライアントの最大同時接続数の設定」に接続制限の動作に関するメモ書きを追加しました。 ・「17 章 WLAN RRM の設定」に「帯域幅自動調整の設定」および「帯域幅自動調整の設定例」を追加しました。 ・「17 章 WLAN RRM の設定」のスケジュール auto-DFS の設定例を見直しました。 ・「19 章 デュアルリンクバックアップ」の設定例に、AC 切り戻し時の動作に関する記述を追加しました。 ・誤記訂正

版数	日付	改版内容
1.12	2022/06	・「3 章 無線管理の設定」の「OFDMA の設定」、「BSS カラーリングの設定」、「TWT ネゴシエーションの設定」の機能デフォルト値表記を変更しました。 ・「10 章 WLAN ローミングの設定」に「 モビリティドメイン ID の設定」を追加しました。 ・誤記訂正
1.13	2022/09	・「2 章 AP 管理」に「 AC が AP イメージファイルを取得するための優先ロケーションの指定」と「オンライン AP へのイメージファイルの展開」を追加しました。 ・「3 章 無線管理の設定」に「 チャネル使用率アラーム閾値の設定」を追加しました。 ・「4 章 WLAN アクセスの設定」に「SSID にもとづくアクセス制御」と「クライアントアソシエーションを許可する SSID の設定」と「ローカル MAC アドレス認証でクライアントアソシエーションを許可する SSID の設定例」を追加しました。 ・誤記訂正
1.14	2022/12	・「2 章 AP 管理」の「AP 管理情報の表示」にコマンドを追加しました。 ・「4 章 WLAN アクセスの設定」の「WLAN アクセスの表示と維持」にクライアントのデバイス情報表示コマンドを追記しました。 ・「4 章 WLAN アクセスの設定」に「ACL にもとづくアクセス制御」と「ACL にもとづくアクセス制御の設定例」を追加しました。 ・「5 章 WLAN セキュリティ」に「WPA3-SAE の SAE 交換時の PWE 生成方式の設定」を追加しました。 ・「5 章 WLAN セキュリティ」の「GTK アップデートの設定」のデフォルト値表記を変更しました。 ・「5 章 WLAN セキュリティ」の「PTK ライフタイムの設定」のデフォルト値表記を変更しました。 ・「5 章 WLAN セキュリティ」に WEP に関する重要事項を記載しました。 ・「9 章 WLAN QoS の設定」に「MU EDCA パラメータの設定」を追加しました。 ・「15 章スペクトル管理」の内容は「17 章 WLAN RRM」に記載されているため「15 章スペクトル管理」を削除しました。 ・「17 章 WLAN RRM の設定」に「最大送信電力の設定」を追加しました。 ・「17 章 WLAN RRM の設定」に「死角検出の設定」を追加しました。 ・「19 章 デュアルリンクバックアップの設定」の「マスタ CAPWAP トンネルの優先接続の設定」の説明を見直しました。 ・「22 章 コンフィグレーションプロファイルの設定」を追加しました。 ・誤記訂正

版数	日付	改版内容
1.15	2023/04	・「1 章 Anchor-AC の設定」の「AC 選出機能の設定」に global configuration view での設定に関する記述を追加しました。 ・「3 章 無線管理の設定」に「サービステンプレートの無線モードの設定」を追加しました。 ・「3 章 無線管理の設定」の「TxBF の設定」のデフォルト値を変更しました。 ・誤記訂正
1.16	2023/06	・「3 章 無線管理の設定」の「TxBF の設定」のデフォルト値を変更しました。・「22 章 コンフィグレーションプロファイルの設定」の「標準 ACL の設定」、「拡張 ACL の設定」、「L2ACL の設定」に、**acl number** *acl-number* 形式での ACL 作成手順を追記しました。 ・「23 章 Web リダイレクトの設定」を追加しました。 ・誤記訂正
1.17	2024/01	・「1 章 Anchor AC の設定」の「AC 選出」に、バックアップ AP が Anchor-AC モードとして起動するための条件を補足しました。 ・「2 章 AP 管理」に「AP の現在のコンフィグの保存」を追加しました。 ・「3 章 無線管理の設定」の「作動チャネルの指定」のレーダ信号検出時の説明を修正しました。 ・「5 章 WLAN セキュリティ」の「WPA3 の設定」に **enterprise-only-mode**、**enterprise-transition-mode** パラメータに関する内容を追記しました。 ・誤記訂正
1.18	2024/06	・「3 章 無線管理の設定」に「レーダチャネルスイッチバックの設定」を追加しました。 ・「10 章 WLAN ローミングの設定」の「WLAN ローミングメカニズム」と「WLAN ローミングの設定例」に「AC 間ローミング」をそれぞれ追加しました。 ・「24 章 IoT 機能の設定」を追加しました。 ・「25 章 Hotspot 2.0 の設定」を追加しました。 ・誤記訂正
1.19	2024/10	・「24 章 IoT 機能の設定」の「24.5.4 ロケーションパケットのフィルタリングの設定」のメモ欄を削除しました。 ・誤記訂正
1.20	2025/03	・「3 章 無線管理の設定」の説明を更新しました。
1.21	2025/06	・「10 章 WLAN ローミングの設定」の「クライアント anti-sticky の設定」に **force-logoff** パラメータのサポートに関するメモ書きを追加しました。 ・「15 章 WLAN 最適化」に「クライアント高速キープアライブの設定」を追加しました。

版数	日付	改版内容
1.22	2025/12	・「2 章 AP 管理」の「AP グループの設定」の AP グループに設定できる IPv4 アドレスによる AP グループルール最大数の説明を更新しました。 誤記訂正
1.23	2026/7	・「8 章 WIPS の設定」に、無線通信と WIPS センサの併用に関するメモを追加しました。 ・「10 章 WLAN ローミングの設定」の「FT を有効にする」に補足を追加しました。 ・「10 章 WLAN ローミングの設定」に、「802.11k の設定」を追加しました。 ・「15 章 WLAN 最適化」の「クライアント高速キープアライブの設定」の記述を修正しました。 「21 章 WLAN メッシュの設定」に、同シリーズ、同バージョンの組み合わせのみをサポートするメモを追加しました。 ・「21 章 WLAN メッシュの設定」に、メッシュを使う Radio では RRM と WIPS を使わないことを推奨するメモを追加しました。 ・誤記訂正
1.24	2026/11	・「4 章 WLAN アクセスの設定」の下記コマンドのデフォルト値のバージョン差分を記載しました。 **・wlan client idle-timeout** 「5 章 WLAN セキュリティ」の下記コマンドの **private-psk** パラメータは未サポートであるため削除しました。 **・akm mode** ・「8 章 WIPS の設定」の、分類ポリシーの設定にメモを追加しました。

Copyright © NEC Corporation 2019 – 2026

All Rights Reserved

事前に NEC の書面による許可なく、本マニュアルをいかなる形式または方法で複製または配布することを禁止します。

商標

本マニュアルに記載されているその他の商標は、各社が保有します。

注意

- Anchor モードの本装置は *QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC コマンドマニュアル*と、セクション 2 WLAN を除く *QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアル*に記載されているコマンドのみ使用することができます。*QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC コマンドマニュアル*と、セクション 2 WLAN を除く *QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアル*に記載されていないコマンドを使用した場合の動作については保証しません。
- 本マニュアルの内容は、予告なく変更されることがあります。本マニュアルのすべての記述、情報、および推奨事項は、明示的か暗黙的かにかかわらず、いかなる種類の保証の対象になりません。

本マニュアルについて

バージョン

本マニュアルに対応する製品バージョンは Anchor モードの Version 7.2.X を含む以降です。

関連マニュアル

次のマニュアルには、QX-W1000/W1100 シリーズアクセスポイントに関する詳細な説明があります

マニュアル	内容
QX-W1000/W1100 シリーズアクセスポイントインスタレーションマニュアル	システムのインストールについて説明しています。
QX-W1000/W1100 シリーズアクセスポイントオペレーションマニュアル	機能の設定について説明しています。
QX-W1000/W1100 シリーズアクセスポイントコマンドマニュアル	機能に関するコマンドについて説明しています。
QX-W1000/W1100 シリーズアクセスポイント Web コンソール操作マニュアル	Web コンソールからの装置設定、状態確認等についての操作を記述しています。
QX-W1000/W1100 シリーズアクセスポイント Anchor-AC オペレーションマニュアル	Anchor-AC として動作させる場合の機能設定について説明しています。
QX-W1000/W1100 シリーズアクセスポイント Anchor-AC コマンドマニュアル	Anchor-AC として動作させる場合の機能に関するコマンドについて説明しています。

マニュアルの構成

このコマンドマニュアルは以下のセクションで構成されます。

- **WLAN**

  Anchor-AC での WLAN 設定について説明します。

  WLAN 以外については QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルを参照してください。

表記規則

本マニュアルでは、次の表記規則を使用しています。

I. コマンド表記規則

表記規則	説明
太字体	コマンドラインを示すキーワードには**太字体**を使用します。
イタリック体	コマンドの引数は*イタリック体*を使用します。
[ ]	大カッコに囲まれた項目(キーワード、引数)はオプションです。
{ x | y | … }	選択する項目は、中カッコに入れて縦線で区切ってあります。1 つを選択します。
[x | y | …]	オプションの選択項目は、大カッコに入れて縦線で区切ってあります。1 つまたは複数を選択します。
{ x | y | … }*	選択する項目は、中カッコに入れて縦線で区切ってあります。少なくとも 1 つ選択できます。
[x | y | …]*	オプションの選択項目は、大カッコに入れて、縦線で区切ってあります。1 つあるいは複数選択することも、何も選択しないこともできます。
&<1-n>	&の前のキーワードと引数を組み合わせます。引数で指定した数までキーワードを繰り返し指定できます。
#	#で始まる行はコメントを示します。

II. GUI 表記規則

表記規則	説明
< >	ボタン名は三角カッコに入っています。例えば、<OK>ボタンをクリックします。
[ ]	ウィンドウ名、メニュー項目、データ表、およびフィールド名は大カッコに入っています。例えば、[New User]ウィンドウが表示されます。
/	複数レベルのメニューはスラッシュで区切ってあります。例えば、[File/Create/Folder]。

III. キーボード操作

表記規則	説明
<KEY>	KEY のキーを押します。例えば、 <Enter>は Enter キーを押します。
<KEY1 + KEY2>	複数のキーを同時に押します。例えば、<Ctrl+Alt+A>は 3 つのキーを同時に押すことを表します。
<KEY1, KEY2>	複数のキーを順番に押します。例えば、 <Alt, A>は 2 つのキーを順に押すことを表します。

IV. マウス操作

表記規則	説明
クリック	マウスのボタンを素早く押します。特に指定がない場合は左ボタンを押します。
ダブルクリック	マウスの左ボタンを素早く 2 回押します。
ドラッグ	マウスの左ボタンを押したまま移動します。

V. 記号

表記規則	説明
⚠ **警告**	表示を無視したり指示に従わない場合、利用者が怪我などをする恐れのある重要な情報を示します。
⚠ **注意**	表示を無視したり指示に従わない場合、データの損失や破損、ハードウェアやソフトウェアの損傷などが発生する恐れのある重要な情報を示します。
⚠ **重要**	注意を払う必要がある情報を示します。
🕮 **メモ**	追加または補足となる情報を示します。
🕮 **ポイント**	参考となる情報を示します。

VI. ネットワークアイコン

表記規則	説明
	ルータ、スイッチ、またはファイアウォールなどの一般的なネットワークデバイスを表しています。
	ルータまたはレイヤ 3 スイッチなどのルーティング対応のデバイスを表しています。
	レイヤ 2、レイヤ 3 スイッチまたはレイヤ 2 転送機能に対応したルータなどの一般的なスイッチデバイスを表しています。

VII. 設定例

本マニュアルの設定例は各機能での代表的な設定例を示します。インタフェース番号、システム名の表記、display コマンドで表示される情報は、ご使用の装置と異なることがあります。

VIII. セキュリティ強化

セキュリティ強化のため、simple で設定されたパスワードも cipher や hash で登録されます。

本マニュアルは以下に示す 25 個のセクションで構成されています。

01-Anchor-AC の設定

02-AP 管理

03-無線管理の設定

04-WLAN アクセスの設定

05-WLAN セキュリティ

06-WLAN 認証の概要

07-WLAN 認証の設定

08-WIPS の設定

09-WLAN QoS の設定

10-WLAN ローミングの設定

11-WLAN ロードバランスの設定

12-WLAN 無線リソースの計測の設定

13-チャネルスキャンの設定

14-バンドナビゲーションの設定

15-WLAN 最適化

16-WLAN IP スヌーピング

17-WLAN RRM の設定

18-WLAN 無線ロードバランス

19-デュアルリンクバックアップの設定

20-WLAN アップリンクの検出設定

21-WLAN メッシュの設定

22-コンフィグレーションプロファイルの設定

23-Web リダイレクトの設定

24-IoT 機能の設定

25-Hotspot 2.0 の設定

目次

1 章 Anchor-AC の設定 1-1
1.1 Anchor-AC の概要 1-1
1.2 ネットワーク構成 1-2
1.3 AC 選出 1-2
1.3.1 Anchor-FIT モードからの AC 選出 1-3
1.3.2 複数の Anchor-AC が存在する場合の AC 選出 1-4
1.4 設定作業リスト 1-5
1.5 AC 選出機能の設定 1-5
1.6 AC 維持機能の設定 1-6
1.7 QX-W1100 シリーズでの QX-W1000 シリーズの管理設定 1-7
1.8 AC 設定の保存 1-8
1.9 Anchor-AC の設定例 1-9
1.9.1 AC 選出機能の設定例 1-9
1.9.2 QX-W1100 シリーズで QX-W1000 シリーズを管理するための設定例 1-10

1章 Anchor-AC の設定

1.1 Anchor-ACの概要

Anchor-AC は、小規模な無線ネットワークでの AP 管理ができます。

各モデルの Anchor-AC でサポートしている管理対象 AP モデルと動作モードを表 1-1 に示します。

表 1-1 各モデルの Anchor-AC でサポートしている管理対象 AP モデルと動作モード

管理対象 AP モデル / Anchor-AC モードの AP モデル	QX-W1010 QX-W1020 QX-W1030	QX-W1110	QX-W1120	QX-W1130
QX-W1030 の場合	Anchor-FIT	管理対象外	管理対象外	管理対象外
QX-W1110 の場合	FIT	Anchor-FIT	Anchor-FIT	Anchor-FIT
QX-W1120 の場合	FIT (v7.2.47 以降でサポート)	Anchor-FIT (v7.2.55 以降でサポート)	Anchor-FIT	Anchor-FIT
QX-W1130 の場合	FIT (v7.2.47 以降でサポート)	Anchor-FIT (v7.2.55 以降でサポート)	Anchor-FIT	Anchor-FIT

メモ：

QX-W1030、QX-W1110、QX-W1120、QX-W1130 のみ Anchor-AC で動作可能です。
Anchor-FIT は QX-W1000/W1100 シリーズのいずれのモデルも動作できます。
Anchor-AC である QX-W1030 が管理できる AP モデルと動作モードは、QX-W1000 シリーズの Anchor-FIT のみです。
Anchor-AC である QX-W1110 が管理できる AP モデルと動作モードは、QX-W1100 シリーズの Anchor-FIT および QX-W1000 シリーズの FIT です。
Anchor-AC である QX-W1120 および QX-W1130 が管理できる AP モデルと動作モードは、以下の通りです。

- ソフトウェアバージョン 7.2.55 を含む以降のソフトウェアでは、QX-W1100 シリーズの Anchor-FIT および QX-W1000 シリーズの FIT を管理できます。
- ソフトウェアバージョン 7.2.47 を含む以降のソフトウェアでは、QX-W1120、QX-W1130 の Anchor-FIT および QX-W1000 シリーズの FIT を管理できます。
- ソフトウェアバージョン 7.2.44 を含む以前のソフトウェアでは QX-W1120、QX-W1130 の Anchor-FIT のみを管理できます。

モードの詳細は QX-W1000/W1100 シリーズ アクセスポイント インスタレーションマニュアルの *“ソフトウェアのアップグレード”* を参照してください。

Anchor-AC は、Anchor-FIT と同様に自身を管理するために自動的に内部 AP を生成します。内部 AP の AP 名には初期値として Anchor-AC 自身の MAC アドレスが使用されますが、**wlan rename-ap** コマンドで名称を変更できます。

1.2 ネットワーク構成

図 1-1 は、AP が配置されている一般的な無線ネットワークを示しています。

AC 選出機能を設定したバックアップ AP である Anchor-FIT は、Anchor-AC と同一セグメントに存在するように環境構築する必要があります。

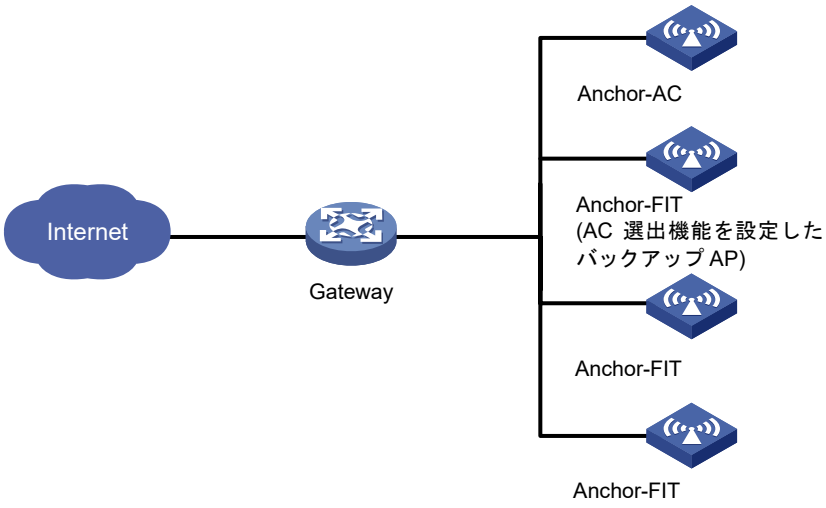


図 1-1 WLAN アクセスプロセス

1.3 AC選出

ネットワーク内の AP を管理するために Anchor-AC を選択する必要があります。Anchor-AC モードとして機能できるのは同一ネットワーク内に 1 台のみです。AC 選出機能を有効にすることで、Anchor-FIT モードの AP は Anchor-AC のバックアップ AP となり、Anchor-AC モードの AP が存在しない場合に、自動的に Anchor-AC モードとして起動しなおします。ただし、AC 選出機能のバックアップ AP が Anchor-AC モードとして起動するには、バックアップ AP が Anchor-AC に管理される（CAPWAP 通信が開始される）必要があります。

🕮 **メモ：**

QX-W1010 および QX-W1020 は AC 選出に参加できません。

1.3.1 Anchor-FIT モードからの AC 選出

AC 選出機能を有効にしたすべての AP は、接続可能な Anchor-AC が検出されない場合、AC 選出に参加します。AC 選出時に複数の AP で AC 選出機能が有効な場合、MAC アドレスが最も小さい AP が Anchor-AC として選出されます。AC 選出機能の設定をサポートしている AP モデルは、Anchor-AC モードの AP モデルによって異なります。Anchor-AC のバックアップ候補として AC 選出機能を設定可能な AP モデルを表 1-2 に示します。

表 1-2 AC 選出機能（バックアップ AP）のサポート対応表

管理対象 / AP モデル / Anchor-AC モードの AP モデル	QX-W1030	QX-W1110	QX-W1120	QX-W1130
QX-W1030 の場合	AC 選出機能設定可	管理対象外	管理対象外	管理対象外
QX-W1110 の場合	AC 選出機能設定禁止	AC 選出機能設定可	AC 選出機能設定禁止	AC 選出機能設定禁止
QX-W1120 の場合	AC 選出機能設定禁止	AC 選出機能設定禁止	AC 選出機能設定可	AC 選出機能設定可
QX-W1130 の場合	AC 選出機能設定禁止	AC 選出機能設定禁止	AC 選出機能設定可	AC 選出機能設定可

注意：

QX-W1100 シリーズのバージョン 7.2.47 を含む以降のソフトウェアでは、QX-W1000 シリーズを管理できますが、QX-W1100 シリーズで QX-W1000 シリーズを管理する際にサポートするモードは FIT モードです。QX-W1000 シリーズに対して AC 選出機能を設定しないでください。
誤って Anchor-FIT モードの QX-W1000 シリーズを管理した場合、管理状態での動作は問題ありませんが、誤設定した AC 候補設定によって Anchor-AC 不在時に QX-W1030 が Anchor-AC に切り替わってしまいます。また、Anchor-AC のバージョンアップ時に QX-W1000 シリーズで FIT 用ソフトウェアのための空き容量不足になり、バージョンアップに失敗する場合があります。

図 1-2 に示すように、AC 選出では以下のプロセスが実行されます。

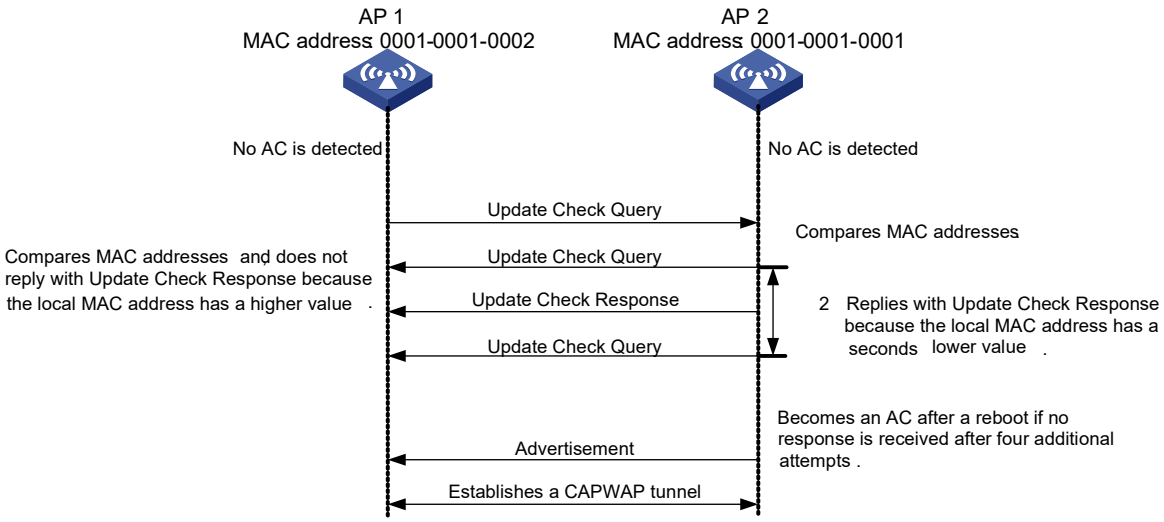


図 1-2 ネットワーク図

1) AP1 と AP2 は、それぞれ Update Check Query パケットをブロードキャストします。
2) 互いに Update Check Query パケットを受信すると、AP はそれぞれ、パケット内の MAC アドレスとローカル MAC アドレスを比較します。
   - AP2 のローカル MAC アドレスの値が、受信した AP1 の MAC アドレスの値よりも小さいため、AP2 が Anchor-AC として選出されます。AP2 は、Update Check 応答パケットを AP1 に送信し、Anchor-AC として動作することを通知します。
   - AP1 のローカル MAC アドレスの値は、受信した AP2 の MAC アドレスの値よりも大きいため、AP1 は Anchor-AC として選出されません。AP1 は、受信した Update Check Query パケットに応答せず、Update Check Query パケットの送信も停止します。
3) AP2 は、Update Check Query パケットを 2 秒ごとに 4 回ブロードキャストします。応答がない場合は、自動再起動後に AP2 が Anchor-AC になります。
4) AP2 は、Anchor-AC として動作していることをネットワークに通知するために、2 秒ごとにアドバタイズメントパケットをブロードキャストします。他の AP を Anchor-AC に接続するには、Anchor-AC で手動 AP を設定するか、自動 AP を有効にします。
5) AP1 は、受信したアドバタイズメントパケットに応答する形で、Anchor-AC を発見するための検出要求パケットをブロードキャストし、Anchor-AC との CAPWAP トンネルを確立します。

Anchor-AC がオフラインになった場合は、他の AP の AC 選出機能を有効にして、新しい Anchor-AC を確実に選択できるようにする必要があります。AC 選出機能の設定の詳細は QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“AC の設定”* の *“AC 選出機能の設定”* を参照してください。

1.3.2 複数の Anchor-AC が存在する場合の AC 選出

次の条件が満たされる場合、Anchor-AC として動作する 2 台の AP が WLAN に存在します。

- Anchor-AC がオフラインになり、新しい Anchor-AC が選出されたあと、オフラインになっていた Anchor-AC が、再びオンラインになります。
- Anchor-AC が存在するネットワークに、誤って別の Anchor-AC を接続します。

このシナリオでは、次のプロセスを使用して新しい Anchor-AC の選出が行われます。

1) 互いにアドバタイズメントパケットを受信すると、2 つの Anchor-AC はそれぞれ、パケット内の MAC アドレスとローカル MAC アドレスを比較します。
2) 大きい MAC アドレスを持つ Anchor-AC が再起動し、Anchor-FIT モードに切り替わり、小さい MAC アドレスを持つ Anchor-AC に接続します。Anchor-FIT モードに切り替わったあと、他の AP は、新しい Anchor-AC に再度関連付けられます。

1.4 設定作業リスト

作業リスト
（オプション設定項目）AC選出機能の設定
（オプション設定項目）AC維持機能の設定
（オプション設定項目）QX-W1100シリーズでのQX-W1000シリーズの管理設定
（必須設定項目） AC設定の保存

1.5 AC選出機能の設定

注意：

- **map-configuration** コマンドを使用している場合、AC 選出機能を有効にする AP にも"mpcfg"形式のファイルを格納してください。
- QX-W1100 シリーズのバージョン 7.2.47 を含む以降のソフトウェアでは、QX-W1100 シリーズの Anchor-AC で QX-W1000 シリーズを管理できますが、QX-W1100 シリーズで QX-W1000 シリーズを管理する際にサポートするモードは FIT モードです。QX-W1000 シリーズに対して AC 選出機能を設定しないでください。
- global configuration view での AC 選出機能の設定は、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。

以下に AP view での AC 選出機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 手動 AP を作成し、その AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし AP viewを作成する場合、モデルを指定してください。

操作	コマンド	補足
3． AC 選出機能を設定する	**anchor-ap** { **disable** | **enable** }	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.59を含む以前のソフトウェアでは無効です。 ソフトウェアバージョン 7.2.63を含む以降のソフトウェアでは、global configuration viewの設定を使用します。

以下に global configuration view での AC 選出機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**global configuration view**	—
3． AC 選出機能を設定する	**anchor-ap** { **disable** | **enable** }	デフォルト：無効

1.6 AC維持機能の設定

🕮 **メモ：**

- 本機能はソフトウェアバージョン 7.2.21 を含む以降のソフトウェアからサポートしています。
- “**wlan anchor-ap persistent-mode ac**”コマンドは“**save**”コマンドにて管理下の AP には保存されません。“**save**”コマンドの詳細は QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“Anchor-AC の設定”* の *“AC 設定の保存”* を参照してください。

I. AC 維持機能について

本機能を使用した場合、ネットワーク内に複数の Anchor-AC が存在する状況が発生した際、AC 維持機能を設定している Anchor-AC のみ MAC アドレスに関わらず Anchor-AC モードを維持できます。

本機能を使用しない場合、ネットワーク内に複数の Anchor-AC が存在する状況が発生してしまった際、MAC アドレスが最小の Anchor-AC のみ Anchor-AC モードを維持し、その他は Anchor-FIT モードとして再起動します。

II. 設定手順

以下に AC 維持機能の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AC 維持機能を設定する	**wlan anchor-ap persistent-mode ac**	デフォルト：設定なし

1.7 QX-W1100シリーズでのQX-W1000シリーズの管理設定

⚠ **注意**：

- QX-W1100 シリーズで QX-W1000 を管理する際にサポートするモードは、FIT モードです。誤って Anchor-FIT モードの QX-W1000 を管理した場合、管理状態での動作は問題ありませんが、誤設定した AC 候補設定によって Anchor-AC 不在時に QX-W1030 が Anchor-AC に切り替わってしまいます。また、Anchor-AC のバージョンアップ時に QX-W1000 で FIT 用ソフトウェアのための空き容量不足になり、バージョンアップに失敗する場合があります。
- QX-W1100 シリーズで QX-W1000 を 1 台でも管理する場合は、管理 AP 台数が 51 台(Anchor-AC 自身を含む)を超えないように設定してください。

I. QX-W1100 シリーズでの QX-W1000 シリーズの管理について

QX-W1100 シリーズで QX-W1000 シリーズを管理する設定がされているとき、異なるバージョンの QX-W1000 シリーズの AP が接続された場合、ソフトウェアバージョンを同一にするために、QX-W1100 シリーズは QX-W1000 シリーズに対してソフトウェアを自動的に配布します。

ただし、QX-W1100 用のソフトウェアには QX-W1000 FIT 用のソフトウェアは含まれませんので、QX-W1100 シリーズのディレクトリに FTP/TFTP 等で事前に QX-W1000 FIT 用のソフトウェアを格納してください。

II. Anchor-AC から Anchor-FIT へのファイル転送について

AC 選出機能を有効にする場合、Anchor-AC 候補の Anchor-FIT に対しても QX-W1000 シリーズの FIT 用ソフトウェア（ファイル名：qx-w1000-fit.ipe）を格納する必要があります。**download file** コマンドを使用して、AC 選出候補の Anchor-FIT に対してソフトウェアを転送してください。

以下にファイル転送の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 手動 AP を作成し、その AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし AP viewを作成する場合、モデルを指定してください。
3． Anchor-FIT にファイルを転送する	**download file** *file-name*	転送するファイルと同じ名称のファイルがAnchor-FITにすでに存在する場合、ファイルの転送に失敗します。

操作	コマンド	補足
4.　（オプション設定項目）Anchor-FIT のファイルを削除する	**delete file** *file-name*	Anchor-FITに「qx-w1000-fit.ipe」がすでに存在しており、**download file**コマンドでのファイル転送に失敗する場合は、本コマンドを使用して「qx-w1000-fit.ipe」を削除してください。
5.　（オプション設定項目）Anchor-FIT のファイルを確認する	**display wlan ap name** *ap-name* **files**	このコマンドはソフトウェアバージョン7.2.49を含む以降のソフトウェアからサポートしています。

⚠ **注意：**

- 転送するソフトウェアのバージョンはAnchor-ACのバージョンに揃えてください。また、ファイル名は「qx-w1000-fit.ipe」のファイルである必要があります。
- 「qx-w1000-fit.ipe」が Anchor-FIT にすでに存在する場合、Anchor-AC はファイル転送に失敗します。**delete file** コマンドを使用して「qx-w1000-fit.ipe」を削除した後、**download file** コマンドでソフトウェアを転送してください。

1.8 AC設定の保存

AP を管理した状態で“**save**”コマンドを実行すると、Anchor-AC 本体および、管理下のすべての AP に Anchor-AC の設定が保存されます。これにより、動作中の AC がオフラインになったあと、AC 選出機能により新しく選出された Anchor-AC が設定を引き継ぎます。AC 選出機能の詳細は QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“Anchor AC の設定”* の *“AC 選出”* を参照してください。

操作	コマンド
1.　system view に移行する	**system-view**
2.　Anchor-AC の設定を管理下のすべての AP に保存する	**save**

🕮 **メモ：**

- Anchor-AC の設定は管理下の QX-W1010 および QX-W1020 には保存されません。v7.2.21 を含む以前のバージョンでは、**save** 実行時に QX-W1010 および QX-W1020 への設定の保存に失敗したことを示す Fail メッセージが表示されますが、運用に問題はありません。V7.2.27 を含む以降のバージョンでは、**anchor-ap enable** が設定された Anchor-FIT にのみ Anchor-AC の設定を保存します。
- “**wlan anchor-ap persistent-mode ac**”コマンドは、管理下のいずれの Anchor-FIT にも保存されません。“**wlan anchor-ap persistent-mode ac**”コマンドの詳細は QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“Anchor-AC の設定”* の *“AC 維持機能の設定”* を参照してください。

1.9 Anchor-ACの設定例

1.9.1 AC 選出機能の設定例

I. ネットワーク要件

図 1-3 に示すように、AP1 は Anchor-AC モードであり、AP2、AP3、AP4 を手動 AP として管理しています。

AP1 がオフラインになったとき、AP2 が再起動して Anchor-AC に切り替わるように、以下のタスクを実行します。

- AC 選出機能を AP2 で有効にします。
- Anchor-AC（AP1）の設定を次のスタートアップコンフィグレーションファイルとして AP2 に保存します。

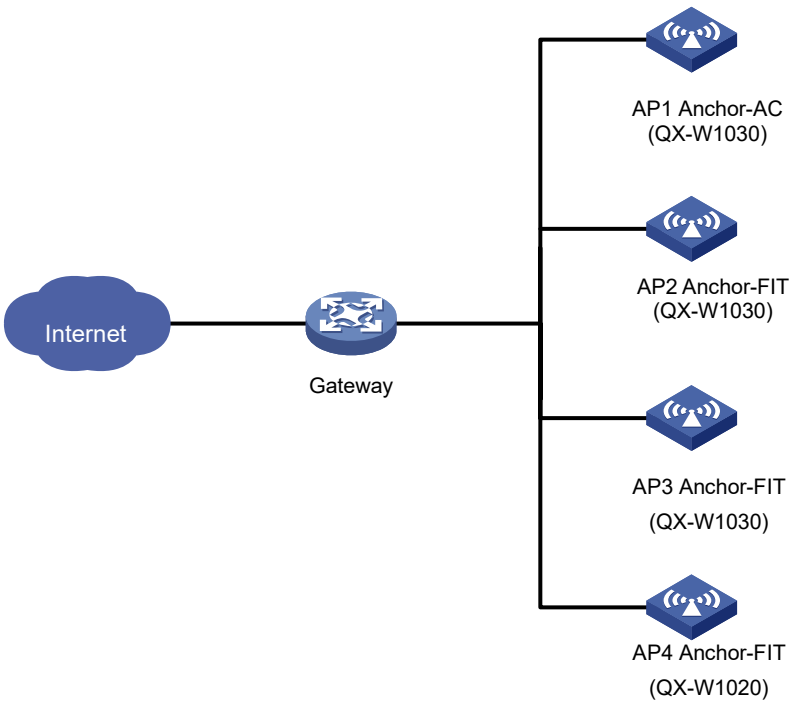


図 1-3 ネットワーク図

II. 設定手順

AP **ap2** に対して AC 選出機能を有効にします。

```
<AC> system-view
[AC] wlan ap ap2 model QX-W1030
[AC-wlan-ap-ap2] anchor-ap enable
[AC-wlan-ap-ap2] quit
```

Anchor-AC（AP1）に AC 維持機能を有効にします。

```
[AC] wlan anchor-ap persistent-mode ac
```

Anchor-AC（AP1）の設定を、次のスタートアップコンフィグレーションファイルとして AP2 に保存します。

```
[AC] save
```

III. 設定の確認

Anchor-AC（AP1）がオフラインになったときに AP2 が Anchor-AC として起動することを確認します 。

```
<AP2> display wlan ap all
Total number of APs: 3
Total number of connected APs: 2
Total number of connected manual APs: 2
Total number of connected auto APs: 0
Total number of connected common APs: 2
Total number of connected WTUs: 0
Total number of inside APs: 1
Maximum supported APs: 50
Remaining APs: 48
Total AP licenses: 50
Local AP licenses: 50
Server AP licenses: 0
Remaining Local AP licenses: 48
Sync AP licenses: 0
                              AP information
 State : I = Idle,       J  = Join,       JA = JoinAck,     IL = ImageLoad
         C = Config,     DC = DataCheck,  R  = Run    M = Master,  B = Backup
AP name                 AP ID   State   Model            Serial ID
ap3                     2       R/M     QX-W1030         219801A1JY8184E0002N
ap4                     3       R/M     QX-W1020         219801A1JY8184E0003N
48bd-3d66-2940          1       R/M     QX-W1030         219801A1K09182G0000R
```

1.9.2 QX-W1100 シリーズで QX-W1000 シリーズを管理するための設定例

🕮 メモ：

QX-W1100 シリーズのバージョン 7.2.47 を含む以降のソフトウェアでは、QX-W1100 シリーズでの QX-W1000 シリーズの FIT 管理をサポートしています。

I. ネットワーク要件

図 1-4 に示すように、AP1 は Anchor-AC モードであり、AP2、AP3、AP4 を手動 AP として管理しています。

AP1 がオフラインになったとき、AP2 が再起動して Anchor-AC に切り替わるように、以下のタスクを実行します。

- AC 選出機能を AP2 で有効にします。
- Anchor-AC（AP1）の設定を次のスタートアップコンフィグレーションファイルとして AP2 に保存します。

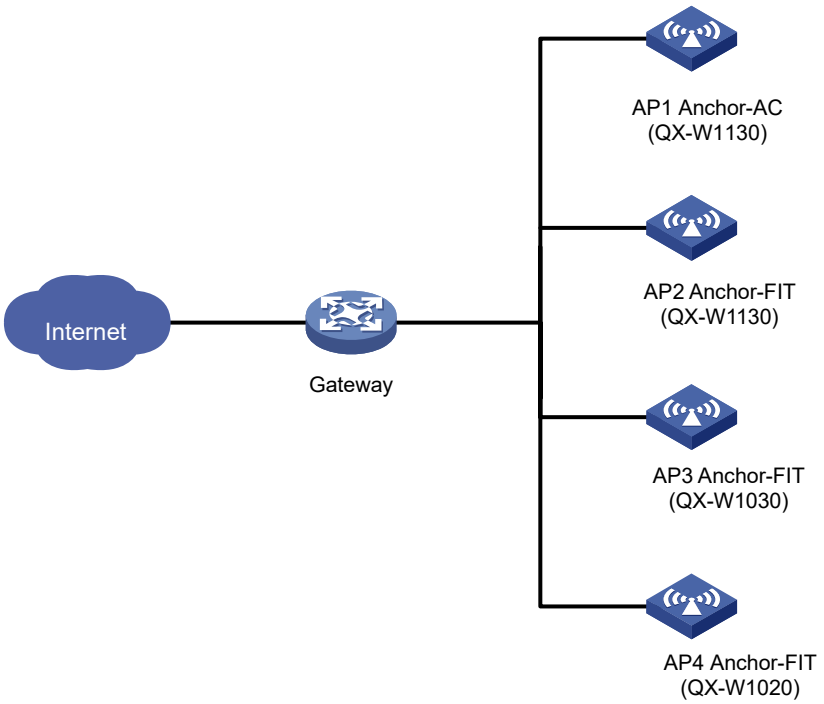


図 1-4 ネットワーク図

II. 設定手順

Anchor-AC（AP1）のディレクトリに QX-W1000 シリーズ FIT 用ソフトウェア（ファイル名：qx-w1000-fit.ipe）を格納します。（詳細は省略します）

```
TFTP を使用した例
<AC> tftp 192.168.1.60 get qw-w1000-fit.ipe
```

AP **ap2** を管理するために AP view を作成し、シリアル ID を設定します。

```
<AC> system-view
[AC] wlan ap ap2 model QX-W1130
[AC-wlan-ap-ap2] serial-id 219801A2EJ8214E0000R
```

AP **ap2** に対して AC 選出機能を有効にします。

```
[AC-wlan-ap-ap2] anchor-ap enable
```

AP **ap2** に対して QX-W1000 シリーズの FIT 用ソフトウェア（ファイル名：qx-w1000-fit.ipe）を転送します。転送するファイル名は「qx-w1000-fit.ipe」から変更しないでください。

```
[AC-wlan-ap-ap2] download file flash:/qx-w1000-fit.ipe
[AC-wlan-ap-ap2] quit
```

Anchor-AC（AP1）に AC 維持機能を有効にします。

```
[AC] wlan anchor-ap persistent-mode ac
```

QX-W1000 シリーズの AP **ap3** を管理するために AP view を作成し、シリアル ID を設定します。

```
[AC] wlan ap ap3 model QX-W1030
[AC-wlan-ap-ap3] serial-id 219801A1R78187E00009
[AC-wlan-ap-ap3] quit
```

同様に、QX-W1000 シリーズの AP **ap4** を管理するために AP view を作成し、シリアル ID を設定します。（詳細は省略します。）

Anchor-AC（AP1）の設定を、次のスタートアップコンフィグレーションファイルとして AP2 に保存します。

```
[AC] save
```

III. 設定の確認

Anchor-AC（AP1）がオフラインになったときに AP2 が Anchor-AC として起動することを確認します 。

```
<AP2> display wlan ap all
Total number of APs: 4
Total number of connected APs: 2
Total number of connected manual APs: 2
Total number of connected auto APs: 0
Total number of connected common APs: 2
Total number of connected WTUs: 0
Total number of inside APs: 1
Maximum supported APs: 100
Remaining APs: 98
Total AP licenses: 100
Local AP licenses: 100
Server AP licenses: 0
Remaining Local AP licenses: 98
Sync AP licenses: 0

                                AP information
 State : I = Idle,      J  = Join,        JA = JoinAck,     IL = ImageLoad
         C = Config,    DC = DataCheck,   R  = Run,    M = Master,  B = Backup

AP name                       APID  State Model           Serial ID
ap2                           3     R/M   QX-W1130        219801A2EJ8214E0000R
ap3                           4     R/M   QX-W1030        219801A1R78187E00009
ap4                           5     R/M   QX-W1020        219801A1JY8182E0002Y
882a-5f6c-4e60                1       I   QX-W1130        219801A2GH8212E00009
```

目次

2 章 AP 管理 2-1
2.1 概要 2-1
2.1.1 CAPWAP トンネル 2-1
2.1.2 AP 設定方式 2-3
2.1.3 APDB 2-3
2.1.4 プロトコルと基準 2-4
2.2 設定操作リスト 2-4
2.3 設定要件 2-4
2.4 CAPWAP トンネルの確立 2-5
2.4.1 手動 AP の作成 2-5
2.4.2 自動 AP の管理 2-5
2.4.3 自動 AP から手動 AP への切り替え設定 2-6
2.4.4 検出応答タイムアウトタイマの設定 2-6
2.4.5 ユニキャスト検出要求のみ応答する AC の設定 2-7
2.5 AP のソフトウェアのアップグレード 2-7
2.5.1 概要 2-7
2.5.2 ソフトウェアのアップグレードの設定 2-7
2.5.3 AC が AP イメージファイルを取得するための優先ロケーションの指定 2-8
2.5.4 オンライン AP へのイメージファイルの展開 2-9
2.6 AP の VLAN 設定 2-10
2.6.1 VLAN の基本設定 2-10
2.6.2 ポートベース VLAN の設定 2-11
2.7 信頼されたパケットプライオリティタイプの設定 2-15
2.8 ポートプライオリティの設定 2-17
2.9 リモート設定の割り当て設定 2-18
2.10 AP グループの設定 2-19
2.10.1 設定の制限とガイドライン 2-19
2.10.2 AP group の作成 2-20
2.11 CAPWAP トンネルの設定 2-20
2.11.1 CAPWAP トンネル暗号化 2-20
2.11.2 CAPWAP トンネルの待ち時間検出の設定 2-21
2.11.3 AP に対する制御トンネルの keepalive 時間の設定 2-22
2.11.4 AP に対するデータトンネルの keepalive 時間の設定 2-23
2.11.5 CAPWAP パケットの最大フラグメントサイズの設定 2-23
2.12 AC 要求の再送信の設定 2-24
2.13 統計情報報告間隔の設定 2-24
2.14 AP 保守 2-25
2.14.1 AP のリセット 2-25
2.14.2 手動 AP の名前の変更 2-25
2.14.3 AP のファイルシステムの管理 2-25
2.14.4 AP の現在のコンフィグの保存 2-26
2.14.5 LED 点灯モードの設定 2-26
2.15 SNMP 通知の有効化 2-27
2.16 AP 管理の応用設定 2-27

2.16.1 リモート AP の設定 2-27
2.16.2 APDB ユーザスクリプトのローディング 2-28
2.17 AP 管理の表示と維持 2-29
2.17.1 AP 管理情報の削除 2-30
2.18 AP 管理の設定例 2-30
2.18.1 DHCP を通した CAPWAP トンネル確立の設定例 2-30
2.18.2 DNS を通した CAPWAP トンネル確立の設定例 2-34
2.18.3 自動 AP の設定例 2-39
2.18.4 AP group の設定例 2-43

2章 AP 管理

2.1 概要

数多くの AP（Access Point）を管理するのは、時間を浪費しコストもかかります。AP＋AC 適合ネットワーク構築により、AC は数多くの AP を有する CAPWAP（Control And Provisioning of Wireless Access Points）トンネルを確立でき、集約した AP の管理と保守が可能となります。

2.1.1 CAPWAP トンネル

CAPWAP は、AP と AC の通信方法を定義します。CAPWAP は、AP と AC 間に包括的なカプセル化とトランスポート構造を提供します。CAPWAP は UDP を使用し、IPv4 をサポートします。

図 2-1 に示すように、AC と AP は、データパケットを転送するためにデータトンネルを確立します。また、制御パケットを転送するために、制御トンネルを確立します。

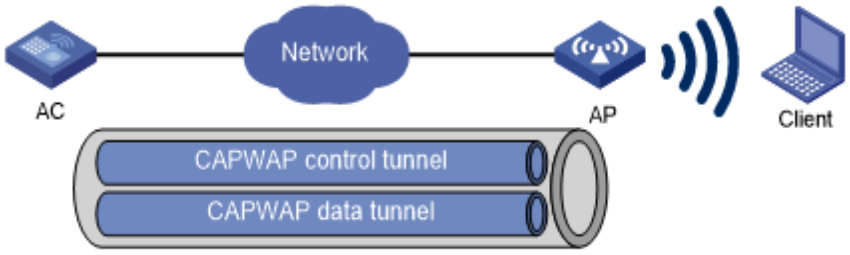


図 2-1 CAPWAP トンネル

I. AC 検出

使用するコンフィグレーションファイルが設定されていない状態で、AP は自動的に VLAN-interface1 を作成し、インタフェース上で DHCP クライアント、DHCPv6 クライアント、DNS 機能を使用可能にします。その後、DHCP サーバから自身の IP アドレスを取得し、以下の手法を用いて AC を検出します。

- DHCP オプション

  AP は、Option 138 および Option 43 から AC の IPv4 アドレスを取得します。IPv4 アドレスは後の操作で使用します。

  DHCP オプションに関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 5 *IP サービス "DHCP"* を参照してください。

- DNS

a) APはDHCPサーバからドメイン名のサフィックスを取得します。

b)　APは、取得したサフィックスをホスト名に追加します。

c)　DNSサーバは、ドメイン名をIPアドレスに変換します。

DNS に関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 5 *IP サービス　"DNS"* を参照してください。

- ブロードキャスト

  AP は AC を検出するために、IP アドレス 255.255.255.255 に対してブロードキャスト検出要求を送信します。

- IPv4 マルチキャスト

  AP は AC を検出するために、IPv4 アドレス 224.0.1.140 に対してマルチキャスト検出要求を送信します。

AP は、検出した AC の 1 つとの CAPWAP トンネルを確立するまで AC 検出を停止しません。

II. CAPWAP トンネル確立

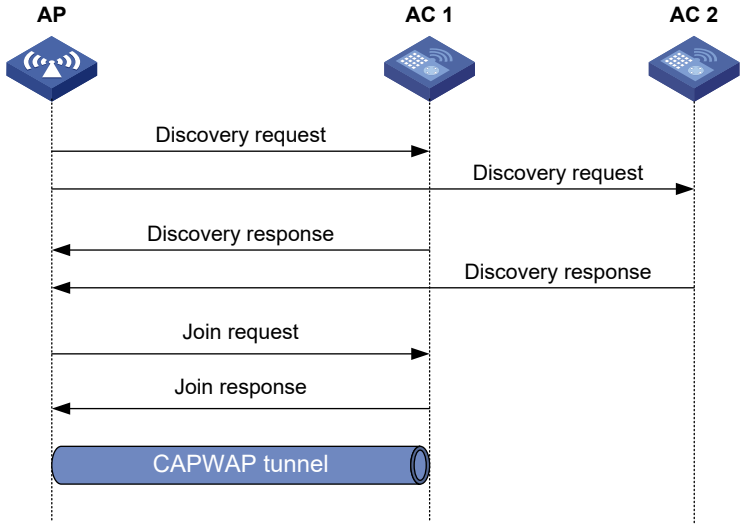


図 2-2 CAPWAP トンネルの確立

図 2-2 に示すように、AP と AC は、以下の手順で CAPWAP トンネルを確立します。

1)　AP は AC を検出するために、各 AC に対して検出要求を送信します。
2)　検出要求を受信したあと、各 AC は、自身のローカル設定と要求内の情報にもとづき、検出応答を送信するかどうか決定します。

a)　検出要求がユニキャストパケットかどうかを識別します。

- **ユニキャストパケット**－AC はステップ B に進みます。
- **ブロードキャストあるいはマルチキャストパケット**－ユニキャスト検出要求のみ応答する機能が無効の場合、AC はステップ B に進みます。ユニキャスト検出要求のみ応答する機能が有効の場合、AC は検出応答を送信しません。

b)　検出要求で指定されたACモデルで手動APの設定があるかどうかを識別します。

- 手動 AP の設定が存在する場合、AC は AP に検出応答を送信します。検出応答には、AP で手動設定があるかどうかの情報、AP の接続優先度、AC の負荷状態が含まれます。
- 手動 AP の設定が存在する場合、AC はステップ C に進みます。

c) 自動APが有効かどうかを識別します。

- 自動 AP が有効の場合、AC は AP に検出応答を送信します。検出応答には、自動 AP の有効化機能の状態、AP の接続優先度、AC の負荷状態が含まれます。
- 自動 AP が無効の場合、AP は検出応答を送信しません。

3) 検出応答を受信すると、AP は下記の順に条件を比較し、最適な AC を選択します。

- 1. AP に関する情報を保存している AC
- 2. 自動 AP 機能が有効な AC
- 3. AP 接続の優先度が高い AC
- 4. 管理している AP 数が少ない AC

4) AP は、AC に対して参加要求を送信します。
5) 参加要求を受信したあと、AC は AP に対してアクセスサービスを提供するかどうかを決定するために、要求内の情報を調査し、参加応答を送信します。
6) 参加応答を受信したあと、AP は応答内のリザルトコードを調査します。

- リザルトコードが失敗と表示された場合、AP は AC との CAPWAP トンネルを確立しません。
- リザルトコードが成功と表示された場合、AP は AC との CAPWAP トンネルを確立します。

2.1.2 AP 設定方式

以下のいずれかの方式で AP を設定することができます。

- AP view で 1 つずつ AP を設定します。
- AP グループに AP を割り当て、AP group view の AP グループを設定します。
- global configuration view ですべての AP を設定します。

AP の設定の優先度は、AP view、AP group view、global configuration view の順番で優先されます。

2.1.3 APDB

AC の APDB（Access Point Information Database）は以下の AP 情報を記録します。

- AP のモデル名
- ハードウェアバージョン、ソフトウェアバージョンの対応表
- AP モデル名でサポートされる無線情報
  - □ 無線数
  - □ 無線タイプ
  - □ 有効な region code
  - □ 有効なアンテナタイプ
  - □ 最大出力電力

APDB に対応する AP モデル情報が含まれるときのみ、AC は AP と CAPWAP トンネルを確立することができます。

APDB のデータを管理するため、システムスクリプトとユーザスクリプトを使用することができます。システムスクリプトは AC のソフトウェアによってリリースされます。AC

が起動するたびに自動で読み込まれます。新しい AP モデルを追加する場合、以下の作業が必要となります。

- AP ソフトウェアバージョンをアップグレードします。（AP ソフトウェアバージョンについては QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 1 *はじめに*を参照してください。）
- ユーザスクリプトを作成します。
- AC でスクリプトを読み込ませます。（QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“AP 管理”の“APDB ユーザスクリプトのローディング”* を参照してください。）

2.1.4 プロトコルと基準

- RFC 5415, *Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification*
- RFC 5416, *Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11*
- RFC 5417, *Control And Provisioning of Wireless Access Points (CAPWAP) Access Controller DHCP Option*

2.2 設定操作リスト

操作リスト
（必須設定項目）CAPWAPトンネルの確立
（オプション設定項目）APのソフトウェアのアップグレード
（オプション設定項目）APのVLANの設定
（オプション設定項目）APグループの設定
（オプション設定項目）CAPWAPトンネルの設定
（オプション設定項目）AC要求の再送信の設定
（オプション設定項目）統計情報報告間隔の設定
（オプション設定項目）AP保守
（オプション設定項目）SNMP通知の有効化
（オプション設定項目）AP管理の上級機能の設定

2.3 設定要件

AP を管理する前に、以下の操作を完了しなければなりません。

- AP に IP アドレスを割り当てるために、DHPC サーバ上で DHCP アドレスプールを作成します。
- DHCP オプションを AC 検出に使用する場合、DHCP サーバ上の特定の DHCP アドレスプール内に、Option 138、Option 43、または Option 52 を設定します。
- DNS を AC 検出に使用する場合、DHCP サーバ上の特定の DHCP アドレスプール内に、DNS サーバの IP アドレスと AC ドメイン名のサフィックスを設定します。その後、DHCP サーバ上でドメイン名と AC IP アドレス間のマッピングを設定します。
- AP と AC が互いに通信可能なことを確認します。

DHCP と DNS に関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 5 *IP サービス “DHCP”、“DNS”* を参照してください。

2.4 CAPWAPトンネルの確立

2.4.1 手動 AP の作成

手動 AP は、手動でのみ作成、削除、修正が可能です。手動 AP は、手動 AP コンフィグレーションを保存した AC で CAPWAP トンネルを確立することを優先します。

以下に手動 AP の設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 手動 AP を作成し、手動 AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：手動APは存在しません。 APを作成するときは、モデル名を指定しなければなりません。
3． AP に対してシリアル ID または MAC アドレスを指定する	● APに対してシリアルIDを指定する： **serial-id** *serial-id* ● APに対してMACアドレスを指定する： **mac-address** *mac-address*	いずれかのコマンドを使用します。
4． （オプション設定項目） AP に対して記述を設定する	**description** *text*	デフォルト：設定なし

2.4.2 自動 AP の管理

I. 自動 AP 機能の概要

自動 AP 機能を有効にすることで、AC に手動 AP の設定をしなくても AP は AC と接続できるようになります。本機能により、WLAN で多くの AP を配置する際の設定が単純化されます。

II. 制限とガイドライン

不正な AP が AC に関連付くのを防ぐために、必要な AP がすべて AC に関連付いた後は自動 AP 機能を無効にしてください。

自動 AP がすべてオンラインになったら、手動 AP に切り替えてください。

自動 AP を手動 AP に切り替えない場合、

- AC が再起動したとき、または CAPWAP トンネルが切断されたとき、AP は AC に再関連付けされません。
- 個別に AP の設定を行うことができません。

III. 自動 AP 機能の設定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 自動 AP 機能を有効にする	**wlan auto-ap enable**	デフォルト：無効

2.4.3 自動 AP から手動 AP への切り替え設定

自動 AP を手動 AP に変換するために本操作を実行します。

以下に自動 AP から手動 AP への切り替え手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 自動 AP パーシステンスを設定する	● オンライン自動APを手動APに変換する： **wlan auto-ap persistent** { **all** | **name** *auto-ap-name* [*new-ap-name*] } ● 自動APがオンラインになったあと、自動的に自動APを手動APに変換する： **wlan auto-persistent enable**	いずれかのコマンドを使用します。 すでにオンラインの自動APに対しては、**wlan auto-persistent enable** コマンドは適用しません。

2.4.4 検出応答タイムアウトタイマの設定

I. 検出応答タイムアウトタイマの概要

検出応答タイムアウトタイマとは、AP が別の検出応答を待つために指定するタイマです。AP が検出応答パケットを受け取ると、検出応答タイムアウトタイマが作成または更新されます。タイムアウトタイマが終了する時、AP は最適な AC に対して参加要求を送信します。

II. 制限とガイドライン

ネットワーク状態がよくない場合、検出応答タイムアウトタイマを長めに設定してください。

III. 設定手順

以下に AP view での検出応答タイムアウトタイマの設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． 検出応答タイムアウトタイマを設定する	**discovery-response wait-time** *seconds*	デフォルト：APはAP group viewの設定を使用します。

以下に AP group view での検出応答タイムアウトタイマの設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． 検出応答タイムアウトタイマを設定する	**discovery-response wait-time** *seconds*	デフォルト：2秒

2.4.5 ユニキャスト検出要求のみ応答する AC の設定

AP は、検出した AC に対してユニキャスト、マルチキャスト、ブロードキャスト検出要求を送信できます。本機能により、AC はユニキャスト検出要求に対してのみ応答することができるようになります。

以下に AC にユニキャスト検出要求のみに応答させる設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． ユニキャスト検出要求に対してのみ応答する AC を設定する	**wlan capwap discovery-policy unicast**	デフォルト：ACは、ユニキャスト、マルチキャスト、ブロードキャスト検出要求に応答できます。

2.5 APのソフトウェアのアップグレード

2.5.1 概要

AP のソフトウェアのアップグレードは以下の手順で行われます。

1) AP は AC にソフトウェアバージョン、AP モデル情報を通知します。
2) AC は受信した AP のソフトウェアバージョンを確認します。
   - □ バージョンが同一である場合、AC は AP と CAPWAP トンネルを確立します。
   - □ バージョンが異なる場合、AC は AP に AP ソフトウェアバージョンの不一致を通知するメッセージを送信します。
3) 不一致を通知するメッセージを受信すると、AP は AC からソフトウェアバージョンを要求します。
4) AP からリクエストを受信したあと、AC は AP にソフトウェアバージョンを割り当てます。
5) AP はソフトウェアバージョンをアップグレードし、AC との CAPWAP トンネルを再確立します。

2.5.2 ソフトウェアのアップグレードの設定

ソフトウェアのアップグレード機能が有効である場合、AC は CAPWAP トンネルの確立中に AP ソフトウェアバージョンを確認します。ソフトウェアのアップグレード機能が無

効である場合、AC は AP のソフトウェアバージョンを調査せず、AP を有する CAPWAP トンネルを直接確立します。

I. AP view でのソフトウェアアップグレードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． ソフトウェアアップグレードを設定する	**firmware-upgrade** { **disable** | **enable** }	デフォルト：APはAP group viewの設定を使用します。AP group viewにソフトウェアアップグレードの設定がない場合、APはglobal configuration viewの設定を使用します。

II. AP group view でのソフトウェアアップグレードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． ソフトウェアアップグレードを設定する	**firmware-upgrade** { **disable** | **enable** }	デフォルト：APはglobal configuration viewの設定を使用します。

III. global configuration view でのソフトウェアアップグレードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan global-configuration**	—
3． ソフトウェアアップグレードを設定する	**firmware-upgrade** { **disable** | **enable** }	デフォルト： 有効

2.5.3 AC が AP イメージファイルを取得するための優先ロケーションの指定

AP が CAPWAP トンネルの確立中にソフトウェアバージョンを要求した場合、AC は AP に AP イメージファイルを割り当てます。AC が AP イメージファイルを取得するための AC の RAM またはローカルフォルダとして、優先する場所を指定できます。AC が優先ロケーションから AP イメージファイルを取得できない場合、AC は他のロケーションから AP イメージファイルを取得します。AP イメージファイルが存在しない場合、AC はイメージファイルの取得に失敗し、AP にソフトウェアバージョンを割り当てることができません。

🕮 **メモ：**

- このコマンドは QX-W1100 シリーズの AP でのみサポートしています。
- このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

I. 設定の制限とガイドライン

AC は、.ipe AP イメージファイルのみを AP に割り当てることができます。

ローカルフォルダを指定する場合は、AC がデフォルトのファイルシステムとして CF またはフラッシュカードを使用し、AP イメージファイルが AC 上のファイルシステムのルートディレクトリに保存されていることを確認します。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AC が AP イメージファイルを取得するための優先ロケーションを指定する	**wlan image-load filepath** { **local** | **ram** }	デフォルトでは、ACは、APにソフトウェアバージョンを割り当てるときに、RAMに保存されているAPイメージファイルを優先します。

2.5.4 オンライン AP へのイメージファイルの展開

この機能を使用すると、すべてのオンライン AP のイメージをアップグレードできます。アップグレードを有効にするには、アップグレード後に AP を再起動します。

🕮 **メモ：**

- このコマンドは Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。
- このコマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． すべてのオンライン AP にイメージファイルを展開する。	**wlan ap-image-deploy { all | name** *ap-name* **| ap-group** *group-name* **}**	—

2.6 APのVLAN設定

AC は、パケットの転送やパケットを隔離するため、AP に VLAN の設定を行うことができます。たとえば、クライアントデータのトラフィックを転送する AP を有効にするため、異なる VLAN からのトラフィックを許可するように AP のポートを設定する必要があります。

VLAN の詳細は QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 4 *アクセス "VLAN"* を参照してください。クライアントデータのトラフィックフォワーダの詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN アクセスの設定"* を参照してください。

AP の設定を行なう場合、**remote-configuration** コマンドもしくは **map-configuration** コマンドを使用できます。

🕮 **メモ：**

- **remote-configuration synchronize** コマンドの詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"AP 管理"* の *"AP の VLAN 設定"* の *"リモート設定の割り当て設定"* を参照してください。
- AP の設定には **remote-configuration** を使用することを推奨します。**remote-configuration** を有効にした場合、**remote-configuration** で設定可能なコマンドがデフォルト値として適用されます。**remote-configuration** で設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**remote-configuration** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。**map-configuration** コマンドの詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN アクセスの設定"* の *"AP コンフィグレーションファイルの設定"* を参照してください。

2.6.1 VLAN の基本設定

I. AP view での VLAN の基本設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. （オプション設定項目）VLAN を作成し、その view に移行する、あるいは VLAN リストを作成する	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	デフォルト：VLAN1のみ（システムデフォルトVLAN）
4. VLAN view に移行する	**vlan** *vlan-id*	VLANリストを作成する場合、必要です。
5. VLAN の名前を設定する	**name** *text*	デフォルト：APはAP group viewの設定を使用します。
6. VLAN の説明を設定する	**description** *text*	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での VLAN の基本設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. （オプション設定項目）VLAN を作成し、その view に移行する、あるいは VLAN リストを作成する	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	デフォルト：VLAN1のみ（システムデフォルトVLAN）
4. VLAN view に移行する	**vlan** *vlan-id*	VLANリストを作成する場合、必要です。
5. VLAN の名前を設定する	**name** *text*	デフォルト：**VLAN** *vlan-id* *vlan-id*は4桁のフォーマットでVLAN IDを指定します。3桁で指定した先頭に0が追加されます。たとえばVLAN 100のVLAN名はVLAN 0100です。
6. VLAN の説明を設定する	**description** *text*	デフォルト：**VLAN** *vlan-id* *vlan-id*は4桁のフォーマットでVLAN IDを指定します。3桁で指定した先頭に0が追加されます。たとえばVLAN 100のVLAN名はVLAN 0100です。

2.6.2 ポートベース VLAN の設定

🕮 **メモ：**

- **map-configuration** コマンドについては、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN アクセスの設定"* の *"AP へのコンフィグレーションファイルの設定"* を参照してください。
- AC のポート設定は、interface view に設定をしてください。

I. アクセスポート VLAN の設定

以下に AP の Layer 2 Ethernet interface view の VLAN にアクセスポートを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. Layer 2 Ethernet interface view に移行する	GigabitEthernet interface viewに移行する： **gigabitethernet** *interface-number*	—
4. リンクタイプをアクセスに設定する	**port link-type** *access*	デフォルト：APグループのLayer 2 Ethernet interface viewの設定を使用します。

操作	コマンド	補足
5. アクセスポートを VLAN に割り当てる	**port access vlan** *vlan-id*	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。

以下に AP グループの Layer 2 Ethernet interface view の VLAN にアクセスポートを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. Layer 2 Ethernet interface view に移行する	GigabitEthernet interface viewに移行する：**gigabitethernet** *interface-number*	—
5. リンクタイプをアクセスに設定する	**port link-type access**	デフォルト：アクセス
6. アクセスポートを VLAN に割り当てる	**port access vlan** *vlan-id*	デフォルト：VLAN 1に属します。

II. トランクポート VLAN の設定

以下に AP の Layer 2 Ethernet interface view の VLAN にトランクポートを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. Layer 2 Ethernet interface view に移行する	GigabitEthernet interface viewに移行する：**gigabitethernet** *interface-number*	—
4. リンクタイプをトランクに設定する	**port link-type trunk**	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。
5. トランクポートで許可する VLAN を設定する	**port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。
6. （オプション設定項目）トランクポートの PVID を設定する	**port trunk pvid vlan** *vlan-id*	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。

以下に AP グループの Layer 2 Ethernet interface view の VLAN にトランクポートを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—

操作	コマンド	補足
4． Layer 2 Ethernet interface view に移行する	GigabitEthernet interface viewに移行する：**gigabitethernet** *interface-number*	—
5． リンクタイプをトランクに設定する	**port link-type trunk**	デフォルト：アクセス
6． トランクポートで許可する VLAN を設定する	**port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：VLAN 1のみ許可
7． （オプション設定項目）トランクポートの PVID を設定する	**port trunk pvid vlan** *vlan-id*	デフォルト：VLAN 1

III. ハイブリッドポート VLAN の設定

以下に AP の Layer 2 Ethernet interface view の VLAN にハイブリッドポートを設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． Layer 2 Ethernet interface view に移行する	GigabitEthernet interface viewに移行する：**gigabitethernet** *interface-number*	—
4． リンクタイプをハイブリッドに設定する	**port link-type** hybrid	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。
5． ハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。
6． （オプション設定項目）トランクポートの PVID を設定する	**port hybrid pvid vlan** *vlan-id*	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。

以下に AP グループの Layer 2 Ethernet interface view の VLAN にハイブリッドポートを設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． Layer 2 Ethernet interface view に移行する	GigabitEthernet interface viewに移行する：**gigabitethernet** *interface-number*	—
5． リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
6． ハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：ハイブリッドポートは、リンクタイプがアクセスであるときに、ポートが所属しているVLANのタグなしメンバです。

操作	コマンド	補足
7. （オプション設定項目）トランクポートの PVID を設定する	**port hybrid pvid vlan** *vlan-id*	デフォルト：ハイブリッドポートのPVIDは、リンクタイプがアクセスであるときに、ポートが所属しているVLANのIDです。

IV. リンクアグリゲーションの設定

🕮 **メモ：**
リンクアグリゲーションを使用する場合、ポートアイソレーションを無効にしてください。

以下に AP の Layer 2 Ethernet interface view にリンクアグリゲーショングループを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. リンクアグリゲーショングループを作成する	**bridge-aggregation** *interface-number*	—
4. ポートアイソレーションを無効にする	**port-isolate disable**	—
5. Layer 2 Ethernet interface view に移行する	GigabitEthernet interface viewに移行する：**gigabitethernet** *interface-number*	—
6. ポートアイソレーションを無効にする	**port-isolate disable**	—
7. リンクアグリゲーショングループを設定する	**port link-aggregation group** *group-id*	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。

以下に AP グループの Layer 2 Ethernet interface view にリンクアグリゲーショングループを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. リンクアグリゲーショングループを作成する	**bridge-aggregation** *interface-number*	—
5. ポートアイソレーションを無効にする	**port-isolate disable**	—
6. Layer 2 Ethernet interface view に移行する	GigabitEthernet interface viewに移行する：**gigabitethernet** *interface-number*	—
7. ポートアイソレーションを無効にする	**port-isolate disable**	—

操作	コマンド	補足
8. リンクアグリゲーショングループを設定する	**port link-aggregation group** *group-id*	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。

V. ポートアイソレーションの設定

以下に AP の Layer 2 Ethernet interface view にポートアイソレーションを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. Layer 2 Ethernet interface view に移行する	GigabitEthernet interface viewに移行する：**gigabitethernet** *interface-number*	—
4. ポートアイソレーションを設定する	**port-isolate** { **enable** | **disable** }	デフォルト：APグループの Layer 2 Ethernet interface viewの設定を使用します。

以下に AP グループの Layer 2 Ethernet interface view にポートアイソレーションを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. Layer 2 Ethernet interface view に移行する	• GigabitEthernet interface view に移行する：**gigabitethernet** *interface-number*	—
5. ポートアイソレーションを設定する	**port-isolate** { **enable** | **disable** }	デフォルト：有効

2.7 信頼されたパケットプライオリティタイプの設定

🕮 **メモ：**

- **qos trust** コマンドはソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。
- **qos trust** コマンドは **remote-configuration** コマンドにて設定可能です。

I. 概要

インタフェースに指定されたプライオリティタイプとポートプライオリティ値に基づき、AP はインタフェースで受信したすべてのパケットに、指定されたタイプのプライオリティを割り当てます。

システムでは以下の信頼されたパケットプライオリティタイプをサポートします。

- **dot11p**－802.1p プライオリティをマッピングに使用します。
- **dscp**－DSCP プライオリティをマッピングに使用します。

II. 設定手順

以下に AP の Layer 2 Ethernet interface view もしくは Layer 2 aggregate interface view にプライオリティタイプを設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． Layer 2 Ethernet interface view もしくは Layer 2 aggregate interface view に移行する	● GigabitEthernet interface view に移行する：**gigabitethernet** *interface-number* ● aggregate interface viewに移行する：**bridge-aggregation** *interface-number*	—
4． 信頼されたパケットプライオリティタイプを設定する	**qos trust** { **dot1p** | **dscp** }	デフォルト：Layer 2 Ethernet interface view では、APグループのLayer 2 Ethernet interface viewの設定を使用します。Layer 2 aggregate interface view では、APグループのLayer 2 aggregate interface viewの設定を使用します。

以下に AP グループの Layer 2 Ethernet interface view もしくは Layer 2 aggregate interface view にプライオリティタイプを設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． Layer 2 Ethernet interface view もしくは Layer 2 aggregate interface view に移行する	● GigabitEthernet interface view に移行する：**gigabitethernet** *interface-number* ● aggregate interface viewに移行する：**bridge-aggregation** *interface-number*	—

操作	コマンド	補足
5. 信頼されたパケットプライオリティタイプを設定する	**qos trust** { **dot1p** | **dscp** }	デフォルト Layer 2 Ethernet interface view：設定なし Layer 2 aggregate interface view：設定なし

2.8 ポートプライオリティの設定

🕮 **メモ：**

- **qos priority** コマンドはソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。
- **qos priority** コマンドは **remote-configuration** コマンドにて設定可能です。

I. 概要

インタフェースに指定されたプライオリティタイプとポートプライオリティ値に基づき、AP はインタフェースで受信したすべてのパケットに、指定されたタイプのプライオリティを割り当てます。

II. 設定手順

以下に AP の Layer 2 Ethernet interface view もしくは Layer 2 aggregate interface view にポートプライオリティを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. Layer 2 Ethernet interface view もしくは Layer 2 aggregate interface view に移行する	• GigabitEthernet interface view に移行する：**gigabitethernet** *interface-number* • aggregate interface viewに移行する：**bridge-aggregation** *interface-number*	—
4. ポートプライオリティを設定する	**qos priority** *priority-value*	デフォルト Layer 2 Ethernet interface view ：APグループのLayer 2 Ethernet interface viewの設定を使用します。 Layer 2 aggregate interface view：APグループのLayer 2 aggregate interface viewの設定を使用します。

以下に AP グループの Layer 2 Ethernet interface view もしくは Layer 2 aggregate interface view にポートプライオリティを設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． Layer 2 Ethernet interface view もしくは Layer 2 aggregate interface view に移行する	• GigabitEthernet interface view に移行する：**gigabitethernet** *interface-number* • aggregate interface viewに移行する：**bridge-aggregation** *interface-number*	—
5． ポートプライオリティを設定する	**qos priority** *priority-value*	デフォルト Layer 2 Ethernet interface view：0 Layer 2 aggregate interface view：0

2.9 リモート設定の割り当て設定

AP の設定を行なう場合、**remote-configuration** コマンドもしくは **map-configuration** コマンドを使用できます。

remote-configuration を使用するとき、**remote-configuration synchronize** コマンドを使用して、AP view の設定を任意の AP に即座に同期します。なお、AP が AC に接続された状態で、AP の設定内容を AC 上で変更した場合、**remote-configuration synchronize** コマンドを実行するまで変更内容が AP に反映されません。

🕮 **メモ：**

remote-configuration を使用することを推奨します。**remote-configuration** を有効にした場合、**remote-configuration** で設定可能なコマンドがデフォルト値として適用されます。**remote-configuration** で設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**remote-configuration** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。**map-configuration** コマンドの詳細は、QX-W1000/W1100 シリーズアクセスポイント Anchor-AC オペレーションマニュアルの *“WLAN アクセスの設定”* の *“AP コンフィグレーションファイルの設定”* を参照してください。

---

remote-configuration synchronize コマンドを使用する前に、**remote-configuration enable** が設定されていることを確認してください。

AP view の設定は、AP group view の設定よりも優先されます。

I. AP view でのリモート設定の割り当て

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—

操作	コマンド	補足
3． リモート設定を割り当てる	**remote-configuration** { **disable** | **enable** }	デフォルト：APはAP group viewの設定を使用します。
4． リモートコンフィグレーションシンクロナイゼーションを使用して設定を AP に同期する。	**remote-configuration synchronize**	デフォルト：AP group viewの設定を使用します。 ソフトウェアバージョン 7.1.10を含む以降のバージョンでのみ使用可能なコマンドです。

II. AP group view でのリモート設定の割り当て

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． リモート設定を割り当てる	**remote-configuration** { **disable** | **enable** }	デフォルト：無効
4． リモートコンフィグレーションシンクロナイゼーションを使用して設定を AP に同期する。	**remote-configuration synchronize**	デフォルト：無効 ソフトウェアバージョン 7.1.10を含む以降のバージョンでのみ使用可能なコマンドです。

2.10 APグループの設定

本機能により、バッチ内で複数の AP 設定ができるようになり、作業負担の低減につながります。

AP group 内の AP は、AP group の設定を使用します。デフォルトでは、すべての AP はデフォルト AP グループ（default-group）に属します。デフォルト AP グループを作成、削除することはできません。

指定された AP グループに AP を追加するために、AP 名、シリアル ID、MAC アドレス、IPv4 アドレスを用いて AP グループルールを設定できます。これらのグループルールの優先度は上記の順序に準じます。AP がどのグループルールにも適合しない場合、デフォルト AP グループに追加されます。

2.10.1 設定の制限とガイドライン

AP グループを設定するときは、以下に示す制限とガイドラインに従います。

- 異なる AP グループに対して同じグループルールを作成することはできません。同一のグループルールを作成した場合、最後に行った設定が適用されます。
- デフォルト AP グループに対してグループルールを作成することはできません。
- AP グループあるいは異なる AP グループの IPv4 アドレスによる AP グループルールは互いに重複させることができません。
- QX-W1030 Anchor-AC は、AP グループに設定できる IPv4 アドレスによる AP グループルールの設定可能数は最大 32 個です。

- QX-W1100 シリーズの Anchor-AC は、ソフトウェアバージョンにより AP グループに設定できる IPv4 アドレスによる AP グループルールの設定可能数が異なります。
  - □ ソフトウェアバージョン 7.2.85a を含む以前のソフトウェアでは、AP グループに最大 32 個ルールを設定できます。
  - □ ソフトウェアバージョン 7.2.89 を含む以降のソフトウェアでは、AP グループに最大 64 個のルールを設定できます。

2.10.2 AP group の作成

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group を作成し、AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP groupがあります。
3. （オプション設定項目） AP group に対して記述を設定する	**description** *text*	デフォルト：AP groupに対して記述は設定されません。
4. AP 名で AP group ルールを作成する	**ap** *ap-name-list*	—
5. シリアル ID で AP group ルールを作成する	**serial-id** *serial-id*	—
6. MAC アドレスで AP group ルールを作成する	**mac-address** *mac-address*	—
7. IPv4 アドレスで AP group ルールを作成する	**if-match ip** *ip-address* { *mask-length* | *mask* }	—
8. （オプション設定項目） AP グループルールを作成する	**wlan re-group** { **ap** *ap-name* | **ap-group** *old-group-name* | **mac-address** *mac-address* | **serial-id** *serial-id* } *group-name*	—

2.11 CAPWAPトンネルの設定

2.11.1 CAPWAP トンネル暗号化

CAPWAP トンネル経由で送られた制御パケットとデータパケットを暗号化するために、CAPWAP トンネル暗号化はデータグラムトランスポート層セキュリティ(DTLS)プロトコルを使います。

CAPWAP 制御トンネル暗号化が有効の場合、暗号化フラグのついた検出応答を AP が AC から受信後、AP は AC と CAPWAP トンネルを確立できます。CAPWAP トンネルが確立されると、AC と AP は DTLS ハンドシェイク後に CAPWAP 制御トンネルで送られた制御パケットを暗号化します。

CAPWAP データトンネル暗号化が有効の場合、AP は AC から keepalive パケットを初めて受信すると、AP は鍵を含む暗号化情報を、CAPWAP 制御トンネルを通して AC と交換します。交換後、AC と AP は CAPWAP データトンネルで送られたデータパケットを暗号化します。Keepalive パケットは暗号化されません。

メモ：

CAPWAP データトンネル暗号化には独自の証明書をしており、時刻の有効性を確認しています。CAPWAP トンネル暗号化を利用する場合は、事前に装置の時刻が正しく設定されているか確認してください。

I. 制限とガイドライン

CAPWAP トンネル暗号化は、AP が再起動後に適用されます。

II. 設定手順

以下に AP view での CAPWAP トンネル暗号化の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. CAPWAP 制御トンネル暗号化を設定する	**tunnel encryption** { **disable** | **enable** }	デフォルト：APはAP group viewの設定を使用します。
4. CAPWAP データトンネル暗号化を設定する	**data-tunnel encryption** { **disable** | **enable** }	デフォルト：APはAP group viewの設定を使用します。

以下に AP group view での CAPWAP トンネル暗号化の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. CAPWAP 制御トンネル暗号化を設定する	**tunnel encryption** { **disable** | **enable** }	デフォルト：無効
4. CAPWAP データトンネル暗号化を設定する	**data-tunnel encryption** { **disable** | **enable** }	デフォルト：無効

2.11.2 CAPWAP トンネルの待ち時間検出の設定

本機能により AC は、CAPWAP 制御フレームもしくは AP から AC へのデータフレームを送信する待ち時間を検出することができます。

本機能は、CAPWAP トンネルが確立されたあと、マスタ AC にのみ適用されます。

AP がオフラインのとき、CAPWAP トンネルの待ち時間検出は自動的に停止します。AP が再びオンラインになると、**tunnel latency-detect start** コマンドを使用して CAPWAP トンネルの待ち時間検出を再始動させる必要があります。

CAPWAP トンネル待ち時間情報を表示させるには、**display wlan ap name tunnel latency** コマンドを使用します。

以下に CAPWAP トンネル待ち時間を検出するための手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. CAPWAP トンネル待ち時間検出を設定する	**tunnel latency-detect** { **start** | **stop** }	デフォルト：CAPWAP トンネルの待ち時間検出は開始しません。

2.11.3 AP に対する制御トンネルの keepalive 時間の設定

AP は、CAPWAP トンネルが正しく動作しているかどうか確認するために、指定されたエコー間隔で AC にエコー要求を送信します。AC は、エコー応答を送信することで応答します。AC が keepalive 時間以内にエコー要求を受信しない場合、AP の接続が終了します。

制御トンネルの keepalive 時間は、”**echo-interval**”と” **echo-count**”の積です。

🕮 **メモ：**

CAPWAP トンネルがダウンしたかどうかを AC もしくは AP が判断する時間は、ポートのリンクダウンの有無により異なります。

- ポートのリンクダウンが伴う場合、AC および AP は即座に CAPWAP トンネルがダウンしたと判断します。
- ポートのリンクダウンが伴わない場合、AC および AP は keepalive 時間（”**echo-interval**”と” **echo-count**”の積）により CAPWAP トンネルのダウンを判断します。ただし、AC は 120 秒間は CAPWAP トンネルを維持するため、keepalive 時間が 120 秒未満でも 120 秒間は CAPWAP トンネルがダウンしたと判断しません。

I. AP view での AP に対する keepalive 時間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. AP がエコー要求を送信する間隔を設定する	**echo-interval** *interval*	デフォルト：APはAP group viewの設定を使用します。
4. エコー要求の再送試行回数の最大値を設定する	**echo-count** *count*	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での AP に対する keepalive 時間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP がエコー要求を送信する間隔を設定する	**echo-interval** *interval*	デフォルト：10秒
4. エコー要求の再送試行回数の最大値を設定する	**echo-count** *count*	デフォルト：3

2.11.4 AP に対するデータトンネルの keepalive 時間の設定

AP は AP と AC 間で CAPWAP トンネルが確立されたのち、指定した keepalive 時間で AC にデータトンネルの keepalive パケットを送信します。

I. AP view での AP に対する keepalive 時間の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． AP がエコー要求を送信する間隔を設定する	**keepalive-interval** *interval*	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での AP に対する keepalive 時間の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP がエコー要求を送信する間隔を設定する	**keepalive-interval** *interval*	デフォルト：10秒

2.11.5 CAPWAP パケットの最大フラグメントサイズの設定

AP がインタネットを経由して AC と接続している場合、中継装置でパケットの廃棄を防ぐことができます。

最大フラグメントサイズの変更はオンライン中の AP でのみ適用されます。

I. AP view での CAPWAP パケットの最大フラグメントサイズの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． CAPWAP 制御、データパケットの最大フラグメントサイズを設定する	**fragment-size** { **control** *control-size* | **data** *data-size* }	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での CAPWAP パケットの最大フラグメントサイズの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—

操作	コマンド	補足
3． CAPWAP 制御、データパケットの最大フラグメントサイズを設定する	**fragment-size** { **control** *control-size* | **data** *data-size* }	デフォルト：CAPWAP制御パケットの最大フラグメントサイズは1450バイト、データパケットの最大フラグメントサイズは1500バイトです。

2.12 AC要求の再送信の設定

AC は、AP 要求の再送信の試行が最大数に達するまで、あるいは応答が受信されるまで、AP に送信された要求を再送信隔で送信します。

I. AP view での AC 要求再伝送の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． 要求再伝送の最大試行回数を設定する	**retransmit-count** *value*	デフォルト：APはAP group viewの設定を使用します。
4． AC 要求が再伝送される間隔を設定する	**retransmit-interval** *interval*	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での AC 要求の再送信の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． 要求再伝送の最大試行回数を設定する	**retransmit-count** value	デフォルト：3
4． AC 要求が再伝送される間隔を設定する	**retransmit-interval** *interval*	デフォルト：5秒

2.13 統計情報報告間隔の設定

AP が統計情報を報告する間隔を変えるために、本操作を実行します。AP 上での無線通信の作動状況を監視するために、報告された統計情報を用いることができます。

I. AP view での統計情報報告間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*[	—
3． 統計情報報告間隔を設定する	**statistics-interval** *interval*	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での統計情報報告間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． 統計情報の通知間隔を設定する	**statistics-interval** *interval*	デフォルト：50秒

2.14 AP保守

2.14.1 AP のリセット

user view で以下の操作を実行します。

操作	コマンド
すべてのAPもしくは指定されたAPをリセットする	**reset wlan ap** { **all** | **name** *ap-name* | **model** *model-name* | **ap-group** *group-name* }

2.14.2 手動 AP の名前の変更

操作	コマンド
1． system view に移行する	s**ystem-view**
2． 手動 AP の名前を変更する	**wlan rename-ap** *ap-name new-ap-name*

2.14.3 AP のファイルシステムの管理

CAPWAP トンネルが確立されたあと、AC で AP のファイルを管理する項目を行うことができます。

- AP のファイル情報を確認します。
- AP からファイルを削除します。
- AC から AP にイメージファイルをダウンロードします。

本機能は、マスタ AC に対してのみ適用されます。

以下に AP のファイルシステムを管理する手順を示します。

操作	コマンド
system viewに移行する	**system-view**
AP viewに移行する	**wlan ap** *ap-name*
APからファイルを削除する	**delete file** *filename*
APにイメージファイルをダウンロードする	**download file** *file-name*

2.14.4 AP の現在のコンフィグの保存

🕮 **メモ：**

wlan save ap-configuration コマンドはソフトウェアバージョン 7. 2. 73 を含む以降のソフトウェアからサポートしています。

AC から、指定した AP、AP グループ、または全てのオンライン状態の AP を対象に、現在のコンフィグを AP 上に保存し、次回の起動に使用するスタートアップコンフィグレーションファイルとして設定することができます。

以下に、AP の現在のコンフィグを保存する手順を示します。

操作	コマンド
1． system view に移行する	**system-view**
2． AP の現在のコンフィグを保存する	**wlan save ap-configuration** { **all** | **ap-group** *group-name* | **name** *ap-name* }

2.14.5 LED 点灯モードの設定

AP 上で以下のモードで LED を点灯させるように設定できます。

- **quiet**－すべての LED をオフにします。
- **awake**－すべての LED を 1 分毎に点灯させます。
- **always-on**－すべての LED を常にオンにします。
- **normal**－本モードでの LED 点灯の仕方は、AP モデルにより変わります。本モードでは AP の作動状況を識別します。

I. AP view での LED 点灯モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** ap-name	—
3． LED 点灯モードを設定する	**led-mode** { **always-on** | **awake** | **normal** | **quiet** }	デフォルト：APはAP group view内の設定を使用します。

II. AP group view での LED 点灯モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP group（default-group）が存在します。 デフォルトAP group削除することができません。
3． LED 点灯モードを設定する	**led-mode** { **always-on** | **awake** | **normal** | **quiet** }	デフォルト：normal

2.15 SNMP通知の有効化

NMS に対して重要な WLAN 事例を報告するために、SNMP 通知を有効化します。WLAN 事例通知を正確に送信するため SNMP の設定を行ってください。SNMP の詳細は QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* を参照してください。

以下に SNMP 通知を有効にする手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. SNMP 通知を有効にする	• AP管理に対してSNMP通知を有効にする：**snmp-agent trap enable wlan ap** • CAPWAPに対してSNMP通知を有効にする：**snmp-agent trap enable wlan capwap**	デフォルト：AP管理とCAPWAPに対するSNMP通知は無効化されます。

2.16 AP管理の応用設定

2.16.1 リモート AP の設定

リモート AP 機能は、AP と AC 間のトンネルが接続されていないとき、以下の操作を自動で実行します。

- クライアントトラフィックを転送します。
- ローカル認証が有効かつ AP で関連付けが有効な場合、クライアントにアクセスサービスを提供します。

リモート AP はテレコミュニケーション、スモールブランチ、SOHO ソリューションに適用可能です。

I. 制限とガイドライン

リモート AP は、ローカル転送モード内で作動する AP でのみ有効です。

AC と AP 間のトンネルが復元されると、AC を有するクライアントは認証者として再認証を必要とします。

II. AP view でのリモート AP の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP view に移行する	**wlan ap** *ap-name*	—
3． リモート AP を設定する	**hybrid-remote-ap** { **disable** | **enable** }	デフォルト：APはAP group viewの設定を使用します。

III. AP group view でのリモート AP の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． リモート AP を設定する	**hybrid-remote-ap** { **disable** | **enable** }	デフォルト：無効

2.16.2 APDB ユーザスクリプトのローディング

この機能は AC ソフトウェアをアップグレードすることなく APDB に新しい AP モデルを追加します。

I. 設定の制限とガイドライン

APDB ユーザスクリプトをロードするとき、以下の制限とガイドラインに従ってください。

- ユーザスクリプトが有効であることを確認します。無効なスクリプトはローディングの失敗の原因となる可能性があります。
- ユーザスクリプト内の AP モデルは、システムスクリプト内の AP モデルと異なる必要があります。
- AC 上で複数のユーザスクリプトをロードする場合、直近でロードされたユーザスクリプトは、古いユーザスクリプトを上書きします。
- ファイルシステムでユーザスクリプトの名前を変更する場合、ユーザスクリプトの AP モデルの設定が再起動後に削除してしまわないように、ユーザスクリプトをリロードしてください。
- ユーザスクリプトをファイルシステムの新しいユーザスクリプトに置き換える場合、新しいユーザスクリプトをリロードします。置き換えられるユーザスクリプトにある AP モデル情報が、新しいユーザスクリプトに含まれていない場合、AC の再起動後に AP モデル情報は失われます。
- ファイルシステムでユーザスクリプトを削除する場合、AC の再起動後に AP モデル情報は失われます。

古いユーザスクリプトが存在する場合、APDB ユーザスクリプトをロードするとき、以下の制限とガイドラインに従ってください。

- 手動 AP または、古いユーザスクリプト内にモデルが記載されているオンラインの自動 AC が存在するとき、AC 上で一致する AP モデル情報を削除します。
- AP がすでに AP グループに追加されている場合、古いユーザスクリプト内にモデルが記載されている AP を、AP グループから取り除きます。
- 古いユーザスクリプトが、ソフトウェアバージョンがすでに設定された AP モデルを含む場合、もとのソフトウェアバージョンを復元するために **wlan apdb** コマンドを使用します。

II. 設定手順

以下に APDB ユーザスクリプトをロードするための手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． APDB ユーザスクリプトをロードする	**wlan apdb file** *user.apdb*	デフォルト：ユーザスクリプトはACにロードされません。

2.17 AP管理の表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
すべてのAPもしくは指定したAPに関する情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } [**verbose**]
すべてのAPもしくは指定したAPのアドレス情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **address**
CAPWAPトンネル機能の設定状況を表示する	**display wlan ap all feature capwap**
すべてのAPあるいは特定のAPのAPグループ情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **group**
AC上でAP接続記録を表示する	**display wlan ap** { **all** | **name** *ap-name* } **connection-record**
APのオンライン時間を表示する	**display wlan ap** { **all** | **name** *ap-name* } **online-time**
特定のAPの再起動ログを表示する	**display wlan ap name** *ap-name* **reboot-log**
APイメージのダウンロードに関する情報を表示します	**display wlan ap statistics image-download [failed | in-progress | succeeded]**
すべてのAPもしくは指定したAPに対するカレントコンフィグレーションを表示する	**display wlan ap** { **all** | **ap-name** ap-name } **running-configuration** [**verbose**]
APのお関連付け失敗記録を表示する	**display wlan ap statistics association-failure-record**
オンラインAP数の記録を表示する	**display wlan ap statistics online-record** [**time** *date time* [**count** *count*]]
CAPWAPトンネルがダウンした記録を表示する	**display wlan ap statistics tunnel-down-record**
すべてのAP groupもしくは指定したAP groupに関する情報を表示する	**display wlan ap-group** [**brief** | **name** *group-name*]
APモデル情報を表示する	**display wlan ap-model** { **all** | **name** *model-name* }
指定したCAPWAPトンネルに対してトンネル待ち時間情報を表示する	**display wlan ap name** *ap-name* **tunnel latency**

操作	コマンド
ACに所属しているAPの区分を表示する	**display wlan ap-distribution all**
APの接続位置を表示する	**display wlan ap-distribution ap-name** *ap-name*

2.17.1 AP 管理情報の削除

user view で reset コマンドを実行することができます。

操作	コマンド
すべてのAPもしくは指定したAPの再起動ログを削除する	**reset wlan ap reboot-log** { **all** | **name** *ap-name* }
CAPWAPトンネルもしくは指定したCAPWAPトンネルに対するトンネル待ち時間情報を削除する	**reset wlan tunnel latency ap** { **all** | **name** *ap-name* }

2.18 AP管理の設定例

2.18.1 DHCP を通した CAPWAP トンネル確立の設定例

I. ネットワーク要件

図 2-3 に示すように、AP が DHCP Option 43 を通して DHCP サーバから自身の IP アドレスと AC の IP アドレスを取得できるように設定します。AP は、AC との CAPWAP トンネルを確立するために、AC の IP アドレスを使用します。

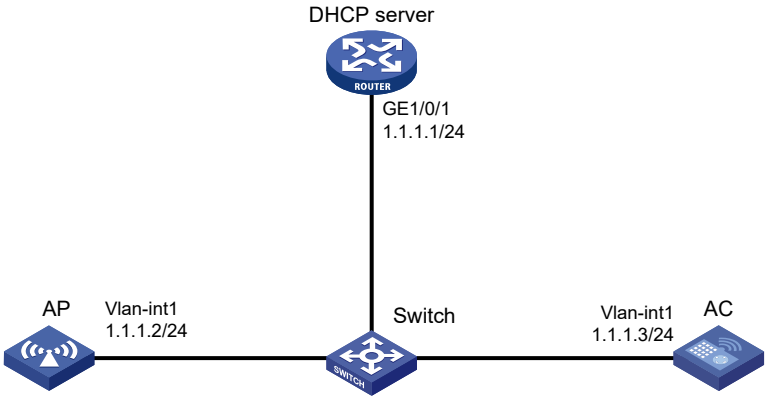


図 2-3 ネットワーク図

II. 設定手順

1)　DHCP サーバを設定します。

DHCP を有効にします。

```
<DHCP server> system-view
[DHCP server] dhcp enable
```

DHCP address pool 1 を設定します。

```
[DHCP server] dhcp server ip-pool 1
[DHCP server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
```

address pool 0 に AC の IP アドレスを指定するために Option 43 を設定します。右端のバイト 01010103（1.1.1.3）は AC の IP アドレスを示します。

```
[DHCP server-dhcp-pool-1] option 43 hex 800700000101010103
```

2)　AC を設定します。

AC 上の VLAN-interface 1 の IP アドレスに 1.1.1.3/24 を設定します。

```
<AC> system-view
[AC] interface vlan-interface 1
[AC-Vlan-interface1] ip address 1.1.1.3 24
[AC-Vlan-interface1] quit
```

QX-W1020 を有する AP 名が ap1 の AP を作成し、シリアル ID を 210235A1BSC123000050 に設定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
[AC-wlan-ap-ap1] quit
```

#AP を始動させます。AP は以下の操作を実行します。

- DHCP サーバから自身の IP アドレス 1.1.1.2 を取得します。
- Option 43 を通して AC の IP アドレスを取得します。
- AC との CAPWAP トンネルを確立します。

III. 設定の確認

以下の情報を検証します。

- AP は、DHCP を通して AC の IP アドレスを取得します。
- AP と AC が、確立された CAPWAP トンネルを有します。
- AP は稼働状態です。

```
[AC] display wlan ap name ap1 verbose
AP name                          : ap1
AP ID                            : 1
AP group name                    : default-group
State                            : Run
Backup type                      : Master
Online time                      : 0 days 1 hours 25 minutes 12 seconds
System up time                   : 0 days 2 hours 22 minutes 12 seconds
Model                            : QX-W1020
Region code                      : JP
Region code lock                 : Disable
Serial ID                        : 219801A1JY817BE00001
```

```
MAC address                    : 0AFB-423B-893C
IP address                     : 1.1.1.2
UDP port number                : 18313
H/W version                    : Ver.C
S/W version                    : 7.2.1
Boot version                   : 0.15
USB state                      : N/A
Power Level                    : N/A
Power info                     : N/A
Description                    : wtp1
Priority                       : 4
Echo interval                  : 10 seconds
Echo count                     : 3 counts
Keepalive interval             : 10 seconds
Discovery-response wait-time   : 2 seconds
Statistics report interval     : 50 seconds
Fragment size (data)           : 1500
Fragment size (control)        : 1450
MAC type                       : Local MAC & Split MAC
Tunnel mode                    : Local Bridging & 802.3 Frame & Native Frame
CWPCAP data-tunnel status      : Up
Discovery type                 : DHCP
Retransmission count           : 3
Retransmission interval        : 5 seconds
Firmware upgrade               : Enabled
Sent control packets           : 1
Received control packets       : 1
Echo requests                  : 147
Lost echo responses            : 0
Average echo delay             : 3
Last reboot reason             : User soft reboot
Latest IP address              : 10.1.0.2
Current AC IP                  : N/A
Tunnel down reason             : Request wait timer expired
Connection count               : 1
Backup Ipv4                    : Not configured
Backup Ipv6                    : Not configured
Tunnel encryption              : Disabled
Data-tunnel encryption         : Disabled
Data-tunnel encryption state   : Not encrypted
Data-tunnel encryption state   : Not encrypted
LED mode                       : Normal
Remote configuration           : Disabled
Radio 1:
    Basic BSSID                : 7848-59f6-3940
    Admin state                : Up
    Radio type                 : 802.11ac
    Antenna type               : internal
    Client dot11ac-only        : Disabled
    Client dot11n-only         : Disabled
    Channel band-width         : 20/40/80MHz
    Active band-width          : 20/40/80MHz
    Secondary channel offset   : SCB
    Short GI for 20MHz         : Supported
    Short GI for 40MHz         : Supported
    Short GI for 80MHz         : Supported
    Short GI for 160MHz        : Not supported
    mimo                       : Not Config
    Green-Energy-Management    : Disabled
    A-MSDU                     : Enabled
    A-MPDU                     : Enabled
    LDPC                       : Not Supported
    STBC                       : Supported
    Operational VHT-MCS Set:
        Mandatory              : Not configured
        Supported              : NSS1 0,1,2,3,4,5,6,7,8,9
                                 NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast              : Not configured
    Operational HT MCS Set:
        Mandatory              : Not configured
```

```
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 44(auto)
    Channel usage(%)          : 15
    Max power                 : 20 dBm
    Operational rate:
        Mandatory             : 6, 12, 24 Mbps
        Multicast             : Auto
        Supported             : 9, 18, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -102 dBm
    Protection mode           : rts-cts
    MU-TxBF                   : Enabled
    SU-TxBF                   : Enabled
    Continuous mode           : N/A
    HT protection mode        : No protection
Radio 2:
    Basic BSSID               : 7848-59f6-3950
    Admin state               : Down
    Radio type                : 802.11b
    Antenna type              : internal
    Client dot11n-only        : Disabled
    Channel band-width        : 20MHz
    Active band-width         : 20MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    Short GI for 80MHz        : Supported
    Short GI for 160MHz       : Not supported
    mimo                      : Not Config
    Green-Energy-Management   : Disabled
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : NSS1 0,1,2,3,4,5,6,7,8,9
                                NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast             : Not configured
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
    Channel                   : 5(auto)
    Channel usage(%)          : 0
    Max power                 : 20 dBm
    Preamble type             : Short
    Operational rate:
        Mandatory             : 6, 12, 24 Mbps
        Multicast             : Auto
        Supported             : 9, 18, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
```

```
    Noise Floor               : 0 dBm
    Protection mode           : rts-cts
    MU-TxBF                   : Enabled
    SU-TxBF                   : Enabled
    Continuous mode           : N/A
    HT protection mode        : No protection
Radio 3:
    Basic BSSID               : N/A
    Admin state               : Down
    Radio type                : 802.11n(2.4GHz)
    Antenna type              : internal
    Client dot11n-only        : Disabled
    Channel band-width        : 20MHz
    Active band-width         : 20MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    mimo                      : Not Config
    Green-Energy-Management   : Disabled
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 6(auto)
    Channel usage(%)          : 0
    Max power                 : 20 dBm
    Preamble type             : Short
    Operational rate:
        Mandatory             : 1, 2, 5.5, 11 Mbps
        Multicast             : Auto
        Supported             : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise floor               : 0 dBm
    Protection mode           : cts-to-self
    Continuous mode           : N/A
    HT protection mode        : No protection
```

2.18.2 DNS を通した CAPWAP トンネル確立の設定例

I. ネットワーク要件

図 2-4 に示すように、AP が DNS を通して AC の IP アドレスを取得できるように設定します。

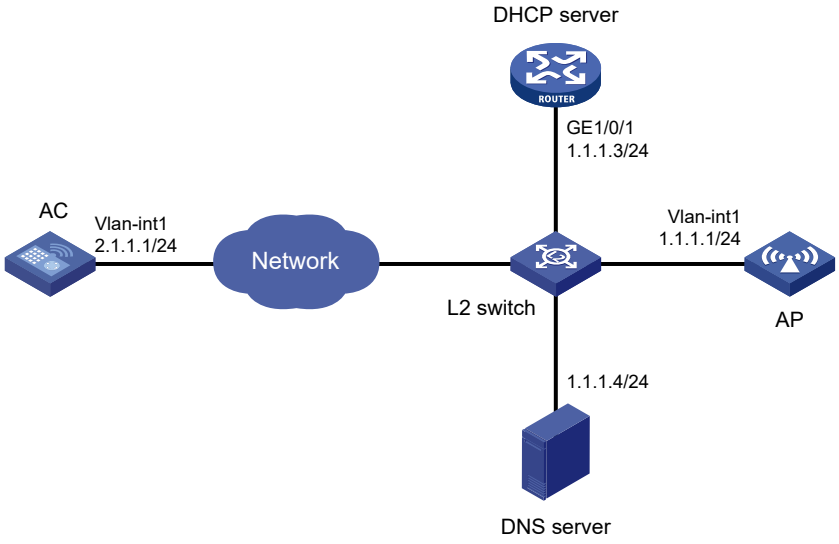


図 2-4 ネットワーク図

II. 設定手順

1)　DHCP サーバを設定します。

```
<DHCP server> system-view
[DHCP server] dhcp enable
[DHCP server] dhcp server ip-pool 1
[DHCP server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
[DHCP server-dhcp-pool-1] domain-name abc
```

2)　ドメイン名（host.abc）と IP アドレス 2.1.1.1/24 の間のマッピングを設定します。詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 5 *IP サービス "IP アドレス"*を参照してください。（詳細は省略します。）

3)　AC を設定します。

VLAN-interface の IP アドレスを 2.1.1.1/24 に設定します。

```
<AC> system-view
[AC] interface vlan-interface 1
[AC-Vlan-interface1] ip address 2.1.1.1 24
[AC-Vlan-interface1] quit
```

ap 1 と名づけた AP を作成し、モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
```

AP を起動させます。

```
[AC-wlan-ap-ap1] quit
```

AP は以下の操作を実行します。

- DHCP サーバから、自身の IP アドレス 1.1.1.1、AC のドメイン名サフィックス、DNS サーバの IP アドレスを取得します。
- ドメイン名サフィックスをホスト名に追加します。
- ドメイン名を IP アドレスに変換するように DNS クライアントに知らせます。
- AC との CAPWAP トンネルを確立するために、AC の IP アドレスを使用します。

III. 設定の確認

#以下の操作を検証します。

- AP と AC が、確立された CAPWAP トンネルを有します。
- AP は稼働状態です。
- AP は、DNS を通して AC の IP アドレスを取得します。

[AC] display wlan ap name ap1 verbose

```
AP name                          : ap1
AP ID                            : 1
AP group name                    : default-group
State                            : Run
Backup type                      : Master
Online time                      : 0 days 1 hours 25 minutes 12 seconds
System up time                   : 0 days 2 hours 22 minutes 12 seconds
Model                            : QX-W1020
Region code                      : JP
Region code lock                 : Disable
Serial ID                        : 219801A1JY817BE00001
MAC address                      : 0AFB-423B-893C
IP address                       : 1.1.1.2
UDP port number                  : 18313
H/W version                      : Ver.C
S/W version                      : 7.2.1
Boot version                     : 0.15
USB state                        : N/A
Power Level                      : N/A
Power info                       : N/A
Description                      : wtp1
Priority                         : 4
Echo interval                    : 10 seconds
Echo count                       : 3 counts
Keepalive interval               : 10 seconds
Discovery-response wait-time     : 2 seconds
Statistics report interval       : 50 seconds
Fragment size (data)             : 1500
Fragment size (control)          : 1450
MAC type                         : Local MAC & Split MAC
Tunnel mode                      : Local Bridging & 802.3 Frame & Native Frame
CWPCAP data-tunnel status        : Up
Discovery type                   : DNS
Retransmission count             : 3
Retransmission interval          : 5 seconds
Firmware upgrade                 : Enabled
Sent control packets             : 1
Received control packets         : 1
Echo requests                    : 147
Lost echo responses              : 0
Average echo delay               : 3
Last reboot reason               : User soft reboot
Latest IP address                : 10.1.0.2
Current AC IP                    : N/A
Tunnel down reason               : Request wait timer expired
Connection count                 : 1
Backup Ipv4                      : Not configured
Backup Ipv6                      : Not configured
Tunnel encryption                : Disabled
Data-tunnel encryption           : Disabled
```

```
Data-tunnel encryption state  : Not encrypted
LED mode                      : Normal
Remote configuration          : Disabled
Radio 1:
    Basic BSSID               : 7848-59f6-3940
    Admin state               : Up
    Radio type                : 802.11ac
    Antenna type              : internal
    Client dot11ac-only       : Disabled
    Client dot11n-only        : Disabled
    Channel band-width        : 20/40/80MHz
    Active band-width         : 20/40/80MHz
    Secondary channel offset  : SCB
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    Short GI for 80MHz        : Supported
    Short GI for 160MHz       : Not supported
    mimo                      : Not Config
    Green-Energy-Management   : Disabled
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational VHT-MCS Set:
        Mandatory             : Not configured
        Supported             : NSS1 0,1,2,3,4,5,6,7,8,9
                                NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast             : Not configured
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 44(auto)
    Channel usage(%)          : 15
    Max power                 : 20 dBm
    Operational rate:
        Mandatory             : 6, 12, 24 Mbps
        Multicast             : Auto
        Supported             : 9, 18, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -102 dBm
    Protection mode           : rts-cts
    MU-TxBF                   : Enabled
    SU-TxBF                   : Enabled
    Continuous mode           : N/A
    HT protection mode        : No protection
Radio 2:
    Basic BSSID               : 7848-59f6-3950
    Admin state               : Down
    Radio type                : 802.11b
    Antenna type              : internal
    Client dot11n-only        : Disabled
    Channel band-width        : 20MHz
    Active band-width         : 20MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    Short GI for 80MHz        : Supported
    Short GI for 160MHz       : Not supported
    mimo                      : Not Config
    Green-Energy-Management   : Disabled
```

```
    A-MSDU                      : Enabled
    A-MPDU                      : Enabled
    LDPC                        : Not Supported
    STBC                        : Supported
    Operational HT MCS Set:
        Mandatory               : Not configured
        Supported               : NSS1 0,1,2,3,4,5,6,7,8,9
                                  NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast               : Not configured
    Operational HT MCS Set:
        Mandatory               : Not configured
        Supported               : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                  10, 11, 12, 13, 14, 15
    Channel                     : 5(auto)
    Channel usage(%)            : 0
    Max power                   : 20 dBm
    Preamble type               : Short
    Operational rate:
        Mandatory               : 6, 12, 24 Mbps
        Multicast               : Auto
        Supported               : 9, 18, 36, 48, 54 Mbps
        Disabled                : Not configured
    Distance                    : 1 km
    ANI                         : Enabled
    Fragmentation threshold     : 2346 bytes
    Beacon interval             : 100 TU
    Protection threshold        : 2346 bytes
    Long retry threshold        : 4
    Short retry threshold       : 7
    Maximum rx duration         : 2000 ms
    Noise Floor                 : 0 dBm
    Protection mode             : rts-cts
    MU-TxBF                     : Enabled
    SU-TxBF                     : Enabled
    Continuous mode             : N/A
    HT protection mode          : No protection
Radio 3:
    Basic BSSID                 : N/A
    Admin state                 : Down
    Radio type                  : 802.11n(2.4GHz)
    Antenna type                : internal
    Client dot11n-only          : Disabled
    Channel band-width          : 20MHz
    Active band-width           : 20MHz
    Secondary channel offset    : SCN
    Short GI for 20MHz          : Supported
    Short GI for 40MHz          : Supported
    mimo                        : Not Config
    Green-Energy-Management     : Disabled
    A-MSDU                      : Enabled
    A-MPDU                      : Enabled
    LDPC                        : Not Supported
    STBC                        : Supported
    Operational HT MCS Set:
        Mandatory               : Not configured
        Supported               : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                  10, 11, 12, 13, 14, 15
        Multicast               : Not configured
    Channel                     : 6(auto)
    Channel usage(%)            : 0
    Max power                   : 20 dBm
    Preamble type               : Short
    Operational rate:
        Mandatory               : 1, 2, 5.5, 11 Mbps
        Multicast               : Auto
        Supported               : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
        Disabled                : Not configured
    Distance                    : 1 km
    ANI                         : Enabled
    Fragmentation threshold     : 2346 bytes
```

```
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise floor               : 0 dBm
    Protection mode           : cts-to-self
    Continuous mode           : N/A
    HT protection mode        : No protection
```

2.18.3 自動 AP の設定例

I. ネットワーク要件

図 2-5 に示すように、AC 上で自動 AP 機能を有効にします。AP は、DHCP Option 43 を通して AC の IP アドレスを取得し、AC との CAPWAP トンネルを確立します。

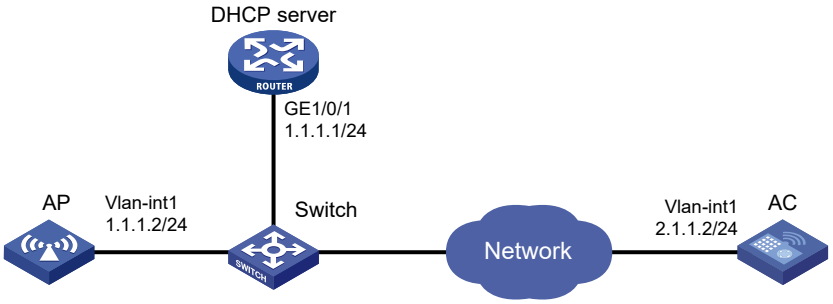


図 2-5 ネットワーク図

II. 設定手順

1)　DHCP サーバを設定します。

DHCP サーバを有効にします。

```
<DHCP server> system-view
[DHCP server] dhcp enable
```

DHCP address pool 1 を設定します。

```
[DHCP server] dhcp server ip-pool 1
[DHCP server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
```

address pool 0 内で AC の IP アドレスを指定するために Option 43 を設定します。右端のバイト 02010102 （2.1.1.2）は AC の IP アドレスを示します。

```
[DHCP server-dhcp-pool-1] option 43 ip-address hex 800700000101010102
```

2)　AC を設定します。

AC 上で VLAN-interface 1 の IP アドレスを 2.1.1.2/24 に設定します。

```
<AC> system-view
[AC] interface vlan-interface 1
```

```
[AC-Vlan-interface1] ip address 2.1.1.2 24
[AC-Vlan-interface1] quit
```

自動 AP を有効にします。

```
[AC] wlan auto-ap
```

III. 設定の確認

#AP が AC との CAPWAP トンネルを確立したか検証します。

```
[AC] display wlan ap name 0011-2200-0101 verbose
AP name                          : 0011-2200-0101
AP ID                            : 1
AP group name                    : default-group
State                            : Run
Backup type                      : Master
Online time                      : 0 days 1 hours 25 minutes 12 seconds
System up time                   : 0 days 2 hours 22 minutes 12 seconds
Model                            : QX-W1020
Region code                      : JP
Region code lock                 : Disable
Serial ID                        : 219801A1JY817BE00001
MAC address                      : 0011-2200-0101
IP address                       : 1.1.1.2
UDP port number                  : 18313
H/W version                      : Ver.C
S/W version                      : 7.2.1
Boot version                     : 0.15
USB state                        : N/A
Power Level                      : N/A
Power info                       : N/A
Description                      : wtp1
Priority                         : 4
Echo interval                    : 10 seconds
Echo count                       : 3 counts
Keepalive interval               : 10 seconds
Discovery-response wait-time     : 2 seconds
Statistics report interval       : 50 seconds
Fragment size (data)             : 1500
Fragment size (control)          : 1450
MAC type                         : Local MAC & Split MAC
Tunnel mode                      : Local Bridging & 802.3 Frame & Native Frame
CWPCAP data-tunnel status        : Up
Discovery type                   : DHCP
Retransmission count             : 3
Retransmission interval          : 5 seconds
Firmware upgrade                 : Enabled
Sent control packets             : 1
Received control packets         : 1
Echo requests                    : 147
Lost echo responses              : 0
Average echo delay               : 3
Last reboot reason               : User soft reboot
Latest IP address                : 10.1.0.2
Current AC IP                    : N/A
Tunnel down reason               : Request wait timer expired
Connection count                 : 1
Backup Ipv4                      : Not configured
Backup Ipv6                      : Not configured
Tunnel encryption                : Disabled
Data-tunnel encryption           : Disabled
Data-tunnel encryption state     : Not encrypted
LED mode                         : Normal
```

```
Remote configuration          : Disabled
Radio 1:
    Basic BSSID               : 7848-59f6-3940
    Admin state               : Up
    Radio type                : 802.11ac
    Antenna type              : internal
    Client dot11ac-only       : Disabled
    Client dot11n-only        : Disabled
    Channel band-width        : 20/40/80MHz
    Active band-width         : 20/40/80MHz
    Secondary channel offset  : SCB
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    Short GI for 80MHz        : Supported
    Short GI for 160MHz       : Not supported
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    mimo                      : Not Config
    Green-Energy-Management   : Disabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational VHT-MCS Set:
        Mandatory             : Not configured
        Supported             : NSS1 0,1,2,3,4,5,6,7,8,9
                                NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast             : Not configured
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 44(auto)
    Channel usage(%)          : 15
    Max power                 : 20 dBm
    Operational rate:
        Mandatory             : 6, 12, 24 Mbps
        Multicast             : Auto
        Supported             : 9, 18, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -102 dBm
    Protection mode           : rts-cts
    MU-TxBF                   : Enabled
    SU-TxBF                   : Enabled
    Continuous mode           : N/A
    HT protection mode        : No protection
Radio 2:
    Basic BSSID               : 7848-59f6-3950
    Admin state               : Down
    Radio type                : 802.11b
    Antenna type              : internal
    Client dot11n-only        : Disabled
    Channel band-width        : 20MHz
    Active band-width         : 20MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    Short GI for 80MHz        : Supported
    Short GI for 160MHz       : Not supported
    mimo                      : Not Config
    Green-Energy-Management   : Disabled
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
```

```
    LDPC                        : Not Supported
    STBC                        : Supported
    Operational HT MCS Set:
        Mandatory               : Not configured
        Supported               : NSS1 0,1,2,3,4,5,6,7,8,9
                                  NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast               : Not configured
    Operational HT MCS Set:
        Mandatory               : Not configured
        Supported               : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                  10, 11, 12, 13, 14, 15
    Channel                     : 5(auto)
    Channel usage(%)            : 0
    Max power                   : 20 dBm
    Preamble type               : Short
    Operational rate:
        Mandatory               : 6, 12, 24 Mbps
        Multicast               : Auto
        Supported               : 9, 18, 36, 48, 54 Mbps
        Disabled                : Not configured
    Distance                    : 1 km
    ANI                         : Enabled
    Fragmentation threshold     : 2346 bytes
    Beacon interval             : 100 TU
    Protection threshold        : 2346 bytes
    Long retry threshold        : 4
    Short retry threshold       : 7
    Maximum rx duration         : 2000 ms
    Noise Floor                 : 0 dBm
    Protection mode             : rts-cts
    MU-TxBF                     : Enabled
    SU-TxBF                     : Enabled
    Continuous mode             : N/A
    HT protection mode          : No protection
Radio 3:
    Basic BSSID                 : N/A
    Admin state                 : Down
    Radio type                  : 802.11n(2.4GHz)
    Antenna type                : internal
    Client dot11n-only          : Disabled
    Channel band-width          : 20MHz
    Active band-width           : 20MHz
    Secondary channel offset    : SCN
    Short GI for 20MHz          : Supported
    Short GI for 40MHz          : Supported
    mimo                        : Not Config
    Green-Energy-Management     : Disabled
    A-MSDU                      : Enabled
    A-MPDU                      : Enabled
    LDPC                        : Not Supported
    STBC                        : Supported
    Operational HT MCS Set:
        Mandatory               : Not configured
        Supported               : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                  10, 11, 12, 13, 14, 15
        Multicast               : Not configured
    Channel                     : 6(auto)
    Channel usage(%)            : 0
    Max power                   : 20 dBm
    Preamble type               : Short
    Operational rate:
        Mandatory               : 1, 2, 5.5, 11 Mbps
        Multicast               : Auto
        Supported               : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
        Disabled                : Not configured
    Distance                    : 1 km
    ANI                         : Enabled
    Fragmentation threshold     : 2346 bytes
    Beacon interval             : 100 TU
    Protection threshold        : 2346 bytes
```

```
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise floor               : 0 dBm
    Protection mode           : cts-to-self
    Continuous mode           : N/A
    HT protection mode        : No protection
```

2.18.4 AP group の設定例

I. ネットワーク要件

図 2-6 に示すように、AP group を設定し、AP 1 を AP group group 1 に、AP 2、AP 3、AP 4 を AP group group 2 に追加します。

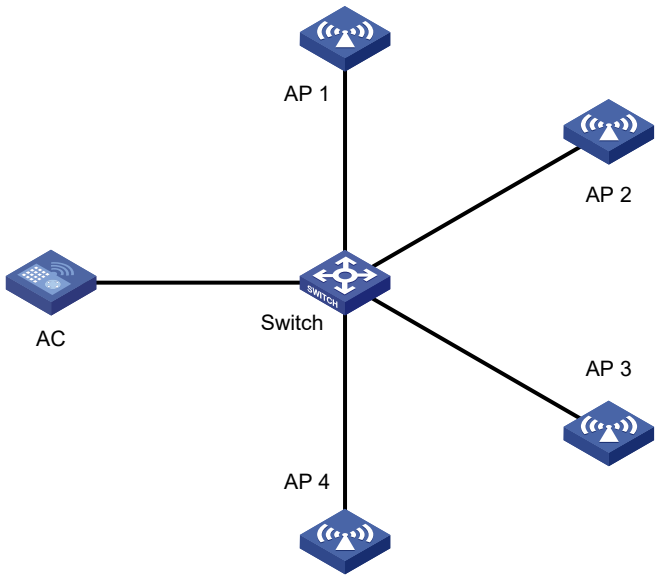


図 2-6 ネットワーク図

II. 設定手順

1) 各 AP が、DHCP サーバから各自の AP の IP アドレスと AC の IP アドレスを入手するように設定します。（詳細は省略します。）
2) 手動 AP を設定します。（詳細は省略します。）
3) AP group を設定します。（詳細は省略します。）

AP group group 1 を作成します。

```
<System> system-view
[System] wlan ap-group group1
```

AP group group 2 を作成します。

```
<System> system-view
[System] wlan ap-group group2
```

#AP 1 を AP group group 1 を追加します。

```
[System] wlan ap-group group1
[System-wlan-ap-group-group1] ap ap1
```

#AP 2、AP 3、AP 4 を AP group group 2 に追加します。

```
[System] wlan ap-group group2
[System-wlan-ap-group-group2] ap ap2 ap3 ap4
```

III. 設定の確認

#AP 1 が AP group group1 内に存在し、AP 2、AP 3、AP 4 が AP group group 2 内に存在することを検証します。

```
[System-wlan-ap-group-group2] display wlan ap-group
Total number of AP groups: 3
AP group name       : default-group
Description         : Not configured
AP model            : Not configured
APs                 : Not configured

AP group name       : group1
Description         : Not configured
AP model            : QX-W1020
AP grouping rules:
  AP name           : ap1
  Serial ID         : Not configured
  MAC address       : Not configured
  IPv4 address      : Not configured
  IPv6 address      : Not configured
APs                 : ap1 (AP name)

AP group name       : group2
Description         : Not configured
AP model            : QX-W1020
AP grouping rules:
  AP name           : ap2, ap3, ap4
  Serial ID         : Not configured
  MAC address       : Not configured
  IPv4 address      : Not configured
  IPv6 address      : Not configured
APs                 : ap2 (AP name), ap3 (AP name), ap4 (AP name)
```

目次

3 章 無線管理の設定 3-1
3.1 概要 3-1
3.1.1 無線モード 3-1
3.1.2 チャネル 3-1
3.1.3 伝送電力 3-2
3.1.4 伝送速度 3-2
3.1.5 MPDU アグリゲーション 3-2
3.1.6 MSDU アグリゲーション 3-3
3.1.7 MCS 3-3
3.1.8 VHT-MCS 3-6
3.1.9 HE-MCS 3-10
3.1.10 OFDMA 3-14
3.1.11 MU-MIMO 3-15
3.1.12 Spatial reuse 3-16
3.2 設定の制限とガイドライン 3-16
3.3 設定作業リスト 3-16
3.4 無線の有効化/無効化 3-18
3.4.1 すべての無線の有効化/無効化 3-18
3.4.2 radio view での無線の有効化/無効化 3-18
3.4.3 AP group radio view での無線の有効化/無効化 3-18
3.5 無線モードの指定 3-19
3.6 基本的な無線機能の設定 3-20
3.6.1 作動チャネルの指定 3-20
3.6.2 自動チャネル選択による欧州チャネルギャップを使用する 2.4GHz の設定 3-21
3.6.3 ブラックリスト、ホワイトリストのチャネル選択の設定 3-21
3.6.4 最大伝送電力の設定 3-22
3.6.5 電力ロックの設定 3-23
3.6.6 伝送速度の設定 3-24
3.6.7 ビーコン間隔の設定 3-25
3.6.8 DTIM 間隔の設定 3-26
3.6.9 衝突回避モードの指定 3-27
3.6.10 RTS しきい値の設定 3-28
3.6.11 フラグメンテーションしきい値の設定 3-29
3.6.12 ハードウェア再伝送の最大数の設定 3-29
3.6.13 AP に関連づけるクライアントの最大数の設定 3-30
3.6.14 802.11b クライアント拒否の設定 3-31
3.6.15 802.11g 保護の設定 3-32
3.6.16 ANI の設定 3-33
3.6.17 プリアンプルタイプの設定 3-33
3.6.18 最大伝送距離の設定 3-34
3.6.19 オンデマンドでのチャネル使用率の測定 3-35
3.6.20 チャネル使用率アラーム閾値の設定 3-35
3.6.21 サービステンプレートの無線モードの設定 3-36
3.6.22 レーダチャネルスイッチバックの設定 3-37
3.7 802.11n 機能の設定 3-37

3.7.1 A-MPDU アグリゲーション方式の指定 3-38
3.7.2 A-MSDU アグリゲーション方式の指定 3-38
3.7.3 ショート GI の設定 3-39
3.7.4 LDPC の設定 3-40
3.7.5 STBC の設定 3-40
3.7.6 MCS インデックスの設定 3-41
3.7.7 802.11n/ac/ax クライアント限定アクセスの設定 3-43
3.7.8 802.11n 帯域幅モードの設定 3-44
3.7.9 エネルギ節約機能の設定 3-45
3.7.10 802.11n 保護の設定 3-46
3.8 802.11ac/ax 機能の設定 3-47
3.8.1 NSS の設定 3-47
3.8.2 802.11ac/ax クライアント限定アクセスの設定 3-49
3.8.3 802.11ac/ax 帯域幅モードの設定 3-50
3.8.4 TxBF の設定 3-51
3.8.5 OFDMA の設定 3-53
3.8.6 BSS カラーリングの設定 3-54
3.8.7 TWT ネゴシエーションの設定 3-56
3.9 無線管理の表示および管理 3-57
3.10 無線管理の設定例 3-57
3.10.1 基本無線機能の設定例 3-57
3.10.2 802.11n 設定例 3-60

3章 無線管理の設定

3.1 概要

RF（Radio Frequency）は、300kHz～300GHz の範囲内で電気的に振動する割合を示します。WLAN は、2.4GHz 帯（2.4GHz～2.4835GHz）と 5GHz 帯（5.150GHz～5.350GHz、および 5.470～5.730GHz）の無線周波数を伝送メディアとして使用します。

“無線周波数”もしくはその略語“RF”は、無線コミュニケーションの“無線”に対する同義語としても使用されます。

3.1.1 無線モード

IEEE 基準では、802.11a、802.11b、802.11g、802.11n、802.11ac、802.11ax を定義しています。

表 3-1 802.11 基準の比較

IEEE 基準	周波数帯	最大速度
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4GHz or 5GHz	600Mbps
802.11ac	5GHz	6900Mbps
802.11gac	2.4GHz	1600Mbps
802.11ax	5GHz	9600Mbps
802.11gax	2.4GHz	2294Mbps

🕮 **メモ：**

- 802.11ac を 2.4GHz で使用するモードを 802.11gac と定義します。
- 802.11ax を 2.4GHz で使用するモードを 802.11gax と定義します。
- 特に指定が無い場合、文中に登場する“802.11ax”には 802.11gac を含みます。
- 特に指定が無い場合、文中に登場する“802.11ax”には 802.11gax が含まれます。
- 到達範囲は、ご利用の環境(電波状況、パソコン性能、遮蔽物など)により異なります。

3.1.2 チャネル

チャネルとは、特定の帯域幅をもつ周波数の範囲のことです。2.4GHz 帯の中には、指定された 14 のチャネルがあります。各チャネルに対する帯域幅は 20MHz で、2 チャネル間は 5MHz 離れています。14 チャネル中、4 グループは重複のないチャネルとして存在し、もっとも一般的に使用されるのはチャネル 1、6、11 です。

5GHz 帯はより高い速度を供給でき、インタフェースに対してより影響を受ける可能性が低いです。5GHz 帯の中には、指定された 19 の重複しないチャネルが存在します。そのチャネルは 20MHz の帯域幅を有し、20MHz の間隔をおいて配置されます。

3.1.3 伝送電力

伝送電力は、無線装置の信号強度を表します。無線は、伝送電力が高いほどより広範囲のエリアをカバーできますが、隣接する装置により多くの影響をもたらします。信号強度は、伝送距離が大きくなるにつれて減衰します。

3.1.4 伝送速度

伝送速度は、無線装置が通信する速度について言及します。伝送速度は、無線モード、拡散方式、コーディング方式、変調方式により変わります。異なる無線モードにサポートされた速度を以下に示します。

- **802.11a**－6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps
- **802.11b**－1Mbps、2Mbps、5.5Mbps、11Mbps
- **802.11g**－1Mbps、2Mbps、5.5Mbps、6Mbps、9Mbps、11Mbps、12 Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps
- **802.11n**－802.11n 無線に対する速度は、チャネル帯域幅により変化します。詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“無線管理の設定”* の *“概要”* の *“MCS”* を参照してください。
- **802.11ac**－802.11ac 無線に対する速度は、チャネル帯域幅および NSS（Number of Spatial Streams）により変化します。詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“無線管理の設定”* の *“MCS”* を参照してください。
- **802.11gac**－2.4GHz 帯で作動し、802.11ac と互換性があります。伝送帯域と NSS（number of spatial streams）によって変わります。詳細は QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“無線管理の設定”* の *“VHT-MCS”* を参照してください。
- **802.11ax**－802.11ax に対する速度は、チャネル帯域幅および NSS（Number of Spatial Streams）により変化します。詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“無線管理の設定”* の *“HE-MCS”* を参照してください。
- **802.11gax**－2.4GHz 帯で作動し、802.11ax と互換性があります。伝送帯域と NSS（number of spatial streams）によって変わります。詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“無線管理の設定”* の *“HE-MCS”* を参照してください。

3.1.5 MPDU アグリゲーション

MPDU（MAC Protocol Data Unit）は、802.11 フォーマット内のデータフレームについて言及します。MPDU アグリゲーションにより、多重の MPDU が 1 つの A-MPDU（Aggregate MPDU）に集約します。これにより、追加情報、ACK（Acknowledgement）フレーム、PLCP

（Physical Layer Convergence Procedure）ヘッダオーバーヘッドが削減され、ネットワーク処理能力とチャネル効率が向上します。

A-MPDU 内のすべての MPDU は、同じ QoS（Quality of Service）優先度、送信元アドレス、宛先アドレスをもたなければなりません。

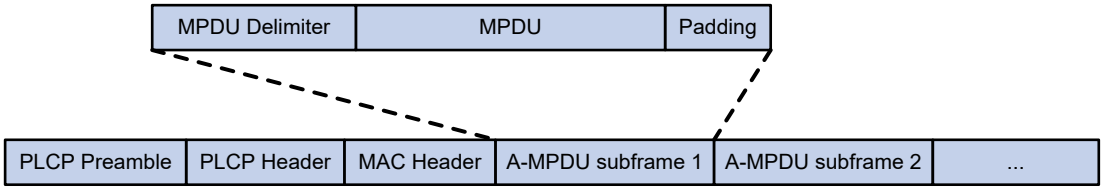


図 3-1 A-MPDU フォーマット

3.1.6 MSDU アグリゲーション

AP もしくはクライアントは、イーサネットヘッダを有する MSDU （MAC Service Data Unit）をカプセル化し、転送するために、フレームを 802.11 フォーマットに変換します。

MSDU アグリゲーションにより、多重の MSDU が 1 つの A-MSDU（Aggregate MSDU）に集約します。これにより、PLCP 序文、PLCP ヘッダ、MAC ヘッダオーバーヘッドが削減され、ネットワーク処理能力と転送効率が向上します。

A-MSDU 内のすべての MSDU は、同じ QoS 優先度、送信元アドレス、宛先アドレスをもたなければなりません。装置が A-MSDU を受信すると、処理のために A-MSDU を多重 MSDU に記憶します。

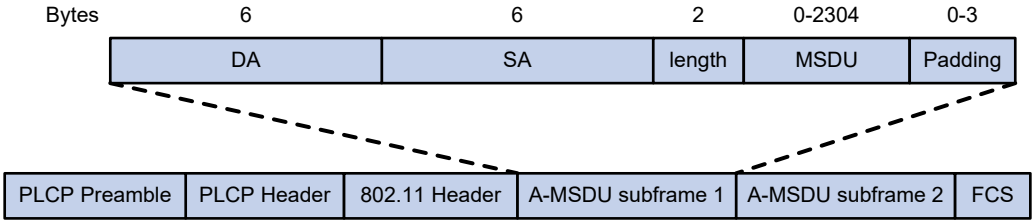


図 3-2 A-MSDU フォーマット

3.1.7 MCS

IEEE 802.11n-2009 内で定義される MCS（Modulation and Coding Scheme）は、変調方式、コーディング、および NSS を決定する値です。MCS は MCS インデックスにより指定され、MCS インデックスは 0～76 の整数で示されます。MCS パラメータは、MCS インデックスからデータ速度までをマッピングしたものです。

表 3-2～表 3-9 は、20MHz と 40MHz の両方に対する MCS パラメータの例を示します。

帯域幅モードが 20MHz のとき、0～15 の MCS インデックスは AP に対して必須であり、0～7 の MCS インデックスはクライアントに対して必須です。

表 3-2 MCS パラメータ（20MHz,NSS=1）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
0	1	BPSK	6.5	7.2
1	1	QPSK	13.0	14.4
2	1	QPSK	19.5	21.7
3	1	16-QAM	26.0	28.9
4	1	16-QAM	39.0	43.3
5	1	64-QAM	52.0	57.8
6	1	64-QAM	58.5	65.0
7	1	64-QAM	65.0	72.2

表 3-3 MCS パラメータ（20MHz,NSS=2）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
8	2	BPSK	13.0	14.4
9	2	QPSK	26.0	28.9
10	2	QPSK	39.0	43.3
11	2	16-QAM	52.0	57.8
12	2	16-QAM	78.0	86.7
13	2	64-QAM	104.0	115.6
14	2	64-QAM	117.0	130.0
15	2	64-QAM	130.0	144.4

表 3-4 MCS パラメータ（20MHz,NSS=3）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
16	3	BPSK	19.5	21.7
17	3	QPSK	39.0	43.3
18	3	QPSK	58.5	65.0
19	3	16-QAM	78.0	86.7
20	3	16-QAM	117.0	130.0
21	3	64-QAM	156.0	173.3
22	3	64-QAM	175.5	195.0
23	3	64-QAM	195.0	216.7

表 3-5 MCS パラメータ（20MHz,NSS=4）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
24	4	BPSK	26.0	28.9
25	4	QPSK	52.0	57.8
26	4	QPSK	78.0	86.7
27	4	16-QAM	104.0	115.6
28	4	16-QAM	156.0	173.3
29	4	64-QAM	208.0	231.1
30	4	64-QAM	234.0	260.0
31	4	64-QAM	260.0	288.9

表 3-6 MCS パラメータ（40MHz,NSS=1）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
0	1	BPSK	13.5	15.0
1	1	QPSK	27.0	30.0
2	1	QPSK	40.5	45.0
3	1	16-QAM	54.0	60.0
4	1	16-QAM	81.0	90.0
5	1	64-QAM	108.0	120.0
6	1	64-QAM	121.5	135.0
7	1	64-QAM	135.0	150.0

表 3-7 MCS パラメータ（40MHz,NSS=2）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
8	2	BPSK	27.0	30.0
9	2	QPSK	54.0	60.0
10	2	QPSK	81.0	90.0
11	2	16-QAM	108.0	120.0
12	2	16-QAM	162.0	180.0
13	2	64-QAM	216.0	240.0
14	2	64-QAM	243.0	270.0
15	2	64-QAM	270.0	300.0

表 3-8 MCS パラメータ（40MHz,NSS=3）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
16	3	BPSK	40.5	45.0
17	3	QPSK	81.0	90.0
18	3	QPSK	121.5	135.0
19	3	16-QAM	162.0	180.0
20	3	16-QAM	243.0	270.0
21	3	64-QAM	324.0	360.0
22	3	64-QAM	364.5	405.0
23	3	64-QAM	405.0	450.0

表 3-9 MCS パラメータ（40MHz,NSS=4）

MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			800 ns GI	400 ns GI
24	4	BPSK	54.0	60.0
25	4	QPSK	108.0	120.0
26	4	QPSK	162.0	180.0
27	4	16-QAM	216.0	240.0
28	4	16-QAM	324.0	360.0
29	4	64-QAM	432.0	480.0
30	4	64-QAM	486.0	540.0
31	4	64-QAM	540.0	600.0

MCS インデックスは以下のタイプに分類されます。

- **必須 MCS インデックス**—AP に対して必須の MCS インデックスです。クライアントは、必須 MCS インデックスを AP に対してサポートするときのみ、802.11n AP に関連づけることができます。
- **サポート MCS インデックス**—AP によりサポートされた MCS インデックスです（必須 MCS インデックスは除きます）。サポート MCS インデックスにより、必須 MCS インデックスとサポート MCS インデックスの両方をサポートするクライアントは、AP と接続するためにより高い速度を使用できます。
- **マルチキャスト MCS インデックス**—AP がマルチキャストフレームを転送する速度と一致する MCS インデックスです。

🕮 **メモ：**

- MCS データ速度については IEEE 802.11n-2009 を参照してください。

3.1.8 VHT-MCS

802.11ac は、無線データ速度を示すために、VHT-MCS（Very High Throughput Modulation and Coding Scheme）インデックスを使用します。VHT-MCS は VHT-MCS インデックスにより識別され、VHT-MCS インデックスは 0～9 の整数で表されます。VHT-MCS パラメータは、VHT-MCS インデックスからデータ速度までをマッピングしたものです。

802.11ac は 20MHz、40MHz、80MHz、160MHz の帯域幅モードをサポートし、最大で 8 つの空間ストリームをサポートします。802.11gac は 20MHz、40MHz の帯域幅モードをサポートします。

表 3-10～表 3-21 は、AP にサポートされた VHT-MCS パラメータを示します。

表 3-10 VHT-MCS パラメータ （20MHz,NSS=1）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	6.5	7.2
1	QPSK	13.0	14.4
2	QPSK	19.5	21.7
3	16-QAM	26.0	28.9
4	16-QAM	39.0	43.3
5	64-QAM	52.0	57.8
6	64-QAM	58.5	65.0
7	64-QAM	65.0	72.2
8	256-QAM	78.0	86.7
9	無効		

表 3-11 VHT-MCS パラメータ （20MHz,NSS=2）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	13.0	14.4
1	QPSK	26.0	28.9
2	QPSK	39.0	43.3
3	16-QAM	52.0	57.8

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
4	16-QAM	78.0	86.7
5	64-QAM	104.0	115.6
6	64-QAM	117.0	130.0
7	64-QAM	130.0	144.4
8	256-QAM	156.0	173.3
9	無効		

表 3-12 VHT-MCS パラメータ（20MHz,NSS=3）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	19.5	21.7
1	QPSK	39.0	43.3
2	QPSK	58.5	65.0
3	16-QAM	78.0	86.7
4	16-QAM	117.0	130.0
5	64-QAM	156.0	173.3
6	64-QAM	175.5	195.0
7	64-QAM	195.0	216.7
8	256-QAM	234.0	260.0
9	256-QAM	260.0	288.9

表 3-13 VHT-MCS パラメータ（20MHz,NSS=4）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	26.0	28.9
1	QPSK	52.0	57.8
2	QPSK	78.0	86.7
3	16-QAM	104.0	115.6
4	16-QAM	156.0	173.3
5	64-QAM	208.0	231.1
6	64-QAM	234.0	260.0
7	64-QAM	260.0	288.9
8	256-QAM	312.0	346.7
9	無効		

表 3-14 VHT-MCS パラメータ（40MHz,NSS=1）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	13.5	15.0
1	QPSK	27.0	30.0
2	QPSK	40.5	45.0
3	16-QAM	54.0	60.0
4	16-QAM	81.0	90.0
5	64-QAM	108.0	120.0
6	64-QAM	121.5	135.0
7	64-QAM	135.0	150.0
8	256-QAM	162.0	180.0

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
9	256-QAM	180.0	200.0

表 3-15 VHT-MCS パラメータ（40MHz,NSS=2）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	27.0	30.0
1	QPSK	54.0	60.0
2	QPSK	81.0	90.0
3	16-QAM	108.0	120.0
4	16-QAM	162.0	180.0
5	64-QAM	216.0	240.0
6	64-QAM	243.0	270.0
7	64-QAM	270.0	300.0
8	256-QAM	324.0	360.0
9	256-QAM	360.0	400.0

表 3-16 VHT-MCS パラメータ（40MHz,NSS=3）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	40.5	45.0
1	QPSK	81.0	90.0
2	QPSK	121.5	135.0
3	16-QAM	162.0	180.0
4	16-QAM	243.0	270.0
5	64-QAM	324.0	360.0
6	64-QAM	364.5	405.0
7	64-QAM	405.0	450.0
8	256-QAM	486.0	540.0
9	256-QAM	540.0	600.0

表 3-17 VHT-MCS パラメータ（40MHz,NSS=4）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	54.0	60.0
1	QPSK	108.0	120.0
2	QPSK	162.0	180.0
3	16-QAM	216.0	240.0
4	16-QAM	324.0	360.0
5	64-QAM	432.0	480.0
6	64-QAM	486.0	540.0
7	64-QAM	540.0	600.0
8	256-QAM	648.0	720.0
9	256-QAM	720.0	800.0

表 3-18 VHT-MCS パラメータ （80MHz,NSS=1）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	29.3	32.5
1	QPSK	58.5	65.0
2	QPSK	87.8	97.5
3	16-QAM	117.0	130.0
4	16-QAM	175.5	195.0
5	64-QAM	234.0	260.0
6	64-QAM	263.0	292.5
7	64-QAM	292.5	325.0
8	256-QAM	351.0	390.0
9	256-QAM	390.0	433.3

表 3-19 VHT-MCS パラメータ （80MHz,NSS=2）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	58.5	65.0
1	QPSK	117.0	130.0
2	QPSK	175.5	195.0
3	16-QAM	234.0	260.0
4	16-QAM	351.0	390.0
5	64-QAM	468.0	520.0
6	64-QAM	526.5	585.0
7	64-QAM	585.0	650.0
8	256-QAM	702.0	780.0
9	256-QAM	780.0	866.7

表 3-20 VHT-MCS パラメータ （80MHz,NSS=3）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	87.8	97.5
1	QPSK	175.5	195.0
2	QPSK	263.3	292.5
3	16-QAM	351.0	390.0
4	16-QAM	526.5	585.0
5	64-QAM	702.0	780.0
6	無効		
7	64-QAM	877.5	975.0
8	256-QAM	1053.0	1170.0
9	256-QAM	1170.0	1300.0

表 3-21 VHT-MCS パラメータ （80MHz,NSS=4）

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
0	BPSK	117.0	130.0
1	QPSK	234.0	260.0
2	QPSK	351.0	390.0
3	16-QAM	468.0	520.0

VHT-MCS インデックス	変調方式	データ速度（Mbps）	
		800 ns GI	400 ns GI
4	16-QAM	702.0	780.0
5	64-QAM	936.0	1040.0
6	64-QAM	1053.0	1170.0
7	64-QAM	1170.0	1300.0
8	256-QAM	1404.0	1560.0
9	256-QAM	1560.0	1733.3

802.11ac の NSS は、以下のタイプに分類されます。

- **必須 NSS**－AP に対して必須の NSS です。クライアントは、AP に対する必須 NSS をサポートするときのみ 802.11ac AP と関連づけることができます。
- **サポート NSS**－AP にサポートされた NSS です（必須 NSS は除きます）。サポート NSS により、必須 NSS とサポート NSS の両方をサポートするクライアントは、AP と接続するためにより高い速度を使用することができます。
- **マルチキャスト NSS**－AP は、マルチキャストフレームを転送するために、VHT-MCS データ速度表内の速度を使用します。

🕮 **メモ：**

- VHT-MCS データ速度については IEEE 802.11ac-2013 を参照してください。

3.1.9 HE-MCS

HE-MCS は、0～11 の整数で表される HE-MCS インデックスによって識別されます。HE-MCS パラメータは、HE-MCS インデックスからデータ速度までをマッピングしたものです。

802.11ax は、20MHz、40MHz、80MHz、および 160MHz の帯域幅モードをサポートし、最大 8 つの空間ストリームをサポートします。802.11gax は、20MHz および 40MHz の帯域幅モードをサポートします。

表 3-22～表 3-33 に、AP でサポートされている HE-MCS パラメータを示します。

表 3-22 HE-MCS パラメータ（20MHz,NSS =1）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	1	BPSK	8.0	8.6
1	1	QPSK	16.0	17.2
2	1	QPSK	24.0	25.8
3	1	16-QAM	33.0	34.4
4	1	16-QAM	49.0	51.6
5	1	64-QAM	65.0	68.8
6	1	64-QAM	73.0	77.4
7	1	64-QAM	81.0	86.0
8	1	256-QAM	98.0	103.2
9	1	256-QAM	108.0	114.7
10	1	1024-QAM	122.0	129.0
11	1	1024-QAM	135.0	143.4

表 3-23 HE-MCS パラメータ （20MHz,NSS =2）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	2	BPSK	16.0	17.2
1	2	QPSK	32.0	34.4
2	2	QPSK	48.0	51.6
3	2	16-QAM	66.0	68.8
4	2	16-QAM	98.0	103.2
5	2	64-QAM	130.0	137.6
6	2	64-QAM	146.0	154.8
7	2	64-QAM	162.0	172.0
8	2	256-QAM	196.0	206.4
9	2	256-QAM	216.0	229.4
10	2	1024-QAM	244.0	258.0
11	2	1024-QAM	270.0	286.8

表 3-24 HE-MCS パラメータ （20MHz,NSS =3）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	3	BPSK	24.0	25.8
1	3	QPSK	48.0	51.6
2	3	QPSK	72.0	77.4
3	3	16-QAM	99.0	103.2
4	3	16-QAM	147.0	154.8
5	3	64-QAM	195.0	206.4
6	3	64-QAM	219.0	232.2
7	3	64-QAM	243.0	258.0
8	3	256-QAM	294.0	309.6
9	3	256-QAM	324.0	344.1
10	3	1024-QAM	366.0	387.0
11	3	1024-QAM	405.0	430.2

表 3-25 HE-MCS パラメータ （20MHz,NSS =4）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	4	BPSK	32.0	34.4
1	4	QPSK	64.0	68.8
2	4	QPSK	96.0	103.2
3	4	16-QAM	132.0	137.6
4	4	16-QAM	196.0	206.4
5	4	64-QAM	260.0	275.2
6	4	64-QAM	292.0	309.6
7	4	64-QAM	324.0	344.0
8	4	256-QAM	392.0	412.8
9	4	256-QAM	432.0	458.8
10	4	1024-QAM	488.0	516.0
11	4	1024-QAM	540.0	573.6

表 3-26 HE-MCS パラメータ （40MHz,NSS =1）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	1	BPSK	16.0	17.2
1	1	QPSK	33.0	34.4
2	1	QPSK	49.0	51.6
3	1	16-QAM	65.0	68.8
4	1	16-QAM	98.0	103.2
5	1	64-QAM	130.0	137.6
6	1	64-QAM	146.0	154.9
7	1	64-QAM	163.0	172.1
8	1	256-QAM	195.0	206.5
9	1	256-QAM	217.0	229.4
10	1	1024-QAM	244.0	258.1
11	1	1024-QAM	271.0	286.8

表 3-27 HE-MCS パラメータ （40MHz,NSS =2）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	2	BPSK	32.0	34.4
1	2	QPSK	66.0	68.8
2	2	QPSK	98.0	103.2
3	2	16-QAM	130.0	137.6
4	2	16-QAM	196.0	206.4
5	2	64-QAM	260.0	275.2
6	2	64-QAM	292.0	309.8
7	2	64-QAM	326.0	344.2
8	2	256-QAM	390.0	413.0
9	2	256-QAM	434.0	458.8
10	2	1024-QAM	488.0	516.2
11	2	1024-QAM	542.0	573.6

表 3-28 HE-MCS パラメータ （40MHz,NSS =3）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	3	BPSK	48.0	51.6
1	3	QPSK	99.0	103.2
2	3	QPSK	147.0	154.8
3	3	16-QAM	195.0	206.4
4	3	16-QAM	294.0	309.6
5	3	64-QAM	390.0	412.8
6	3	64-QAM	438.0	464.7
7	3	64-QAM	489.0	516.3
8	3	256-QAM	585.0	619.5
9	3	256-QAM	651.0	688.2
10	3	1024-QAM	732.0	774.3
11	3	1024-QAM	813.0	860.4

表 3-29 HE-MCS パラメータ （40MHz,NSS =4）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	4	BPSK	64.0	68.8
1	4	QPSK	132.0	137.6
2	4	QPSK	196.0	206.4
3	4	16-QAM	260.0	275.2
4	4	16-QAM	392.0	412.8
5	4	64-QAM	520.0	550.4
6	4	64-QAM	584.0	619.6
7	4	64-QAM	652.0	688.4
8	4	256-QAM	780.0	826.0
9	4	256-QAM	868.0	917.6
10	4	1024-QAM	976.0	1032.4
11	4	1024-QAM	1084.0	1147.2

表 3-30 HE-MCS パラメータ （80MHz,NSS =1）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	1	BPSK	34.0	36.0
1	1	QPSK	68.0	72.1
2	1	QPSK	102.0	108.1
3	1	16-QAM	136.0	144.1
4	1	16-QAM	204.0	216.2
5	1	64-QAM	272.0	288.2
6	1	64-QAM	306.0	324.4
7	1	64-QAM	340.0	360.3
8	1	256-QAM	408.0	432.4
9	1	256-QAM	453.0	480.4
10	1	1024-QAM	510.0	540.4
11	1	1024-QAM	567.0	600.5

表 3-31 HE-MCS パラメータ （80MHz,NSS =2）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	2	BPSK	68.0	72.0
1	2	QPSK	136.0	144.2
2	2	QPSK	204.0	216.2
3	2	16-QAM	272.0	288.2
4	2	16-QAM	408.0	432.4
5	2	64-QAM	544.0	576.4
6	2	64-QAM	612.0	648.8
7	2	64-QAM	680.0	720.6
8	2	256-QAM	816.0	864.8
9	4	256-QAM	906.0	960.8
10	4	1024-QAM	1020.0	1080.8
11	4	1024-QAM	1134.0	1201.0

表 3-32 HE-MCS パラメータ （80MHz,NSS =3）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	3	BPSK	102.0	108.0
1	3	QPSK	204.0	216.3
2	3	QPSK	306.0	324.3
3	3	16-QAM	408.0	432.3
4	3	16-QAM	612.0	648.6
5	3	64-QAM	816.0	864.6
6	3	64-QAM	918.0	973.2
7	3	64-QAM	1020.0	1080.9
8	3	256-QAM	1224.0	1297.2
9	4	256-QAM	1359.0	1441.2
10	4	1024-QAM	1530.0	1621.2
11	4	1024-QAM	1701.0	1801.5

表 3-33 HE-MCS パラメータ （80MHz,NSS =4）

HE-MCS インデックス	NSS	変調方式	データ速度（Mbps）	
			1600 ns GI	800 ns GI
0	4	BPSK	136.0	144.0
1	4	QPSK	272.0	288.4
2	4	QPSK	408.0	432.4
3	4	16-QAM	544.0	576.4
4	4	16-QAM	816.0	864.8
5	4	64-QAM	1088.0	1152.8
6	4	64-QAM	1224.0	1297.6
7	4	64-QAM	1360.0	1441.2
8	4	256-QAM	1632.0	1729.6
9	4	256-QAM	1812.0	1921.6
10	4	1024-QAM	2040.0	2161.6
11	4	1024-QAM	2268.0	2402.0

802.11ax の HE-MCS は、以下のタイプに分類されます。

- **必須 HE-MCS**－AP に対して必須の HE-MCS です。802.11ax AP に関連づけるには、クライアントは AP に対する必須 HE-MCS をサポートする必要があります。
- **サポート HE-MCS**－必須 HE-MCS に加えて、AP によってサポートされる HE-MCS です。クライアントが必須とサポートされている HE-MCS の両方をサポートしている場合、クライアントはサポートされている速度を使用して AP と通信できます。
- **マルチキャスト HE-MCS**－AP がマルチキャストフレームを送信する速度の HE-MCS です。

🕮 **メモ：**

- すべての HE-MCS データ速度については、IEEE802.11ax を参照してください。

3.1.10 OFDMA

802.11 a、802.11 g、802.11 n、および 802.11 ac では、データ伝送に直交周波数分割多重方式 (OFDM) を使用して、1 人のユーザが特定の時間帯にすべてのサブキャリアでデータ

を伝送できるようにします。OFDM に基づき、直交周波数分割多元接続 (OFDMA) は、特定のサブキャリア (トーン) を持つ Resource Unit (RU) として知られるサブチャネルにチャネルを分割し、同時伝送のために異なる RU を異なるユーザに割り当てます。これにより、データレートが増加し、伝送遅延が減少します。

802.11 ax は OFDMA を使用し、いくつかのヌルサブキャリアを予約して、RU でのサブキャリア間干渉を低減します。

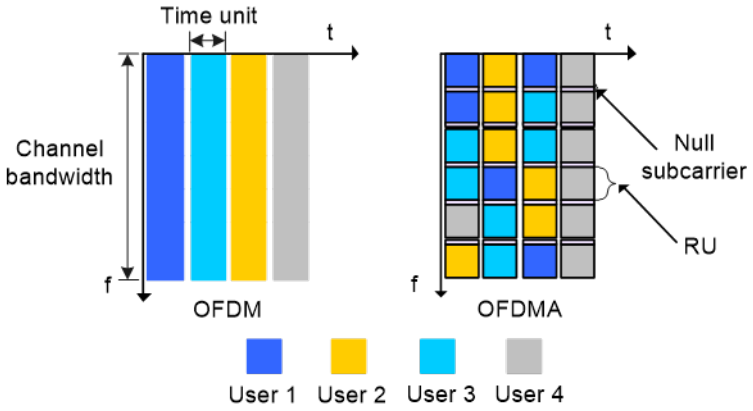


図 3-3 OFDM および OFDMA の動作モード

3.1.11 MU-MIMO

マルチユーザ Multiple-Input Multiple-Output (MU-MIMO) は、帯域幅を個々のストリームに分割して、複数のユーザが同時にデータを送受信できるようにします。

- ダウンリンク MU-MIMO では、AP はビームフォーミングを使用して、異なる場所にある無線クライアントにパケットを送信します。複数の無線クライアントは AP から同時にデータを受信できるようになります。

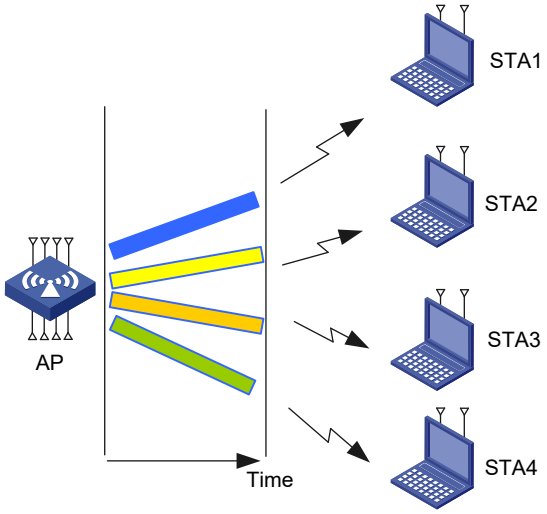


図 3-4 ダウンリンク MU-MIMO

3.1.12 Spatial reuse

Spatial reuse は、無線クライアントが重複する基本サービスセット (OBSS) からの信号を識別し、無線の衝突を回避し、干渉を管理するために特定の情報を使用するのに役立ちます。高密度環境におけるシステム性能とスペクトル資源利用を効果的に改善できます。

802.11 ax は、BSS ごとに BSS カラーと呼ばれる一意でない ID (1 から 63 の範囲)を割り当てて、パケットがクライアントと同じ BSS からのものかどうかを識別できるようにします。

クライアントは 802.11 ax パケットを受信すると、まずパケットヘッダの色を調べます。カラーが関連する AP の BSS のカラーと同じである場合、クライアントはそのパケットが Intra-BSS パケットであると判断します。色が関連する AP の BSS の色と異なる場合、クライアントはそのパケットが BSS 間パケットであると判断します。クライアントは内部 BSS パケットだけを処理し、内部 BSS パケットは無視します。

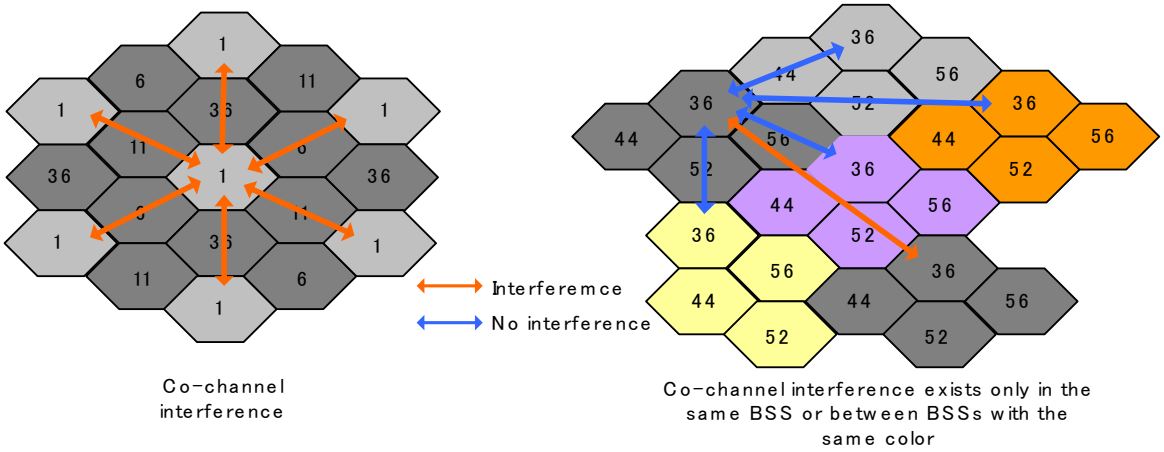


図 3-5 BSS カラーリング

3.2 設定の制限とガイドライン

設定の優先順位は radio view、AP group radio view、global configuration view の順番で優先します。

3.3 設定作業リスト

操作	補足
（必須設定項目） 無線の有効化/無効化	—
（必須設定項目） 無線モードの指定	—
（オプション設定項目） 基本的な無線機能の設定 • 作動チャネルの指定	基本的な無線機能はすべての無線に適用されます。

操作	補足
● 自動チャネル選択による欧州チャネルギャップを使用する2.4GHzの設定 ● ブラックリスト、ホワイトリストのチャネル選択の設定 ● アンテナタイプの設定 ● アンテナゲインの設定 ● 最大伝送電力の設定 ● 電力ロックの設定 ● 伝送速度の設定 ● プリアンプルタイプの設定 ● 最大伝送距離の設定 ● ビーコン間隔の設定 ● DTIM間隔の設定 ● APに関連づけるクライアントの最大数の設定 ● 802.11bクライアントアクセスの設定 ● ANIの設定 ● 衝突回避モードの指定 ● RTSしきい値の設定 ● 802.11g保護の設定 ● フラグメンテーションしきい値の設定 ● ハードウェアの再伝送の最大数の設定 ● オンデマンドでのチャネル使用率の測定 ● チャネル使用率アラーム閾値の設定 ● サービステンプレートの無線モードの設定	
（オプション設定項目） 802.11n機能の設定 ● A-MPDUアグリゲーション方式の指定 ● A-MSDUアグリゲーション方式の指定 ● ショートGIの設定 ● LDPCの設定 ● STBCの設定 ● MCSインデックスの設定 ● 802.11nと802.11ac/axクライアント限定のアクセスの設定 ● 802.11n帯域幅モードの設定 ● エネルギ節約機能の設定 ● 802.11n保護の設定	80211n機能は802.11an、802.11gn、802.11ac、802.11gac、802.11ax、802.11gax無線にのみ適用されます。
（オプション設定項目） 802.11ac/ax機能の設定 ● NSSの設定 ● 802.11ac/axクライアント限定アクセスの設定 ● 802.11ac/ax帯域幅モードの設定	802.11ac/ax機能は802.11ac、802.11gac、802.11ax、802.11gax無線にのみ適用されます。

操作	補足
• TxBFの設定	
（オプション設定項目）スマートアンテナ機能の設定	—

3.4 無線の有効化/無効化

3.4.1 すべての無線の有効化/無効化

注意：
すべての無線を無効にした場合、ワイヤレスサービスが終了します。無効にする場合、影響を十分に考慮して行ってください。

この機能は手動 AP とオンライン自動 AP でのみ適用します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． すべての無線を有効あるいは無効にする	**wlan radio** { **enable** | **disable** }	デフォルト：無線はradio viewあるいはAP group radio viewで有効にしない限り無効です。

3.4.2 radio view での無線の有効化/無効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 無線を有効あるいは無効にする	**radio** { **enable** | **disable** }	デフォルト：**wlan radio enable**コマンドがsystem viewで実行されている場合、有効です。実行されていない場合、AP group radio viewの設定を使用します。

3.4.3 AP group radio view での無線の有効化/無効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 無線を有効にする	**radio** { **enable** | **disable** }	デフォルト：**wlan radio enable**コマンドがsystem view で実行されていない場合、無効です。

3.5 無線モードの指定

注意：

有効化した無線モードを修正すると、関連したすべてのクライアントがログオフになります。

メモ：

- QX-W1100 シリーズは Raido3 で 802.11a、ac、an も指定できますが設定した場合 Raido3 が無効になります。
- QX-W1120 は Radio3 で 802.11gax を設定することができません。Radio 3 を 802.11a、ac、an のいずれかに設定することで、Radio 2 を 802.11gax に設定することができます。

無線モードに応じてチャネルと伝送電力をサポートします。無線モードを変更するとき、システムはチャネルと電力パラメータを自動で無線に適用します。

I. radio view での無線モードの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 無線モードを指定する	**type** { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gn** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での無線モードの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 無線モードを指定する	**type** { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** | **dot11b** | **dot11g** | **dot11gac** | **dot11gax** | **dot11gn** }	デフォルト：APモデルにより異なります。

3.6 基本的な無線機能の設定

3.6.1 作動チャネルの指定

無線装置と非無線装置の両方からのインタフェースを削減するためにこのタスクを実行します。

無線チャネルを選択するため、手動もしくはシステムで自動に設定することができます。

無線の作動チャネル上でレーダ信号が検出されると、チャネルが手動で指定されているか自動的に割り当てられているかにかかわらず、無線は使用中のチャネルを変更します。レーダチャネルスイッチバックが有効の場合は、30 分経過後に変更前に使用していたチャネルに戻り、静止タイマを起動します。静止時間内にレーダ信号が検出されなければ、無線はそのチャネルの使用を開始します。静止時間内にレーダ信号が検出されると、無線は再びチャネルを変更します。

レーダチャネルスイッチバックが無効の場合は、30 分経過しても変更後のチャネルを使用し続けます。

I. radio view での作動チャネルの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 作動チャネルを指定する	**channel** { *channel-number* | **auto** { **lock** | **unlock** } }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での作動チャネルの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. 作動チャネルを指定する	**channel** { *channel-number* | **auto** { **lock** | **unlock** } }	デフォルト：ACは無線に対して自動でチャネルを選択し、ロックしません。

3.6.2 自動チャネル選択による欧州チャネルギャップを使用する 2.4GHz の設定

2.4GHz 無線は、チャネル 1、6、11 を自動で選択するため、デフォルトで非欧州チャネルのギャップ 5 を使用します。この機能を有効にすることで、欧州チャネルギャップ 6 を使用し、チャネル 1、7、13 を自動で選択することができます。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. global configuration view に移行する	**wlan global-configuration**	—
3. 自動チャネル選択による欧州チャネルギャップを使用する 2.4GHz を設定する	**auto-channel european-gap enable**	デフォルト：無効

3.6.3 ブラックリスト、ホワイトリストのチャネル選択の設定

本機能を行うと、AP で自動チャネルを使用するとき、ブラックリストのチャネルを選択しない、あるいはホワイトリストのチャネルのみ選択することができます。同一 AP でブラックリストとホワイトリストのチャネルの両方を設定することはできません。

I. 制限とガイドライン

本機能は自動チャネル選択モードで動作する AP にのみ適用可能です。

II. radio view でのブラックリスト、ホワイトリストのチャネル選択の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—

操作	コマンド	補足
3． radio view へ移行する	**radio** *radio-id*	—
4． ブラックリスト、ホワイトリストのチャネル選択を設定する	**channel auto-select** { **blacklist** | **whitelist** } *channel-number*	デフォルト：無線はAP group radio viewの設定を使用します。

III. AP group radio view でのブラックリスト、ホワイトリストのチャネル選択の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	—
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． ブラックリスト、ホワイトリストのチャネル選択を設定する	**channel auto-select** { **blacklist** | **whitelist** } *channel-number*	デフォルト：設定なし

3.6.4 最大伝送電力の設定

最大伝送電力が、無線にサポートされた伝送電力範囲内であることを確認します。無線にサポートされた伝送電力範囲は、カントリーコード、チャネル、AP モデル、無線モード、アンテナタイプ、帯域幅モードにより変化します。最大伝送電力を設定後、無線に対するこれらの特性を変更する場合、設定された最大伝送電力がサポートされた伝送電力の範囲を超える可能性があります。範囲を超えた場合、システムは自動的に最大伝送電力を有効な値に適応させます。

電力ロックを有効にする場合、ロックされた電力が最大伝送電力になります。電力ロックに関する詳細な情報については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“無線管理の設定”* の *“電力ロックの設定”* を参照してください。

I. radio view での最大伝送電力の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 最大伝送電力を設定する	**max-power** *radio-power*	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での最大伝送電力の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 最大伝送電力を設定する	**max-power** *radio-power*	デフォルト：無線はサポートされた最大伝送電力を使用します。

3.6.5 電力ロックの設定

電力ロックを有効にする場合、現在の電力はロックされ、最大伝送電力となります。ロックされた電力は、AC を再始動したのちも適用されます。

電力ロックを有効にした無線が、ロックされた電力より低い電力を供給する新たなチャネルに切り替わる場合、新規のチャネルによってサポートされた最大電力が適用されます。

I. radio view での電力ロックの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 電力ロックを設定する	**power-lock** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での電力ロックの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—

操作	コマンド	補足
4． radio view へ移行する	**radio** *radio-id*	—
5． 電力ロックを設定する	**power-lock** { **disable** | **enable** }	デフォルト：無効

3.6.6 伝送速度の設定

伝送速度は以下のタイプに分類されます。

- **禁止速度**—AP により使用できない速度です。
- **必須速度**—AP と関連づけるためにクライアントがサポートしなければならない速度です。
- **サポート速度**—AP がサポートする速度です。クライアントが AP と関連づけられたたあと、クライアントは AP と接続するために、サポートされた速度より高い速度を選択することができます。多くのインタフェース、再伝送、あるいはパケット廃棄を検出したとき、AP は自動的に伝送速度を低減します。また少ないインタフェース、再伝送、パケット廃棄を検出したとき、自動的に伝送速度を増加します。
- **マルチキャスト速度**—AP 伝送マルチキャストとブロードキャストが伝送する速度です。マルチキャスト速度は必須速度から選択する必要があります。

I. radio view での伝送速度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 無線に伝送速度を設定する	**rate** { **multicast** { **auto** | *rate-value* } | { **disabled** | **mandatory** | **supported** } *rate-value* }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での伝送速度の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view を入力する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 無線に伝送速度を設定する	**rate** { **multicast** { **auto** | *rate-value* } | { **disabled** | **mandatory** | **supported** } *rate-value* }	デフォルト： • 802.11a/802.11an/802.11ac/802.11ax無線： 　• **禁止速度**：なし

操作	コマンド	補足
		• **必須速度**：6、12、24 • **マルチキャスト速度**：必須速度から選択します。 • **サポート速度**：9、18、36、48、54 ● 802.11b 無線： • **禁止速度**：なし • **必須速度**：1、2 • **マルチキャスト速度**：必須速度から選択します。 • **サポート速度**：5.5、11 ● 802.11g/802.11gn/802.11gac/802.11gax無線： • **禁止速度**：なし • **必須速度**：1、2、5.5、11 • **マルチキャスト速度**：必須速度から選択します。 • **サポート速度**：9、12、18、24、36、48、54

3.6.7 ビーコン間隔の設定

AP が、指定された間隔でビーコンフレームをブロードキャストできるように、ビーコン間隔を設定します。小さなビーコン間隔により、クライアントは AP を容易に検出することができますが、より多くのシステムリソースを消費します。

I. radio view でのビーコン間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． ビーコン間隔を設定する	**beacon-interval** *interval*	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view でのビーコン間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． ビーコン間隔を設定する	**beacon-interval** *interval*	デフォルト：100 TU

3.6.8 DTIM 間隔の設定

AP は、DTIM（Delivery Traffic Indication Map）に従ったビーコンを周期的にブロードキャストします。ビーコンをブロードキャストしたのち、AP は DTIM 間隔の値にもとづいてバッファされたブロードキャストとマルチキャストフレームを送信します。たとえば、DTIM 間隔を 5 に設定した場合、AP はバッファされたブロードキャストとマルチキャストフレームを 5 ビーコンフレームごとに送信します。

I. radio view での DTIM 間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． DTIM 間隔を設定する	**dtim** *counter*	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での DTIM 間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． DTIM 間隔を設定する	**dtim** *counter*	デフォルト：1

3.6.9 衝突回避モードの指定

無線装置は半二重モードで作動し、データの送受信を同時に行うことはできません。802.11 により、衝突を回避するために、無線装置は RTS（Request to Send）パケットもしくは CTS（Clear to Send）パケットを送信できるようになります。

AP に対して以下の衝突回避モードのいずれかを指定することができます。

- **RTS/CTS**－AP は、クライアントにデータを送信する前に、RTS パケットを送信します。RTS パケットを受信したあと、クライアントは CTS パケットを AP に送信します。CTS パケット受信後、AP はデータの送信を開始します。また、その RTS パケットもしくは CTS パケットを検出した別の装置が、指定された時間内にデータを送信することはありません。

🕮 **メモ：**

802.11b 無線は RTS/CTS モードのみサポートします。

- **CTS-to-self**－AP は、クライアントにデータを送信する前に、CTS パケットを送信します。この CTS パケットには、AP 自体の MAC アドレスが宛先 MAC アドレスとして付随されています。CTS-to-self パケット受信後、AP はデータの送信を開始します。また、その CTS-to-self パケットを受信した別の装置が、指定された時間内にデータを送信することはありません。CTS-to-self モードにより伝送時間は減少しますが、隠れたノード問題を引き起こす可能性があります。

無線リソース効率を保証するために、以下の条件が満たされるときに限り衝突回避が適用されます。

- 送信されるパケットが、RTS しきい値 2346 バイトより長い場合。
- 802.11g 保護もしくは 802.11n 保護が有効な場合。802.11g 保護もしくは 802.11n 保護に関する詳細な情報は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“無線管理の設定”*の *“802.11g 保護の設定”*と *“802.11n 保護の設定”* を参照してください。

I. radio view での衝突回避モードの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． 衝突回避モードを指定する	**protection-mode** { **cts-to-self** | **rts-cts** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での衝突回避モードの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view へ移行する	**wlan ap-group** *group-name*	—

操作	コマンド	補足
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 衝突回避モードを指定する	**protection-mode** { **cts-to-self** | **rts-cts** }	デフォルト：CTS-to-selfモード

3.6.10 RTS しきい値の設定

802.11 により、無線装置は衝突回避のために RTS パケットもしくは CTS パケットを送信できるようになります。しかし、過度な RTS パケットや CTS パケットはシステムリソースの過剰消費の原因となり、伝送効率を低下させます。この問題を解決するために、RTS しきい値を設定することができます。このシステムは、パケットが RTS しきい値より大きい場合に限り衝突回避を実行します。

低密度 WLAN 内では、ネットワークの処理能力と効率を向上させるために RTS しきい値を増加させます。

高密度 WLAN 内では、ネットワーク内の衝突を減少させるために RTS しきい値を低下させます。

I. radio view での RTS しきい値の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． RTS しきい値を設定する	**protection-threshold** *size*	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での RTS しきい値の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view へ移行する	**wlan ap-group** *group-name*	—
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． RTS しきい値を設定する	**protection-threshold** *size*	デフォルト： 2346 バイト

3.6.11 フラグメンテーションしきい値の設定

フラグメンテーションのしきい値より大きいフレームは、伝送の前にフラグメントされます。フラグメンテーションのしきい値より小さいフレームは、フラグメントされずに伝送されます。

多くのインタフェースを有する WLAN 内では、ネットワーク処理能力と効率を向上させるために、フラグメンテーションのしきい値を低く設定してください。

I. radio view でのフラグメンテーションしきい値の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view へ移行する	**radio** *radio-id*	—
4. フラグメンテーションしきい値を設定する	**fragment-threshold** *size*	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view でのフラグメンテーションしきい値の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view へ移行する	**wlan ap-group** *group-name*	—
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. フラグメンテーションしきい値を設定する	**fragment-threshold** *size*	デフォルト： 2346バイト

3.6.12 ハードウェア再伝送の最大数の設定

無線ネットワークにおいて、ユニキャストフレームは Acknowledgement を必要とします。装置がパケットに対する Acknowledgement の受信に失敗した場合、装置はパケットを再伝送します。

装置が Acknowledgement の受信に失敗しつづけ、フレーム再伝送の最大値に達した場合、装置はパケットを破棄し上位レイヤに伝送失敗のプロトコルを通知します。

ハードウェア再伝送の最大数の値を、大きいフレームと小さいフレームに対して異なる値で設定することができます。大きいフレームとは、RTS しきい値より大きいフレームを示し、小さいフレームとは、RTS しきい値以下のフレームを示します。

大きいフレームの伝送には、大きなバッファサイズと長い時間が必要となります。なぜなら、システムは大きなフレームを伝送する前に、衝突回避を実行しなければならないからです。したがって、システムバッファと伝送時間を節約するために、大きなフレームに対するハードウェア再伝送の最大数を小さくすることができます。

I. radio view でのフレーム再伝送の最大数の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view へ移行する	**radio** *radio-id*	—
4. 小さいフレームに対するフレーム再伝送の最大数を設定する	**short-retry threshold** *count*	デフォルト：無線はAP group radio viewの設定を使用します。
5. 大きいフレームに対するフレーム再伝送の最大数を設定する	**long-retry threshold** *count*	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view でのフレーム再伝送の最大数の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view へ移行する	**wlan ap-group** *group-name*	—
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. 小さいフレームに対するフレーム再伝送の最大数を設定する	**short-retry threshold** *count*	デフォルト：7
6. 大きいフレームに対するフレーム再伝送の最大数を設定する	**long-retry threshold** *count*	デフォルト：4

3.6.13 AP に関連づけるクライアントの最大数の設定

クライアントの数が AP 上で最大になると、AP は新たなクライアントの許可を停止します。これにより、AP に過負荷がかかることを防ぎます。

I. radio view での AP に関連づけるクライアントの最大数の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. AP に関連づけるクライアントの最大数を設定する	**client max-count** *max-number*	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での AP に関連づけるクライアントの最大数の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． AP に関連づけるクライアントの最大数を設定する	**client max-count** *max-number*	デフォルト：設定なし（各APの最大接続数）

3.6.14 802.11b クライアント拒否の設定

低速度の 802.11b クライアントの影響を軽減し、無線データ伝送の速度をあげるために、802.11g 無線、802.11gn 無線、802.11gac 無線、802.11gax 無線に 802.11b クライアントにアクセスするのを禁止するように設定できます。

I. radio view での 802.11b クライアント拒否の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 802.11b クライアント拒否を設定する	**client dot11b-forbidden** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での 802.11b クライアント拒否の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11b クライアント拒否を設定する	**client dot11b-forbidden** { **disable** | **enable** }	デフォルト：無効

3.6.15 802.11g 保護の設定

重要：

この機能は、802.11g 無線、802.11n（2.4GHz）無線、802.11gac 無線、802.11gax 無線にのみ適用されます。

802.11b と 802.11g のクライアントの両方が WLAN 内に存在しているとき、両者は異なる変調モードを使用するため伝送衝突が生じる可能性があります。802.11g 保護を設定することにより、そのような衝突を回避することができます。また、メディアに対するアクセスを遅らせるように 802.11b クライアントに知らせるために、802.11g、802.11n、802.11ac、802.11ax 装置が RTS/CTS パケットまたは CTS-to-self パケットを送信できるようになります。RTS/CTS または CTS-to-self に関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"無線管理の設定"* の *"衝突回避モードの指定"* を参照してください。

802.11g、802.11n、802.11gac 装置は、チャネル上で 802.11b 信号を検出したときに限り、データを送信する前に RTS/CTS パケットもしくは CTS-to-self パケットを送信します。

802.11g 保護は、802.11b クライアントが 802.11g、802.11n（2.4GHz）、802.11gac 、802.11gax AP に関連づけされたとき、自動的に適用されます。

I. radio view での 802.11g 保護の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． 802.11g 保護を設定する	**dot11g protection** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での 802.11g 保護の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view へ移行する	**wlan ap-group** *group-name*	—
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11g 保護を設定する	**dot11g protection** { **disable** | **enable** }	デフォルト：無効

3.6.16 ANI の設定

ANI（Adaptive Noise Immunity）は、周辺環境からの干渉を減少させるために、無線装置が環境にもとづいた騒音防止レベルを調整できるようにします。

I. radio view での ANI の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． ANI を設定する	**ani** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での ANI の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． ANI を設定する	**ani** { **disable** | **enable** }	デフォルト：有効

3.6.17 プリアンプルタイプの設定

⚠ **重要**：
プリアンプルタイプの設定機能は、802.11b 無線、802.11g 無線、802.11gn 無線に対してのみ適用されます。

プリアンプルは、送信側と受信側の間で伝送信号を同期させるためのパケットヘッダ内のビットのセットです。short プリアンプルはネットワーク性能を改善し、long プリアンプルは初期モデルのすべての無線装置との互換性を保証します。

I. radio view でのプリアンプルタイプの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． プリアンプルタイプを設定する	**preamble** { **long** | **short** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view でのプリアンプルタイプの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． プリアンプルタイプを設定する	**preamble** { **long** | **short** }	デフォルト：**short**

3.6.18 最大伝送距離の設定

無線信号の強さは、伝送距離が大きくなるにつれて徐々に低下します。無線信号の最大伝送距離は、周辺の環境や外部アンテナの使用の有無に依存します。

- **外部アンテナ不使用**—約 300m。
- **外部アンテナ使用**—30km～50km
- **障害のあるエリア**—35m～50m

I. radio view での最大伝送距離の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 最大伝送距離を設定する	**distance** *distance*	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での最大伝送距離の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. 最大伝送距離を設定する	**distance** *distance*	デフォルト：1km

3.6.19 オンデマンドでのチャネル使用率の測定

この機能は、AP でサポートされるチャネルと、スキャニングを行った後、チャネルの使用率を表示します。

以下にオンデマンドでのチャネル使用率を測定する手順を示します。

操作	コマンド
1. system view に移行する	**system-view**
2. AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]
3. radio view へ移行する	**radio** *radio-id*
4. オンデマンドでのチャネル使用率を測定する	**channel-usage measure**

3.6.20 チャネル使用率アラーム閾値の設定

🕮 **メモ：**

チャネル使用率アラーム閾値の設定は、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

チャネル使用率がしきい値を超えると、装置は info-center にアラームを報告します。

以下にチャネル使用率アラームしきい値を設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—

操作	コマンド	補足
4. チャネル使用率アラームのしきい値を設定する	**channel-usage threshold** *threshold*	デフォルト：90%。

3.6.21 サービステンプレートの無線モードの設定

メモ：

サービステンプレートの無線モードの設定は、ソフトウェアバージョン 7.2.63 を含む以降のソ フトウェアからサポートしています。

デフォルトでは、無線に設定した無線モードが、この無線によって提供されるすべての BSS に適用されます。

無線が異なる無線モードを使用して BSS を提供するには、サービステンプレート毎に異なる無線モードを指定しサービステンプレートを無線にバインドします。

2.4 GHz 無線モードのレベルは、802.11gax、802.11gac、802.11gn、802.11g の順に低くなります。

5 GHz 無線モードのレベルは、802.11ax、802.11ac、802.11an、802.11a の順に低くなります。

Service template view と Radio view の両方で無線モードを設定すると、下位レベルの無線モードが有効になります。Radio view で指定した無線モードのレベルが、バインドされたサービステンプレートのいずれかで指定した無線モードよりも高いことを確認してください。

この作業を実行する前に、サービステンプレートが無効になっていることを確認してください。

以下にサービステンプレートの無線モードの設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Service template view に移行する	**wlan service-template** *service-template-name*	—
3. 無線モードを指定する	• **radio-type 2.4g** { **dot11g** | **dot11gac** | **dot11gax** | **dot11gn** } • **radio-type 5g** { **dot11a** | **dot11ac** | **dot11an** | **dot11ax** }	デフォルト：設定なし

3.6.22 レーダチャネルスイッチバックの設定

🕮 **メモ：**

- QX-W1100 シリーズの Anchor-AC は、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからレーダチャネルスイッチバックの設定をサポートしています。
- QX-W1000 シリーズの Anchor-AC は、ソフトウェアバージョン 7.2.74 を含む以降のソフトウェアからレーダチャネルスイッチバックの設定をサポートしています。

無線の作動チャネル上でレーダ信号が検出されると、チャネルが手動で指定されているか自動的に割り当てられているかにかかわらず、無線は使用中のチャネルを変更します。

レーダチャネルスイッチバックを無効にすると、レーダ信号の検出によるチャネル変更をしてから 30 分経過しても、AP が元のチャネルに切り替えないようにすることができます。この場合、AP は新しいチャネルを使用し続けます。

以下にレーダチャネルスイッチバックの設定手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view へ移行する	**wlan global-configuration**	—
3． レーダチャネルスイッチバックを設定する	**radar-channel-switchback disable**	デフォルト：有効

3.7 802.11n機能の設定

🕮 **メモ：**

802.11n に対するサポートは装置のモデルに依存します。

⚠ **重要：**

AP に対して 802.11n 機能を設定するとき、別のユーザが同じ AP に対して 802.1n 機能を設定している場合、設定は失敗します。

IEEE 802.11n は、高品質の無線サービスを提供し、WLAN が Ethernet と同じネットワークパフォーマンスを実現できるように定義されました。802.11n は、物理レイヤと MAC（Media Access Control）レイヤを最適化することにより、WLAN の処理能力と伝送速度を向上させます。

802.11n の物理レイヤは、OFDM にもとづいています。802.11n は、物理レイヤでの高い処理能力を実現するために、MIMO（Multiple Input Multiple Output）、40MHz 帯域幅、ショート GI（Guard Interval）、STBC（Space-Time Block Coding）、および LDPC（Low-Density Parity Check）を使用します。また、802.11n は、MAC レイヤでの伝送効率を向

上させるために、A-MPDU、A-MSDU、および BA（Block Acknowledgment）を使用します。

3.7.1 A-MPDU アグリゲーション方式の指定

I. radio view での A-MPDU アグリゲーション方式の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． A-MPDU アグリゲーション方式を指定する	**a-mpdu** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での A-MPDU アグリゲーション方式の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． A-MPDU アグリゲーション方式を指定する	**a-mpdu** { **disable** | **enable** }	デフォルト： 無効

3.7.2 A-MSDU アグリゲーション方式の指定

I. radio view での A-MSDU アグリゲーション方式の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． A-MSDU アグリゲーション方式を指定する	**a-msdu** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での A-MSDU アグリゲーション方式の指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. A-MSDU アグリゲーション方式を指定する	**a-msdu** { **disable** | **enable** }	デフォルト：有効

3.7.3 ショート GI の設定

802.11 OFDM は、伝送するためフレームをデータブロックにフラグメントします。また、データブロック伝送が互いに干渉せず、伝送遅延の影響を受けづらくなることを保障するため、802.11 OFDM は GI を使用します。

802.11a/g に使用される GI は 800ns です。802.11n は 400ns のショート GI をサポートします。ショート GI により、データ速度は 10%向上します。

20MHz 帯域幅モードと 40MHz 帯域幅モードのどちらもショート GI をサポートします。

I. radio view でのショート GI の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. ショート GI を設定する	**short-gi** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view でのショート GI の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。

操作	コマンド	補足
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． ショート GI を設定する	**short-gi** { **disable** | **enable** }	デフォルト：有効

3.7.4 LDPC の設定

802.11n は、S/N 比（信号対雑音比）と伝送品質を向上させるために、LDPC（Low-Density Parity Check）機能を導入します。LDPC は、両端が LDPC をサポートするときに限り適用されます。

I. radio view での LDPC の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． LDPC を設定する	**ldpc** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での LDPC の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． LDPC を設定する	**ldpc** { **disable** | **enable** }	デフォルト：無効

3.7.5 STBC の設定

STBC（Space-Time Block Coding）機能により、データ伝送の信頼性を向上させることができます。また、STBC 機能は、クライアントに対して高い伝送速度を要求しません。

I. radio view での STBC の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． STBC を設定する	**stbc** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での STBC の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． STBC を設定する	**stbc** { **disable** | **enable** }	デフォルト：有効

3.7.6 MCS インデックスの設定

802.11n AP に対して MCS インデックスを設定するとき、以下の制限とガイドラインに従ってください。

- 802.11n クライアントは、ユニキャストフレームを送信するために、MCS インデックスと一致した速度を使用します。802.11a/b/g クライアントは、ユニキャストフレームを送信するために、802.11a/b/g 速度を使用します。
- マルチキャスト MCS インデックスを設定しない場合、802.11n クライアントと AP は、マルチキャストフレームを送信するために、802.11a/b/g マルチキャスト速度を使用します。マルチキャスト MCS インデックスを設定する場合、以下のケースのいずれかが発生します。
  - □ すべてのクライアントが 802.11n クライアントの場合、AP とクライアントはマルチキャストフレームを送信するために、マルチキャスト MCS インデックスと一致する速度を使用します。
  - □ 802.11a/b/g クライアントが存在する場合、AP とクライアントはマルチキャストフレームを送信するために、802.11a/b/g マルチキャスト速度を使用します。
- 最大必須 MCS インデックスあるいはサポート MCS インデックスを設定するとき、実際に範囲を指定します。たとえば、最大必須 MCS インデックスを 5 に設定する場合、0～5 の MCS インデックスに一致する速度が 802.11n 必須速度として設定されます。
- マルチキャスト MCS インデックスは最大必須 MCS インデックスより大きくすることはできません。

- 最大サポート MCS インデックスは最大必須 MCS インデックスより小さくすることはできません。

I. radio view での MCS インデックスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. 最大必須 MCS インデックスを設定する	**dot11n mandatory maximum-mcs** *index*	デフォルト： ● 最大サポートMCSインデックスが設定されている場合、最大必須MCSインデックスは設定されません。 ● 最大サポートMCSインデックスが設定されていない場合、無線はAP group radio viewの設定を使用します。
5. 最大サポート MCS インデックスを設定する	**dot11n support maximum-mcs** *index*	デフォルト： ● 最大必須MCSインデックスが設定されている場合、最大サポートMCSインデックスは76です。 ● 最大必須MCSインデックスが設定されていない場合、無線はAP group radio viewの設定を使用します。 最大サポートMCSインデックスは、最大必須MCSインデックスより小さくすることはできません。
6. マルチキャスト MCS インデックスを設定する	**dot11n multicast-mcs** *index*	デフォルト： ● 最大サポートMCSインデックスまたは最大必須MCSインデックスが設定されている場合、マルチキャストMCSインデックスは設定されません。 ● 最大サポートMCSインデックスと最大必須MCSインデックスのどちらも設定されていない場合、無線はAP group radio viewの設定を使用します。 マルチキャストMCSインデックスは、最大必須MCSインデックスより大きくすることはできません。

II. AP group radio view での MCS インデックスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. 最大必須 MCS インデックスを設定する	**dot11n mandatory maximum-mcs** *index*	デフォルト：設定なし
6. 最大サポート MCS インデックスを設定する	**dot11n support maximum-mcs** *index*	デフォルト： 76 最大サポートMCSインデックスは、最大必須MCSインデックスより小さくすることはできません。
7. マルチキャスト MCS インデックスを設定する	**dot11n multicast-mcs** *index*	デフォルト：設定なし マルチキャストMCSインデックスは、最大必須MCSインデックスより大きくすることはできません。

3.7.7 802.11n/ac/ax クライアント限定アクセスの設定

低速の 802.11a/b/g クライアントの影響を減らし、無線データ通信を加速するために、802.11n/ac/ax クライアントにのみアクセスできるように AP を設定することができます。

I. radio view での 802.11n/ac/ax クライアント限定アクセスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. 802.11n/ac/ax クライアント限定アクセスを設定する	**client dot11n-only** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での 802.11n/ac/ax クライアント限定アクセスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11n/ac/ax クライアント限定アクセスを設定する	**client dot11n-only** { **disable** | **enable** }	デフォルト：無効

3.7.8 802.11n 帯域幅モードの設定

802.11n は 802.11a/b/g のチャネル構造を使用しますが、データを送信するための 20MHz のチャネルにおけるサブチャネルの数は 52 まで増加します。これにより、データ通信速度は向上します。

802.11n は、2 つの隣接した 20MHz のチャネルに対して、40MHz のチャネル（一方は 1 次チャネル、もう一方は 2 次チャネル）を形成することを義務づけます。これは、データ転送速度を 2 倍にする簡単な方法を提供します。

無線のための帯域幅は帯域幅モード設定とチップ機能により変化します。

I. radio view での 802.11n 帯域幅モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 802.11n 帯域幅モードを設定する	**channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト：無線はAP group radio viewの設定を使用します。 802.11gn無線のみ**auto-switch** パラメータをサポートします。

II. AP group radio view での 802.11n 帯域幅モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11n 帯域幅モードを設定する	**channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト：802.11an無線のデフォルトは40MHzです。802.11gn無線のデフォルトは20MHzです。802.11gn無線のみ**auto-switch**パラメータをサポートします。

3.7.9 エネルギ節約機能の設定

エネルギ節約機能を有効にしたあと、無線に関連づけられたクライアントが存在しない場合、無線の MIMO モードは自動的に 1x1 に変更されます。これにより電力の消費を抑えることができます。

I. radio view でのエネルギ節約機能の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． エネルギ節約機能を設定する	**green-energy-management** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view でのエネルギ節約機能の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． エネルギ節約機能を設定する	**green-energy-management** { **disable** | **enable** }	デフォルト：無効

3.7.10 802.11n 保護の設定

802.11n と 802.11n 以外のクライアントの両方が WLAN 内に存在しているとき、両者は異なる変調モードを使用するため伝送衝突が生じる可能性があります。802.11n 保護はそのような衝突を避けることができます。802.11n 保護により、802.11n 機器は 802.11n 以外のクライアントに対してメディアへのアクセスを延期するよう知らせるために、RTS/CTS または CTS-to-self パケットを送信することができるようになります。RTS/CTS または CTS-to-self に関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“無線管理の設定”* の *“衝突回避モードの指定”* を参照してください。

802.11n 機器は、チャネルの上で 802.11n 以外の信号が検出された場合に限り、データを送信する前に RTS/CTS または CTS-to-self パケットを送信します。

802.11n 保護は、802.11n 以外のクライアントが 802.11n AP と関連づけられたとき、自動的に適用されます。

🕮 **メモ：**

802.11n 装置は、802.11n 装置と 802.11ac/ax 装置を指します。

I. radio view での 802.11n 保護の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view へ移行する	**radio** *radio-id*	—
4． 802.11n 保護を設定する	**dot11n protection** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での 802.11n 保護の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view へ移行する	**wlan ap-group** *group-name*	—
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11n 保護を設定する	**dot11n protection** { **disable** | **enable** }	デフォルト：無効

3.8 802.11ac/ax機能の設定

🕮 **メモ：**

802.11ac/ax 装置に対するサポートは、装置モデルに依存します。

⚠ **重要：**

AP に対して 802.11ac/ax 機能を設定するとき、別のユーザが同じ AP に対して 802.11ac/ax 機能を設定している場合、設定は失敗します。

3.8.1 NSS の設定

802.11ac/ax AP に対して NSS を設定するときは、以下の制限とガイドラインに従ってください。

- AP が NSS をサポートする場合、AP は NSS に対するすべての VHT-MCS/HE-MCS インデックスをサポートします。
- 802.11ac/ax クライアントは、ユニキャストフレームを送信するために、NSS に対して VHT-MCS/HE-MCS インデックスと一致した速度を使用します。また、802.11ac/ax 以外のクライアントは、ユニキャストフレームを送信するために、802.11a/b/g/n 速度を使用します。
- マルチキャスト NSS を送信しない場合、802.11ac/ax クライアントと AP は、マルチキャストフレームを送信するために 802.11a/b/g/n マルチキャスト速度を使用します。NSS を設定し、VHT-MCS/HE-MCS インデックスを指定した場合、以下のケースのうちいずれかが発生します。
  - □ すべてのクライアントが 802.11ac/ax クライアントである場合、AP とクライアントはマルチキャストフレームを送信するために、VHT-MCS/HE-MCS インデックスと一致した速度を使用します。
  - □ 802.11ac/ax 以外のクライアントが存在する場合、AP とクライアントはマルチキャストフレームを送信するために、802.11a/b/g/n マルチキャスト速度を使用します。
- 最大必須 NSS または最大サポート NSS を設定するとき、実際に範囲を指定します。たとえば、最大必須 NSS を 5 に設定する場合、1～5 までの NSS に対して VHT-MCS/HE-MCS インデックスと一致する速度が、802.11ac/ax 必須速度として設定されます。

I. radio view での NSS の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—

操作	コマンド	補足
4. 最大必須 NSS を設定する	• 802.11ac **dot11ac mandatory maximum-nss** *nss-number* • 802.11ax **dot11ax mandatory maximum-nss** *nss-number*	デフォルト： • 最大サポートNSSが設定されている場合、最大必須NSSは設定されません。 • 最大サポートNSSが設定されていない場合、無線はAP group radio viewの設定を使用します。
5. 最大サポート NSS を設定する	• 802.11ac **dot11ac support maximum-nss** *nss-number* • 802.11ax **dot11ax support maximum-nss** *nss-number*	デフォルト： • 最大必須NSSが設定されている場合、最大サポートNSSは8です。 • 最大必須NSSが設定されていない場合、無線はAP group radio viewの設定を使用します。 最大サポートNSSは、最大必須NSSより小さくすることはできません。
6. マルチキャスト NSS の設定と VHT-MCS/HE-MCS インデックスを指定する	• 802.11ac **dot11ac multicast-nss** *nss-number* **vht-mcs** *index* • 802.11ax **dot11ax multicast-nss** *nss-number* **he-mcs** *index*	デフォルト： • 最大サポートNSSまたは最大必須NSSが設定されている場合、マルチキャストNSSは設定されません。 • 最大サポートNSSと最大必須NSSのどちらも設定されていない場合、無線はAP group radio viewの設定を使用します。 マルチキャストNSSは、最大必須NSSより大きくすることはできません。

II. AP group radio view での NSS の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—

操作	コマンド	補足
5. 最大必須 NSS を設定する	● 802.11ac **dot11ac mandatory maximum-nss** *nss-number* ● 802.11ax **dot11ax mandatory maximum-nss** *nss-number*	デフォルト：設定なし
6. 最大サポート NSS を設定する	● 802.11ac **dot11ac support maximum-nss** *nss-number* ● 802.11ax **dot11ax support maximum-nss** *nss-number*	デフォルト： 8
7. マルチキャスト NSS の設定と VHT-MCS/HE-MCS インデックスを指定する	● 802.11ac **dot11ac multicast-nss** *nss-number* **vht-mcs** *index* ● 802.11ax **dot11ax multicast-nss** *nss-number* **he-mcs** *index*	デフォルト：設定なし

3.8.2 802.11ac/ax クライアント限定アクセスの設定

低速 802.11a/b/g/n クライアントの影響を低減し、無線データ伝送を加速させるために、AP が 802.11ac/ax クライアントのみを許可するように設定することができます。

I. radio view での 802.11ac/ax クライアント限定アクセスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—
4. 802.11ac/ax クライアント限定アクセスを設定する	● 802.11acクライアント限定アクセス **client dot11ac-only** { **disable** | **enable** } ● 802.11axクライアント限定アクセス **client dot11ax-only** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での 802.11ac/ax クライアント限定アクセスの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11ac/ax クライアント限定アクセスを設定する	● 802.11acクライアント限定アクセス **client dot11ac-only** { **disable** | **enable** } ● 802.11axクライアント限定アクセス **client dot11ax-only** { **disable** | **enable** }	デフォルト： 無効

3.8.3 802.11ac/ax 帯域幅モードの設定

802.11ac/ax は 802.11n のチャネル構造を使用し、最大帯域幅を 40MHz から 160MHz まで増大させます。802.11ac/ax は、2 つの隣接した 20MHz のチャネルに対して 40MHz のチャネルを関連づけることができ、2 つの隣接した 40MHz チャネルに対して、80MHz のチャネルを形成することを関連づけることができます。また、2 つの隣接した 80MHz チャネルに対して、160MHz のチャネルを形成することを関連づけることができます。

🕮 **メモ：**

160MHz は QX-W1130 の Radio1 のみでサポートします。

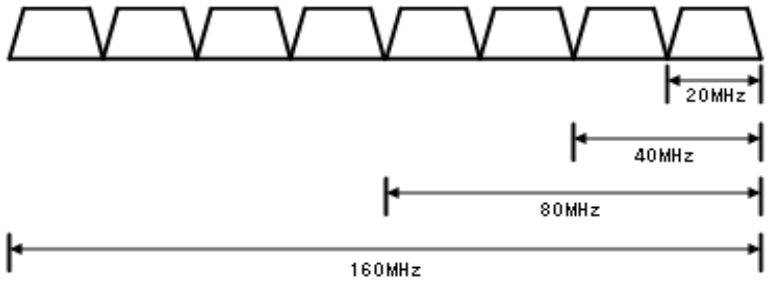


図 3-6 802.11ac/ax 帯域幅モード

I. radio view での 802.11ac/ax 帯域幅モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． 802.11ac/ax 帯域幅モードを設定する	● 802.11ac/ax帯域幅モードを設定する： **channel band-width** { **20** | **40** | **80** | **160** } ● 802.11gac/gax帯域幅モードを設定する： **channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での 802.11ac/ax 帯域幅モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAP グループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． 802.11ac/ax 帯域幅モードを設定する	● 802.11ac/ax帯域幅モードを設定する： **channel band-width** { **20** | **40** | **80** | **160** } ● 802.11gac/gax帯域幅モードを設定する： **channel band-width** { **20** | **40** [**auto-switch**] }	デフォルト： 802.11ac/ax帯域幅モード：80 802.11gac/gax帯域幅モード：20

3.8.4 TxBF の設定

TxBF（Transmit beamforming）は、クライアントに意図した RF 信号に焦点を合わせるため、AP がチャネル情報にもとづいて送信するパラメータを適合させます。この機能は RF 信号の品質を向上させます。TxBF はシングルユーザ TxBF とマルチユーザ TxBF があります。

- **シングルユーザ TxBF**－意図した 1 クライアントへの信号を向上します。シングルユーザ TxBF はクライアントが広範囲にわたっている、品質が低いネットワーク、信号の減衰に対して厳しい WLAN に適しています。
- **マルチユーザ TxBF**－802.11ac wave2 の一部です。マルチユーザ TxBF は干渉と伝送遅延を縮小させるため、AP が意図したクライアントに異なる RF 信号の焦点を合わせます。

I. radio view での TxBF の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． シングルユーザ TxBF を設定する	**su-txbf** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。
5． マルチユーザ TxBF を設定する	**mu-txbf** { **disable** | **enable** }	デフォルト：無線はAP group radio viewの設定を使用します。

II. AP group radio view での TxBF の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． シングルユーザ TxBF を設定する	**su-txbf** { **disable** | **enable** }	デフォルト：ソフトウェアバージョン7.2.21を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。 ソフトウェアバージョン7.2.27, 7.2.27aから7.2.59のソフトウェアでは無効(コンフィグ上は非表示)です。 ソフトウェアバージョン7.2.63のソフトウェアでは有効(コンフィグ上は非表示)です。 ソフトウェアバージョン7.2.67を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

操作	コマンド	補足
6. マルチユーザ TxBF を設定する	**mu-txbf** { **disable** | **enable** }	デフォルト：ソフトウェアバージョン7.2.21を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。 ソフトウェアバージョン7.2.27, 7.2.27aから7.2.59のソフトウェアでは無効(コンフィグ上は非表示)です。 ソフトウェアバージョン7.2.63のソフトウェアでは有効(コンフィグ上は非表示)です。 ソフトウェアバージョン7.2.67を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。 マルチユーザTxBFはシングルユーザTxBFが有効である場合のみ適用します。

3.8.5 OFDMA の設定

🕮 **メモ：**

- **dl-ofdma** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- **ul-ofdma** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- OFDMA は QX-W1100 シリーズの AP でのみサポートしています。

I. OFDMA について

OFDMA は、小さなデータパケットが送信される高密度環境で有効にすると、次の利点があります。

- 複数ユーザへの同時通信
- 無線使用率の向上
- 転送遅延の短縮
- 衝突バックオフの削減

II. radio view での OFDMA の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3. radio view へ移行する	**radio** *radio-id*	—

操作	コマンド	補足
4. ダウンリンク OFDMA を設定する	**dl-ofdma** { **disable** | **enable** }	デフォルト：AP group radio viewの設定を使用
5. アップリンク OFDMA を設定する	**ul-ofdma** { **disable** | **enable** }	デフォルト：AP group radio viewの設定を使用

III. AP group radio view での OFDMA の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. AP model view へ移行する	**ap-model** *ap-model*	—
4. radio view へ移行する	**radio** *radio-id*	—
5. ダウンリンク OFDMA を設定する	**dl-ofdma** { **disable** | **enable** }	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン7.2.55を含む以前のバージョンでは無効(コンフィグ上は非表示)です。 ソフトウェアバージョン7.2.56を含む以降のバージョンでは有効(コンフィグ上は非表示)です。
6. アップリンク OFDMA を設定する	**ul-ofdma** { **disable** | **enable** }	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン7.2.55を含む以前のバージョンでは無効(コンフィグ上は非表示)です。 ソフトウェアバージョン7.2.56を含む以降のバージョンでは有効(コンフィグ上は非表示)です。

3.8.6 BSS カラーリングの設定

🕮 **メモ：**

- **bss-color** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- BSS カラーリングは QX-W1100 シリーズの AP でのみサポートしています。

I. BSS カラーリングについて

BSS カラーリングを使用すると、システムは各 BSS にカラーを割り当て、クライアントへのデータパケットにカラーID を含めることができます。データパケットにカラーID が含まれることで、クライアントは関連付いた AP からパケットが送信されたかどうかを識別できます。衝突を避けるために、関連付けられた BSS と同じカラーの 802.11 ax データパケットを検出したクライアントは送信を延期します。

II. 制限とガイドライン

本機能は 802.11ax 無線でのみ設定可能です。

III. radio view での BSS カラーリングの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． BSS カラーリングを設定する	**bss-color** { **disable** | **enable** }	デフォルト：AP group radio viewの設定を使用

IV. AP group radio view での BSS カラーリングの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． BSS カラーリングを設定する	**bss-color** { **disable** | **enable** }	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.55を含む以前のバージョンでは無効(コンフィグ上は非表示)です。 ソフトウェアバージョン 7.2.56を含む以降のバージョンでは有効(コンフィグ上は非表示)です。

3.8.7 TWT ネゴシエーションの設定

🕮 **メモ：**

- **twt negotiate** コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。
- TWT ネゴシエーションは QX-W1100 シリーズの AP でのみサポートしています。

I. TWT ネゴシエーションについて

Trget Wake Time (TWT) ネゴシエーションを使用すると、クライアントと AP はサービス期間中にのみデータパケットを交換し、クライアントの休止状態をスケジュールして、クライアントの電力消費量と無線リソースの競合を減らすことができます。

TWT ネゴシエーションを有効にすると、クライアントはサービス期間、TWT 間隔、および最初のスリープ状態解除時間(クライアントによって計算される)を含むネゴシエーション要求を AP に送信します。このような要求を受信すると、AP は応答を送信します。クライアントはスケジュールに従って起動し、その AP からのトリガーフレームを待機します。トリガーフレームを受信すると、クライアントはサービス期間に入り、その AP とのデータパケットの交換を開始します。サービス期間が終了すると、データパケットの交換が完了していなくても、クライアントは休止モードに入ります。

II. 制限とガイドライン

無線は、最大 8 台のクライアントに TWT サービスを提供できます。8 つのクライアントの TWT ネゴシエーション要求に応答した後、無線は他のクライアントからの要求を拒否します。

本機能は、802.11 ax および 802.11 gax でのみ有効です。無線タイプを 802.11 ax または 802.11 gax 以外に変更すると、設定が削除されます。

III. radio view での TWT ネゴシエーションの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	デフォルト：設定なし APを作成するときは名前とモデルを指定する必要があります。
3． radio view へ移行する	**radio** *radio-id*	—
4． TWT ネゴシエーションを設定する	**twt negotiate** { **disable** | **enable** }	デフォルト：AP group radio viewの設定を使用

IV. AP group radio view での TWT ネゴシエーションの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP グループを作成し、AP group view へ移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． AP model view へ移行する	**ap-model** *ap-model*	—
4． radio view へ移行する	**radio** *radio-id*	—
5． TWT ネゴシエーションを設定する	**twt negotiate** { **disable** | **enable** }	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.55を含む以前のバージョンでは無効(コンフィグ上は非表示)です。 ソフトウェアバージョン 7.2.56を含む以降のバージョンでは有効(コンフィグ上は非表示)です。

3.9 無線管理の表示および管理

すべての view で **display** コマンドを実行できます。

操作	コマンド
無線の情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **radio** [**frequency-band** { **5** | **2.4** }]
無線チャネルの情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **radio channel**
無線タイプの情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **radio type**
無線の統計情報を表示する	**display wlan statistics ap { all | name** *ap-name* **} radio**
無線の統計情報を削除する	**reset wlan statistics ap { all | name** *ap-name* **} radio**

3.10 無線管理の設定例

3.10.1 基本無線機能の設定例

I. ネットワーク要件

図 3-7 に示すように、手動 AP を作成し、無線モード、作動チャネル、最大伝送電力に対してそれぞれ 802.11gn、channel 11、19 dBm を設定します。

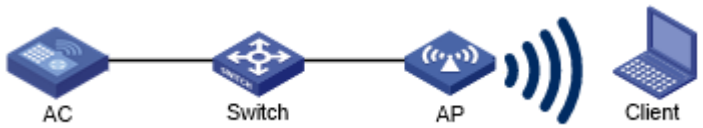


図 3-7 ネットワーク図

II. 設定手順

AP 名が ap1 の手動 AP を作成し、モデル名、シリアル ID を指定します。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

radio 2 の radio view に移行します。

```
[AC-wlan-ap-ap1] radio 2
```

無線モードを dot11gn に設定します。

```
[AC-wlan-ap-ap1-radio-2] type dot11gn
```

radio 2 の作動チャネルを channel 11 に設定します。

```
[AC-wlan-ap-ap1-radio-2] channel 11
```

最大伝送電力を 19 dBm に設定します。

```
[AC-wlan-ap-ap1-radio-2] max-power 19
```

radio 2 を有効にします。

```
[AC-wlan-ap-ap1-radio-2] radio enable
```

III. 設定の確認

すべての無線の情報を表示します。

```
[AC] display wlan ap all verbose
Total number of APs: 1
Total number of connected APs: 1
Total number of connected manual APs: 1
Total number of connected auto APs: 0
Total number of connected common APs: 1
Total number of connected WTUs: 0
Total number of inside APs: 0
Maximum supported APs: 256
Remaining APs: 255
Total AP licenses: 128
Remaining AP licenses: 127

AP name                         : ap1
AP ID                           : 1
AP group name                   : default-group
Backup Type                     : Master
```

```
State                          : Run
Backup Type                    : Master
Online time                    : 0 days 1 hours 25 minutes 12 seconds
System up time                 : 0 days 2 hours 22 minutes 12 seconds
Model                          : QX-W1030
Region code                    : CN
Region code lock               : Disable
Serial ID                      : 219801A0CNC138011454
MAC address                    : 0AFB-423B-893C
IP address                     : 192.168.1.50
UDP port number                : 65488
H/W version                    : Ver.C
S/W version                    : V700R001B49D001
Boot version                   : 1.01
Description                    : wtp1
Priority                       : 4
Echo interval                  : 10 seconds
Statistics report interval     : 50 seconds
Fragment size (data)           : 1500
Fragment size (control)        : 1450
MAC type                       : Local MAC & Split MAC
Tunnel mode                    : Local Bridging & 802.3 Frame & Native Frame
Discovery type                 : Static Configuration
Retransmission count           : 3
Retransmission interval        : 5 seconds
Firmware upgrade               : Enabled
Sent control packets           : 1
Received control packets       : 1
Echo requests                  : 147
Lost echo responses            : 0
Average echo delay             : 3
Last reboot reason             : User soft reboot
Latest IP address              : 10.1.0.2
Tunnel down reason             : Request wait timer expired
Connection count               : 1
Backup Ipv4                    : Not configured
Backup Ipv6                    : Not configured
Tunnel encryption              : Disabled
LED mode                       : Normal
Remote configuration           : Enabled
Radio 1:
    Basic BSSID                : 7848-59f6-3940
    Admin state                : Up
    Radio type                 : 802.11ac
    Antenna type               : internal
    Client dot11ac-only        : Disabled
    Client dot11n-only         : Disabled
    Channel band-width         : 20/40/80MHz
    Secondary channel offset   : SCB
    Short GI for 20MHz         : Supported
    Short GI for 40MHz         : Supported
    Short GI for 80MHz         : Supported
    Short GI for 160MHz        : Not supported
    A-MSDU                     : Enabled
    A-MPDU                     : Enabled
    LDPC                       : Not Supported
    STBC                       : Supported
    Operational VHT-MCS Set:
        Mandatory              : Not configured
        Supported              : NSS1 0,1,2,3,4,5,6,7,8,9
                                 NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast              : Not configured
    Operational HT MCS Set:
        Mandatory              : Not configured
        Supported              : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                 10, 11, 12, 13, 14, 15
        Multicast              : Not configured
    Channel                    : 44(auto)
    Max power                  : 20 dBm
    Operational rate:
```

```
        Mandatory             : 6, 12, 24 Mbps
        Multicast             : Auto
        Supported             : 9, 18, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -102 dBm
    Smart antenna             : Enabled
    Smart antenna policy      : Auto
    Protection mode           : rts-cts
Radio 2:
    Basic BSSID               : 7848-59f6-3950
    Admin state               : Up
    Radio type                : 802.11n(2.4GHz)
    Antenna type              : internal
    Client dot11n-only        : Disabled
    Channel band-width        : 20MHz
    Secondary channel offset  : SCN
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 11
    Max power                 : 19 dBm
    Preamble type             : Short
    Operational rate:
        Mandatory             : 1, 2, 5.5, 11 Mbps
        Multicast             : Auto
        Supported             : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -105 dBm
    Smart antenna             : Enabled
    Smart antenna policy      : Auto
    Protection mode           : rts-cts
```

3.10.2 802.11n 設定例

I. ネットワーク要件

図 3-8 に示すように、AP 上で無線 1 を 802.11an 無線として指定し、無線上で A-MSDU アグリゲーションと A-MPDU アグリゲーション方式を有効にします。

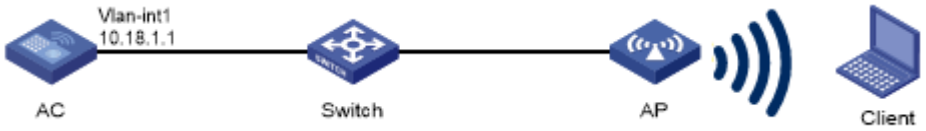


図 3-8 ネットワーク図

II. 設定手順

AP 名が ap1 の手動 AP を作成し、モデル名、シリアル ID を指定します。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
```

ap1 の radio 1 の radio view に移行し、802.11an 無線を指定します。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] type dot11an
```

A-MPDU、A-MSDU アグリゲーション方式を有効にします。

```
[AC-wlan-ap-ap1-radio-1] a-mpdu enable
[AC-wlan-ap-ap1-radio-1] a-msdu enable
```

radio 1 を有効にします。

```
[AC-wlan-ap-ap1-radio-1] radio enable
```

III. 設定の確認

ap1 の無線の情報を表示します。

```
[AC-wlan-ap-ap1-radio-1] display wlan ap name ap1 verbose
AP name                          : ap1
AP ID                            : 1
AP group name                    : default-group
State                            : Run
Backup Type                      : Master
Online time                      : 0 days 1 hours 25 minutes 12 seconds
System up time                   : 0 days 2 hours 22 minutes 12 seconds
Model                            : 219801A0CNC138011454
Region code                      : CN
Region code lock                 : Disable
Serial ID                        : 219801A0CNC138011454
MAC address                      : 0AFB-423B-893C
IP address                       : 192.168.1.50
UDP port number                  : 65488
H/W version                      : Ver.C
S/W version                      : V700R001B49D001
Boot version                     : 1.01
Description                      : wtp1
Priority                         : 4
Echo interval                    : 10 seconds
Statistics report interval       : 50 seconds
```

```
Fragment size (data)          : 1500
Fragment size (control)       : 1450
MAC type                      : Local MAC & Split MAC
Tunnel mode                   : Local Bridging & 802.3 Frame & Native Frame
Discovery type                : Static Configuration
Retransmission count          : 3
Retransmission interval       : 5 seconds
Firmware upgrade              : Enabled
Sent control packets          : 1
Received control packets      : 1
Echo requests                 : 147
Lost echo responses           : 0
Average echo delay            : 3
Last reboot reason            : User soft reboot
Latest IP address             : 10.1.0.2
Tunnel down reason            : Request wait timer expired
Connection count              : 1
Backup Ipv4                   : Not configured
Backup Ipv6                   : Not configured
Tunnel encryption             : Disabled
LED mode                      : Normal
Remote configuration          : Enabled
Radio 1:
    Basic BSSID               : 7848-59f6-3940
    Admin state               : Up
    Radio type                : 802.11n(5GHz)
    Antenna type              : internal
    Client dot11ac-only       : Disabled
    Client dot11n-only        : Disabled
    Channel band-width        : 20/40/80MHz
    Secondary channel offset  : SCB
    Short GI for 20MHz        : Supported
    Short GI for 40MHz        : Supported
    Short GI for 80MHz        : Supported
    Short GI for 160MHz       : Not supported
    A-MSDU                    : Enabled
    A-MPDU                    : Enabled
    LDPC                      : Not Supported
    STBC                      : Supported
    Operational VHT-MCS Set:
        Mandatory             : Not configured
        Supported             : NSS1 0,1,2,3,4,5,6,7,8,9
                                NSS2 0,1,2,3,4,5,6,7,8,9
        Multicast             : Not configured
    Operational HT MCS Set:
        Mandatory             : Not configured
        Supported             : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                10, 11, 12, 13, 14, 15
        Multicast             : Not configured
    Channel                   : 44(auto)
    Max power                 : 20 dBm
    Operational rate:
        Mandatory             : 6, 12, 24 Mbps
        Multicast             : Auto
        Supported             : 9, 18, 36, 48, 54 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : -102 dBm
    Smart antenna             : Enabled
    Smart antenna policy      : Auto
    Protection mode           : rts-cts
Radio 2:
    Basic BSSID               : 7848-59f6-3950
```

```
    Admin state                : Up
    Radio type                 : 802.11n(2.4GHz)
    Antenna type               : internal
    Client dot11n-only         : Disabled
    Channel band-width         : 20MHz
    Secondary channel offset   : SCN
    Short GI for 20MHz         : Supported
    Short GI for 40MHz         : Supported
    A-MSDU                     : Enabled
    A-MPDU                     : Enabled
    LDPC                       : Not Supported
    STBC                       : Supported
    Operational HT MCS Set:
        Mandatory              : Not configured
        Supported              : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                 10, 11, 12, 13, 14, 15
        Multicast              : Not configured
    Channel                    : 11
    Max power                  : 19 dBm
    Preamble type              : Short
    Operational rate:
        Mandatory              : 1, 2, 5.5, 11 Mbps
        Multicast              : Auto
        Supported              : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
        Disabled               : Not configured
    Distance                   : 1 km
    ANI                        : Enabled
    Fragmentation threshold    : 2346 bytes
    Beacon interval            : 100 TU
    Protection threshold       : 2346 bytes
    Long retry threshold       : 4
    Short retry threshold      : 7
    Maximum rx duration        : 2000 ms
    Noise Floor                : -105 dBm
    Smart antenna              : Enabled
    Smart antenna policy       : Auto
    Protection mode            : rts-cts
```

目次

4章 WLANアクセスの設定 4-1
4.1 WLANアクセスの概要 4-1
4.1.1 スキャニング 4-1
4.1.2 関連づけ 4-3
4.2 SSIDにもとづくアクセス制御 4-3
4.3 ホワイトリスト、ブラックリストにもとづくアクセス制御 4-4
4.4 ACLにもとづくアクセス制御 4-5
4.5 設定の制限とガイドライン 4-5
4.6 設定作業リスト 4-5
4.7 サービステンプレートの設定 4-6
4.8 SSIDの設定 4-7
4.9 サービステンプレートの有効化 4-7
4.10 無線に対するサービステンプレートの設定 4-7
4.10.1 radio viewでの無線に対するサービステンプレートの設定 4-8
4.10.2 AP group radio viewでの無線に対するサービステンプレートの設定 4-8
4.11 サービステンプレートに対する記述の設定 4-8
4.12 サービステンプレートに関連付く最大クライアント数の設定 4-8
4.13 APが指定されたサービステンプレートをAPグループから引き継がないための設定 4-9
4.14 クライアントアイドルタイムアウトタイマの設定 4-9
4.14.1 AP view でのクライアントアイドルタイムアウトタイマの設定 4-9
4.14.2 AP group viewでのクライアントアイドルタイムアウトタイマの設定 4-10
4.15 クライアントkeepaliveの設定 4-10
4.15.1 AP view でのクライアントkeepaliveの設定 4-10
4.15.2 AP group view でのクライアントkeepaliveの設定 4-10
4.16 クライアントのVLANの割り当て方式の指定 4-11
4.17 ローミング後のクライアントの許可VLANの選択の設定 4-11
4.18 クライアントキャッシュエージングタイマの設定 4-11
4.19 ACまたはAPでのクライアントの関連づけの有効化 4-12
4.20 クライアントトラフィック転送モードの指定 4-12
4.21 クライアントのトラフィック転送の有効化 4-13
4.22 クライアントデータフレームに対するカプセル化フォーマットの設定 4-13
4.23 クイックアソシエーションの有効化 4-14
4.24 クライアント再認証を行う前のアイドル時間の設定 4-14
4.25 APが未知のクライアントからのトラフィックを処理する方法の設定 4-14
4.26 クライアント情報報告先のWebサーバの指定 4-15
4.27 クライアントアソシエーションを許可するSSIDの設定 4-15
4.28 ホワイトリストへのクライアントの追加 4-16
4.29 スタティックブラックリストへのクライアントの追加 4-16
4.30 ダイナミックブラックリストの設定 4-16
4.31 ACLにもとづくアクセス制御の設定 4-17
4.31.1 サービステンプレートViewでのACLにもとづくアクセス制御の設定 4-17
4.31.2 AP ViewでのACLにもとづくアクセス制御の設定 4-18
4.32 領域コードの指定 4-18
4.32.1 AP viewでの領域コードの指定 4-18

4.32.2 AP group viewでの領域コードの指定 4-18
4.32.3 グローバル領域コードの指定 4-19
4.33 APのブロードキャストプローブ要求への応答の無効化 4-19
4.33.1 AP viewでのAPのブロードキャストプローブ要求への応答の無効化 4-19
4.33.2 AP group viewでのAPのブロードキャストプローブ要求への応答の無効化 4-19
4.34 NAS IDの設定 4-20
4.34.1 AP viewでのNAS IDの設定 4-20
4.34.2 AP group viewでのNAS IDの設定 4-20
4.34.3 グローバルNAS IDの設定 4-21
4.35 APへのコンフィグレーションファイルの設定 4-21
4.36 WLANアクセスのSNMP notificationの有効化 4-22
4.37 WLANアクセスの表示と維持 4-22
4.38 WLANアクセスの設定例 4-23
4.38.1 WLANアクセスの設定例 4-23
4.38.2 ローカルMACアドレス認証でクライアントアソシエーションを許可するSSIDの設定例 4-25
4.38.3 ホワイトリストの設定例 4-29
4.38.4 スタティックブラックリストの設定例 4-29
4.38.5 AP viewでのACLにもとづくアクセス制御の設定例 4-30
4.38.6 サービステンプレート viewでのACLにもとづくアクセス制御の設定例 4-31

4章 WLAN アクセスの設定

本章では WLAN アクセスの設定方法について記述します。

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

4.1 WLANアクセスの概要

無線クライアントは、スキャニング、リンクレイヤ認証、関連づけ、WLAN 認証プロセスが完了したときのみ WLAN にアクセスすることができます。

データリンクレイヤ認証に関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“WLAN セキュリティの設定”* を参照してください。

WLAN 認証に関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“WLAN 認証の設定”* を参照してください。

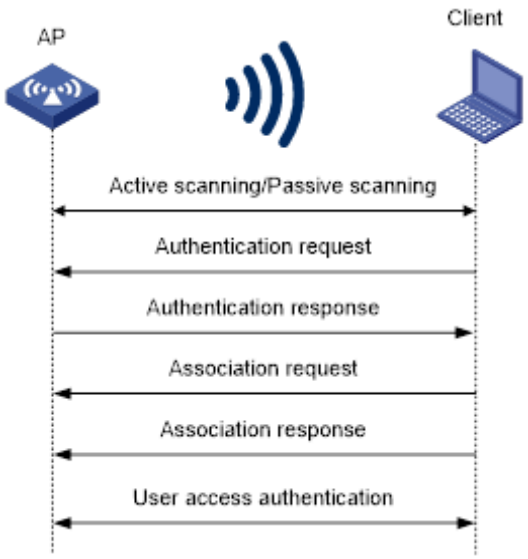


図 4-1 WLAN アクセスプロセス

4.1.1 スキャニング

I. アクティブスキャニング

無線クライアントは、プローブ要求を送信することで、定期的に周辺の無線ネットワークをスキャンします。無線クライアントは、受信したプローブ応答からネットワーク情報を取得します。プローブ要求が SSID を運ぶか否かにもとづき、アクティブスキャニングは以下のタイプに分類できます。

- すべての無線ネットワークのアクティブスキャニング
  - 図 4-2に示すように、クライアントは無線ネットワークをスキャンするために、サポートされた各々のチャネル上で定期的にプローブ要求を送信します。プローブ要求を受信した AP は、プローブ応答を送信します。これにより、入手可能な無線ネットワーク情報を運びます。クライアントは、最適 AP と関連づけられます。

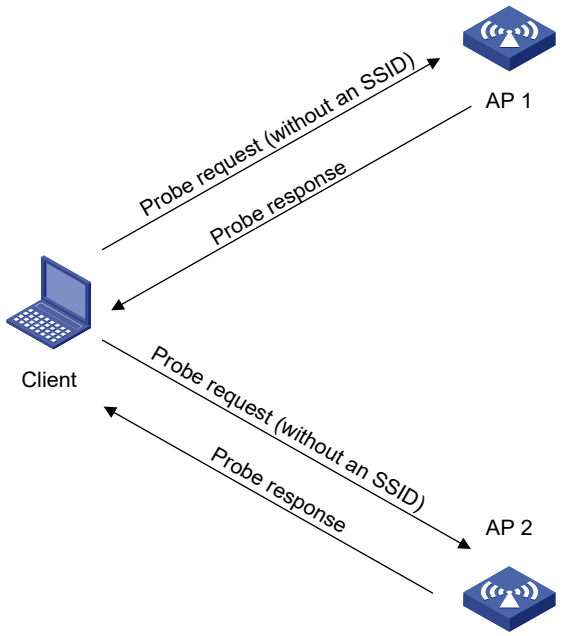


図 4-2 すべての無線ネットワークのスキャニング

- 特定の無線ネットワークのアクティブスキャニング
  - 無線クライアントが SSID を設定される、もしくは SSID に関連づけられる場合、図 4-3に示すように、クライアントは指定された SSID を運ぶプローブ要求を定期的に送信します。特定の SSID で無線サービスを提供できる AP がプローブ要求を受信したとき、AP はプローブ応答を送信します。

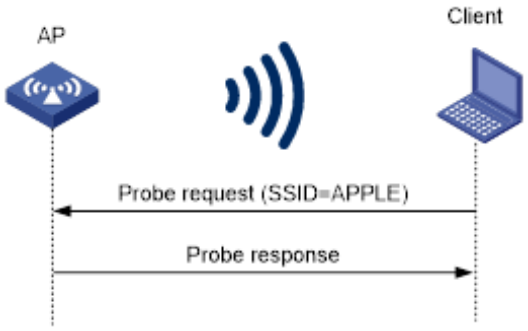


図 4-3 特定の無線ネットワークのスキャニング

II. パッシブスキャニング

□ 図 4-4に示すように、クライアントは周辺の無線ネットワークに関する情報を入手するために、サポートされたチャネル上で AP によって送信されたビーコンフレームを受信します。クライアントは認証のために AP を選択します。パッシブスキャニングは電力消費を抑えたいときに使用します。

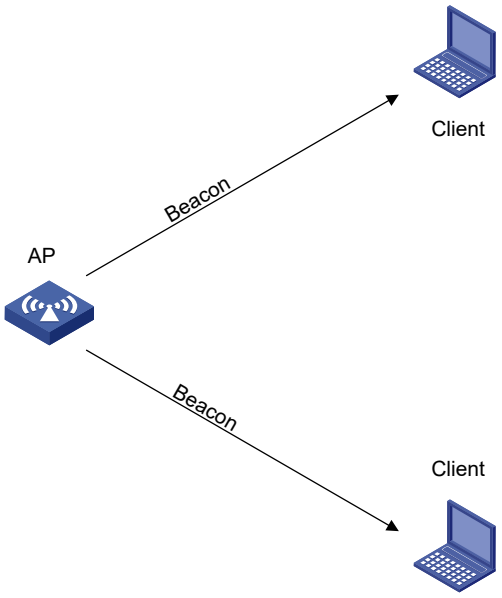


図 4-4 パッシブスキャニング

4.1.2 関連づけ

クライアントは、データリンクレイヤ認証を通過したあと、関連づけられた AP に対して関連づけ要求を送信します。関連づけ要求を受信すると、AP は無線クライアントによってサポートされた容量を決定し、クライアントに対して関連づけ応答を送信します。これにより、クライアントは AP に関連づけられます。

4.2 SSIDにもとづくアクセス制御

図 4-5図 4-5に示すように、SSID にもとづくアクセス制御では、ssida を Client1 と Client2 の許可された SSID として設定し、ssidb を Client3 の許可された SSID として設定します。

クライアントが認証に合格すると、サーバは関連するユーザプロファイルを AC に送信します。AC は、クライアントの関連付けられた SSID が許可された SSID であるかどうかを調べます。許可された SSID の場合、クライアントは WLAN へのアクセスを許可されます。許可されていない SSID の場合、AC はクライアントをログオフします。

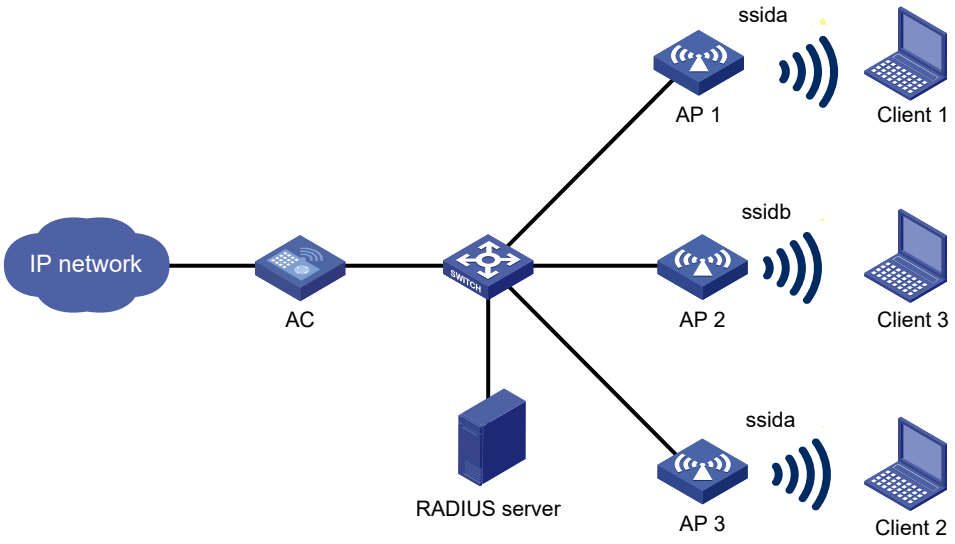


図 4-5 SSID にもとづくアクセス制御

4.3 ホワイトリスト、ブラックリストにもとづくアクセス制御

WLAN クライアントからのフレームをフィルタリングし、クライアントアクセス制御を実行するために、ホワイトリストとブラックリストを設定することができます。

- **ホワイトリスト**－WLAN にアクセスすることを許可されたすべてのクライアントの MAC アドレスを含みます。ホワイトリスト内に存在しないクライアントからのフレームは破棄されます。ホワイトリストは手動で設定されます。
- **スタティックブラックリスト**－WLAN にアクセスすることを禁止されたクライアントの MAC アドレスを含みます。スタティックブラックリストは手動で設定されます。
- **ダイナミックブラックリスト**－WLAN にアクセスすることを禁止されたクライアントの MAC アドレスを含みます。AP は、WIDS が設定された場合、あるいは URL リダイレクションが WLAN MAC 認証クライアントのために URL リダイレクションが有効である場合、リストに WLAN にアクセスすることを禁止されたクライアントの MAC アドレスを追加します。WIDS に関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“WIPS の設定”* を参照してください。WLAN MAC 認証クライアントの詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“WLAN 認証の設定”* を参照してください。

AP が関連づけ要求を受信し、AC に追加モバイルメッセージを送信すると、AC はクライアントを許可するかどうか判断するために、以下の操作を実行します。

1) ホワイトリストを捜索します。
- クライアント MAC アドレスがホワイトリスト内のいずれのエントリとも一致しない場合、クライアントは拒否されます。
- クライアント MAC アドレスがホワイトリスト内のエントリと一致する場合、クライアントは許可されます。

2) ホワイトリストエントリが存在しない場合、スタティック、ダイナミックブラックリストを捜索します。

- クライアント MAC アドレスがいずれかのブラックリスト内のエントリと一致する場合、クライアントは拒否されます。
- クライアント MAC アドレスがいずれのブラックリスト内のエントリとも一致しない場合、もしくはブラックリストエントリが存在しない場合、クライアントは許可されます。

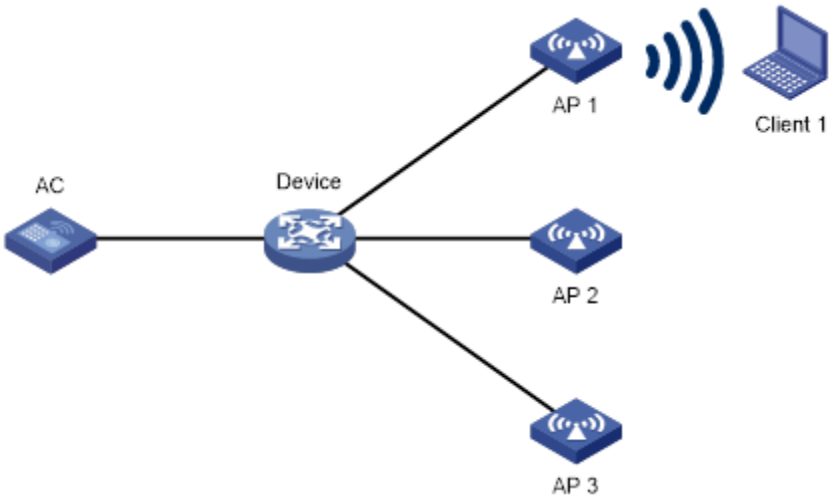


図 4-6 ホワイトリスト、ブラックリストにもとづくアクセス制御

4.4 ACLにもとづくアクセス制御

ACL にもとづくアクセスコントロールと、ホワイトリストおよびブラックリストベースのアクセスコントロールの両方を同じ装置に設定しないでください。

指定した ACL に permit ルールが設定されていない場合、クライアントのアクセスは許可されません。

AP View の設定は、サービステンプレート View の設定よりも優先されます。

この機能は、レイヤ 2 ACL だけをサポートし、一致基準として送信元 MAC アドレスだけを使用できます。

4.5 設定の制限とガイドライン

設定の優先順位は AP view、AP group view、global configuration view の順番で優先します。

4.6 設定作業リスト

作業リスト
（必須設定項目） サービステンプレートの設定

作業リスト
（必須設定項目） SSIDの設定
（必須設定項目） サービステンプレートの有効化
（必須設定項目） 無線に対するサービステンプレートの設定
（オプション設定項目） サービステンプレートに対する記述の設定
（オプション設定項目） サービステンプレートに関連付く最大クライアント数の設定
（オプション設定項目） APが指定されたサービステンプレートをAPグループから引き継がないための設定
（オプション設定項目） クライアントアイドルタイムアウトタイマの設定
（オプション設定項目） クライアントkeepaliveの設定
（オプション設定項目）クライアントのVLANの割り当て方式の指定
（オプション設定項目）ローミング後のクライアントの許可VLANの選択の設定
（オプション設定項目） クライアントキャッシュエージングタイマの設定
（オプション設定項目） ACまたはAPでのクライアント関連づけの有効化
（オプション設定項目） クライアントトラフィック転送モードの指定
（オプション設定項目）クライアントのトラフィック転送の有効化
（オプション設定項目） クライアントデータフレームに対するカプセル化フォーマットの設定
（オプション設定項目） クイックアソシエーションの有効化
（オプション設定項目）クライアント再認証を行う前のアイドル時間の設定
（オプション設定項目） APが未知のクライアントからのトラフィックを処理する方法の設定
（オプション設定項目）クライアントアソシエーションを許可するSSIDの設定
（オプション設定項目）クライアント情報が通知されるWebサーバの指定
（オプション設定項目） ホワイトリストへのクライアントの追加
（オプション設定項目） スタティックブラックリストへのクライアントの追加
（オプション設定項目）ダイナミックブラックリストの設定
（オプション設定項目）ACLにもとづくアクセス制御の設定
（オプション設定項目） 領域コードの指定
（オプション設定項目） APのブロードキャストプローブ要求への応答の無効化
（オプション設定項目） NAS IDの設定
（オプション設定項目） APへのコンフィグレーションファイルの設定
（オプション設定項目） WLANアクセスのSNMP notificationの有効化

4.7 サービステンプレートの設定

サービステンプレートは、SSID や認証方法のような無線サービス認証方式を定義します。

以下にサービステンプレートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレートを作成する	**wlan service-template** *service-template-name*	デフォルト：設定なし
3. VLAN をサービステンプレートに結びつける	**vlan** *vlan-id*	デフォルト：VLAN 1

4.8 SSIDの設定

AP は、ビーコンフレーム内で SSID を配信します。BSS 内のクライアント数が制限を越える、もしくは BSS が入手不可能な場合、クライアントが BSS を発見することを防ぐために SSID-hidden を有効にすることができます。SSID-hidden が有効のとき、BSS は SSID をビーコンフレーム内に隠し、ブロードキャストプローブ要求に応答しません。クライアントは、WLAN にアクセスするために、指定された SSID とともにプローブ要求を送信しなければなりません。この機能により、WLAN は攻撃から保護されます。

SSID の設定手順は以下のとおりです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートに SSID を設定する	**ssid** *ssid-name*	デフォルト：設定なし NECは、サービステンプレートに対して独自のSSIDを設定することを推奨します。
4. （オプション設定項目）ビーコンフレーム内で SSID-hidden を有効にする	**beacon ssid-hide**	デフォルト：設定なし

4.9 サービステンプレートの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートを有効にする	**service-template enable**	デフォルト：無効

4.10 無線に対するサービステンプレートの設定

無線に対してサービステンプレートを設定する場合、AP はサービステンプレート内で定義された無線サービスを提供できる BSS を作成します。

無線に対してサービステンプレートを設定する場合、以下の作業を実行することができます。

- BSS に関連づけられたクライアントが、VLAN グループ内のすべての VLAN に対して均等に割り当てられるように、無線に VLAN グループを結びつけます。
- ネットワークアクセスサーバを識別するために、無線に NAS ポート ID もしくは NAS ID を結びつけます。
- AP がビーコンフレーム内に SSID を隠せるようにします。

4.10.1 radio view での無線に対するサービステンプレートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** radio-id	—
4. 無線に対してサービステンプレートを設定する	**service-template** *service-template-name* [**vlan** *vlan-id* | **vlan-group** *vlan-group-name*] [**ssid-hide**] [**nas-id** *nas-id* | **nas-port-id** *nas-port-id*]	デフォルト：AP group viewの設定が使用されます。 無線に対して最大16のサービステンプレートを設定することができます。

4.10.2 AP group radio view での無線に対するサービステンプレートの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	
4. radio view に移行する	**radio** *radio-id*	—
5. 無線に対してサービステンプレートを設定する	**service-template** *service-template-name* [**vlan** *vlan-id* | **vlan-group** *vlan-group-name*] [**ssid-hide**] [**nas-id** *nas-id* | **nas-port-id** *nas-port-id*]	デフォルト：設定なし 無線に対して最大16のサービステンプレートを設定することができます。

4.11 サービステンプレートに対する記述の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートに対して記述を設定する	**description** *text*	デフォルト：設定なし

4.12 サービステンプレートに関連付く最大クライアント数の設定

本機能により、接続するクライアント数が過負荷になるのを防ぎます。本機能を設定すると、クライアント数が最大に達したとき新規のクライアントは WLAN にアクセスできません。

以下にサービステンプレートに関連付く最大クライアント数の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートに関連付く最大クライアント数を設定する	**client max-count** *max-number*	デフォルト：制限なし

4.13 APが指定されたサービステンプレートをAPグループから引き継がないための設定

デフォルトでは、AP グループ内の AP は、AP グループに設定されたサービステンプレートを引き継ぎ、BSS を作成します。

本設定により、AP が、指定されたサービステンプレートを AP グループから引き継がないように設定することができます。

AP が、指定されたサービステンプレートを AP グループから引き継がないように設定するための設定手順は、以下のとおりです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. AP が指定されたサービステンプレートを AP グループから引き継がないように設定する	**inherit exclude service-template** *service-template-name*	デフォルト：設定なし

4.14 クライアントアイドルタイムアウトタイマの設定

クライアントアイドルタイムアウトタイマが終了する前に､関連づけられた AP に対して、オンラインのクライアントが任意のフレームを送信しない場合、AP はクライアントをログオフします。

4.14.1 AP view でのクライアントアイドルタイムアウトタイマの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. クライアントアイドルタイムアウトタイマを設定する	**client idle-timeout** *interval*	デフォルト：APは、AP group view の設定を使用します。

4.14.2 AP group view でのクライアントアイドルタイムアウトタイマの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． クライアントアイドルタイムアウトタイマを設定する	**client idle-timeout** *interval*	デフォルト： ソフトウェアバージョン7.2.79bを含む以前のソフトウェアは3600秒。 ソフトウェアバージョン7.2.85aを含む以降のソフトウェアは300秒。

4.15 クライアントkeepaliveの設定

クライアント keepalive の設定機能により、AP はクライアントがオンラインかどうか識別するために、クライアントに対して指定された間隔で keepalive パケットを送信することができます。keepalive が 3 回送信される間隔以内に AP で応答を受信しない場合、クライアントをログオフします。

4.15.1 AP view でのクライアント keepalive の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． クライアント keepalive を有効にする	**client keep-alive enable**	デフォルト：APは、AP group view の設定を使用します。
4． （オプション設定項目）クライアント keepalive 間隔を設定する	**client keep-alive interval** *value*	デフォルト：APは、AP group view の設定を使用します。

4.15.2 AP group view でのクライアント keepalive の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． クライアント keepalive を有効にする	**client keep-alive enable**	デフォルト：無効
4． （オプション設定項目）クライアント keepalive 間隔を設定する	**client keep-alive interval** *value*	デフォルト： 300秒

4.16 クライアントのVLANの割り当て方式の指定

クライアントが初回にオンラインになったとき、無線はクライアントにランダムな VLAN を割り当てます。クライアントが再度オンラインになったとき、割り当て方式に依存してクライアントに VLAN を割り当てます。

- **スタティック割り当て**－クライアントは前回に割り当てられた VLAN を引き継ぎます。IP アドレスのリース期間が期限切れでない場合、クライアントは同一の IP アドレスを使用します。この方式は IP アドレス数を削減するのに役立ちます。
- **ダイナミック割り当て**－クライアントに VLAN が再度割り当てられます。すべての VLAN にクライアントがバランスよく振り分けられます。

以下にクライアントの VLAN の割り当て方式を指定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. クライアントの VLAN の割り当て方式を指定する	**client vlan-alloc** { **dynamic** | **static** }	デフォルト：**dynamic**

4.17 ローミング後のクライアントの許可VLANの選択の設定

移動する可能性のあるグループでは、すべての AC はこの機能を設定することを推奨します。

クライアントのローミングが行われた後、通常、クライアントの VLAN は変更されません。

クライアントが別の AP にローミングした後、QMC で設定されたセキュリティ警告が開始した場合、ユーザを適切に隔離するため許可 VLAN が適用されます。

この機能は 802.1X、MAC アドレス認証のクライアントのみ適用します。

以下にローミング後のクライアントの許可 VLAN の選択の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. ローミング後のクライアントの許可 VLAN の選択を設定する	**client preferred-vlan authorized**	デフォルト：有効

4.18 クライアントキャッシュエージングタイマの設定

クライアントキャッシュは、クライアントのアクセス VLAN や PMK リストのような情報を保存します。キャッシュエージングタイマが終了する前に、クライアントが別の AP にローミングする場合、クライアントはキャッシュ情報を引き継ぐことができます。キャッ

シュエージングタイマが終了する前に、クライアントがオンラインにならない場合、キャッシュ情報は削除されます。

以下にクライアントキャッシュエージングタイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. クライアントキャッシュエージングタイマを設定する	**client cache aging-time** *aging-time*	デフォルト： 180秒

4.19 ACまたはAPでのクライアントの関連づけの有効化

AC でクライアントの関連づけを有効にする場合、管理フレームが CAPWAP トンネルを通じて AC に送信されます。これにより、安全性が保証され、管理が容易になります。AC と AP 間のネットワークが複雑なとき、NEC は AP でのクライアントの関連づけを推奨します。

クライアントの関連づけが AP で有効な場合、レイヤ 3 ローミングはサポートされません。**service-template** コマンドを使用する場合、同一のサービステンプレートを使用し、カバーエリアが重なる AP は、同一の VLAN を指定しなければなりません。

以下に AC または AP でクライアントの関連づけを有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. AC または AP でクライアントの関連づけを有効にする	**client association-location** { **ac** | **ap** }	デフォルト： AC

4.20 クライアントトラフィック転送モードの指定

クライアントトラフィック転送モードは、AC（中央転送モード）もしくは AP（ローカル転送モード）を選択可能です。中央転送モードは、クライアントトラフィックを AC で転送するモードです。ローカル転送モードは、クライアントトラフィックを AP で転送するモードです。ローカル転送モードを使用することで、クライアントトラフィックは AC に転送されず、AC の転送負荷は軽減されます。

AP がクライアントトラフィックを転送する場合、指定された VLAN からトラフィックを転送するために、AP に対して VLAN もしくは VLAN 範囲を指定することができます。AC は、別の VLAN からデータトラフィックを転送します。

AC（中央転送モード）を指定する場合、“*クライアントのトラフィック転送の有効化*”が有効であることを確認してください。

以下にクライアントトラフィック転送モードの指定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. クライアントトラフィック転送モードを指定する	**client forwarding-location** { **ac** | **ap**	デフォルト： AP

4.21 クライアントのトラフィック転送の有効化

“*クライアントトラフィック転送モードの指定*”で AC（中央転送モード）を指定する場合、クライアントのトラフィック転送を有効にする必要があります。

以下にクライアントのトラフィック転送の有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアントのトラフィック転送を有効にする	**wlan client forwarding enable**	デフォルト：有効

4.22 クライアントデータフレームに対するカプセル化フォーマットの設定

“*クライアントトラフィック転送モードの指定*”で AC（中央転送モード）を指定する場合、AP はデータフレームをクライアントから AC に対して CAPWAP トンネルを通して送信します。クライアントデータフレームに対して、カプセル化フォーマットを 802.3 または 802.11 に設定できます。フォーマットを 802.3 に設定することで、AC がフレームフォーマット変換を実行する必要がなくなるため、NEC は 802.3 の設定を推奨します。

クライアントデータフレームに対するカプセル化フォーマットの設定手順は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. クライアントデータフレームに対してカプセル化フォーマットを設定する	**client frame-format** { **dot3** | **dot11** }	デフォルト：クライアントデータフレームは、802.3フォーマット内でカプセル化されます。

4.23 クイックアソシエーションの有効化

ロードバランスまたはバンドナビゲーションを有効にすることで、クライアント関連づけ効率に影響がでる可能性があります。遅延が許されないサービス、あるいはロードバランス、帯域幅のナビゲーションが必要ない環境では、サービステンプレートに対するすばやい関連づけを有効にすることができます。

この機能により、WLAN 内でロードバランスまたはバンドナビゲーションが有効な場合でも、装置がサービステンプレートに関連づけられたクライアント上で、ロードバランスまたはバンドナビゲーションを実行するのを無効にできます。

以下にクイックアソシエーションを有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. クイックアソシエーションを有効にする	**quick-association enable**	デフォルト：無効

4.24 クライアント再認証を行う前のアイドル時間の設定

再認証の失敗を削減するため、クライアントに再認証を行う前のアイドル時間を設定します。

WLAN MAC アドレス認証のクライアントで URL リダイレクションが有効である場合、AP は MAC アドレス認証にパスしたクライアントをログオフします。次回の MAC アドレス認証の施行時、クライアントは MAC アドレス認証にパスし、WLAN にアクセスすることができます。アイドル時間が設定されている場合、AP はクライアントをログオフしたのち、ダイナミックブラックリストにクライアントを追加し、指定したアイドル時間後にクライアントのエントリがエージアウトします。

以下にクライアント再認証を行う前のアイドル時間の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアント再認証を行う前のアイドル時間を設定する	**wlan client reauthentication-period** [*period-value*]	デフォルト：設定なし

4.25 APが未知のクライアントからのトラフィックを処理する方法の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—

操作	コマンド	補足
3． APが未知のクライアントからのトラフィックを処理する方法を設定する	**unknown-client** [**deauthenticate** | **drop**]	デフォルト：APは、未知のクライアントからのパケットを廃棄し、未知のクライアントを認証しません。

4.26 クライアント情報報告先のWebサーバの指定

指定した Web サーバに対し、HTTP を使用してクライアントの情報を報告します。報告されたクライアント情報は、クライアントの MAC アドレス、紐付けされた AP、紐付いた時間を含みます。Web サーバは、サーバのホスト名、ポート番号、経路が指定された場合に限りクライアント情報を承認します。

クライアント情報報告先の Web サーバの指定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Web サーバのホスト名とポート番号を指定する	**wlan web-server host** *host-name* **port** *port-number*	デフォルト：設定なし
3． Web サーバの経路を指定する	**wlan web-server api-path** *path*	デフォルト：設定なし
4． 1 度に報告するクライアントエントリの最大数を設定する	**wlan web-server max-client-entry** *number*	デフォルト：10

4.27 クライアントアソシエーションを許可するSSIDの設定

🕮 **メモ：**

クライアントアソシエーションを許可する SSID の設定はソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

クライアントが指定された SSID を介して WLAN にアクセスできるようにします。

クライアントアソシエーションの許可された SSID の設定手順は以下のとおりです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． user-profile view に移行する	**user-profile** *profile-name*	—
3． クライアントアソシエーションを許可する SSID を設定する。	**wlan permit-ssid** *ssid-name*	デフォルト：設定なし
4． ローカルユーザを作成し、その View に移行する	local-user *user-name* **class network**	—

操作	コマンド	補足
5. ローカルユーザにユーザプロファイルを適用する	**authorization-attribute user-profile** *profile-name*	デフォルト：設定なし

4.28 ホワイトリストへのクライアントの追加

最初のクライアントをホワイトリストに追加するとき、システムは、すべてのオンラインのクライアントを切断するかどうか尋ねます。ホワイトリストを設定するために、設定画面で“Y”を入力してください。

ホワイトリストへのクライアントの追加手順は以下のとおりです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ホワイトリストにクライアントを追加する	**wlan whitelist mac-address** *mac-address*	デフォルト：設定なし

4.29 スタティックブラックリストへのクライアントの追加

ホワイトリストとスタティックブラックリストの両方にクライアントを追加することはできません。

スタティックブラックリストへのクライアントの追加手順は以下のとおりです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. スタティックブラックリストにクライアントを追加する	**wlan static-blacklist mac-address** *mac-address*	デフォルト：設定なし

4.30 ダイナミックブラックリストの設定

AC あるいは AP でダイナミックブラックリストを設定することができます。

AC でダイナミックブラックリストを設定した場合、AC に接続されたすべての AP はダイナミックブラックリストにあるクライアントを拒否します。

AP でダイナミックブラックリストを設定した場合、AP はダイナミックブラックリストにあるクライアントを拒否することができますが、クライアントは AC に接続された別の AP と関連し続けることができます。多くのクライアントが存在する環境では AC でダイナミックブラックリストを設定することを推奨します。

その後、ダイナミックブラックリストに追加されたエントリは設定されたエージングタイマの間、拒否されます。

ホワイトリスト、ブラックリストの両方が設定されている場合、ホワイトリストの設定が適用されます。

以下にダイナミックブラックリストの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. ダイナミックブラックリストを設定する	• APでダイナミックブラックリストを設定する：**wlan dynamic-blacklist active-on-ap** • ACでダイナミックブラックリストを設定する：**undo wlan dynamic-blacklist active-on-ap**	デフォルト：APでダイナミックブラックリストが設定されています。
3. ダイナミックブラックリストのエージングタイマを設定する	**wlan dynamic-blacklist lifetime** *lifetime*	デフォルト：300秒 偽のクライアントエントリのみ適用されます。

4.31 ACLにもとづくアクセス制御の設定

🕮 **メモ：**

ACL にもとづくアクセス制御の設定はソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

クライアントが指定された ACL にもとづいて WLAN にアクセスできるようにします。ACL にもとづくアクセス制御と、ホワイトリストおよびブラックリストの両方を同じ装置に設定しないでください。

AP View の設定は、サービステンプレート View の設定よりも優先されます。

この機能は、レイヤ 2 ACL だけをサポートし、一致基準として送信元 MAC アドレスだけを使用できます。

以下に ACL にもとづくアクセス制御の設定を示します。

4.31.1 サービステンプレート View での ACL にもとづくアクセス制御の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. ACL にもとづくアクセス制御を設定する	**access control acl** *acl-number*	デフォルト：設定なし

4.31.2 AP View での ACL にもとづくアクセス制御の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. ACL にもとづくアクセス制御を設定する	**access control acl** *acl-number*	デフォルト：設定なし

4.32 領域コードの指定

領域コードは、使用可能周波数、使用可能チャネル、伝送電力レベルなどの性質を決定します。AP を設定する前に、有効な領域コードを設定してください。

領域コードの変更により引き起こされる規制違反を防止するために、領域コードをロックしてください。

4.32.1 AP view での領域コードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. 領域コードを指定する	**region-code** *code*	デフォルト：APは、AP group view の設定を使用します。AP group view に領域コードが存在しない場合、APはglobal configuration view の設定を使用します。
4. 領域コードをロックする	**region-code-lock enable**	デフォルト：APは、AP group view の設定を使用します。AP group view に領域コードが存在しない場合、APはglobal configuration view の設定を使用します。

4.32.2 AP group view での領域コードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. 領域コードを指定する	**region-code** *code*	デフォルト：APはglobal configuration view の設定を使用します。
4. 領域コードをロックする	**region-code-lock enable**	デフォルト：APはglobal configuration view の設定を使用します。

4.32.3 グローバル領域コードの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan global-configuration**	—
3. 領域コードを指定する	**region-code** *code*	デフォルト：領域コードはJPです。
4. 領域コードをロックする	**region-code-lock enable**	デフォルト：設定なし

4.33 APのブロードキャストプローブ要求への応答の無効化

ブロードキャストプローブ要求は、SSID が空欄の ANY 接続です。

この機能によってブロードキャストプローブ要求への応答を無効(SSID が空欄の ANY 接続拒否)ができます。

🕮 **メモ：**

SSID が“ANY”の文字列である ANY 接続は、本機能に限らず“ANY”の文字列を持つサービステンプレートを作成しなければ接続されません。

4.33.1 AP view での AP のブロードキャストプローブ要求への応答の無効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. AP でブロードキャストプローブ要求への応答を無効にする	**broadcast-probe reply disable**	デフォルト：APは、AP group view の設定を使用します。

4.33.2 AP group view での AP のブロードキャストプローブ要求への応答の無効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP でブロードキャストプローブ要求への応答を無効にする	**broadcast-probe reply disable**	デフォルト：APは、ブロードキャストプローブ要求に応答します。

4.34 NAS IDの設定

NAS ID（Network Access Server IDentifier）、NAS port ID（Network Access Server Port IDentifier）は、クライアントのネットワークアクセスサーバを独自に識別し、クライアントトラフィックの送信元を区別します。

無線にサービステンプレートが設定された状態で NAS ID あるいは NAS port ID を指定する場合、無線はサービステンプレートに対して NAS ID あるいは NAS port ID を使用します。

4.34.1 AP view での NAS ID の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． NAS ID を設定する	**nas-id** *nas-id*	デフォルト：APは、AP group view の設定を使用します。AP group view にNAS IDが存在しない場合、APはglobal configuration view の設定を使用します。
4． NAS port ID を設定する	**nas-port-id** *nas-port-id*	デフォルト：APは、AP group view の設定を使用します。AP group view にNAS port IDが存在しない場合、APはglobal configuration view の設定を使用します。
5． NAS VLAN ID を設定し、AC で RADIUS 要求の VLAN ID にカプセル化することを有効にする	**nas-vlan** vlan-id	デフォルト：設定なし RADIUSサーバに送信される認証要求はNAS VLAN IDフィールドがありません。 他ベンダのセキュリティアカウント管理サーバ（SAM、Security Accounting Management）がRADIUSサーバとして使用している場合、NAS VLAN ID を設定してください。

4.34.2 AP group view での NAS ID の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． NAS ID を設定する	**nas-port-id** *nas-port-id*	デフォルト：AP groupは、APはglobal configuration view の設定を使用します。
4． NAS port ID を設定する	**nas-port-id** *nas-port-id*	デフォルト：APはglobal configuration view の設定を使用します。

4.34.3 グローバル NAS ID の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan global-configuration**	—
3． グローバル NAS ID を設定する	**nas-id** *nas-id*	デフォルト：設定なし
4． NAS port ID を設定する	**nas-port-id** *nas-port-id*	デフォルト：設定なし

4.35 APへのコンフィグレーションファイルの設定

🕮 **メモ：**

remote-configuration を使用することを推奨します。**remote-configuration** コマンドの詳細は、QX-W1000/W1100 シリーズアクセスポイント Anchor-AC オペレーションマニュアルの *“AP 管理”* の *“リモート設定の割り当て設定”* を参照してください。

- **remote-configuration** を有効にした場合、**remote-configuration** で設定可能なコマンドがデフォルト値として適用されます。**remote-configuration** で設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**remote-configuration** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

AC から AP の設定を行なう場合、**map-configuration** コマンドを使用してコンフィグレーションファイルを AP に設定できます。コンフィグレーションファイルは手動で作成し、予め FTP などによって AC の **flash:/**内に保存しておく必要があります。

コンフィグファイルの内容は **more** *file-name* コマンドでも確認可能です。

AC までの CAPWAP トンネルが稼働した後、コンフィグレーションファイルが適用されます。AP を再起動すると、コンフィグレーションファイルは失効します。

コンフィグレーションファイルの内容は、正しいフォーマットで入力されたコマンド完全なコマンドにする必要があり、省略したコマンドを使用することはできません。

map-configuration コマンドで使用可能なコマンドは AP のコマンドマニュアルの“*インタフェース*”及び“*アクセス*”のセクションに記載されているコマンドです。

AP がコンフィグレーションファイルを使用して設定される場合、AC までの CAPWAP トンネルが確立可能なネットワークである必要があります。

AP へのコンフィグレーションファイルの設定手順は以下のとおりです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—

操作	コマンド	補足
3. APで使用するコンフィグレーションファイルを設定する	**map-configuration** *filename*	デフォルト：設定なし ACのストレージメディアに使用するコンフィグレーションファイルが格納されていることを確認してください。

4.36 WLANアクセスのSNMP notificationの有効化

SNMP notification の通知機能は重要な WLAN アクセスに関するイベントを NMS に通知するため、SNMP notification を作成します。NMS は設定された出力ルールにしたがって notification を出力する方法を決定します。SNMP notification の詳細は QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 11 *システム管理の "SNMP"* を参照してください。

WLAN アクセスの SNMP notification を有効にする手順は以下のとおりです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN アクセスの SNMP notification を有効にする	**snmp-agent trap enable wlan client**	デフォルト：無効
3. クライアント監査の SNMP notification を有効にする	**snmp-agent trap enable wlan client-audit**	デフォルト：無効

4.37 WLANアクセスの表示と維持

すべての view で **display** コマンドと **wlan link-test** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
ブラックリストエントリを表示する	**display wlan blacklist** { **dynamic** | **static** }
各ラジオのオンラインクライアント数とチャネル情報を表示する	**display wlan ap all radio client-number**
各APグループのクライアント数を表示する	**display wlan ap-group all client-number**
2.4GHzと5GHz帯でオンラインのクライアント数を表示する	**display wlan ap all client-number**
クライアント情報を表示する	**display wlan client** [**ap** *ap-name* [**radio** *radio-id*] | **mac-address** *mac-address* | **service-template** *service-template-name* | **frequency-band** { **2.4** | **5** }] [**verbose**]
クライアントのデバイス情報を表示する	**display wlan client device-information [mac-address** *mac-address* **]**
クライアントのオンライン期間を表示する	**display wlan client online-duration** [**ap** *ap-name*]

操作	コマンド
APに対する領域コード情報を表示する	**display wlan ap** { **all** | **name** *ap-name* } **region-code**
サービステンプレート情報を表示する	**display wlan service-template** [*service-template-name*] [**verbose**]
クライアントスタティスティックまたはサービステンプレートスタティスティックを表示する	**display wlan statistics** { **ap** { **all** | **name** *ap-name* } **connect-history** | **client** [**mac-address** *mac-address*] | **service-template** *service-template-name* [**connect-history**] }
ホワイトリストエントリを表示する	**display wlan whitelist**
クライアントのステータス情報を表示する	**display wlan client status** [**mac-address** *mac-address*] [**verbose**]
クライアントをログオフする	**reset wlan client** { **all** | **mac-address** *mac-address* }
指定されたクライアントまたはすべてのクライアントをダイナミックブラックリストから除去する	**reset wlan dynamic-blacklist** [**mac-address** *mac-address*]
クライアントの統計情報を消去する	**reset wlan statistics client** { **all** | **mac-address** *mac-address* }
サービステンプレートの統計情報を消去する	**reset wlan statistics service-template** *service-template-name*
クライアントへの無線リンクの品質をテストする	**wlan link-test** *mac-address*

4.38 WLANアクセスの設定例

4.38.1 WLAN アクセスの設定例

I. ネットワーク要件

図 4-7に示すように、スイッチは AP とクライアントに IP アドレスを割り当てるための DHCP サーバとして動作します。AP は、無線サービスに SSID trade-off を提供します。



図 4-7 ネットワーク図

II. 設定手順

1)　VLAN 100 を作成します。

```
<AC> system-view
[AC] vlan 100
```

```
[AC-vlan100] quit
```

2)　VLAN-interface 100 を作成し、IP アドレスに VLAN-interface 100 を割り当てます。

```
[AC] interface vlan-interface 100
[AC-Vlan-interface100] ip address 10.1.9.58 16
```

3)　手動 AP ap1 を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

4)　サービステンプレートを作成し、AP にサービステンプレートを設定します。

サービステンプレート service1 を作成します。サービステンプレートに SSID として trade-off を設定し、VLAN 100 を設定します。サービステンプレートを有効にします。

```
<AC> system-view
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid trade-off
[AC-wlan-st-service1] vlan 100
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

AP の radio1 の作動チャネルをチャネル 64 に設定します。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] channel 64
```

radio 1 に対してサービステンプレート service1 を設定します。

```
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] service-template service1
```

III. 設定の確認

SSID が trade-off か検証し、サービステンプレートを有効にします。

```
[AC] display wlan service-template verbose
Service template name          : service1
Description                    : Not configured
SSID                           : trade-off
SSID-hide                      : Disabled
User-isolation                 : Disabled
Service template status        : Enabled
Maximum clients per BSS        : 64
Frame format                   : Dot3
Seamless roam status           : Disabled
Seamless roam RSSI threshold   : 50
Seamless roam RSSI gap         : 20
VLAN ID                        : 100
AKM mode                       : Not configured
Security IE                    : Not configured
Cipher suite                   : Not configured
TKIP countermeasure time       : 0 sec
```

```
PTK life time                   : 43200 sec
PTK rekey                       : Enabled
GTK rekey                       : Enabled
GTK rekey method                : Time-based
GTK rekey time                  : 86400 sec
GTK rekey client-offline        : Disabled
User authentication mode        : Bypass
Intrusion protection            : Disabled
Intrusion protection mode       : Temporary-block
Temporary block time            : 180 sec
Temporary service stop time     : 20 sec
Fail VLAN ID                    : 1
Critical VLAN ID                : Not configured
802.1X handshake                : Enabled
802.1X handshake secure         : Disabled
802.1X domain                   : my-domain
MAC-auth domain                 : Not configured
Max 802.1X users per BSS        : 4096
Max MAC-auth users per BSS      : 4096
802.1X re-authenticate          : Enabled
Authorization fail mode         : Online
Accounting fail mode            : Online
Authorization                   : Permitted
Key derivation                  : N/A
PMF status                      : Disabled
Hotspot policy number           : Not configured
Forwarding policy status        : Disabled
Forwarding policy name          : Not configured
Forwarder                       : AC
FT status                       : Disabled
QoS trust                       : Port
QoS priority                    : 0
```

クライアントを AP に関連づけます。（詳細は省略します。）

クライアントが WLAN にアクセスできるか確認します。

```
[AC] display wlan client service-template service1
Total number of clients: 1

MAC address      Username   AP name    RID   IP address      IPv6 address   VLAN
0023-8933-223b    N/A        ap1        1     3.0.0.3                       100
1024/1    3.0.0.3                   100
```

4.38.2 ローカル MAC アドレス認証でクライアントアソシエーションを許可する SSID の設定例

I. ネットワーク要件

図 4-8に示すように、クライアント 1 が接続できる SSID を ssida、クライアント 2 の接続できる SSID を ssidb に設定します。ローカル MAC アドレス認証を AC に設定します。

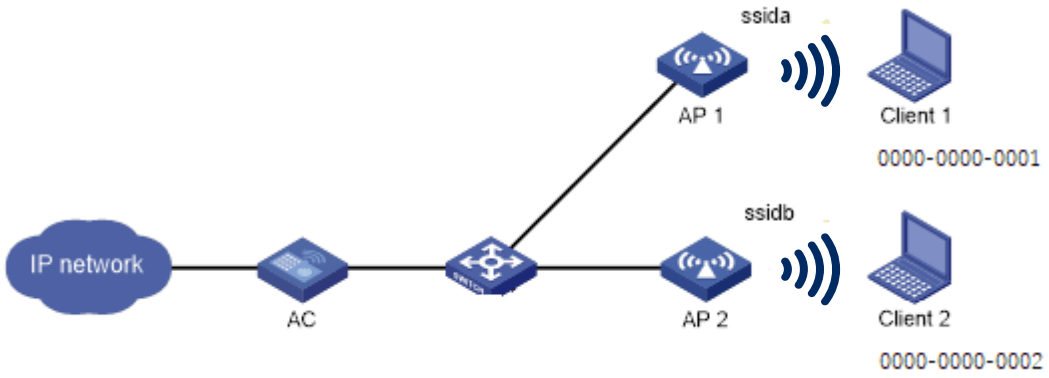


図 4-8 ネットワーク図

II. 設定手順

1)　MAC アドレス認証を設定します。

MAC アドレス認証をグローバルで有効にします

```
[AC] mac-authentication
```

MAC ベースのアカウントを使うように MAC アドレス認証を設定します。ユーザ名とパスワードはハイフンありで、小文字を指定します。

```
[AC] mac-authentication user-name-format mac-address with-hyphen lowercase
```

2)　サービステンプレート ssida を作成します。サービステンプレートの SSID 名を設定します。

```
[AC]  system-view
[AC] wlan service-template ssida
[AC-wlan-st-ssida] ssid ssida
```

3)　WLAN セキュリティを設定します。

#AKM モードとして PSK を設定し、プレーンテキストで鍵 12345678 を指定します。

```
[AC-wlan-st-ssida] akm mode psk
[AC-wlan-st-ssida] preshared-key pass-phrase simple 12345678
```

#cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-ssida] cipher-suite ccmp
[AC-wlan-st-ssida] security-ie rsn
```

#MAC アドレス認証を設定します。

```
[AC-wlan-st-ssida] client-security authentication-mode mac
```

#サービステンプレート ssida を有効にします。

```
[AC-wlan-st-ssida] service-template enable
[AC-wlan-st-ssida] quit
```

4)　サービステンプレート ssidb を作成します。サービステンプレートの SSID 名を設定します。

```
[AC]  system-view
[AC] wlan service-template ssidb
[AC-wlan-st-ssidb] ssid ssidb
```

5)　WLAN セキュリティを設定します。

#AKM モードとして PSK を設定し、プレーンテキストで鍵 12345678 を指定します。

```
[AC-wlan-st-ssidb] akm mode psk
[AC-wlan-st-ssidb] preshared-key pass-phrase simple 12345678
```

#cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-ssidb] cipher-suite ccmp
[AC-wlan-st-ssidb] security-ie rsn
```

#MAC アドレス認証を設定します。

```
[AC-wlan-st-ssidb] client-security authentication-mode mac
```

#サービステンプレート ssidb を有効にします。

```
[AC-wlan-st-ssidb] service-template enable
[AC-wlan-st-ssidb] quit
```

6)　ISP ドメイン dom1 を作成し、ローカル認証を設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access local
[AC-isp- dom1] authorization lan-access local
[AC-isp- dom1] accounting lan-access local
[AC-isp- dom1] quit
```

7)　MAC アドレス認証に ISP ドメイン dom1 を使用するように設定します。

```
[AC] mac-authentication domain dom1
```

8)　ユーザプロファイル ssdia を作成します。アソシエーションを許可する SSID 名として ssida を設定します。

```
[AC] user-profile ssida
[AC-user-profile-ssida] wlan permit-ssid ssida
[AC-user-profile-ssida] quit
```

9)　ユーザプロファイル ssidb を作成します。アソシエーションを許可する SSID 名として ssidb を設定します。

```
[AC] user-profile ssidb
[AC-user-profile-ssidb] wlan permit-ssid ssidb
[AC-user-profile-ssidb] quit
```

10)　ローカルユーザを追加します。

#ホストの MAC アドレス 00-00-00-00-00-01 をユーザ名とパスワードに設定し、LAN アクセスサービスを有効にします。

```
<AC> system-view
[AC] local-user 00-00-00-00-00-01 class network
[AC-luser-network-00-00-00-00-00-01] password simple 00-00-00-00-00-01
```

#ユーザの LAN アクセスサービスを指定します。

```
[AC-luser-network-00-00-00-00-00-01] service-type lan-access
```

#ユーザプロファイル ssida を適用します。

```
[AC-luser-network-00-00-00-00-00-01] authorization-attribute user-profile ssida
[AC-luser-network-00-00-00-00-00-01] quit
```

#ホストの MAC アドレス 00-00-00-00-00-02 をユーザ名とパスワードに設定し、LAN アクセスサービスを有効にします。

```
<AC> system-view
[AC] local-user 00-00-00-00-00-02 class network
[AC-luser-network-00-00-00-00-00-02] password simple 00-00-00-00-00-02
```

#ユーザの LAN アクセスサービスを指定します。

```
[AC-luser-network-00-00-00-00-00-02] service-type lan-access
```

#ユーザプロファイル ssidb を適用します。

```
[AC-luser-network-00-00-00-00-00-02] authorization-attribute user-profile ssidb
[AC-luser-network-00-00-00-00-00-02] quit
```

11）AP 名 AP1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap AP1 model QX-W1020
[AC-wlan-ap-AP1] serial-id 219801A0CNC138011454
```

12）サービステンプレート ssida を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-AP1] radio 1
[AC-wlan-ap-AP1-radio-1] service-template service1
[AC-wlan-ap-AP1-radio-1] radio enable
[AC-wlan-ap-AP1-radio-1] return
```

13）AP 名 AP2 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap AP2 model QX-W1020
[AC-wlan-ap-AP2] serial-id 219801A0CNC138011455
```

14）サービステンプレート ssidb を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-AP2] radio 1
[AC-wlan-ap-AP2-radio-1] service-template service1
[AC-wlan-ap-AP2-radio-1] radio enable
[AC-wlan-ap-AP2-radio-1] return
```

III. 設定の確認

#クライアント 1 が ssida に接続できること、クライアント 2 が ssidb に接続できることを確認します。(詳細は省略します。)

#クライアント 1 が ssidb に接続できないこと、クライアント 2 が ssida に接続できないことを確認します。(詳細は省略します。)

4.38.3 ホワイトリストの設定例

I. ネットワーク要件

図 4-9に示すように、MAC アドレスが 0000-000f-1211 のクライアントのみが WLAN へのアクセスを許可されるように、ホワイトリストを設定します。

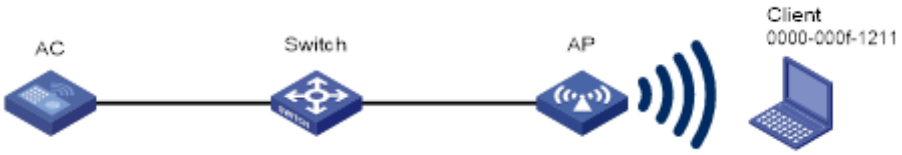


図 4-9 ネットワーク図

II. 設定手順

#ホワイトリストに MAC アドレス 0000-000f-1211 を追加します。

```
<AC> system-view
[AC] wlan whitelist mac-address 0000-000f-1211
```

III. 設定の確認

MAC アドレス 0000-000f-1211 がホワイトリストにあるか確認します。

```
[AC] display wlan whitelist
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```

4.38.4 スタティックブラックリストの設定例

I. ネットワーク要件

図 4-10に示すように、MAC アドレスが 0000-000f-1211 のクライアントのみが WLAN へのアクセスを拒否されるように、スタティックブラックリストを設定します。

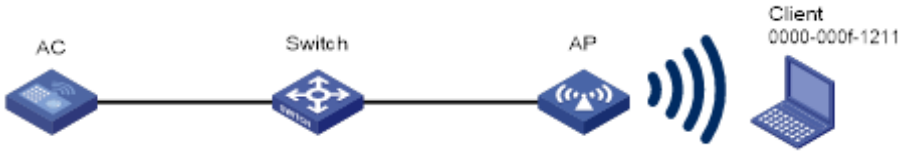


図 4-10 ネットワーク図

II. 設定手順

スタティックブラックリストに MAC アドレス 0000-000f-1211 を追加します。

```
<AC> system-view
[AC] wlan static-blacklist mac-address 0000-000f-1211
```

III. 設定の確認

MAC アドレス 0000-000f-1211 がスタティックブラックリストにあるか確認します。

```
[AC] display wlan blacklist static
Total number of clients: 1
 MAC addresses:
  0000-000f-1211
```

4.38.5 AP view での ACL にもとづくアクセス制御の設定例

I. ネットワーク要件

図 4-11に示すように、MAC アドレスが 0000-000f-1211 のクライアントのみが WLAN へのアクセスを許可されるように、AP に ACL を設定します。

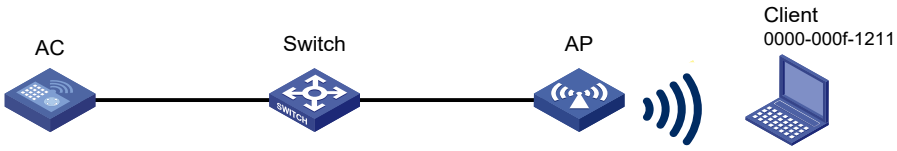


図 4-11 ネットワーク図

II. 設定手順

ACL 4000 に、送信元 MAC アドレス 0000-000f-1211 を許可する設定を追加します。

```
<AC> system-view
[AC] acl number 4000
[AC-acl-mac-4000] rule 1 permit source-mac 0000-000f-1211 ffff-ffff-ffff
```

```
[AC-acl-mac-4000] quit
```

#AP ap1 に ACL4000 を設定します。

```
[AC] wlan ap ap1 model QX-W1010
[AC-wlan-ap-ap1] access-control acl 4000
```

III. 設定の確認

MAC アドレス 0000-000f-1211 のクライアントが AP に接続できることを確認します。
(詳細は省略します。)

4.38.6 サービステンプレート view での ACL にもとづくアクセス制御の設定例

I. ネットワーク要件

図 4-12に示すように、MAC アドレスが 0000-000f-1211 のクライアントのみが WLAN へのアクセスを許可されるように、サービステンプレートに ACL を設定します。

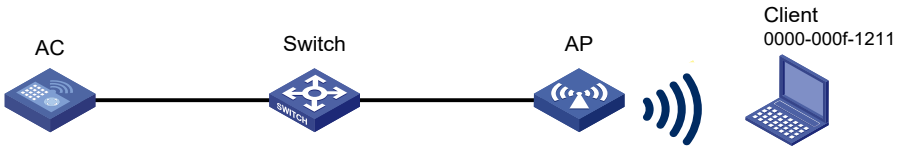


図 4-12 ネットワーク図

II. 設定手順

ACL 4000 に、送信元 MAC アドレス 0000-000f-1211 を許可する設定を追加します。

```
<AC> system-view
[AC] acl number 4000
[AC-acl-mac-4000] rule 1 permit source-mac 0000-000f-1211 ffff-ffff-ffff
[AC-acl-mac-4000] quit
```

#サービステンプレート service1 に ACL4000 を設定します。

```
[AC] wlan service-template service1
[AC-wlan-st-service1] access-control acl 4000
```

III. 設定の確認

MAC アドレス 0000-000f-1211 のクライアントが AP に接続できることを確認します。
(詳細は省略します。)

目次

5 章 WLAN セキュリティ 5-1
5.1 WLAN セキュリティ概要 5-1
5.2 Pre-RSNA メカニズム 5-1
5.2.1 オープンシステム認証 5-1
5.2.2 共有鍵認証 5-2
5.3 RSNA メカニズム 5-3
5.3.1 認証 5-3
5.3.2 鍵管理 5-3
5.3.3 暗号化方式 5-8
5.4 管理フレームの保護 5-9
5.5 ダイナミック WEP メカニズム 5-11
5.6 プロトコルと標準 5-11
5.7 WLAN セキュリティ設定作業リスト 5-12
5.7.1 AKM モードの設定 5-13
5.7.2 暗号化規格の設定 5-13
5.7.3 暗号化方式の設定 5-14
5.7.4 PSK の設定 5-14
5.7.5 KDF の設定 5-15
5.7.6 GTK アップデートの設定 5-15
5.7.7 PTK アップデートの設定 5-16
5.7.8 TKIP MIC failure ホールドタイムの設定 5-16
5.7.9 WEP 鍵の設定 5-17
5.7.10 管理フレーム保護の設定 5-17
5.7.11 ダイナミック WEP メカニズムの有効化 5-18
5.7.12 WPA3 の設定 5-19
5.7.13 Enhanced Open システム認証の設定 5-20
5.7.14 移行モードでの推奨サービステンプレートの指定 5-20
5.7.15 WLAN セキュリティの SNMP notification の有効化 5-21
5.7.16 WPA3-SAE の SAE 交換時の PWE 生成方式の設定 5-22
5.8 WLAN セキュリティの表示と維持 5-22
5.9 WLAN セキュリティの設定例 5-23
5.9.1 共有鍵認証設定例 5-23
5.9.2 WPA-PSK(TKIP)設定例 5-25
5.9.3 WPA2-PSK(AES)＋MAC アドレス認証設定例 5-27
5.9.4 802.1X AKM 設定例 5-30
5.9.5 管理フレーム保護設定例 5-33
5.9.6 ダイナミック WEP メカニズム設定例 5-35
5.9.7 WPA3 エンタープライズ(192bit セキュリティなし)設定例 5-38
5.9.8 WPA3 パーソナル設定例 5-41

5章 WLAN セキュリティ

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

5.1 WLANセキュリティ概要

オリジナルの IEEE802.11 は Pre-RSNA（Pre Robust Security Network Association）メカニズムを使用します。このメカニズムは鍵露出（key exposure）、トラフィック妨害（traffic interception）、改変（tampering）などの攻撃に対してセキュリティ上で脆弱性があります。WLAN セキュリティを拡張させるため、IEEE802.11i（RSNA メカニズム）が導入されました。WLAN のセキュリティを向上させるため、必要に応じて Pre-RSNA あるいは RSNA のどちらかを選択することができます。

IEEE802.11i は WLAN データトラフィックのみを暗号化します。暗号化されていない WLAN 管理フレームは機密性、確実性、完全性への攻撃に対して無防備となります。IEEE802.11w は 802.11i フレームワークをもとにして管理フレームの保護を行うことで、偽造された認証されていないフレームや分離されたフレームを使用した攻撃を防ぐことができます。

5.2 Pre-RSNAメカニズム

⚠ **重要**：
WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

Pre-RSNA メカニズムは、認証にオープンシステムと共有鍵アルゴリズムを使用し、データの暗号に WEP を使用します。WEP（Wired Equivalent Privacy）は機密性を保持するためストリーム暗号として RC4 を使用します。鍵は 40 ビット（WEP40）、104 ビット（WEP104）、128 ビット（WEP128）をサポートしています。

5.2.1 オープンシステム認証

オープンシステム認証はデフォルトでもっとも簡単な認証アルゴリズムです。オープンシステム認証を使用して認証を要求するクライアントは認証にパスすることができます。

オープンシステム認証は以下のプロセスを使用します。

1) クライアントは AP に認証を要求します。
2) クライアントが認証にパスしたのち、AP はクライアントに認証の応答を送信します。

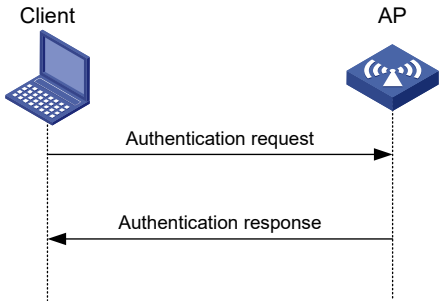


図 5-1 オープンシステム認証のプロセス

5.2.2 共有鍵認証

共有鍵認証は、認証を行うため AP とクライアントの WEP 鍵を使用します。

共有鍵認証は以下のプロセスを使用します。

1) クライアントは AP に認証要求を送信します。
2) AP はランダムに作成したチャレンジテキスト（乱数）をクライアントに送信します。
3) クライアントはチャレンジテキストを暗号化するためクライアントの WEP 鍵を使用し、AP に暗号化したチャレンジテキストを送信します。
4) AP はチャレンジテキストを復号化するため、AP の WEP 鍵を使用します。もとのチャレンジテキストと復号化したチャレンジテキストを比較します。2 つのチャレンジテキストが一致した場合、クライアントは認証にパスします。一致しない場合、クライアントは認証に失敗します。

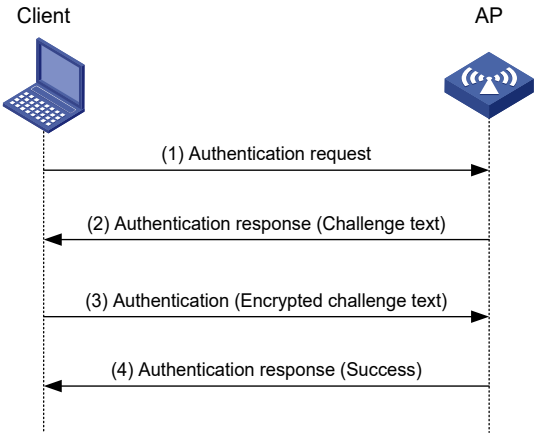


図 5-2 共有鍵の認証プロセス

5.3 RSNAメカニズム

重要：
RSNA はリンクレイヤの認証を行うため、オープンシステム認証が必要です。

RSNA メカニズムは WPA（Wi-Fi Protected Access）、RSN（Robust Security Network）セキュリティモードが含まれます。RSNA は以下の機能を提供します。

- ユーザの完全性を認証し、鍵を動的に作成し、鍵のアップデートを行うため、802.1X、PSK（Pre-Shared Key）AKM（Authentication and key management）を使用します。
  - **802.1X**－802.1X はユーザの認証を行います。802.1X は認証を行う際に PMK（pairwise master key）を作成します。クライアントと AP は PTK（pairwise transient key）を作成するために PMK を使用します。
  - **PSK**－PSK は PMK を作成するために使用します。クライアントと AP は PTK を作成するために PMK を使用します。
- データを暗号化するため、TKIP（Temporal key integrity Protocol）、CCMP（Counter Mode CBC-MAC Protocol）を使用します。

5.3.1 認証

802.1X 認証は PSK 認証よりもセキュリティの強度が強くなります。802.1X 認証の詳細は QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“WLAN 認証の概要”*、および *“WLAN 認証の設定”* を参照してください。

PSK 認証は AP とクライアントの両方で設定するため、同一の PSK が必要となります。PSK の完全性は 4-WAY ハンドシェイクを行う間に行われます。PTK の交換が成功した場合、クライアントは認証にパスします。

5.3.2 鍵管理

鍵管理は PTK、GTK（group temporary key）の作成方法およびアップデート方法について定義しています。PTK はユニキャストで使用されます。GTK はマルチキャスト、ブロードキャストで使用されます。

I. PTK、GTK

- PTK の構造



  - EAPOL-KCK（Extensible Authentication Protocol over LAN - Key Confirmation Key）は EAPOL-Key フレームの完全性を確認するために使用します。
  - EAPOL-KEK（Key Encryption Key）は EAPOL-Key フレームの鍵データを暗号化するために使用します。

- TK（Temporal Key）はユニキャストパケットを暗号化するために使用します。

- GTK には TK に加えてほかのフィールドが含まれます。TK はマルチキャストパケット、ブロードキャストパケットを暗号化するために使用します。

II. EAPOL-Key パケット

IEEE802.11i プロトコルは鍵の交換を行う際、EAPOL-Key を使用します。

Descriptor type (1 byte)	
Key information (2 bytes)	Key length (2 bytes)
Key replay counter (8 bytes)	
Key nonce (32 bytes)	
EAPOL Key IV (16 bytes)	
Key RSC (8 bytes)	
Reserved (8 bytes)	
Key MIC (16 bytes)	
Key data length (2 bytes)	Key data (n bytes)

図 5-3 EAPOL-Key の構造

表 5-1 EAPOL-Key フィールドの説明

フィールド	説明
Descriptor type	ネットワークタイプを指定します。 ● WPAネットワーク ● RSNネットワーク
Key information	鍵情報は表 5-2に示します。
Key length	鍵の長さです。
Key replay counter	リプライ攻撃を防ぐため、GTKアップデートの総数を記録します。APの交換が開始されたときにフィールドを0に設定し、連続したEAPOL-Keyフレームの値を増加させます。 クライアントは、以前に記録したフィールドの値より大きい場合、最新のEAPOL-Keyフレームからフィールドを記録します。以下の場合、EAPOL-Keyフレームを再送します。 ● クライアントで受信したフィールドの値が、保存されているフィールドの値と等しいあるいは小さい場合 ● APで受信されたフィールドが、APで記録されているフィールドと異なる場合 再送回数が最大数を超過した場合、APはクライアントを切断します。
Key nonce	PTKを作成するために使用するランダム値です。
EAPOL Key IV	TKIPを暗号化します。 このフィールドは暗号化タイプがCCMPでない場合のみ有効です。
Key RSC	リプライ攻撃を防ぐため、マルチキャストパケットあるいはブロードキャストパケットの総数を記録します。 各マルチキャストパケットあるいはブロードキャストパケットの転送を行うとAPは、このフィールドの値を増加します。

フィールド	説明
Reserved	予約されたフィールドです。
Key MIC	メッセージの完全性のチェックです。
Key data length	鍵データの長さです。
Key data	GTK、PMKID（pairwise master key identifier）などの転送されるデータです。

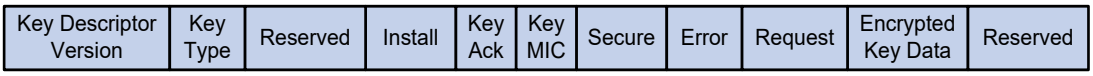


図 5-4 Key information の構造

表 5-2 Key information の説明

フィールド	説明
Key Descriptor Version	3ビットの鍵のバージョンです。 ● **1**－非CCMP鍵です。 ● **2**－CCMP鍵です。
Key Type	1ビットの鍵のタイプです。 ● **0**－マルチキャスト交換鍵です。 ● **1**－ユニキャスト交換鍵です。
Reserved	2ビットのフィールドが予約されています。 送信側でこのフィールドを0にした場合、受信側はこのフィールドを無視します。
Install	1ビットの鍵のインストレーションフィールドです。 鍵のタイプが1である場合、このフィールドは0あるいは1となります。 ● **0**－APはTKをインストールするためにクライアントに要求しません。 ● **1**－APはTKをインストールするためにクライアントに要求します。 鍵のタイプが0である場合、送信側はこのフィールドを0に設定し、受信側はこのフィールドを無視します。
Key Ack	1ビットの鍵のAcknowledgmentフィールドです。 値が1の場合、APはクライアントからAcknowledgmentを要求することを示します。
Key MIC	メッセージの完全性をチェックします。 このフィールドが1の場合、作成されたMIC（message integrity check）はEAPOL-keyフレームの鍵MICフィールドに含まれています。
Secure	1ビットの鍵の状態です。値が1の場合、鍵が既に作成されていることを示します。
Error	1ビットのMICチェックの状態です。 値が1の場合、MICが失敗したことを示します。 Requestフィールドが1の場合、クライアントは、このフィールドを1に設定します。
Request	1ビットのリクエストです。MICの改ざんレポートの4-WAYハンドシェイクあるいはマルチキャストハンドシェイクを初期化するため、クライアントがAPに要求するために使用されます。

フィールド	説明
Encrypted Key Data	1ビットの鍵データの暗号化状態です。値が1の場合、鍵データは暗号化されていることを示します。
Reserved	3ビットの予約されたフィールドです。 送信側でこのフィールドを0にした場合、受信側はこのフィールドを無視します。

III. WPA 鍵の交換

WPA は PTK をネゴシエートするため、4-WAY ハンドシェイクの EAPOL-key パケットを使用し、GTK をネゴシエートするため、2-WAY ハンドシェイクの EAPOL-key パケットを使用します。

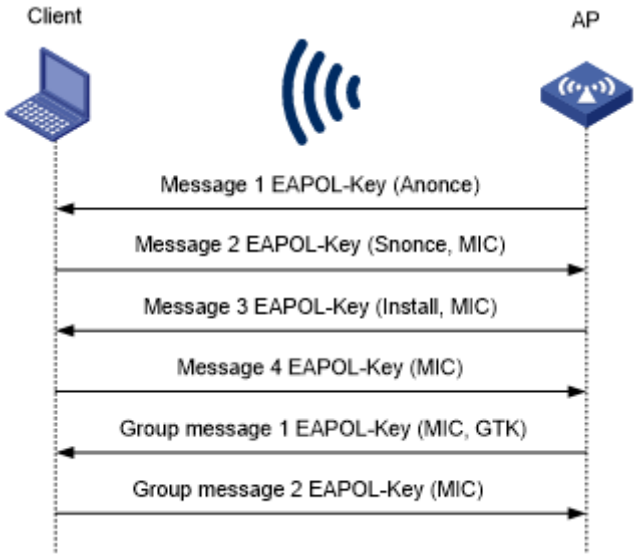


図 5-5 WPA 鍵交換プロセス

WPA 鍵交換は以下のプロセスを用います。

1) AP は ANonce のランダム値が含まれる EAPOL-key メッセージ 1 をクライアントに送信します。
2) クライアントは以下の処理を行います。
   a) KDF（key derivation function）によって PTK を作成するため、ランダム値 SNonce、ANonce、PMK を使用します。
   b) MIC を作成するため PTK の KCK を使用します。
   c) SNonce、MIC が含まれる EAPOL-key メッセージ 2 を返します。
3) AP は以下の処理を行います。
   a) KDF（key derivation function）によって PTK を作成するため、ランダム値 SNonce、ANonce、PMK を使用します。
   b) MIC を作成するため PTK の KCK を使用します。
   c) 受信した MIC とローカルに保存されている MIC を比較します。

d) 2 つの MIC が同一である場合、PTK インストレーションリクエストタグ、MIC が含まれる EAPOL-key メッセージ 3 を返します。

4) クライアントは以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、PTK をインストールし、MIC が含まれる EAPOL-key メッセージ 4 を返します。

5) AP は以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、PTK をインストールし、GMK によって GTK を作成し、KDF によって AP の MAC アドレスを作成します。

c) GTK、MIC が含まれる EAPOL-key グループメッセージ 1 を返します。

6) クライアントは以下の処理を行います。

a) 2 つの MIC が同一である場合、GTK をインストールします。

b) MIC が含まれる EAPOL-key グループメッセージ 2 を返します。

7) AP は以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、GTK をインストールします。

IV. RSN 鍵交換

RSN は PTK と GTK をネゴシエートするため、4-WAY ハンドシェイクの EAPOL-Key パケットを使用します。

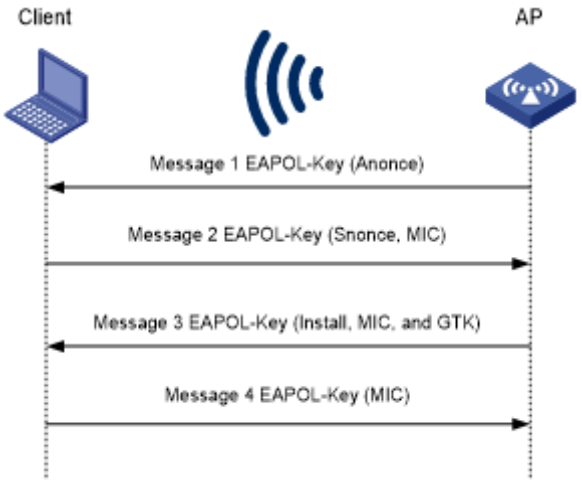


図 5-6 RSN 鍵交換のプロセス

RSN 鍵交換は以下のプロセスを用います。

1) AP は ANonce のランダム値が含まれる EAPOL-key メッセージ 1 をクライアントに送信します。

2) クライアントは以下の処理を行います。

a) KDF によって PTK を作成するため、ランダム値 SNonce、ANonce、PMK を使用します。

b) MIC を作成するため PTK の KCK を使用します。

c) SNonce、MIC が含まれる EAPOL-key メッセージ 2 を返します。

3) AP は以下の処理を行います。

a) KDF（key derivation function）によって PTK を作成するため、ランダム値 SNonce、ANonce、PMK を使用します。

b) MIC を作成するため PTK の KCK を使用します。

c) 受信した MIC とローカルに保存されている MIC を比較します。

d) 2 つの MIC が同一である場合、ランダム GMK によって GTK を作成し、KDF によって AP の MAC アドレスを作成します。

e) 鍵インストレーションリクエストタグ、MIC、GTK が含まれる EAPOL-key メッセージ 3 を返します。

4) クライアントは以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、PTK、GTK をインストールします。

c) MIC が含まれる EAPOL-key メッセージ 4 を返します。

5) AP は以下の処理を行います。

a) 受信した MIC とローカルに保存されている MIC を比較します。

b) 2 つの MIC が同一である場合、PTK、GTK をインストールします。

V. 鍵アップデート

鍵アップデートは WLAN セキュリティを拡張します。鍵アップデートには PTK アップデート、GTK アップデートがあります。

- PTK アップデート–4-WAY ハンドシェイク交換を使用してユニキャスト鍵をアップデートします。
- GTK アップデート–2-WAY ハンドシェイク交換を使用してマルチキャスト鍵をアップデートします。

5.3.3 暗号化方式

I. TKIP

TKIP と WEP は RC4 アルゴリズムを使用します。ハードウェアの変更を行うことなくソフトウェアのアップデートを行うことで WEP から TKIP に暗号化方式を変更することができます。TKIP は WEP に比べて以下の利点があります。

- TKIP は暗号セキュリティを拡張するため、長い IV（initialization vectors）を提供します。WEP の暗号化と比べ、TKIP 暗号化は 128 ビットの RC4 暗号アルゴリズムを使用し、IV の長さは 24 ビットから 48 ビットに増加されています。
- TKIP はスタティックに鍵が割り当てられることを防ぐため、ダイナミック鍵交換を行います。TKIP のダイナミック鍵は簡単に解読することはできません。
- TKIP は MIC、Countermeasure（対策）を提供します。パケットが改ざんされた場合、MIC（message integrity check）に失敗します。2 つのパケットが一定の期間、MIC に失敗した場合、AP は攻撃を防ぐためサービスの提供を停止するため、自動で Countermeasure（対策）を行います。

II. CCMP

CCMP は AES（Advanced Encryption Standard）暗号化アルゴリズムの CCM（Counter-Mode/CBC-MAC）をもとにしています。

CCMP はダイナミック鍵交換と管理方式が含まれます。各クライアントはダイナミックに鍵方式をネゴシエートすることができます。CCMP 暗号化方式のセキュリティを強化するため、定期的にアップデートすることができます。暗号化処理を行う間、CCMP は各暗号化パケットで異なる PN（packet number）を使用するため、48 ビット長の PN を使用します。これによって WLAN セキュリティを向上させています。

5.4 管理フレームの保護

管理フレームの保護サービスは、非認証、分離、強固な管理アクションフレームなどの強固な管理フレームを保護します。管理フレームはユニキャストフレームを暗号化する際に PTK を使用し、秘密性、完全性、リプレイ保護を提供します。BIP（Broadcast Integrity Protocol）を使用し、ブロードキャスト管理フレーム、マルチキャスト管理フレームの秘密性、リプレイ保護を提供します。

AP、クライアントが管理フレームの保護を行う場合、セキュリティを向上させるため SA（security association）クエリメカニズムが使用されます。SA クエリはアクティブ SA クエリ、パッシブ SA クエリがあります。

- アクティブ SA クエリ

図 5-7 に示すようにアクティブ SA クエリは以下のプロセスを使用します。

a) クライアントはAPにアソシエーションあるいは再送アソシエーションリクエストを送信します。

b) 要求を受信すると、AP は要求が拒否されたことと、後でクライアントが接続できることを知らせる応答を送ります。この応答にはアソシエーション復帰時間が含まれます。

c) クライアントの状態を確認するため、APはSAクエリリクエストを送信します。
   - □ AP がタイムアウト時間以内に SA クエリのリプライを受信した場合、AP はクライアントがオンラインであるとみなします。
   - □ AP がタイムアウト時間以内に SA クエリのリプライを受信しない場合、別の SA クエリリクエストを送信します。AP が再送タイムアウト時間以内に SA クエリのリプライを受信した場合、AP はクライアントがオンラインであるとみなします。アソシエーションのコールバックのタイムアウト時間まで、クライアントか

らアソシエーションリクエストあるいは再送アソシエーションリクエストに対して応答しません。

- □ AP が再送タイムアウト時間以内に SA クエリのリプライを受信しない場合、AP はクライアントがオフラインであるとみなします。そしてクライアントが再送アソシエーションを行うことを許可します。

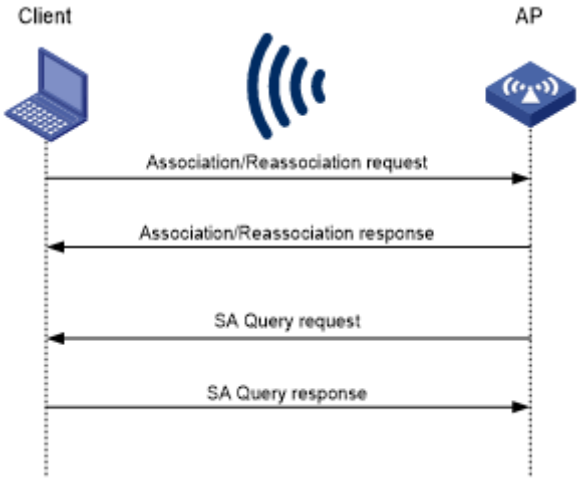


図 5-7 アクティブ SA クエリのプロセス

- パッシブ SA クエリ

図 5-8 に示すようにパッシブ SA クエリは以下のプロセスを使用します。

a) クライアントは暗号化されていないdisassociationフレームあるいはdeauthenticationフレームを受信すると、SAクエリプロセスを開始します。

b) クライアントはAPにSAクエリリクエストを送信します。

c) APはクライアントにSAクエリリプライを送信します。

- □ クライアントがリプライを受信した場合、クライアントは AP がオンラインであることを認識し、disassociation フレームあるいは deauthentication フレームの処理を行いません。
- □ クライアントがリプライを受信しない場合、クライアントは AP がオフラインであることを認識し、AP との関連づけを解除します。

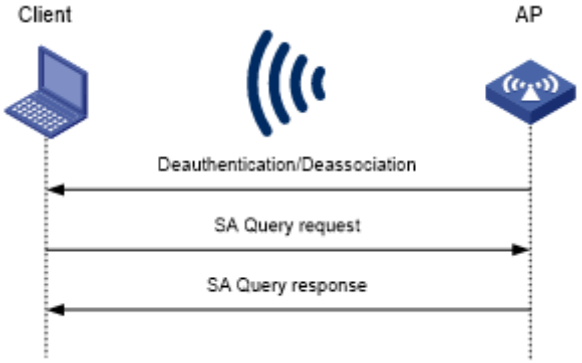


図 5-8 パッシブ SA クエリのプロセス

5.5 ダイナミックWEPメカニズム

重要：

ダイナミック WEP メカニズムはリンクレイヤの認証を行う際にオープンシステム認証を使用します。
WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

IEEE802.11 は、各ユーザがプライベート WEP 鍵の使用することを保証するため、ダイナミック WEP メカニズムを提供します。ユニキャスト通信においては、802.1X 認証を行う間にクライアントとサーバ間で交換が行われた WEP 鍵を使用します。マルチキャスト通信においては、設定された WEP 鍵を使用します。WEP 鍵を設定しない場合、AP はブロードキャスト通信、マルチキャスト通信を行うため WEP 鍵をランダムに作成します。

クライアントが 802.1X 認証にパスしたのち、AP はユニキャスト WEP 鍵、マルチキャストとブロードキャスト WEP 鍵、鍵の ID が含まれる RC4-EAPOL パケットをクライアントに送信します。ユニキャスト WEP 鍵の ID は 4 です。

5.6 プロトコルと標準

- IEEE Standard for Information technology－*Telecommunications and information exchange between systems－Local and metropolitan area networks－Specific requirements－2004*
- WI-FI Protected Access－*Enhanced Security Implementation Based On IEEE P802.11i Standard-Aug 2004*
- Information technology－*Telecommunications and information exchange between systems－Local and metropolitan area networks－Specific requirements－802.11, 1999*
- IEEE Standard for Local and metropolitan area networks *"Port-Based Network Access Control" 802.1X™-2004*
- 802.11i IEEE Standard for Information technology－*Telecommunications and information exchange between systems－Local and metropolitan area networks－Specific requirements*
- 802.11w IEEE Standard for Information technology－*Telecommunications and information exchange between systems－Local and metropolitan area networks－Specific requirements*

5.7 WLANセキュリティ設定作業リスト

注意：

- RSNA はリンクレイヤ認証を行うため、オープンシステム認証が必要です。
- ダイナミック WEP メカニズムはユーザアクセスの認証を行うため、802.1X 認証が必要です。
- AKM モード、暗号化規格、暗号化方式は RSNA ネットワークで設定する必要があります。
- 管理フレームの保護は、RSNA メカニズムを使用し、CCMP 暗号化方式、RSN 暗号化規格が設定されているネットワークでのみ有効です。

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

Pre-RSNA メカニズムの設定作業リストを以下に示します。

作業リスト
（必須設定項目）暗号化方式の設定
（必須設定項目）WEP鍵の設定
（オプション設定項目）SNMP notificationの有効化

RSNA メカニズムの設定作業リストを以下に示します。

作業リスト
（必須設定項目）AKMモードの設定
（必須設定項目）暗号化規格の設定
（必須設定項目）暗号化方式の設定
（オプション設定項目）PSKの設定
（オプション設定項目）KDFの設定
（オプション設定項目）GTKアップデートの設定
（オプション設定項目）PTKライフタイムの設定
（オプション設定項目）TKIP MIC failureホールドタイムの設定
（オプション設定項目）WEP鍵の設定
（オプション設定項目）管理フレーム保護の設定
（オプション設定項目）SNMP notificationの有効化

ダイナミック WEP メカニズムの設定作業リストを以下に示します。

作業リスト
（オプション設定項目）暗号化方式の設定
（オプション設定項目）WEP鍵の設定
（必須設定項目）ダイナミックWEPメカニズムの設定
（オプション設定項目）SNMP notificationの有効化

🕮 **メモ：**

- WEP 鍵が設定されている場合、ダイナミック WEP メカニズムはマルチキャスト WEP 鍵、ブロードキャスト WEP 鍵として設定された WEP 鍵を使用します。ネゴシエートされたユニキャスト WEP の ID は 4 で、暗号化方式長の設定を使用します。
- WEP 鍵が設定されていない場合、マルチキャスト、ブロードキャストの両方のダイナミック WEP 鍵の長さは 104 ビットです。ネゴシエートされたユニキャスト WEP の ID は 4 です。作成されたマルチキャスト WEP 鍵、ブロードキャスト WEP 鍵の ID は 1 です。

5.7.1 AKM モードの設定

以下の各 AKM モードは特定の認証モードを使用します。

- **802.1X AKM**–802.1X 認証モード
- **PSK AKM**–MAC アドレスあるいは認証バイパスモード
- **WiFi alliance anonymous 802.1X AKM**–802.1X 認証モード

以下に AKM モードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. security IE を設定する	**akm mode** { **dot1x** | **psk** | **anonymous-dot1x** }	デフォルト：設定なし

5.7.2 暗号化規格の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. security IE を設定する	**security-ie** { **osen** | **rsn** | **wpa** }	デフォルト：設定なし

🕮 **メモ：**

暗号化規格に WPA2 または WPA3 を使用する場合は RSN、WPA を使用する場合は WPA を設定します。

5.7.3 暗号化方式の設定

🕮 **メモ：**

- QX-W1000 シリーズの AP はソフトウェアバージョン 7.2.19 を含む以降のソフトウェアから **gcmp** パラメータをサポートしています。
- QX-W1100 シリーズの AP はソフトウェアバージョン 7.2.55 を含む以降のソフトウェアから、**gcmp** パラメータをサポートしています。
- QX-W1120 の Radio3 は、**gcmp** パラメータをサポートしていません。
- QX-W1130 の Radio1 は、**gcmp** パラメータをサポートしていません。

⚠ **重要：**

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

暗号化方式には以下があります。

- WEP (WEP40、WEP104、WEP128)
- CCMP
- GCMP
- TKIP

以下に暗号化方式の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. 暗号化方式を設定する	**cipher-suite** { **ccmp** | **gcmp** | **tkip** | **wep40** | **wep104** | **wep128** }	デフォルト：設定なし WEP128とCCMPの両方を設定することはできません。 WEP128とTKIPの両方を設定することはできません。 WEP128とGCMPの両方を設定することはできません。

🕮 **メモ：**

暗号化方式に AES を使用する場合は CCMP を設定します。

5.7.4 PSK の設定

AKM モードが PSK の場合、PSK を設定する必要があります。AKM モードが 802.1X で、PSK を設定した場合、WLAN サービステンプレートを有効にすることができますが PSK の設定は適用されません。

以下に PSK の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3． PSK を設定する	**preshared-key** { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *key*	デフォルト：設定なし

5.7.5 KDF の設定

KDF は PTK と GTK を作成するため RSNA ネットワークで使用します。KDF には HMAC-SHA1、HMAC-SHA256 が含まれます。HMAC-SHA256 アルゴリズムは HMAC-SHA1 よりもセキュリティの強度が強くなります。

以下に KDF の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3． KDF を設定する	**key-derivation** { **sha1** | **sha256** | **sha1-and-sha256** }	デフォルト：HMAC-SHA1

5.7.6 GTK アップデートの設定

AKM、暗号化規格、暗号化方式が設定されている場合、鍵交換を行っている間、システムは GTK を作成します。鍵のセキュリティを拡張するため、以下のアップデートモードにもとづいて GTK をアップデートします。

- **Time-based**–指定した間隔で GTK がアップデートされます。
- **Packet-based**–指定したパケット数が送信された後、GTK がアップデートされます。
- **Offline-triggered**–BSS（basic service set）のクライアントがオフラインになったとき、GTK がアップデートされます。

以下に GTK アップデートの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3． GTK のアップデートを有効にする	**gtk-rekey enable**	デフォルト：デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.56を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。 ソフトウェアバージョン 7.2.58を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。

操作	コマンド	補足
4.　（オプション設定項目）GTK アップデートのモードを設定する	**gtk-rekey method** { **packet-based** [*packet*] | **time-based** [*time*] }	デフォルト：GTKは86400秒ごとにアップデートされます。 **packet-based**モードのデフォルトのパケット数は10000000です。
5.　（オプション設定項目）Offline-triggered モードの GTK アップデートを有効にする	**gtk-rekey client-offline enable**	デフォルト：無効

5.7.7 PTK アップデートの設定

AKM、暗号化規格、暗号化方式が設定されている場合、鍵交換を行っている間、システムは PTK を作成します。PTK ライフタイムが終了したのち、PTK をアップデートします。

以下に PTK アップデートの設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3.　PTK rekey を有効にする	**ptk-rekey enable**	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.56を含む以前のソフトウェアでは有効(コンフィグ上は非表示)です。 ソフトウェアバージョン 7.2.58を含む以降のソフトウェアでは無効(コンフィグ上は非表示)です。
4.　PTK ライフタイムを設定する	**ptk-lifetime** *time*	デフォルト：43200秒

5.7.8 TKIP MIC failure ホールドタイムの設定

TKIP を設定したのち、TKIP MIC failure ホールドタイムを設定することができます。AP は MIC failure ホールドタイム以内に 2 つの MIC の失敗が検出された場合、60 秒の間、すべてのクライアントとのアソシエーションを解除します。

以下に TKIP MIC failure ホールドタイムの設定を示します。

操作	コマンド	補足
1.　system view に移行する	**system-view**	―
2.　WLAN service template view に移行する	**wlan service-template** *service-template-name*	―

操作	コマンド	補足
3． TKIP MIC failure ホールドタイムを設定する	**tkip-cm-time** *time*	デフォルト：0 APは対応しません。

5.7.9 WEP 鍵の設定

⚠ **重要**：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

WEP 鍵は、Pre-RSNA ネットワークのすべてのパケットおよび RSNA ネットワークのマルチキャストパケットを暗号化するために使用します。WEP 鍵が設定されていない場合、以下の対応となります。

- **Pre-RSNA ネットワークのパケット**：暗号化されません。
- **RSNA ネットワークのマルチキャストパケット**：暗号化するために交換された GTK を使用します。

以下に WEP 鍵の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3． WEP 鍵を設定する	**wep key** *key-id* { **wep40** | **wep104** | **wep128** } { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *key*	デフォルト：設定なし
4． （オプション設定項目）WEP 鍵を適用する	**wep key-id** { **1** | **2** | **3** | **4** }	デフォルト：1 ダイナミックWEPメカニズムが有効の場合、WEP鍵**4**を適用しないでください。

5.7.10 管理フレーム保護の設定

🕮 **メモ**：

192bit セキュリティなしの WPA3 エンタープライズは WPA2+管理フレーム保護(**pmf**)と同じです。管理フレーム保護を必須(**Mandatory**)として設定をすることで、192bit セキュリティなしの WPA3 エンタープライズと同等の動作をします。
管理フレーム保護を設定する場合は、KDF の設定”key-derivation sha1-and-sha256”をしてください。

管理フレーム保護は、RSNA メカニズムを使用するネットワークでのみ適用されます。管理フレーム保護は暗号化規格に RSN、暗号化方式に CCMP を設定します。

管理フレーム保護が無効の場合、ネットワークはすべてのクライアントで有効となりますが、管理フレーム保護は実行されません。管理フレーム保護が有効な場合、ネットワークアクセスおよび管理フレーム保護の有効性は管理フレーム保護のモードによって変わります。

- **Optional モード**–すべてのクライアントはネットワークへのアクセスが有効です。管理フレーム保護は、管理フレーム保護がサポートされているクライアントでのみ実行されます。
- **Mandatory モード**–ネットワークアクセスと管理フレーム保護は管理フレーム保護がサポートされているクライアントでのみ実行されます。

以下に管理フレーム保護の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. 管理フレーム保護を有効にする	**pmf** { **optional** | **mandatory** }	デフォルト：無効
4. (オプション設定項目) KDF を設定する	**key-derivation { sha1 | sha256 | sha1-and-sha256 }**	デフォルト：HMAC-SHA1
5. SA クエリリクエストの送信間隔を設定する	**pmf saquery retrytimeout** *timeout*	デフォルト：200 ミリ秒
6. SA クエリリクエストの最大試行回数を設定する	**pmf saquery retrycount** *count*	デフォルト：4
7. アソシエーション復帰時間を設定する	**pmf association-comeback** *time*	デフォルト：1秒

5.7.11 ダイナミック WEP メカニズムの有効化

⚠ **重要**：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

ダイナミック WEP メカニズムは 802.1X 認証モードを使用する必要があります。

以下にダイナミック WEP メカニズムを有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. ダイナミック WEP メカニズムを有効にする	**wep mode dynamic**	デフォルト：無効

5.7.12 WPA3 の設定

🕮 **メモ：**

- **wpa3** コマンドはソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。
- QX-W1100 シリーズの AP はソフトウェアバージョン 7.2.55 を含む以降のソフトウェアから WPA3 エンタープライズの 192bit セキュリティモードをサポートしています。
- QX-W1120 の Radio3 は、WPA3 エンタープライズの 192bit セキュリティをサポートしていません。
- QX-W1130 の Radio1 は、WPA3 エンタープライズの 192bit セキュリティをサポートしていません。
- WPA3 エンタープライズの 192bit セキュリティなしモードについては、管理フレーム保護の設定を参照して下さい。
- **enterprise-only-mode** のパラメータはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。
- **enterprise-transition-mode** のパラメータはソフトウェアバージョン 7.2.73 を含む以降のソフトウェアからサポートしています。
- wpa3 **enterprise-only-mode** と **wpa3 enterprise-transition-mode** を設定する場合、事前に **pmf** コマンドと **key-derivation** コマンドがサービステンプレートに設定されていないことを確認してください。

- WPA3 エンタープライズの 192bit セキュリティモードー**wpa3 enterprise** コマンドで有効にします。暗号化規格を RSN に設定し、暗号化方式を GCMP に設定する必要があります。
- WPA3 エンタープライズの 192bit セキュリティなしモードー**wpa3 enterprise-only-mode**、**wpa3 enterprise-transition-mode**、または **pmf** コマンドで有効にします。暗号化規格を RSN に設定し、暗号化方式を CCMP に設定する必要があります。管理フレーム保護の設定を参照して下さい。
- WPA3 パーソナル **wpa3 personal** コマンドで有効にします。暗号化規格を RSN に設定し、暗号化方式を CCMP に設定する必要があります。
- **mandatory**: WPA3 パーソナルで、WPA3 セキュリティモードを必須モードに指定します。WPA3 セキュリティモードをサポートしていないクライアントはアクセスできません。
- **optional**: WPA3 パーソナルで、WPA3 セキュリティモードをオプションモードに指定します。WPA3 セキュリティモードをサポートしているクライアントとサポートしていないクライアントのどちらもアクセスできます。

以下に WPA3 を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. WPA3 エンタープライズの 192bit セキュリティモード、または WPA3 パーソナルモードを有効にする	**wpa3** { **enterprise** | **enterprise-only-mode** | **enterprise-transition-mode** | **personal** { **mandatory** | **optional** } }	デフォルト：無効

5.7.13 Enhanced Open システム認証の設定

🕮 **メモ：**

enhanced-open enable コマンドはソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。

I. Enhanced Open システム認証について

Enhanced Open システム認証は、Opportunistic Wireless Encryption(OWE)を使用して、OWE 対応クライアントのデータパケットを暗号化するためのキーをネゴシエーションし、セキュリティパフォーマンスが強化されたオープンシステム認証を提供します。

II. 制限とガイドライン

この機能を有効にする前に、WPA 3 セキュリティモード、FT、管理フレーム保護、暗号化規格、暗号化方式、および KDF がデフォルト設定になっていることを確認してください。

この機能を有効にすると、次の操作が実行されます。

- 暗号化規格を RSN として指定します。
- CCMP として暗号化方式を指定します。
- 管理フレーム保護を有効にします。
- HMAC-SHA 1 および HMAC-SHA 256 アルゴリズムを KDF として指定します。

III. 設定手順

以下に Enhanced Open システム認証を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. Enhanced Open システム認証を有効にする	**enhanced-open enable**	デフォルト：無効

5.7.14 移行モードでの推奨サービステンプレートの指定

🕮 **メモ：**

コマンドはソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。

I. 移行モードでの推奨サービステンプレートについて

オープン WLAN から Enhanced Open WLAN への移行時には、OWE 非対応および OWE 対応のクライアントに対応するために、両方のタイプの WLAN が存在する可能性があり

ます。この場合、OWE 対応クライアントがオープン WLAN にアクセスしようとした場合、または OWE 非対応クライアントが拡張オープン WLAN にアクセスしようとした場合、対応する AP はアクセス要求を拒否します。

この機能により、クライアントは適合する適切な WLAN に高速アクセスできます。

II. 制限とガイドライン

オープンサービステンプレートと Enhanced Open サービステンプレートの両方でこの機能を設定し、これらを相互の推奨テンプレートとして指定します。

サービステンプレートとその推奨サービステンプレートを同じ無線に設定します。

Enhanced Open サービステンプレートの SSID 非表示を有効にします。

III. 設定手順

以下に Enhanced Open システム認証を有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	―
3. 移行モードでの推奨サービステンプレートを設定する	**enhanced-open transition-mode service-template** *service-template-name*	デフォルト：設定なし このコマンドを複数回実行した場合、最後の設定が反映されます。

5.7.15 WLAN セキュリティの SNMP notification の有効化

SNMP notification を有効にすることで、WLAN セキュリティに関する重要なイベントを NMS に通知します。NMS は設定された出力ルールにしたがって notification を出力する方法を決定します。

SNMP notification についての詳細は、QX-W1000/W1100 シリーズ アクセスポイントオペレーションマニュアルのセクション 11 *システム管理 “SNMP”* を参照してください。

以下に WLAN セキュリティに関する SNMP notification の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WLAN セキュリティに関する SNMP notification を有効にする	**snmp-agent trap enable wlan usersec**	デフォルト：無効

5.7.16 WPA3-SAE の SAE 交換時の PWE 生成方式の設定

🕮 **メモ：**

- **akm sae pwe** コマンドはソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。
- **both-h2e-hnp** を指定すると **hnp** のみをサポートしたクライアントでローミングに失敗する場合があります。クライアントの問題ですが、ローミング失敗を避けるために”**akm sae pwe hnp**”を設定してください。

WPA3-SAE は、Hunting-and-Pecking (HnP) と Hash-to-Element (H2E) を使用した PWE の生成をサポートしています。H2E は最新の PWE 生成方法であり、強化されたセキュリティパフォーマンスを提供します。

クライアントが指定された PWE 生成方式をサポートしていない場合、クライアントは WLAN にアクセスできません。クライアントの互換性を向上させる場合は、both-h2e-hnp キーワードを指定します。

以下に WPA-SAE の SAE 交換時の PWE 生成方式の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. WLAN service template view に移行する	**wlan service-template** *service-template-name*	—
3. WPA3-SAE の SAE 交換時の PWE 生成方式を設定する	**akm sae pwe { both-h2e-hnp | h2e | hnp }**	デフォルト：both-h2e-hnp

5.8 WLANセキュリティの表示と維持

すべての view で display コマンドを実行できます。

操作	コマンド
WLANサービステンプレート情報を表示する	**display wlan service-template** [*service-template-name*] [VLAN]
クライアント情報を表示する	**display wlan client** [**ap** *ap-name* [**radio** *radio-id*] | **mac-address** *mac-address* | **service-template** *service-template-name*] [**verbose**]

詳細は QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC コマンドマニュアルの *“WLAN アクセス”* を参照してください。

5.9 WLANセキュリティの設定例

5.9.1 共有鍵認証設定例

I. ネットワーク要件

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

図 5-9 に示すように Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。クライアントが WEP 鍵 12345 を使用してネットワークにアクセスできるように、共有鍵認証を設定します。

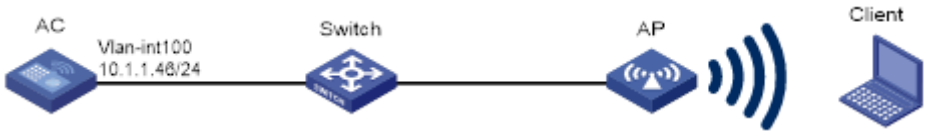


図 5-9 ネットワーク図

II. 設定手順

WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

サービステンプレート service1 の暗号化方式を WEP40 に設定します。プレーンテキストで共有鍵を 12345 に指定します。鍵を ID 1 に割り当てます。

```
[AC-wlan-st-service1] cipher-suite wep40
[AC-wlan-st-service1] wep key 1 wep40 pass-phrase simple 12345
[AC-wlan-st-service1] wep key-id 1
```

サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
```

```
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : service1
 Description                  : Not configured
 SSID                         : service
 SSID-hide                    : Disabled
 User-isolation               : Disabled
 Service template status      : Enabled
 Maximum clients per BSS      : Not configured
 Frame format                 : Dot3
 Seamless roam status         : Disabled
 Seamless roam RSSI threshold : 50
 Seamless roam RSSI gap       : 20
 VLAN ID                      : 1
 AKM mode                     : Not configured
 Security IE                  : Not configured
 Cipher suite                 : WEP40
 TKIP countermeasure time     : 0 sec
 PTK lifetime                 : 43200 sec
 PTK rekey                    : Enabled
 GTK rekey                    : Enabled
 GTK rekey method             : Time-based
 GTK rekey time               : 86400 sec
 GTK rekey client-offline     : Disabled
 User authentication mode     : Bypass
 Intrusion protection         : Disabled
 Intrusion protection mode    : Temporary-block
 Temporary block time         : 180 sec
 Temporary service stop time  : 20 sec
 Fail VLAN ID                 : Not configured
 802.1X handshake             : Disabled
 802.1X handshake secure      : Disabled
 802.1X domain                : Not configured
 MAC-auth domain              : Not configured
 Max 802.1X users per BSS     : 512
 Max MAC-auth users per BSS   : 512
 802.1X re-authenticate       : Disabled
 Authorization fail mode      : Online
 Accounting fail mode         : Online
 Authorization                : Permitted
 Key derivation               : SHA1
 PMF status                   : Disabled
 Hotspot policy number        : Not configured
 Forwarding policy status     : Disabled
 Forwarding policy name       : Not configured
 Forwarder                    : AP
 FT status                    : Disabled
 QoS trust                    : Port
 QoS priority                 : 0
```

5.9.2 WPA-PSK(TKIP)設定例

I. ネットワーク要件

図 5-10 に示すように Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- WPA-PSK(TKIP)を設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

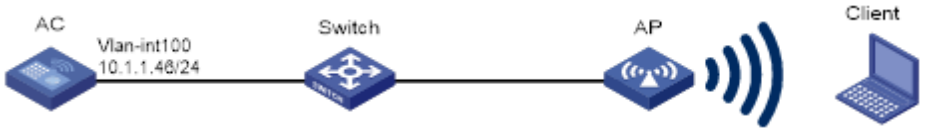


図 5-10 ネットワーク図

II. 設定手順

1)　サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

2)　サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

3)　サービステンプレート service1 の WLAN セキュリティを設定します。

#AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

WPA(TKIP)のために、暗号化規格に WPA、暗号化方式に TKIP を指定します。

```
[AC-wlan-st-service1] cipher-suite tkip
[AC-wlan-st-service1] security-ie wpa
```

4)　サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

5)　AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

6)　サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
```

```
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : service1
 Description                  : Not configured
 SSID                         : service
 SSID-hide                    : Disabled
 User-isolation               : Disabled
 Service template status      : Enabled
 Maximum clients per BSS      : Not configured
 Frame format                 : Dot3
 Seamless roam status         : Disabled
 Seamless roam RSSI threshold : 50
 Seamless roam RSSI gap       : 20
 VLAN ID                      : 1
 AKM mode                     : PSK
 Security IE                  : WPA
 Cipher suite                 : TKIP
 TKIP countermeasure time     : 0 sec
 PTK lifetime                 : 43200 sec
 PTK rekey                    : Enabled
 GTK rekey                    : Enabled
 GTK rekey method             : Time-based
 GTK rekey time               : 86400 sec
 GTK rekey client-offline     : Disabled
 User authentication mode     : Bypass
 Intrusion protection         : Disabled
 Intrusion protection mode    : Temporary-block
 Temporary block time         : 180 sec
 Temporary service stop time  : 20 sec
 Fail VLAN ID                 : Not configured
 802.1X handshake             : Disabled
 802.1X handshake secure      : Disabled
 802.1X domain                : Not configured
 MAC-auth domain              : Not configured
 Max 802.1X users per BSS     : 512
 Max MAC-auth users per BSS   : 512
 802.1X re-authenticate       : Disabled
 Authorization fail mode      : Online
 Accounting fail mode         : Online
 Authorization                : Permitted
 Key derivation               : SHA1
 PMF status                   : Disabled
 Hotspot policy number        : Not configured
 Forwarding policy status     : Disabled
 Forwarding policy name       : Not configured
 Forwarder                    : AP
 FT status                    : Disabled
 QoS trust                    : Port
 QoS priority                 : 0
```

5.9.3 WPA2-PSK(AES)＋MAC アドレス認証設定例

I. ネットワーク要件

図 5-11 に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名 abc、パスワード 123 を使用して、クライアントがネットワークにアクセスできるように WPA2-PSK(AES)と MAC アドレス認証を設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

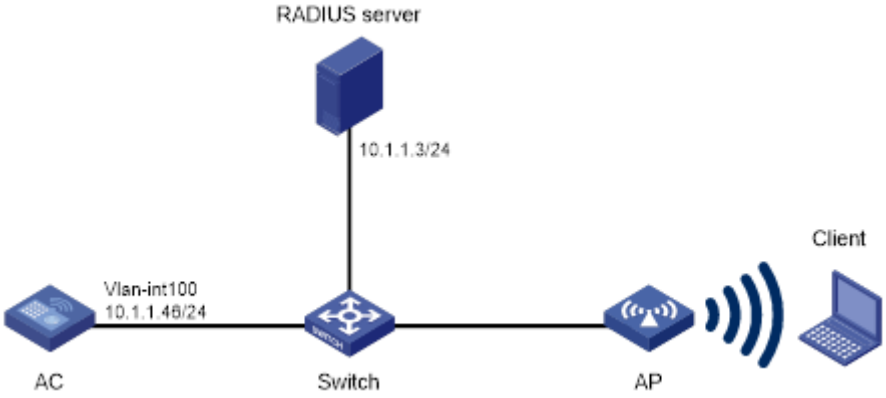


図 5-11 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abc、パスワード 123 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) WLAN サービステンプレート service1 を作成します。サービステンプレートの SSID サービスを指定します。

```
<AC> system-view
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid service
```

3) サービステンプレート service1 の WLAN セキュリティを設定します。

#AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

WPA2(AES)のために、暗号化規格に RSN、暗号化方式に CCMP を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

MAC アドレス認証を設定します。

```
[AC-wlan-st-service1] client-security authentication-mode mac
```

4) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

5)　RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345678 を設定します。

```
[AC-radius-radius1] key authentication simple 12345678
[AC-radius-radius1] key accounting simple 12345678
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

6)　ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

7)　ISP ドメイン dom1 を設定し、ユーザ名 abc、パスワード 123 を指定します。

```
[AC] mac-authentication domain dom1
[AC] mac-authentication user-name-format fixed account abc password simple 123
```

8)　AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

9)　サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

🕮 メモ：

AAA、RADIUS コマンドの詳細は QX-W1000/W1100 シリーズ アクセスポイントコマンドマニュアルのセクション 9 *セキュリティ "AAA"* を参照してください。

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : service1
 Description                  : Not configured
 SSID                         : service
 SSID-hide                    : Disabled
 User-isolation               : Disabled
 Service template status      : Enabled
 Maximum clients per BSS      : Not configured
 Frame format                 : Dot3
 Seamless roam status         : Disabled
 Seamless roam RSSI threshold : 50
 Seamless roam RSSI gap       : 20
 VLAN ID                      : 1
 AKM mode                     : PSK
 Security IE                  : RSN
 Cipher suite                 : CCMP
 TKIP countermeasure time     : 0 sec
 PTK lifetime                 : 43200 sec
 PTK rekey                    : Enabled
 GTK rekey                    : Enabled
 GTK rekey method             : Time-based
 GTK rekey time               : 86400 sec
 GTK rekey client-offline     : Disabled
 User authentication mode     : MAC
 Intrusion protection         : Disabled
 Intrusion protection mode    : Temporary-block
 Temporary block time         : 180 sec
 Temporary service stop time  : 20 sec
 Fail VLAN ID                 : Not configured
 802.1X handshake             : Disabled
 802.1X handshake secure      : Disabled
 802.1X domain                : Not configured
 MAC-auth domain              : Not configured
 Max 802.1X users per BSS     : 512
 Max MAC-auth users per BSS   : 512
 802.1X re-authenticate       : Disabled
 Authorization fail mode      : Online
 Accounting fail mode         : Online
 Authorization                : Permitted
 Key derivation               : SHA1
 PMF status                   : Disabled
 Hotspot policy number        : Not configured
 Forwarding policy status     : Disabled
 Forwarding policy name       : Not configured
 Forwarder                    : AP
 FT status                    : Disabled
 QoS trust                    : Port
 QoS priority                 : 0
```

5.9.4 802.1X AKM 設定例

I. ネットワーク要件

図 5-12 に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名 abcdef、パスワード 123456 を使用して、クライアントがネットワークにアクセスできるように 802.1X 認証を設定します。
- AKM モードとして 802.1X を設定します。

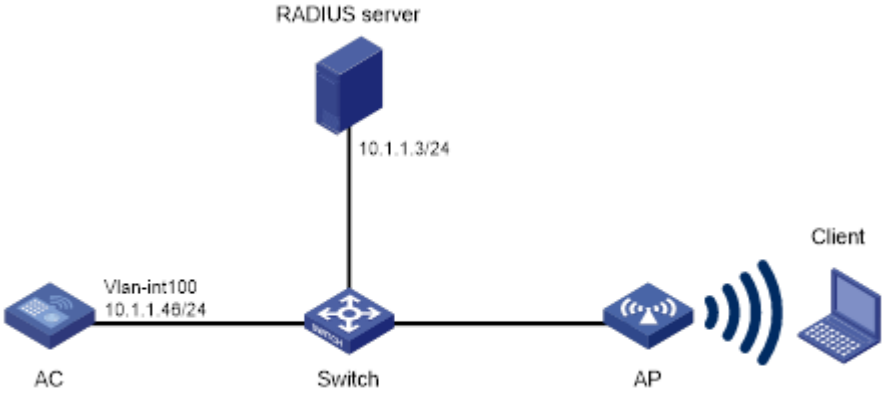


図 5-12 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abcdef、パスワード 123456 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) 802.1X クライアントを設定します。（詳細は省略します。）
3) WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

4) サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

5) サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

暗号化方式に CCMP、暗号化規格に WPA を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie wpa
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1] dot1x domain dom1
```

6)　サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

7)　RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

8)　ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

9)　AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

10)　サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

🕮 **メモ：**

AAA、RADIUS コマンドの詳細は QX-W1000/W1100 シリーズ アクセスポイントコマンドマニュアルのセクション 9 *セキュリティ "AAA"* を参照してください。

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : 1
 Description                  : Not configured
 SSID                         : service
 SSID-hide                    : Disabled
 User-isolation               : Disabled
 Service template status      : Enabled
 Maximum clients per BSS      : Not configured
 Frame format                 : Dot3
 Seamless roam status         : Disabled
 Seamless roam RSSI threshold : 50
 Seamless roam RSSI gap       : 20
 VLAN ID                      : 1
 AKM mode                     : 802.1X
 Security IE                  : WPA
 Cipher suite                 : CCMP
 TKIP countermeasure time     : 0 sec
 PTK lifetime                 : 43200 sec
 PTK rekey                    : Enabled
 GTK rekey                    : Enabled
 GTK rekey method             : Time-based
 GTK rekey time               : 86400 sec
 GTK rekey client-offline     : Disabled
 WPA3 status                  : Disabled
 User authentication mode     : 802.1X
 Intrusion protection         : Disabled
 Intrusion protection mode    : Temporary-block
 Temporary block time         : 180 sec
 Temporary service stop time  : 20 sec
 Fail VLAN ID                 : Not configured
 802.1X handshake             : Disabled
 802.1X handshake secure      : Disabled
 802.1X domain                : Not configured
 MAC-auth domain              : Not configured
 Max 802.1X users per BSS     : 512
 Max MAC-auth users per BSS   : 512
 802.1X re-authenticate       : Disabled
 Authorization fail mode      : Online
 Accounting fail mode         : Online
 Authorization                : Permitted
 Key derivation               : SHA1
 PMF status                   : Disabled
 Hotspot policy number        : Not configured
 Forwarding policy status     : Disabled
 Forwarding policy name       : Not configured
 Forwarder                    : AP
 FT status                    : Disabled
 QoS trust                    : Port
 QoS priority                 : 0
```

5.9.5 管理フレーム保護設定例

I. ネットワーク要件

図 5-13 に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- クライアントがネットワークにアクセスできるように PSK の鍵 12345678 を設定します。
- 暗号化規格に RSN、暗号化方式に CCMP を使用し、管理フレーム保護を設定します。

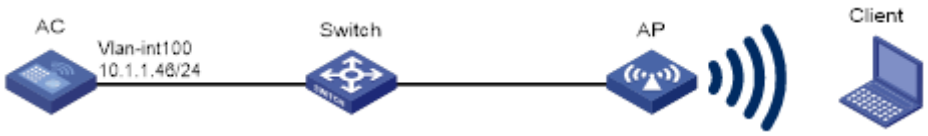


図 5-13 ネットワーク図

II. 設定手順

1)　WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

2)　サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

3)　管理フレーム保護を設定します。

optional モードで管理フレーム保護を有効にします。

```
[AC-wlan-st-service1] pmf optional
```

KDF を sha1-and-sha256 に設定します。

```
[AC-wlan-st-service1] key-derivation sha1-and-sha256
```

4)　RSNA メカニズムを設定します。

AKM モードとして PSK を設定し、プレーンテキストで鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

暗号化方式に CCMP、暗号化規格に RSN を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

5)　サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

6)　AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

7) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name         : service1
 Description                  : Not configured
 SSID                         : service
 SSID-hide                    : Disabled
 User-isolation               : Disabled
 Service template status      : Enabled
 Maximum clients per BSS      : Not configured
 Frame format                 : Dot3
 Seamless roam status         : Disabled
 Seamless roam RSSI threshold : 50
 Seamless roam RSSI gap       : 20
 VLAN ID                      : 1
 AKM mode                     : PSK
 Security IE                  : RSN
 Cipher suite                 : CCMP
 TKIP countermeasure time     : 0 sec
 PTK lifetime                 : 43200 sec
 PTK rekey                    : Enabled
 GTK rekey                    : Enabled
 GTK rekey method             : Time-based
 GTK rekey time               : 86400 sec
 GTK rekey client-offline     : Disabled
 User authentication mode     : Bypass
 Intrusion protection         : Disabled
 Intrusion protection mode    : Temporary-block
 Temporary block time         : 180 sec
 Temporary service stop time  : 20 sec
 Fail VLAN ID                 : Not configured
 802.1X handshake             : Disabled
 802.1X handshake secure      : Disabled
 802.1X domain                : Not configured
 MAC-auth domain              : Not configured
 Max 802.1X users per BSS     : 512
 Max MAC-auth users per BSS   : 512
 802.1X re-authenticate       : Disabled
 Authorization fail mode      : Online
 Accounting fail mode         : Online
 Authorization                : Permitted
 Key derivation               : SHA1
 PMF status                   : Optional
 Hotspot policy number        : Not configured
 Forwarding policy status     : Disabled
 Forwarding policy name       : Not configured
 Forwarder                    : AP
 FT status                    : Disabled
 QoS trust                    : Port
 QoS priority                 : 0
```

802.11w クライアントがオンラインになったのち、管理フレーム保護の交換結果を確認するため、**display wlan client verbose** コマンドを使用します。

```
<AC> display wlan client verbose
Total number of clients: 1

 MAC address                          : fcf8-ae88-2273
 IPv4 address                         : 10.1.1.6
 IPv6 address                         : N/A
 Username                             : N/A
 AID                                  : 978
 AP ID                                : 1
 AP name                              : 1030_c180
 Radio ID                             : 1
 SSID                                 : kenken_sha1
 BSSID                                : 74ea-c8fd-c180
 VLAN ID                              : 1
 Sleep count                          : 1
 Wireless mode                        : 802.11an
 Channel bandwidth                    : 40MHz
 20/40 BSS Coexistence Management     : Not supported
 SM power save                        : Disabled
 Short GI for 20MHz                   : Supported
 Short GI for 40MHz                   : Supported
 STBC RX capability                   : Supported
 STBC TX capability                   : Not supported
 LDPC RX capability                   : Not supported
 Block Ack                            : TID 0  In
 Supported HT MCS set                 : 0, 1, 2, 3, 4, 5, 6, 7,
                                        8, 9, 10, 11, 12, 13, 14,
                                        15
 Supported rates                      : 6, 9, 12, 18, 24, 36,
                                        48, 54 Mbps
 QoS mode                             : WMM
 Listen interval                      : 250
 RSSI                                 : 29
 Rx/Tx rate                           : 300/6 Mbps
 Authentication method                : Open system
 Security mode                        : RSN
 AKM mode                             : PSK
 Cipher suite                         : CCMP
 User authentication mode             : Bypass
 Authorization ACL ID                 : N/A
 Authorization user profile           : N/A
 Authorization CAR                    : N/A
 Roam status                          : N/A
 Key derivation                       : SHA1
 PMF status                           : Disabled
 Forwarding policy name               : Not configured
 Online time                          : 0days 0hours 0minutes 17seconds
 FT status                            : Inactive
```

5.9.6 ダイナミック WEP メカニズム設定例

I. ネットワーク要件

重要：

WEP は設定した暗号化キーが固定であり、解読される危険性があるため、よりセキュリティ強度の高い AES の利用を推奨します。

図 5-14 に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名 abcdef、パスワード 123456 を使用して、クライアントがネットワークにアクセスできるように 802.1X 認証を設定します。
- ダイナミック WEP メカニズムを設定します。

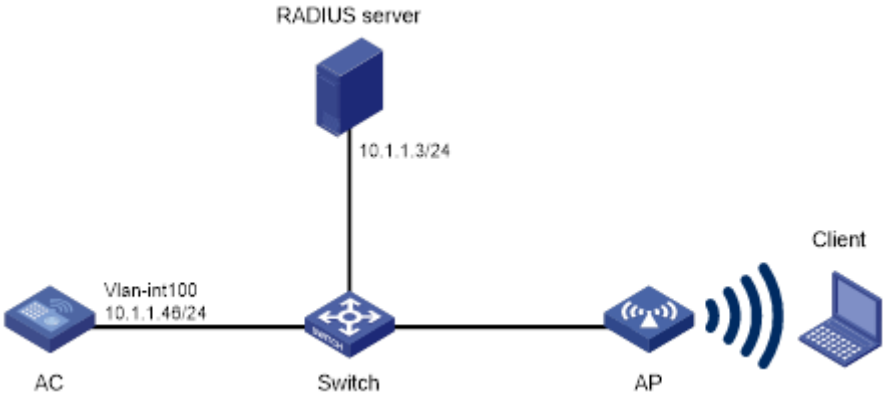


図 5-14 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abcdef、パスワード 123456 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) 802.1X クライアントを設定します。（詳細は省略します。）
3) WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

4) サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

5) ダイナミック WEP メカニズムを有効にします。

```
[AC-wlan-st-service1] wep mode dynamic
```

6) 802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

7) 802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1] dot1x domain dom1
```

8) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

9) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
```

```
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

#RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

10) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

11) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

12) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

🕮 メモ：

AAA、RADIUS コマンドの詳細は QX-W1000/W1100 シリーズ アクセスポイントコマンドマニュアルのセクション 9 *セキュリティ “AAA”* を参照してください。

III. 設定の確認

WLAN サービステンプレートが正常に設定されていることを確認するため、**display wlan service-template** コマンドを使用します。

```
<AC> display wlan service-template service1 verbose
Service template name          : service1
```

```
Description                  : Not configured
SSID                         : service
SSID-hide                    : Disabled
User-isolation               : Disabled
Service template status      : Enabled
Maximum clients per BSS      : Not configured
Frame format                 : Dot3
Seamless roam status         : Disabled
Seamless roam RSSI threshold : 50
Seamless roam RSSI gap       : 20
VLAN ID                      : 1
AKM mode                     : Not configured
Security IE                  : Not configured
Cipher suite                 : WEP104
WEP key ID                   : 1
TKIP countermeasure time     : 0 sec
PTK lifetime                 : 43200 sec
PTK rekey                    : Enabled
GTK rekey                    : Enabled
GTK rekey method             : Time-based
GTK rekey time               : 86400 sec
GTK rekey client-offline     : Disabled
WPA3 status                  : Disabled
User authentication mode     : 802.1X
Intrusion protection         : Disabled
Intrusion protection mode    : Temporary-block
Temporary block time         : 180 sec
Temporary service stop time  : 20 sec
Fail VLAN ID                 : Not configured
802.1X handshake             : Disabled
802.1X handshake secure      : Disabled
802.1X domain                : Not configured
MAC-auth domain              : Not configured
Max 802.1X users per BSS     : 512
Max MAC-auth users per BSS   : 512
802.1X re-authenticate       : Disabled
Authorization fail mode      : Online
Accounting fail mode         : Online
Authorization                : Permitted
Key derivation               : SHA1
PMF status                   : Disabled
Hotspot policy number        : Not configured
Forwarding policy status     : Disabled
Forwarding policy name       : Not configured
Forwarder                    : AP
FT status                    : Disabled
QoS trust                    : Port
QoS priority                 : 0
```

5.9.7 WPA3 エンタープライズ(192bit セキュリティなし)設定例

I. ネットワーク要件

図 5-15 に示すように Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- WPA 3 エンタープライズを 192bit セキュリティなしで使用するために管理フレーム保護を設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

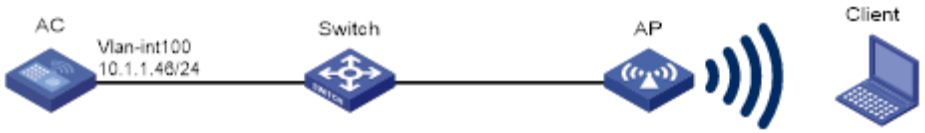


図 5-15 ネットワーク図

II. 設定手順

1)　サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

2)　サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid wpa3_test
```

3)　サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

暗号化方式に CCMP、暗号化規格に RSN を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

4)　管理フレーム保護(192bit セキュリティなし WPA3 エンタープライズ)を設定します。

```
[AC-wlan-st-service1] pmf mandatory
```

KDF を sha1-and-sha256 に設定します。

```
[AC-wlan-st-service1] key-derivation sha1-and-sha256
```

5)　サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

6)　RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

7) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

8) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

9) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

display wlan service-template verbose コマンドを使用します。

```
<AC>dis wlan service-template service1 verbose
 Service template name                              : service1
 Description                                        : Not configured
 SSID                                               : wpa3_test
 SSID-hide                                          : Disabled
 User-isolation                                     : Disabled
 Service template status                            : Enabled
 Maximum clients per BSS                            : Not configured
 VLAN ID                                            : 1
 Customer Vlan                                      : 4294967295
 AKM mode                                           : PSK
 Security IE                                        : RSN
 Cipher suite                                       : CCMP
 TKIP countermeasure time                           : 0 sec
 PTK lifetime                                       : 43200 sec
 PTK rekey                                          : Enabled
 GTK rekey                                          : Enabled
 GTK rekey method                                   : Time-based
```

```
GTK rekey time                                    : 86400 sec
GTK rekey client-offline                          : Disabled
WPA3 status                                       : Disabled
Enhance-open status                               : Disabled
Enhanced-open transition-mode service-template    : N/A
User authentication mode                          : Bypass
Intrusion protection                              : Disabled
Intrusion protection mode                         : Temporary-block
Temporary block time                              : 180 sec
Temporary service stop time                       : 20 sec
Fail VLAN ID                                      : Not configured
802.1X handshake                                  : Disabled
802.1X handshake secure                           : Disabled
802.1X domain                                     : Not configured
MAC-auth domain                                   : Not configured
Max 802.1X users per BSS                          : 512
Max MAC-auth users per BSS                        : 512
802.1X re-authenticate                            : Disabled
Authorization fail mode                           : Online
Accounting fail mode                              : Online
Authorization                                     : Permitted
Key derivation                                    : SHA1
PMF status                                        : Mandatory
Hotspot policy number                             : Not configured
Forwarding policy status                          : Disabled
Forwarding policy name                            : Not configured
Forwarder                                         : AP
FT status                                         : Disabled
QoS trust                                         : Port
QoS priority                                      : 0
```

5.9.8 WPA3 パーソナル設定例

I. ネットワーク要件

図 5-15 に示すように Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- WPA 3 パーソナルを設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

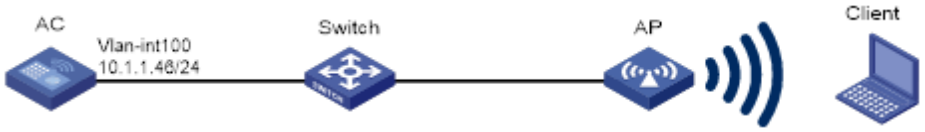


図 5-16 ネットワーク図

II. 設定手順

1)　サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

2)　サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid wpa3_test
```

3)　サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

暗号化方式に CCMP、暗号化規格に RSN を指定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

4) WPA3 の設定を personal に設定し、WPA3 セキュリティモードを optional に設定します。

```
[AC-wlan-st-service1] wpa3 personal optional
```

5) 管理フレーム保護を設定します。

optional モードで管理フレーム保護を有効にします。

```
[AC-wlan-st-service1] pmf optional
```

KDF を sha1-and-sha256 に設定します。

```
[AC-wlan-st-service1] key-derivation sha1-and-sha256
```

6) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

7) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

8) サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

クライアントが AP に接続されていることを確認するため、**display wlan client verbose** コマンドを使用します。

```
<AC> display wlan client verbose
Total number of clients: 1

 MAC address                     : 88e8-7fec-c042
 IPv4 address                    : 192.168.1.140
 IPv6 address                    : N/A
 Username                        : N/A
 AID                             : 1
 AP ID                           : 2
 AP name                         : test1
 Radio ID                        : 1
 SSID                            : wpa3_test
 BSSID                           : 9ce8-9525-f192
```

```
VLAN ID                          : 1
Sleep count                      : 0
Wireless mode                    : 802.11ac
Channel bandwidth                : 80MHz
SM power save                    : Disabled
Short GI for 20MHz               : Supported
Short GI for 40MHz               : Supported
Short GI for 80MHz               : Supported
Short GI for 160/80+80MHz        : Not supported
STBC RX capability               : Not supported
STBC TX capability               : Not supported
LDPC RX capability               : Supported
Beamformee STS capability        : 2
Number of Sounding Dimensions    : 1
SU beamformee capability         : Supported
MU beamformee capability         : Not supported
Block Ack                        : N/A
Supported VHT-MCS set            : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
                                   NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set             : 0, 1, 2, 3, 4, 5, 6, 7,
                                   8, 9, 10, 11, 12, 13, 14,
                                   15
Supported rates                  : 6, 9, 12, 18, 24, 36,
                                   48, 54 Mbps
QoS mode                         : WMM
Listen interval                  : 20
RSSI                             : 0
Rx/Tx rate                       : 0/0 Mbps
Speed                            : N/A
Authentication method            : Open system
Security mode                    : RSN
AKM mode                         : PSK
Cipher suite                     : CCMP
User authentication mode         : Bypass
WPA3 status                      : Enabled
Authorization CAR                : N/A
Authorization ACL ID             : N/A
Authorization user profile       : N/A
Roam status                      : N/A
Key derivation                   : SHA256
PMF status                       : Enabled
Forwarding policy name           : Not configured
Online time                      : 0days 0hours 0minutes 4seconds
FT status                        : Inactive
```

目次

6 章 WLAN 認証の概要 6-1
6.1 アプリケーションシナリオ 6-1
6.2 802.1X 認証 6-1
6.2.1 802.1X 認証のイニシエーション 6-2
6.2.2 802.1X 認証プロセス 6-2
6.3 MAC アドレス認証 6-5
6.3.1 ユーザアカウントポリシー 6-6
6.3.2 認証方式 6-6
6.3.3 OUI 認証 6-6
6.4 認証モード 6-7
6.5 侵入保護 6-7
6.6 WLAN の VLAN 操作 6-8
6.6.1 VLAN 認証 6-8
6.6.2 制限 VLAN 6-9
6.7 ほかの機能を用いた WLAN 認証 6-10
6.7.1 ACL の割り当て 6-10
6.7.2 ユーザプロファイルの割り当て 6-10

6章 WLAN 認証の概要

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

この章は WLAN 認証の実装について記載します。WLAN 認証はアクセスセキュリティを保証するため、WLAN クライアントを MAC アドレスベースでネットワークアクセスの制御を行います。

WLAN 認証は、802.1X 認証、MAC アドレス認証、OUI 認証があります。

6.1 アプリケーションシナリオ

認証装置は WLAN へのアクセスを制御するため、クライアントを認証します。図 6-1の AC を認証装置として使用します。

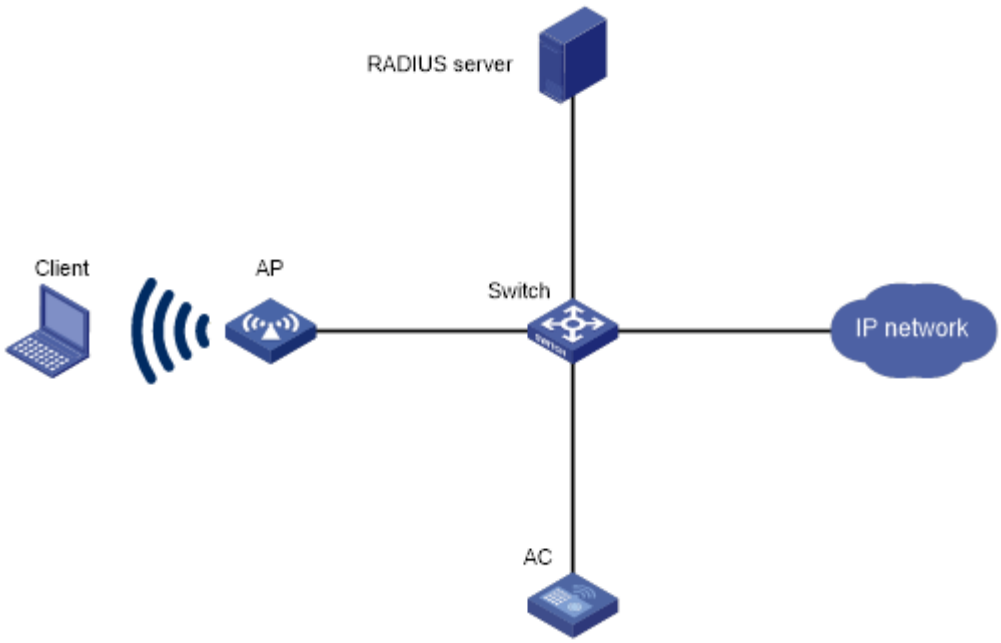


図 6-1 ネットワーク図

6.2 802.1X認証

802.1X はクライアント、認証装置、認証サーバの認証に関する情報を転送するために EAP（Extensible Authentication Protocol）を使用します。

802.1X は WLAN を超えてクライアントと認証装置間で EAP パケットを転送するため、EAPOL（EAP over LAN）を定義しています。認証装置と認証サーバ間で、802.1X は以下の方法の 1 つを使用して認証情報を送信します。

- EAP 中継モードで定義されているように、EAPOR（EAP over RADIUS）を使用して RADIUS の EAP パケットをカプセル化します。
- EAP 終端モードで定義されているように、EAP パケットから認証情報を抽出し、標準 RADIUS パケットの情報をカプセル化します。

EAP パケットのカプセル化の情報については QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 9 *セキュリティ “802.1X”* を参照してください。

6.2.1 802.1X 認証のイニシエーション

クライアントと認証装置は 802.1X 認証を開始することができます。

- **クライアントのイニシエーション**－クライアントが認証装置に関連付けられたのち、802.1X 認証を開始するため、クライアントは EAPOL-Start パケットを認証装置に送信します。
- **認証装置のイニシエーション**－クライアントが認証装置に関連付けられたのち、認証装置は認証を開始するため、EAP-Request/Identity パケットをクライアントに送信します。クライアントのタイムアウトタイマ以内に応答がない場合、認証装置はパケットを再送します。

6.2.2 802.1X 認証プロセス

認証装置は RADIUS サーバと通信するため、EAP 中継モードあるいは EAP 終端モードを使用します。

I. EAP 中継モード

このモードでは、認証装置は認証情報を RADIUS サーバに送信するため EAPOR パケットを使用します。RADIUS サーバは EAP-Message、Message-Authenticator 属性をサポートする必要があります。そして RADIUS サーバはクライアントと同一の認証方式を使用する必要があります。

EAP 中継モードは、認証装置で **dot1x authentication-method eap** コマンドを設定するだけで有効となります。

図 6-2に EAP 中継モードの基本的な 802.1X 認証のプロセスを示します。この例では EAP-MD5 が使用されています。

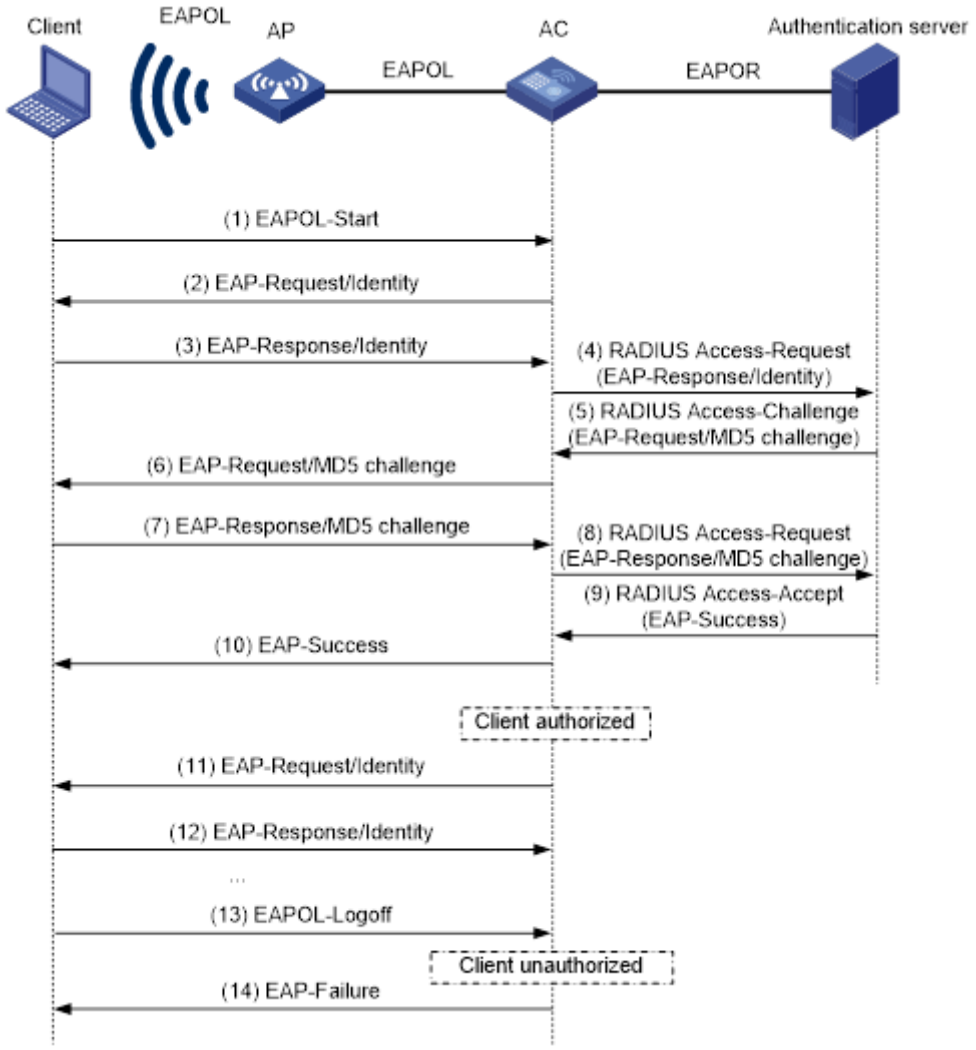


図 6-2 EAP 中継モードの 802.1X 認証プロセス

以下に 802.1X 認証プロセスを示します。

1) ユーザが 802.1X クライアントを実行し、登録されたユーザ名、パスワードを入力したとき、802.1X クライアントは EAPOL-Start パケットを認証装置に送信します。

   クライアントと AP アソシエーションの詳細は QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN セキュリティ"* 参照してください。

2) 認証装置はユーザ名を要求するため、EAP-Request/Identity パケットを送信します。
3) クライアントは EAP-Request/Identity パケットのユーザ名を認証装置に送信します。
4) 認証装置は RADIUS Access-Request パケット内の EAP-Response/Identity パケットを、認証サーバに転送します。
5) 認証サーバは認証サーバにあるユーザデータベースを検索するため、RADIUS Access-Request のユーザ名を使用します。一致するエントリが検出された場合、サーバは、エントリのパスワードを暗号化するため、ランダムに作成されたチャレンジ（EAP-Request/MD5-challenge）を使用します。そしてサーバは RADIUS Access-Challenge のチャレンジデータを認証装置に送信します。
6) 認証装置は EAP-Request/MD5-Challenge パケットをクライアントに転送します。

7) クライアントはパスワードを暗号化するため、受信したチャレンジデータを使用します。EAP-Response/MD5-Challenge パケットの暗号化されたパスワードを認証装置に送信します。
8) 認証装置は RADIUS Access-Request パケット内の EAP-Response/MD5-Challenge パケットを認証サーバに転送します。
9) 認証サーバは受信した暗号パスワードと 5）で作成した暗号パスワードを比較します。2 つのパスワードが等しい場合、認証サーバはクライアントが正式であることを認識し、認証装置に RADIUS Access-Accept packet パケットを送信します。
10) RADIUS Access-Accept packet パケットを受信すると、認証装置はクライアントにネットワークへのアクセスを許可します。
11) クライアントがオンラインになったのち、認証装置は定期的にクライアントがオンラインかどうかを確認するため、ハンドシェイクリクエストを送信します。
12) ハンドシェイクリクエストを受信すると、クライアントは応答を返します。ハンドシェイクの連続試行回数（デフォルトで 2 回です）に到達しても、クライアントが応答を返さなかった場合、認証装置はクライアントをログオフします。ハンドシェイクメカニズムはオフラインとなっている 802.1X クライアントを切断することによってネットワークリソースの浪費を防ぐことができます。
13) クライアントはログオフする場合、認証装置に EAPOL-Logoff パケットを送信します。
14) EAPOL-Logoff パケットを受信した場合、認証装置はクライアントに EAP-Failure パケットを送信します。

II. EAP 終端モード

このモードでは認証装置は以下の処理を行います。

1) クライアントから受信した EAP パケットを終端します。
2) 標準 RADIUS パケットのクライアント認証情報をカプセル化します。
3) RADIUS サーバと通信するため PAP あるいは CHAP を使用します。

図 6-3に EAP 終端モードの基本 802.1X 認証プロセスを示します。この例では CHAP 認証が使用されています。

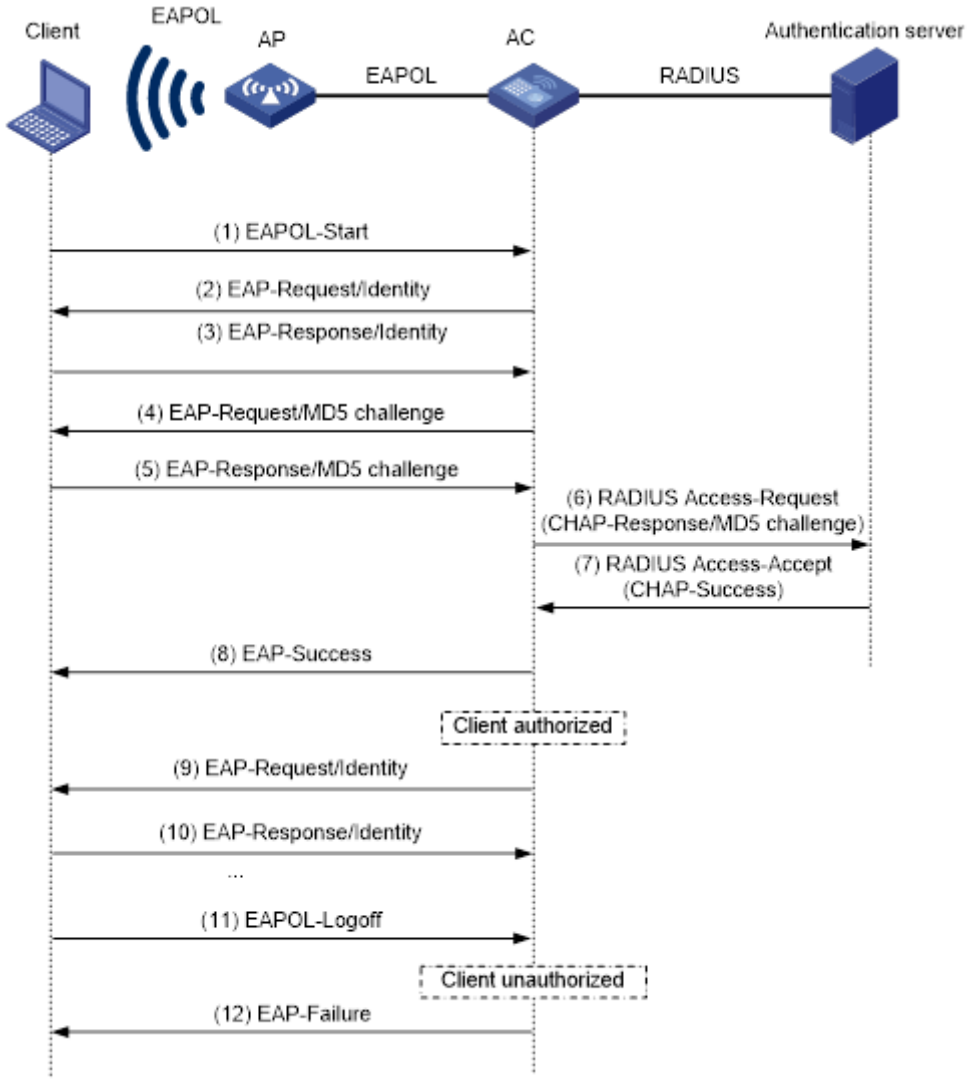


図 6-3 EAP 終端モードの 802.1X 認証プロセス

EAP 終端モードでは、パスワードの暗号化を行うため認証サーバではなく認証装置が MD5 チャレンジを作成します。そして認証装置は MD5 チャレンジに加えて、標準 RADIUS パケットのユーザ名と暗号化されたパスワードを RADIUS サーバに送信します。

6.3 MACアドレス認証

MAC アドレス認証は送信元 MAC アドレスを認証することでネットワークへのアクセスを制御します。この機能はクライアントソフトウェアを必要としません。ユーザは、ネットワークアクセス用のユーザ名とパスワードを入力する必要はありません。

未知の送信元 MAC アドレスが検出された場合、認証装置は、MAC アドレス認証プロセスを開始します。MAC アドレスが認証を通過した場合、クライアントは、許可されたネットワークリソースにアクセスすることができます。認証が失敗した場合、認証装置は、サ

イレント MAC アドレスとして MAC アドレスを記憶し、クライアントのアクセスを拒否します。

6.3.1 ユーザアカウントポリシー

ユーザアカウントはクライアントを識別するために必要です。MAC アドレス認証は、以下のユーザアカウントポリシーをサポートしています。

- **各ユーザのための MAC ベースのユーザアカウント**－認証装置は、MAC アドレス認証を行うため、クライアントのユーザ名、パスワードとしてパケットの未知の送信元 MAC アドレスを使用します。
- **すべてのユーザのための共有のユーザアカウント**－認証装置は、すべての MAC アドレス認証を行うため、クライアントのユーザ名とパスワードを指定します。ユーザ名とパスワードは MAC アドレスでなくても構いません。ユーザ名の設定範囲は 1～55 文字です。大文字、小文字を区別します。@マークを含めることはできません。プレーンテキストのパスワードの設定範囲は 1～63 文字です。暗号テキストのパスワードの設定範囲は 1～117 文字です。

6.3.2 認証方式

認証装置（ローカル認証）あるいは RADIUS サーバを通して MAC アドレス認証を行うことができます。

RADIUS 認証：

- **MAC ベースアカウント**－認証装置は、認証を行うため、ユーザ名、パスワードとしてパケットの送信元 MAC アドレスを RADIUS サーバに送信します。
- **共有アカウント**－認証装置は、認証を行うため共有アカウントのユーザ名とパスワードを RADIUS サーバに送信します。

ローカル認証：

- **MAC ベースアカウント**－認証装置は、ローカルアカウントデータベースに一致するかどうか検索するため、ユーザ名とパスワードとしてパケットの送信元 MAC アドレスを使用します。
- **共有アカウント**－認証装置は、ローカルアカウントデータベースに一致するかどうか検索するため、共有アカウントのユーザ名とパスワードを使用します。

ローカル認証と RADIUS 認証の詳細は QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 9 *セキュリティ “AAA”* を参照してください。

6.3.3 OUI 認証

OUI 認証はクライアントの MAC アドレスの OUI を調査します。認証装置のために設定された OUI の 1 つが、クライアントの OUI に一致している場合、クライアントは OUI 認証にパスします。

🕮 **メモ：**

IEEE によって定義される OUI は、装置ベンダ、メーカー、組織を識別する MAC アドレスの最初の 24 ビットです。MAC アドレスの最初の 3 オクテットは OUI です。

6.4 認証モード

認証モード	動作メカニズム
bypass（デフォルト）	認証を行いません。
dot1x	802.1X認証のみを実行します。
mac	MACアドレス認証のみを実行します。
mac-then-dot1x	MACアドレス認証を最初に実行し、次に802.1X認証を実行します。クライアントがMACアドレス認証にパスした場合、802.1X認証は実行されません。
dot1x-then-mac	802.1X認証を最初に実行し、次にMACアドレス認証を実行します。クライアントが802.1X認証にパスした場合、MACアドレス認証は実行されません。
oui-then-dot1x	OUI認証を最初に実行し、次に802.1X認証を行います。クライアントがOUI認証にパスした場合、802.1X認証は実行されません。
mac-and-dot1x	MACアドレス認証と802.1X認証の２つの認証（マルチステップ認証）を実行します。MACアドレス認証を最初に実行し、MACアドレス認証にパスした場合のみ、802.1X認証を実行します。２つの認証にパスしたクライアントの接続が許可されます。

6.5 侵入保護

認証装置が認証に失敗したクライアントからアソシエーションリクエストを検出した場合、侵入保護が開始されます。

この機能は、リクエストを受信したとき、BSS（basic service set）で以下に示す定義済みのアクションの 1 つが行われます。

- **temporary-block**（デフォルト）－リクエストの送信元 MAC アドレスをブロック MAC アドレスリストに追加し、リクエストパケットを廃棄します。ブロックされた MAC アドレスのクライアントは一定期間、AP と接続を確立することができません。接続を確立できない期間を設定する場合、**client-security intrusion-protection timer temporary-block** コマンドを使用します。
- **service-stop**—radio インタフェースの BSS が手動で有効にされるまで、リクエストが受信された BSS を停止します。
- **temporary-service-stop**—一定期間リクエストが受信された BSS を停止します。

  接続を確立できない期間を設定する場合、**client-security intrusion-protection timer temporary-service-stop** コマンドを使用します。

🕮 **メモ：**
侵入保護はバイパスモードではサポートしません。

6.6 WLANのVLAN操作

6.6.1 VLAN 認証

クライアントがネットワークリソースへのアクセスを制御するため、WLAN クライアント用に許可 VLAN を指定することができます。クライアントが 802.1X あるいは MAC アドレス認証にパスしたとき、認証サーバは許可 VLAN の情報を認証装置に割り当てます。

装置が認証装置として動作するとき、以下の形式でサーバが割り当てた VLAN を解決することができます。

- VLAN ID
- VLAN 名
- VLAN グループ名
- VLAN ID と VLAN 名の組み合わせ

VLAN のグループをサーバに割り当てる場合、アクセス措置は VLAN ID に従い、VLAN を選択し、割り当てます。

許可される VLAN タイプ	VLAN の選択、割り当てルール
• VLAN ID • VLAN名 • VLAN IDとVLAN名の組み合わせ	装置はVLANグループからもっとも小さいIDのVLANを選択します。
VLANグループ名	1. 装置はオンラインユーザがもっとも少ない VLAN を選択します。 2. 複数の VLAN がオンライン 802.1X ユーザの同一番号を持っている場合、装置はもっとも小さい ID を持つ VLAN を選択します。

🕮 **メモ：**
装置は VLAN をクライアントに割り当てる前、VLAN 名、VLAN グループ名を VLAN ID に置き換えます。

以下の場合、装置はクライアントの許可 VLAN を拒否します。

- 装置が許可 VLAN の情報を確定することができません。
- サーバは装置に VLAN 名を割り当てますが、VLAN 名を使用している VLAN が存在しません。
- サーバは装置に VLAN グループ名を割り当てますが、VLAN グループが存在しない、あるいは VLAN グループに VLAN が割り当てられていません。

階層構造の AP ネットワークでは、認証装置と、データの転送を行う装置は異なる装置にすることができます。たとえば、中央の AC は認証を行い、ローカル AC あるいは AP はデータトラフィックを転送します。

許可 VLAN の情報は、データ転送を制御するのに使用します。そのため、許可 VLAN の情報はデータトラフィックを転送する装置に割り当てる必要があります。VLAN 割り当ては、認証装置と転送装置が同一装置であるかによって、ローカル VLAN 割り当て、あるいはリモート VLAN 割り当てにすることができます。

- **ローカル VLAN 割り当て**－認証装置と転送装置は同一装置です。認証装置が許可 VLAN 情報を取得したのち、許可 VLAN 情報を解決し、VLAN を割り当てます。
- **リモート VLAN 割り当て**－認証装置と転送装置は異なる装置です。認証装置が許可 VLAN 情報を取得したのち、リモート転送装置に情報を送信します。転送装置は許可 VLAN 情報を解決し、VLAN を割り当てます。

VLAN の詳細は QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 4 アクセスの *“VLAN”* を参照してください。

6.6.2 制限 VLAN

組織のセキュリティ戦略に遵守できずに失敗したことが原因で WLAN 認証に失敗したクライアントに対応するため、クライアントを WLAN の制限 VLAN に収容することができます。たとえば間違ったパスワードやユーザ名を入力したクライアントに制限 VLAN が適応されます。制限 VLAN は認証タイムアウトあるいはネットワークの接続問題のために認証に失敗した WLAN クライアントに適応しません。

制限 VLAN のクライアントは制限されたネットワークリソースにアクセスすることができます。

認証装置は、30 秒間隔で制限 VLAN のクライアントの再認証を行います。

- クライアントが再認証にパスした場合、認証装置はクライアントを許可 VLAN に割り当てます。許可 VLAN が設定されていない場合、クライアントは最初の VLAN に割り当てられます。
- クライアントが再認証に失敗した場合、クライアントは制限 VLAN にとどまります。

RSNA を使用するクライアントは、クライアントが 802.1X 認証に失敗しても、制限 VLAN に割り当てることはできません。認証装置は RSNA を使用するクライアントを直接ログオフします。

制限 VLAN 機能は侵入保護機能よりも優先されます。クライアントが認証に失敗したとき、最初に制限 VLAN の設定を適用します。制限 VLAN が設定されていない場合、侵入保護機能が適用されます。制限 VLAN 機能、侵入保護機能の両方が設定されていない場合、認証装置はクライアントを直接ログオフします。

6.7 ほかの機能を用いたWLAN認証

6.7.1 ACL の割り当て

クライアントのネットワークリソースへのアクセスを制御するため、802.1X あるいは MAC アドレス認証クライアントに ACL を指定することができます。クライアントが認証にパスしたのち、認証サーバはクライアントのトラフィックをフィルタするため、クライアントに ACL を割り当てます。

認証サーバは認証装置として動作するローカル装置、あるいは RADIUS サーバのどちらにすることができます。どちらの場合でも、認証装置で ACL のルールを設定する必要があります。

クライアントのアクセス制御の基準を変更する場合、以下の方法の 1 つを使用することができます。

- 認証装置で ACL ルールを変更します。
- 認証サーバでクライアント用に別の ACL を指定します。

ACL の詳細は QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 8 *ACL and QoS　“ACL”* を参照してください。

6.7.2 ユーザプロファイルの割り当て

クライアントのネットワークリソースへのアクセスを制御するため、WLAN クライアントにユーザプロファイルを指定することができます。クライアントが 802.1X あるいは MAC アドレス認証にパスしたのち、認証サーバはトラフィックをフィルタするためクライアントにユーザプロファイルを割り当てます。認証サーバは認証装置として動作するローカル装置、あるいは RADIUS サーバのどちらかにすることができます。どちらの場合でも、認証装置でユーザプロファイルを設定する必要があります。

クライアントのアクセス許可を変更する場合、以下の方法の 1 つを使用することができます。

- 認証装置でユーザプロファイルを変更します。
- 認証サーバでクライアント用に別のユーザプロファイルを指定します。

ユーザプロファイルの詳細は QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 8 *ACL and QoS　“ユーザプロファイル”* を参照してください。

目次

7章 WLAN認証の設定 7-1
7.1 設定要件 7-1
7.2 WLAN認証の設定作業リスト 7-2
7.3 グローバルWLAN認証パラメータの設定 7-2
7.3.1 OUI認証のOUIの設定 7-2
7.3.2 802.1Xでサポートされるドメイン名デリミタの設定 7-3
7.3.3 802.1XのEAP中継モード、EAP終端モードの有効化 7-3
7.3.4 802.1X認証リクエストの最大試行回数の設定 7-4
7.3.5 802.1X認証タイマの設定 7-4
7.3.6 MACアドレス認証の認証方式の設定 7-6
7.3.7 MACアドレス認証のユーザアカウントのフォーマットの設定 7-6
7.3.8 グローバルでのMACアドレス認証ドメインの設定 7-6
7.3.9 MACアドレス認証サーバタイムアウトタイマの設定 7-7
7.4 サービス特有のWLAN認証パラメータの設定 7-7
7.4.1 認証モードの設定 7-7
7.4.2 WLANクライアントの認証装置の設定 7-8
7.4.3 WLAN制限VLANの設定 7-8
7.4.4 サーバからの許可情報の無視設定 7-9
7.4.5 authorization-fail-offline機能の有効化 7-9
7.4.6 侵入保護の設定 7-9
7.4.7 オンラインユーザハンドシェイク機能の設定 7-10
7.4.8 802.1X認証ドメインの設定 7-11
7.4.9 802.1X認証クライアントの最大同時接続数の設定 7-11
7.4.10 定期的なオンラインユーザ再認証機能の有効化 7-12
7.4.11 MACアドレス認証クライアントの最大同時接続数の設定 7-12
7.4.12 サービス特有のMACアドレス認証のドメインの設定 7-13
7.4.13 MACアドレス認証クライアントのためのAC内ローミング高速接続有効化 7-13
7.4.14 アカウンティング開始トリガ機能の設定 7-14
7.4.15 アカウンティングアップデートトリガ機能の設定 7-15
7.5 Web認証(ポータル認証)の設定 7-15
7.6 レーダーによる通信停止回避用サービステンプレート設定 7-16
7.6.1 レーダーによる通信停止回避用サービステンプレート設定について 7-16
7.6.2 レーダーによる通信停止回避用サービステンプレートの設定作業リスト 7-16
7.6.3 レーダーによる通信停止回避用サービステンプレートの指定 7-16
7.7 失敗許可機能の有効化 7-17
7.7.1 失敗許可機能について 7-17
7.7.2 失敗許可機能の設定 7-17
7.7.3 RADIUSサーバ検出の設定 7-18
7.8 WLAN認証の表示と維持 7-18
7.9 WLAN認証の設定例 7-19
7.9.1 802.1X CHAPローカル認証の設定例 7-19
7.9.2 レーダーによる通信停止回避用サービステンプレートの設定例 7-21
7.9.3 PSK認証、認証バイパス時の失敗許可機能設定例 7-23
7.9.4 プライベートPSK認証、MACアドレス認証時の失敗許可機能設定例 7-24

7.9.5 802.1X認証時の失敗許可機能設定例 7-27
7.9.6 認証装置をAPに指定時の802.1X認証設定例 7-30

7章 WLAN 認証の設定

この章は WLAN 認証の設定について記載します。

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

7.1 設定要件

WLAN 認証を設定する前に、以下の作業を完了してください。

- WLAN クライアントの ISP ドメイン、AAA スキーム（ローカル認証あるいは RADIUS 認証）を設定してください。
- ローカル認証を使用する場合、装置でローカルユーザアカウント（ユーザ名、パスワードを含みます。）を作成してください。サービスタイプを lan-access に設定してください。
- RADIUS 認証を使用する場合、装置と RADIUS サーバが互いに通信可能であることを確認してください。RADIUS サーバでユーザアカウントを作成してください。MAC アドレス認証のクライアント用に MAC ベースのアカウントを使用している場合、各アカウントのユーザ名とパスワードが、各クライアントの MAC アドレスと同一であることを確認してください。

詳細は QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 9 *セキュリティの “AAA”* を参照してください。

7.2 WLAN認証の設定作業リスト

作業リスト
（オプション設定項目）グローバルWLAN認証パラメータの設定 ● OUI認証のOUIの設定 ● 802.1Xでサポートされるドメイン名デリミタの設定 ● 802.1XのEAP中継モード、EAP終端モードの有効化 ● 802.1X認証リクエストの最大試行回数の設定 ● 802.1X認証タイマの設定 ● MACアドレス認証の認証方式の設定 ● MACアドレス認証のユーザアカウントのフォーマットの設定 ● グローバルでのMACアドレス認証ドメインの設定 ● MACアドレス認証サーバタイムアウトタイマの設定
サービス特有のWLAN認証パラメータの設定 ● （必須設定項目）認証モードの設定 ● （オプション設定項目）WLANクライアントの認証装置の設定 ● （オプション設定項目）802.1X EAPプロトコルモードの設定 ● （オプション設定項目）WLAN制限VLANの設定 ● （オプション設定項目）サーバからの許可情報の無視設定 ● （オプション設定項目）authorization-fail-offline機能の有効化 ● （オプション設定項目）侵入保護の設定 ● （オプション設定項目）オンラインユーザハンドシェイク機能の設定 ● （オプション設定項目）802.1X認証ドメインの設定 ● （オプション設定項目）802.1X認証クライアントの最大同時接続数の設定 ● （オプション設定項目）定期的なオンラインユーザ再認証機能の有効化 ● （オプション設定項目）MACアドレス認証クライアントの最大同時接続数の設定 ● （オプション設定項目）サービス特有のMACアドレス認証のドメインの設定

7.3 グローバルWLAN認証パラメータの設定

7.3.1 OUI 認証の OUI の設定

以下に OUI 認証の OUI の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． OUI 認証の OUI を設定する	**port-security oui index** *index-value* **mac-address** *oui-value*	デフォルト：設定なし このステップはoui-then-dot1xモードでのみ必要です。 OUIを複数設定することができます。装置は最大16 のOUIをサポートします。 コマンドの詳細はQX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ“ポートセキュリティ”*を参照してください。

7.3.2 802.1X でサポートされるドメイン名デリミタの設定

以下に 802.1X でサポートされるドメイン名デリミタの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． 802.1X クライアントのドメイン名デリミタを設定する	**dot1x domain-delimiter** *string*	デフォルト：（@）デリミタのみサポートします。 コマンドの詳細はQX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ “802.1X”*を参照してください。

7.3.3 802.1X の EAP 中継モード、EAP 終端モードの有効化

以下に 802.1X EAP 中継モード、EAP 終端モードの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2. EAP 中継モード、EAP 終端モードを有効にする	**dot1x authentication-method** { **chap** | **eap** | **pap** }	デフォルト：装置はEAP終端モードを実行し、RADIUSサーバとCHAPを使用して通信します。 EAP中継モードを有効にする場合、**eap**パラメータを指定します。 CHAPあるいはPAPが有効なEAP終端モードを有効にする場合、**chap**パラメータあるいは**pap**パラメータを指定します。 コマンドの詳細はQX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ "802.1X"* を参照してください。

🕮 **メモ：**

EAP 中継モードが使用された場合、RADIUS scheme view で設定された **user-name-format** コマンドは適用されません。装置はクライアントからサーバに認証データを変更しないで送信します。**user-name-format** コマンドについての詳細は、QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアルのセクション 9 *セキュリティ "AAA"* を参照してください。

7.3.4 802.1X 認証リクエストの最大試行回数の設定

以下に 802.1X 認証リクエストの最大試行回数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. 802.1X 認証リクエストの最大試行回数を設定する	**dot1x retry** *max-retry-value*	デフォルト：2 コマンドの詳細はQX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティの "802.1X"* を参照してください。

7.3.5 802.1X 認証タイマの設定

802.1X はクライアントと RADIUS サーバ間の相互通信を制御するため、以下のタイマを使用します。

- **クライアントタイムアウトタイマ**－装置がクライアントに EAP-Request/MD5 Challenge パケットを送信するときに起動します。このタイマが時間切れになるまで

クライアントから応答がなかった場合、装置は、クライアントにリクエストを再送します。応答を受信することなく最大試行回数に到達した場合、クライアントは認証に失敗します。最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。

- **サーバタイムアウトタイマ**－装置が認証サーバに RADIUS Access-Request パケットを送信するときに起動します。このタイマが時間切れになるまでに応答がなかった場合、装置は、サーバにリクエストを再送します。
- **ハンドシェイクタイマ**－クライアントが認証にパスしたのち、オンラインユーザのハンドシェイクが有効になったときに起動します。装置は各ハンドシェイク間隔でクライアントにハンドシェイクメッセージを送信します。最大ハンドシェイク試行回数に到達したのち、クライアントから応答を受信しない場合、装置はクライアントをログオフします。最大試行回数を設定する場合、**dot1x retry** コマンドを使用します。
- **定期的再認証タイマ**－クライアントが認証にパスしたのち、定期的なオンラインユーザの再認証が有効になったときに起動します。装置は設定された間隔でクライアントを再認証します。設定の変更を行ったのちに、オンラインになったクライアントのみ設定の変更が適用されます。

ほとんどの場合、デフォルトの設定で十分です。ネットワークの状況に応じてタイマを設定することができます。

- パフォーマンスの低いネットワークで、クライアントタイムアウトタイマを高い値に設定します。
- 異なる性能の認証サーバがあるネットワークでサーバタイムアウトタイマを調整します。

以下に 802.1X 認証タイムアウトタイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	－
2. クライアントタイムアウトタイマを設定する	**dot1x timer supp-timeout** *supp-timeout-value*	デフォルト：30秒 コマンドの詳細は QX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ “802.1X”* を参照してください。
3. サーバタイムアウトタイマを設定する	**dot1x timer server-timeout** *server-timeout-value*	デフォルト：100秒 コマンドの詳細は QX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ “802.1X”* を参照してください。
4. ハンドシェイクタイマを設定する	**dot1x timer handshake-period** *handshake-period-value*	デフォルト：15秒 コマンドの詳細は QX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ “802.1X”* を参照してください。
5. 定期的再認証タイマを設定する	**dot1x timer reauth-period** *reauth-period-value*	デフォルト：3600秒 コマンドの詳細は QX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ “802.1X”* を参照してください。

7.3.6 MAC アドレス認証の認証方式の設定

🕮 **メモ：**

MAC アドレス認証の認証方式の設定は、ソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。

以下に MAC アドレス認証の認証方式の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． MAC アドレス認証の認証方式を設定する	**mac-authentication authentication-method { chap | pap }**	デフォルト：MACアドレス認証にPAPを使用します。 コマンドの詳細は QX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ "MACアドレス認証"* を参照してください。

7.3.7 MAC アドレス認証のユーザアカウントのフォーマットの設定

以下に MAC アドレス認証のユーザアカウントのフォーマットの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． MAC アドレス認証のユーザアカウントのフォーマットを設定する	● 各クライアントにMACベースのユーザアカウントを使用する： **mac-authentication user-name-format mac-address** [{ **with-hyphen** | **without-hyphen** } [**lowercase** | **uppercase**]] ● すべてのユーザに共有ユーザアカウントを使用する： **mac-authentication user-name-format fixed** [**account** *name*] [**password** { **cipher** | **simple** } *password*]	デフォルト：MACアドレス認証のユーザ名とパスワードとしてクライアントのMACアドレスを使用します。MACアドレスは16進数でハイフンなし、小文字のみです。 コマンドの詳細は QX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ "MACアドレス認証"* を参照してください。

7.3.8 グローバルでの MAC アドレス認証ドメインの設定

クライアントで異なるアクセスポリシーを設定する場合、グローバルあるいはサービステンプレートで MAC アドレス認証の ISP ドメインを指定することができます。

WLAN クライアントの MAC アドレス認証は以下の順番で ISP ドメインを選択します。

1) サービステンプレートで設定されたドメイン
2) system view で設定されたグローバルの MAC アドレス認証のドメイン
3) デフォルトドメイン

ISP ドメインの詳細は QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアルのセクション 9 *セキュリティの "AAA"* を参照してください。

以下にグローバルでの MAC アドレス認証クライアントの ISP ドメインの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. グローバルでの MAC アドレス認証ドメインを設定する	**mac-authentication domain** *domain-name*	デフォルト：設定なし コマンドの詳細は QX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ "MACアドレス認証"* を参照してください。

7.3.9 MAC アドレス認証サーバタイムアウトタイマの設定

装置が RADIUS サーバに認証リクエストを送信するとき、MAC アドレス認証はサーバタイムアウトタイマを起動します。装置がタイムアウトタイマ以内に RADIUS サーバから応答を受信しない場合、装置はサーバを到達不能と認識します。MAC アドレス認証の間、タイマが終了した場合、クライアントはネットワークにアクセスすることができません。

以下に MAC アドレス認証サーバタイムアウトタイマの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. MAC アドレス認証サーバタイムアウトタイマを設定する	**mac-authentication timer server-timeout** *server-timeout-value*	デフォルト：100秒 コマンドの詳細は QX-W1000/W1100シリーズ アクセスポイント コマンドマニュアルのセクション9 *セキュリティ "MACアドレス認証"* を参照してください。

7.4 サービス特有のWLAN認証パラメータの設定

7.4.1 認証モードの設定

以下に認証モードの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. service template view に移行する	**wlan service-template** *service-template-name*	ー

操作	コマンド	補足
3. WLAN クライアントの認証モードを設定する	**client-security authentication-mode** { **dot1x** | **dot1x-then-mac** | **mac** | **mac-then-dot1x** | **oui-then-dot1x** | **mac-and-dot1x** }	デフォルト：設定なし。装置は認証を実行しません（認証バイパスモード）。クライアントは直接装置にアクセスすることができます。

7.4.2 WLAN クライアントの認証装置の設定

WLAN クライアントでローカルあるいは RADIUS をもとにした認証を行うため、認証装置として AC あるいは AP を指定することができます。

AC がクライアントにデータトラフィックを転送するように設定されている場合、認証装置は AC にする必要があります。装置でクライアントのデータトラフィックを転送する手順の詳細はセクション 2 *WLAN オペレーションマニュアル*の“*WLAN アクセス*”を参照してください。

AP を認証装置として指定する場合、map-configuration を使用して AP に WLAN 認証の設定をする必要があります。AP を認証装置として指定する設定方法は“*認証装置を AP に指定時の 802.1X 認証設定例*”を参照してください。

🕮 **メモ：**

ap パラメータは、ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。

以下に WLAN クライアントの認証装置の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. service template view に移行する	**wlan service-template** *service-template-name*	―
3. WLAN クライアントの認証装置を設定する	**client-security authentication-location** { **ac** | **ap** }	デフォルト：AC

7.4.3 WLAN 制限 VLAN の設定

以下に WLAN 制限 VLAN の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. service template view に移行する	**wlan service-template** *service-template-name*	―
3. WLAN 制限 VLAN を設定する	**client-security authentication fail-vlan** *vlan-id*	デフォルト：設定なし WLAN制限VLANはサービステンプレートでのみ設定できます。

7.4.4 サーバからの許可情報の無視設定

クライアントが 802.1X 認証あるいは MAC アドレス認証にパスしたのち、サーバ（ローカル、リモート）から受信した許可情報を使用しないように無視することができます。許可情報は VLAN、ACL、ユーザプロファイルがあります。

以下にサーバからの認証情報を無視する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． service template view に移行する	**wlan service-template** *service-template-name*	―
3． 認証サーバから受信した許可情報を無視する	**client-security ignore-authorization**	デフォルト：サーバから受信した許可情報を使用します。

7.4.5 authorization-fail-offline 機能の有効化

authorization-fail-offline 機能は ACL あるいはユーザプロファイルで許可されていない WLAN クライアントをログオフします。

以下の状況の場合、クライアントは ACL あるいはユーザプロファイルの許可に失敗します。

- 装置あるいはサーバは、クライアントに指定した ACL あるいはユーザプロファイルの許可を失敗します。
- 許可された ACL あるいはユーザプロファイルは存在しません。

authorization-fail-offline 機能は VLAN 認証に失敗したクライアントには適用されません。装置はこれらのクライアントを直接ログオフします。

以下に authorization-fail-offline 機能の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． service template view に移行する	**wlan service-template** *service-template-name*	―
3． authorization-fail-offline 機能を有効にする	**client-security authorization-fail offline**	デフォルト：無効 ACLあるいはユーザプロファイルで許可されていないクライアントをログオフしません。そしてシステムのログを出力します。

7.4.6 侵入保護の設定

以下に侵入保護の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． service template view に移行する	**wlan service-template** *service-template-name*	―

操作	コマンド	補足
3. 侵入保護を有効にする	**client-security intrusion-protection enable**	デフォルト：無効
4. （オプション設定項目）侵入保護のアクションを設定する	**client-security intrusion-protection action** { **service-stop** | **temporary-block** | **temporary-service-stop** }	デフォルト：**temporary-block**
5. （オプション設定項目）不正なクライアントに対するブロック期間を設定する	**client-security intrusion-protection timer temporary-block** *value*	デフォルト：180秒
6. （オプション設定項目）BSS が無効状態され続ける silence 期間を設定する	**client-security intrusion-protection timer temporary-service-stop** *value*	デフォルト：20秒

7.4.7 オンラインユーザハンドシェイク機能の設定

オンラインユーザのハンドシェイク機能はオンライン 802.1X クライアントの接続状態を確認します。装置はオンラインクライアントに、**dot1x timer handshake-period** コマンドによって設定された間隔でハンドシェイクメッセージを送信します。最大ハンドシェイク試行回数に到達したのち、クライアントから応答を受信しない場合、装置はクライアントをログオフします。

オンラインユーザハンドシェイクのセキュリティ機能はハンドシェイクメッセージに認証情報を追加します。この機能によって、偽造された 802.1X クライアントから、装置とハンドシェイクメッセージを交換する正式なクライアントを防ぐことができます。この機能において、装置はクライアントから受信したハンドシェイクレスポンスメッセージの認証情報と、認証サーバに割り当てられた認証情報を比較します。一致しない場合、装置はクライアントをログオフします。

I. 設定ガイドライン

オンラインユーザハンドシェイク機能を設定する場合、以下の制限とガイドラインに従ってください。

- オンラインユーザハンドシェイクのセキュリティ機能を使用する場合、オンラインユーザハンドシェイク機能を有効にしてください。
- オンラインユーザハンドシェイクのセキュリティ機能はオンラインで認証された 802.1X クライアントのみ保護します。

II. 設定手順

以下にオンラインユーザハンドシェイク機能の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—

操作	コマンド	補足
3． オンラインユーザハンドシェイク機能を設定する	**dot1x handshake enable**	デフォルト：無効
4． （オプション設定項目）オンラインユーザハンドシェイクのセキュリティ機能を設定する	**dot1x handshake secure enable**	デフォルト：無効

7.4.8 802.1X 認証ドメインの設定

WLAN クライアントの 802.1X 認証は以下の順番で ISP ドメインを選択します。

- サービステンプレートで指定されたドメイン
- ユーザ名で指定されたドメイン
- デフォルトドメイン

以下に 802.1X 認証ドメインの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． service template view に移行する	**wlan service-template** *service-template-name*	―
3． 802.1X 認証ドメインを設定する	**dot1x domain** *domain-name*	デフォルト：設定なし

7.4.9 802.1X 認証クライアントの最大同時接続数の設定

サービステンプレートの 802.1X 認証クライアントの同時接続数が最大になったとき、新規の 802.1X 認証クライアントは拒否されます。

🕮 **メモ：**

- 802.1X 認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は、QX-W1100 シリーズは 512、QX-W1000 シリーズは 256 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

以下に 802.1X 認証クライアントの最大同時接続数の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． service template view に移行する	**wlan service-template** *service-template-name*	―
3． 802.1X 認証クライアントの最大同時接続数を設定する	**dot1x max-user** *count*	デフォルト：512

7.4.10 定期的なオンラインユーザ再認証機能の有効化

オンラインクライアントの接続状態を確認するため、定期的なオンラインユーザの再認証を行い、サーバによって割り当てられた許可属性をアップデートします。属性には ACL、VLAN、QoS ベースのユーザプロファイルが含まれます。再認証の間隔はユーザが設定できます。

サーバによって割り当てられた RADIUS 属性の Session-Timeout、Termination-Action は、定期的なオンラインユーザの再認証に影響します。サーバによって割り当てられた Session-Timeout、Termination-Action を表示する場合、**display dot1x connection** コマンドを使用します。QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアルのセクション 9 *セキュリティ "802.1X"* を参照してください。

- Termination-Action がログオフユーザである場合、定期的な再認証は、定期再認証タイマが Session-Timeout タイマよりも小さいときのみ適用されます。Session-Timeout が定期再認証タイマより小さい場合、Session-Timeout タイマが終了したとき、装置は認証されたオンラインユーザをログオフします。
- Termination-Action が RADIUS リクエストである場合、装置で定期的な再認証は適用されません。Session-Timeout タイマが終了したのち、オンライン 802.1X ユーザを再認証します。

サーバの設定をサポートし、サーバモデルに応じて Session-Timeout タイマと Termination-Action を割り当ててください。

以下に定期的なオンラインユーザ再認証機能の有効にする設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. 定期的なオンラインユーザ再認証機能を有効にする	**dot1x re-authenticate enable**	デフォルト：無効

7.4.11 MAC アドレス認証クライアントの最大同時接続数の設定

サービステンプレートの MAC アドレス認証クライアントの同時接続数が最大になったとき、新規 MAC アドレス認証クライアントは拒否されます。

🕮 **メモ：**

- MAC アドレス認証クライアント同時接続数を、サービステンプレートを設定した無線インタフェースごとに制限します。
- 1 つの無線インタフェースで同時に接続可能なクライアント最大数は、QX-W1100 シリーズは 512、QX-W1000 シリーズは 256 です。
- 無線インタフェースで同時に接続可能なクライアント最大数を超えて接続することはできません。

以下に MAC アドレス認証クライアントの最大同時接続数の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． service template view に移行する	**wlan service-template** *service-template-name*	—
3． MAC アドレス認証クライアントの最大同時接続数を設定する	**mac-authentication max-user** *count*	デフォルト：512

7.4.12 サービス特有の MAC アドレス認証のドメインの設定

WLAN クライアントの MAC アドレス認証は以下の順番で ISP ドメインを選択します。

- サービステンプレートで指定されたドメイン
- system view で指定されたグローバルの MAC アドレス認証のドメイン
- デフォルトドメイン

以下に MAC アドレス認証クライアントの ISP ドメインの設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． service template view に移行する	**wlan service-template** *service-template-name*	—
3． 802.1X 認証ドメインを設定する	**mac-authentication domain** *domain-name*	デフォルト：設定なし

7.4.13 MAC アドレス認証クライアントのための AC 内ローミング高速接続有効化

🕮 **メモ：**

mac-authentication fast-connect enable コマンドはソフトウェアバージョン 7.2.47 を含む以降のソフトウェアからサポートしています。

本機能を有効にすることで、AC で MAC アドレス認証されたクライアントが、同じ AC に管理された別の AP に移動する際、再認証なしでローミングできるようになります。

本機能は MAC アドレス認証を利用する無線クライアントにのみ適用されます。なお、authentication-location と association-location はどちらも AC である必要があります。

本コマンドはサービステンプレートが無効になっているときに設定可能で、有効になった後に適用されます。

以下に MAC アドレス認証クライアントのための AC 内ローミング高速接続を有効化する設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． service template view に移行する	**wlan service-template** *service-template-name*	—

操作	コマンド	補足
3． MAC アドレス認証クライアントのための AC 内ローミング高速接続を有効にする	**mac-authentication fast-connect enable**	デフォルト：有効

7.4.14 アカウンティング開始トリガ機能の設定

クライアントが 802.1X 認証もしくは MAC アドレス認証を通過後、アカウンティング開始トリガは、アカウンティング開始要求を送信する装置の状態を指定します。

アカウンティング開始トリガは以下のいずれかを指定できます。

- ipv4－802.1X 認証あるいは MAC アドレス認証を通過したクライアントが IPv4 アドレスを使用している場合、アカウンティング開始要求を送信します。
- none－クライアントが認証を通過したとき、クライアントの IP アドレスタイプを確認せずにアカウンティング開始要求を送信します。

IP アドレスに基づくアカウンティング開始トリガを指定した場合、アカウンティング遅延タイマを設定できます。アカウンティング遅延タイマは、802.1X 認証あるいは MAC アドレス認証を通過したクライアントの IP アドレスを学習するために装置に対して最大間隔を指定できます。

クライアントが 802.1X 認証もしくは MAC 認証を通過すると、遅延タイマが開始されます。遅延タイマが終了する前に、IP アドレスに基づくアカウンティング開始トリガに一致する IP アドレスの学習に装置が失敗した場合、装置は以下のいずれかのアクションをします。

- no-ip-logoff アクションが指定されていない場合、アカウンティング開始要求を即座に送信します。
- no-ip-logoff アクションが指定されている場合、クライアントをログオフします。

遅延タイマが設定されていない場合、装置はクライアントの IP アドレスを学習しているときにのみ、クライアントに対してアカウンティング開始要求を送信します。

アカウンティングの詳細は、QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアルのセクション 9 *セキュリティ “AAA”* を参照してください。

トリガが IP アドレスのタイプに基づく場合、IP アドレスの学習を有効にする必要があります。無線クライアントの IP アドレスの学習の詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“WLAN IP スヌーピング”* を参照してください。

トリガが適用されるのは、トリガが設定された後にオンラインになったクライアントのみです。

装置がクライアントの IP アドレスを学習するのに要する時間に基づいて、アカウンティング遅延タイマを設定してください。低パフォーマンスのネットワークでは、遅延タイマを増加させることを推奨します。

以下にアカウンティング開始トリガ機能の設定方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	－

操作	コマンド	補足
2． service template view に移行する	**wlan service-template** *service-template-name*	―
3． クライアントに対するアカウンティング開始トリガを設定する	**client-security accounting-start trigger** { **ipv4** | **none** }	デフォルト：**ipv4**
4． （オプション設定項目）アカウンティング遅延タイマを設定する	**client-security accounting-delay time** *time* [**no-ip-logoff**]	デフォルト：装置がクライアントのIPアドレスを学習する場合のみ、クライアントに対してアカウンティング開始要求を送信します。

7.4.15 アカウンティングアップデートトリガ機能の設定

イベントに基づくアカウンティングアップデートトリガを指定するために本機能を使用します。本機能により、802.1X 認証もしくは MAC アドレス認証を通過したオンラインのクライアントの IP アドレスが変化したとき、装置はアカウンティングアップデート要求を送信することができます。

アカウンティングアップデートトリガは、アカウンティング開始トリガとあわせて使用します。アカウンティングアップデートトリガは、**client-security accounting-start trigger** コマンドでアカウンティング開始トリガを設定してある場合のみ適用可能です。

イベントに基づくアカウンティングアップデートトリガに加え、**timer realtime-accounting** コマンドを使用して、定期的なアカウンティングアップデート間隔を設定することができます。

アカウンティングアップデートトリガは、トリガが設定された後にオンラインになったクライアントにのみ適用されます。

以下にアカウンティングアップデートトリガの設定方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． service template view に移行する	**wlan service-template** *service-template-name*	―
3． クライアントに対するアカウンティング開始トリガを設定する	**client-security accounting-update trigger ipv4**	デフォルト：設定あり 装置は、サーバに割り当てられた、もしくはユーザに定義されたリアルタイムアカウンティング間隔で、アカウンティングアップデート要求をアカウンティングサーバに送信します。

7.5 Web認証(ポータル認証)の設定

Web 認証(ポータル認証)の設定に関するコンフィグについては、別紙の共通マニュアル”*QX-W シリーズ Web 認証(ポータル認証)オペレーションマニュアル*”を参照してください。

7.6 レーダーによる通信停止回避用サービステンプレート設定

🕮 **メモ：**
この機能はソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。

7.6.1 レーダーによる通信停止回避用サービステンプレート設定について

レーダー検知時に有効になるサービステンプレート（バックアップ用サービステンプレート）を別の無線に設定することにより、レーダー検知時の通信停止時間を回避します。レーダー検知時、サービステンプレートの切り替えを自動的に行い、SSID を送信するチャネルを切り替えます。SSID に接続中のクライアントを別のチャネルに移動できます。

レーダー検知した無線が別チャネルで通信を開始すると、バックアップ用のサービステンプレートは無効となり、元の無線のサービステンプレートが有効になります。

7.6.2 レーダーによる通信停止回避用サービステンプレートの設定作業リスト

レーダーによる通信停止回避用サービステンプレートを設定するには、次の手順に従います。

作業リスト
• レーダーによる通信停止回避用サービステンプレートの指定

7.6.3 レーダーによる通信停止回避用サービステンプレートの指定

レーダーによる通信停止回避を行うためには 1 つのサービステンプレートに対して、1 つのバックアップ用のサービステンプレートを用意します。

- バックアップ用サービステンプレートには、**fail-permit template** コマンドを追加する点を除き、オリジナルのサービステンプレートと同じ設定を含める必要があります。
- バックアップ用サービステンプレートは、オリジナルのサービステンプレートとは異なる無線にバインドする必要があります。

以下にレーダーによる通信停止回避用サービステンプレートの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—

操作	コマンド	補足
3. サービステンプレートをバックアップ用テンプレートとして指定する	**fail-permit template**	デフォルト：設定なし

7.7 失敗許可機能の有効化

7.7.1 失敗許可機能について

🕮 **メモ：**

- この機能はソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。
- 失敗許可機能は、AP が AC と通信不能になってから数分後に動作します。動作を開始するまでは新規クライアントは接続できません。
- 1つの無線に対して設定できるバックアップ用のサービステンプレート(SSID)は1つのみです。
- リモート AP が設定されている場合、AP が AC と通信不能になってもこの機能は使用できません。

失敗許可機能をサービステンプレートで有効にすることで、AP が AC もしくは RADIUS サーバと通信不能になった場合にも、新規クライアントが SSID に接続できます。また、AP は AC と通信不能になった場合でも、10 分ごとに再起動しません。

この機能は、サービステンプレートが無効になっている場合に設定でき、サービステンプレートが有効になった後に有効になります。

7.7.2 失敗許可機能の設定

PSK 認証で失敗許可機能を使用する場合、サービステンプレートを 1 つ設定します。AP が AC と通信不能となってから数分後、失敗許可機能が動作します。接続済みのクライアントは AC と AP が切断後も接続を維持します。新規クライアントは、失敗許可機能動作後に接続可能です。AC と AP の切断前後でセキュリティレベルは変化しません。設定方法の詳細は、設定例を参照ください。

MAC アドレス認証で失敗許可機能を使用する場合、サービステンプレートを 1 つ設定します。このとき、同一サービステンプレートに PSK 認証も設定する必要があります。AP が AC と通信不能になってから数分後、もしくは RADIUS サーバと通信不能になってから数分後、失敗許可機能が動作します。接続済みのクライアントは、接続を維持します。新規クライアントは、失敗許可機能動作後に接続可能です。AC もしくは RADIUS サーバと AP の切断前は、クライアントは MAC 認証及び PSK 認証で認証されます。切断後は PSK 認証で認証されます。設定方法の詳細は、設定例（*プライベート PSK 認証*、*MAC アドレス認証時の失敗許可機能設定例*）を参照ください。

802.1X 認証で失敗許可機能を使用する場合、サービステンプレートを 2 つ設定します。1 つのサービステンプレートには 802.1X 認証の設定および **fail-permit enable** コマンドを設定します。もう一方のサービステンプレートにはバックアップ用に PSK 認証および **fail-permit template** コマンドを設定します。AP が AC もしくは RADIUS サーバと通信不能になるまではバックアップ用の SSID は表示されません。AP が AC と通信不能になってから、もしくは RADIUS サーバと通信不能になってから数分後に失敗許可機能が動作します。接続済みのクライアントは接続を維持します。新規クライアントは、失敗許可機能動作後に接続可能です。AC もしくは RADIUS サーバと AP の切断前は、クライアントは 802.1X 認証で認証されます。切断後はバックアップ用の PSK 認証で認証されます。設定方法の詳細は、設定例（*802.1X 認証時の失敗許可機能設定例*）を参照ください。

失敗許可の有効化の設定を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． service template view に移行する	**wlan service-template** *service-template-name*	―
3． 失敗許可を有効にする	**fail-permit enable** [**keep-online**]	デフォルト：無効

7.7.3 RADIUS サーバ検出の設定

失敗許可機能を利用する認証に RADIUS サーバを使用する際、RADIUS サーバが利用可能かを検出するために、RADIUS サーバ検出を設定する必要があります。

RADIUS サーバ検出の設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． RADIUS サーバ検出を設定する	**radius-server test-profile** *profile-number* **username** *name* [**interval** *interval*]	デフォルト：設定なし

7.8 WLAN認証の表示と維持

すべての view で **display** コマンドを実行でき、user view で **reset** コマンドを実行できます。

操作	コマンド
オンライン802.1Xクライアントの情報を表示する	**display dot1x connection** [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number* | **user-mac** *mac-address* | **user-name** *name-string*]
802.1Xセッションの接続情報、統計情報、設定情報を表示する	**display dot1x** [**sessions** | **statistics**] [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]
MACアドレス認証の接続を表示する	**display mac-authentication connection** [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number* | **user-mac** *mac-address* | **user-name** *name-string*]
MACアドレス認証の情報を表示する	**display mac-authentication** [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]

操作	コマンド
ブロックしたMACアドレスの情報を表示する	**display wlan client-security block-mac** [**ap** *ap-name* [**radio** *radio-id*]]
802.1Xの統計情報を削除する	**reset dot1x statistics** [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]
MACアドレス認証の統計情報を削除する	**reset mac-authentication statistics** [**ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]

🕮 **メモ：**

display dot1x connection コマンド、**display dot1x** コマンド、**reset dot1x statistics** コマンド、**display mac-authentication connection** コマンド、**display mac-authentication** コマンド、**reset mac-authentication statistics** コマンドの詳細は QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアルのセクション 9 *セキュリティの“802.1X”、“MACアドレス認証”* を参照してください。

7.9 WLAN認証の設定例

7.9.1 802.1X CHAP ローカル認証の設定例

I. ネットワーク要件

図 7-1に示すようにクライアントの 802.1X ローカル認証を行うために AC で CHAP を使用します。



図 7-1 ネットワーク図

II. 設定手順

1)　802.1X、ローカルクライアントを設定します。

EAP 終端を実行し、CHAP を使用するように AC を設定します。

```
<AC> system-view
[AC] dot1x authentication-method chap
```

ユーザ名 chap1、プレーンテキストでパスワード 123456 のローカルネットワークアクセスユーザを追加します。

```
[AC] local-user chap1 class network
[AC-luser-network-chap1] password simple 123456
```

サービスタイプを lan-access に設定します。

```
[AC-luser-network-chap1] service-type lan-access
[AC-luser-network-chap1] quit
```

2) ISP ドメインの AAA 方式を設定します。

ISP ドメイン local を作成します。

```
[AC] domain local
```

LAN クライアントでローカル認証、ローカル許可、ローカルアカウンティングを使用する ISP ドメインを設定します。

```
[AC-isp-local] authentication lan-access local
[AC-isp-local] authorization lan-access local
[AC-isp-local] accounting lan-access local
[AC-isp-local] quit
```

3) サービステンプレートを設定します。

サービステンプレート wlas_local_chap を作成します。

```
[AC] wlan service-template wlas_local_chap
```

認証モードを 802.1X に設定します。

```
[AC-wlan-st-wlas_local_chap] client-security authentication-mode dot1x
```

サービステンプレートの ISP ドメインを local に設定します。

```
[AC-wlan-st-wlas_local_chap] dot1x domain local
```

wlas_local_chap に SSID を設定します。

```
[AC-wlan-st-wlas_local_chap] ssid wlas_local_chap
```

サービステンプレートを有効にします。

```
[AC-wlan-st-wlas_local_chap] service-template enable
[AC-wlan-st-wlas_local_chap] quit
```

4) AP 名が ap1 のマニュアル AP を設定し、サービステンプレートを AP 無線に関連づけます。

AP ap1 を作成し、AP モデル、シリアル ID を設定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
[AC-wlan-ap-ap1] quit
```

AP の radio 1 の動作チャネルとしてチャネル 64 を設定し、radio 1 を有効にします。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] channel 64
[AC-wlan-ap-ap1-radio-1] radio enable
```

サービステンプレート wlas_local_chap を radio 1 に関連づけます。

```
[AC-wlan-ap-ap1-radio-1] service-template wlas_local_chap
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

III. 設定の確認

802.1X の設定を確認します。

```
[AC] display wlan service-template
[AC] display dot1x
```

802.1X クライアントが認証にパスしたのち、クライアント設定の情報を表示します。

```
[AC] display dot1x connection
```

7.9.2 レーダーによる通信停止回避用サービステンプレートの設定例

I. ネットワーク要件

図 7-2に示すように レーダーによる通信停止回避用サービステンプレートを使用します。

オリジナルのサービステンプレートを 2 つ、バックアップ用のサービステンプレートを 2 つ使用します。

通常時はそれぞれの無線に分かれて通信を行いますが、レーダー検知時にはレーダー未検出の無線のみで通信を継続します。



図 7-2 ネットワーク図

II. 設定手順

1)　オリジナルのサービステンプレート service1 を作成します。

SSID service1 を指定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] ssid service1
[AC-wlan-st-service1] akm mode psk
```

```
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

2)　バックアップ用のサービステンプレート service1_BU を作成します。

fail-permit template 以外は 1)と同じ指定にします。

```
[AC-wlan-st-service1_BU] ssid service1
[AC-wlan-st-service1_BU] fail-permit template
[AC-wlan-st-service1_BU] akm mode psk
[AC-wlan-st-service1_BU] preshared-key pass-phrase simple 12345678
[AC-wlan-st-service1_BU] cipher-suite ccmp
[AC-wlan-st-service1_BU] security-ie rsn
[AC-wlan-st-service1_BU] service-template enable
[AC-wlan-st-service1_BU] quit
```

3)　オリジナルのサービステンプレート service2 を作成します。

SSID service2 を指定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service2] ssid service2
[AC-wlan-st-service2] akm mode psk
[AC-wlan-st-service2] preshared-key pass-phrase simple 12345678
[AC-wlan-st-service2] cipher-suite ccmp
[AC-wlan-st-service2] security-ie rsn
[AC-wlan-st-service2] service-template enable
[AC-wlan-st-service2] quit
```

4)　バックアップ用のサービステンプレート service2_BU を作成します。

fail-permit template 以外は 3)と同じ指定にします。

```
[AC-wlan-st-service2_BU] ssid service2
[AC-wlan-st-service2_BU] fail-permit template
[AC-wlan-st-service2_BU] akm mode psk
[AC-wlan-st-service2_BU] preshared-key pass-phrase simple 12345678
[AC-wlan-st-service2_BU] cipher-suite ccmp
[AC-wlan-st-service2_BU] security-ie rsn
[AC-wlan-st-service2_BU] service-template enable
```

```
[AC-wlan-st-service2_BU] quit
```

5)　AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

6)　オリジナルとバックアップ用のサービステンプレートが別 radio に割り当てます。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] service-template service2_BU
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit

[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template service2
[AC-wlan-ap-ap1-radio-2] service-template service1_BU
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
```

7.9.3 PSK 認証、認証バイパス時の失敗許可機能設定例

I. ネットワーク要件

図 7-3に示すように Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- オープンシステム認証と認証バイパスを設定します。
- ネットワークにアクセスするため、クライアントは共有鍵 12345678 を使用します。

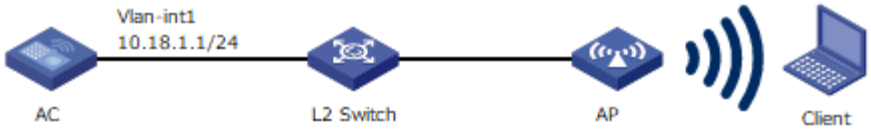


図 7-3 ネットワーク図

II. 設定手順

1)　サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

2)　サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service
```

3)　サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

4)　失敗許可機能を有効にします。

```
[AC-wlan-st-service1] fail-permit enable
```

5)　サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

6)　AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

7)　サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定確認

正しいパスワードでクライアントが SSID に接続できることを確認します。（詳細は省略します。）

AP が AC と切断されてから数分後、失敗許可機能が動作開始し、新規クライアントが SSID に接続できることを確認します。（詳細は省略します。）

7.9.4 プライベート PSK 認証、MAC アドレス認証時の失敗許可機能設定例

I. ネットワーク要件

図 7-4に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名、パスワードとして MAC アドレスを使用して、クライアントがネットワークにアクセスできるように MAC アドレス認証を設定します。
- クライアントが PSK として MAC アドレスを使用できるようにプライベート PSK AKM モードを設定します。

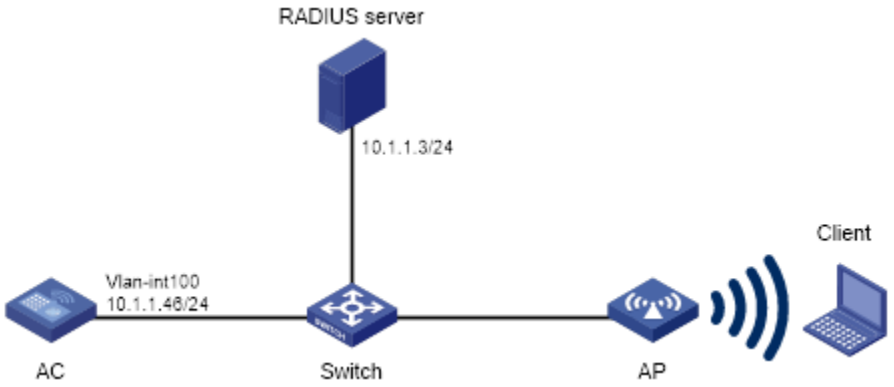


図 7-4 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 00-23-12-45-67-7a、パスワード 00-23-12-45-67-7a を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) WLAN サービステンプレート service1 を作成します。サービステンプレートの SSID サービスを指定します。

```
<AC> system-view
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid service
```

3) サービステンプレート service1 の WLAN セキュリティを設定します。

#AKM モードとして PSK を設定し、プレーンテキストで鍵 12345678 を指定します。

```
[AC-wlan-st-service1] akm mode psk
[AC-wlan-st-service1] preshared-key pass-phrase simple 12345678
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

MAC アドレス認証を設定します。

```
[AC-wlan-st-service1] client-security authentication-mode mac
```

4) 失敗許可機能を有効にします。

```
[AC-wlan-st-service1] fail-permit enable
```

5) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

6) RADIUS サーバ検出を設定します。

```
[AC] radius-server test-profile 1 username nectest interval 1
```

7) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812 test-profile 1
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345678
[AC-radius-radius1] key accounting simple 12345678
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

8)　ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

9)　ISP ドメイン dom1 のユーザ名、パスワードとして MAC アドレスを設定します。

```
[AC] mac-authentication domain dom1
[AC] mac-authentication user-name-format mac-address with-hyphen lowercase
```

10）AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

11）サービステンプレート service1 を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

メモ：

AAA、RADIUS コマンドの詳細は、QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアルのセクション 9 *セキュリティ　"AAA"* を参照してください。

III. 設定の確認

MAC アドレスを登録済みのクライアントが SSID に接続できることを確認します。（詳細は省略します。）

AP が AC と切断されてから数分後、もしくは RADIUS サーバと切断されてから数分後、失敗許可機能が動作開始し、新規クライアントが PSK 認証で SSID に接続できることを確認します。（詳細は省略します。）

7.9.5 802.1X 認証時の失敗許可機能設定例

I. ネットワーク要件

図 7-5に示すように、Switch は AP とクライアントに IP アドレスを割り当てるため、DHCP サーバとして動作します。

- ログイン名 abcdef、パスワード 123456 を使用して、クライアントがネットワークにアクセスできるようにオープンシステム認証と 802.1X 認証を設定します。
- AKM モードとして 802.1X を設定します。

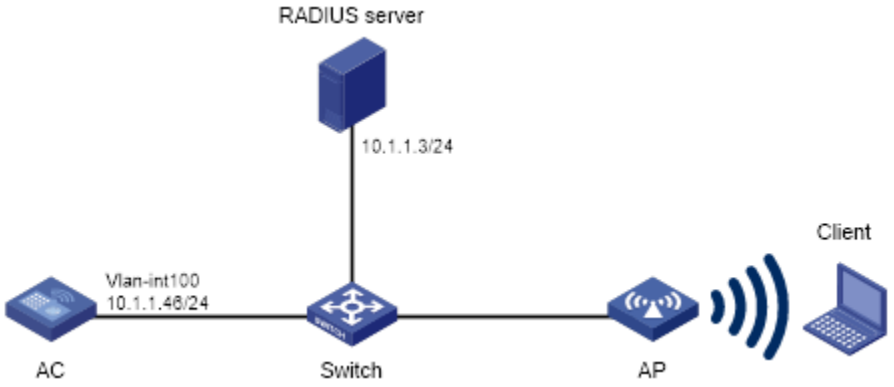


図 7-5 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abcdef、パスワード 123456 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) 802.1X クライアントを設定します。（詳細は省略します。）
3) 802.1X 認証用の WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
```

```
[AC] wlan service-template service1
```

4)　サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service_dot1x
```

5)　サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

6)　802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1] dot1x domain dom1
```

7)　失敗許可機能を有効にします。

```
[AC-wlan-st-service1] fail-permit enable
```

8)　サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

9)　バックアップの PSK 認証用のサービステンプレートを作成します。

```
<AC> system-view
[AC] wlan service-template service1_bu
```

10) サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1_bu] ssid service_psk
```

11) サービステンプレート service1_bu の WLAN セキュリティを設定します。

AKM モードとして PSK を設定し、プレーンテキストで共有鍵 12345678 を指定します。

```
[AC-wlan-st-service1_bu] akm mode psk
[AC-wlan-st-service1_bu] preshared-key pass-phrase simple 12345678
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1_bu] cipher-suite ccmp
[AC-wlan-st-service1_bu] security-ie rsn
```

12) バックアップ用に fail-permit template を設定します。

```
[AC-wlan-st-service1_bu] fail-permit template
```

13) サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1_bu] service-template enable
[AC-wlan-st-service1_bu] quit
```

14) RADIUS サーバ検出を設定します。

```
[AC] radius-server test-profile 1 username nectest interval 1
```

15）RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812 test-profile 1
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

16）ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

17）AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

18）サービステンプレート service1 と service1_bu を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] service-template service1_bu
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

🕮 **メモ：**

AAA、RADIUS コマンドの詳細は、QX-W1000/W1100 シリーズ アクセスポイント コマンドマニュアルのセクション 9 *セキュリティ　"AAA"* を参照してください。

III. 設定の確認

クライアントが SSID に接続できることを確認します。（詳細は省略します。）

AP が AC と切断されてから、もしくは RADIUS サーバと切断されてから数分後、失敗許可機能が動作開始し、新規クライアントが PSK 認証で SSID に接続できることを確認します。（詳細は省略します。）

7.9.6 認証装置を AP に指定時の 802.1X 認証設定例

AC－AP 間で CAPWAP トンネルが確立されている際は、AC が認証装置として動作し、AC－AP 間の CAPWAP トンネルが切断された際は AP が認証装置として動作するための設定例を示します。AP が認証装置として動作することで、AC との CAPWAP トンネルが切断されている間も新規クライアントの接続が可能となります。

I. ネットワーク要件

図 7-6に示すように､Switch は AP とクライアントに IP アドレスを割り当てるため､DHCP サーバとして動作します。

- ログイン名 abcdef、パスワード 123456 を使用して、クライアントがネットワークにアクセスできるようにオープンシステム認証と 802.1X 認証を設定します。
- AKM モードとして 802.1X を設定します。

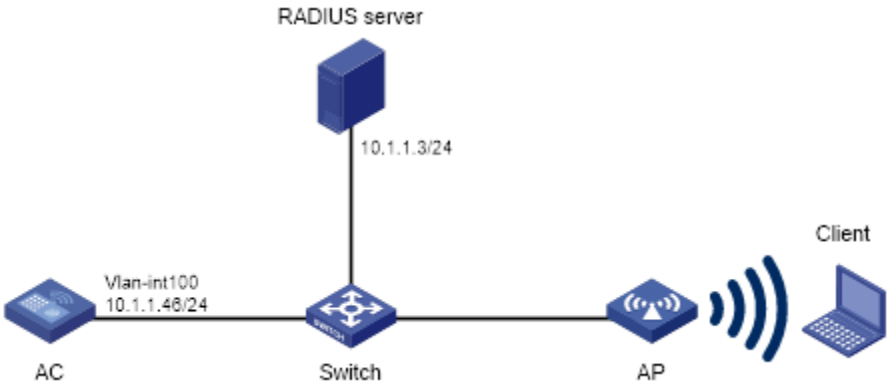


図 7-6 ネットワーク図

II. 設定手順

1) RADIUS サーバでユーザ名 abcdef、パスワード 123456 を設定し、RADIUS サーバと AC が互いに通信可能なことを確認します。（詳細は省略します。）
2) 802.1X クライアントを設定します。（詳細は省略します。）

3)　802.1X 認証用の WLAN サービステンプレート service1 を作成します。

```
<AC> system-view
[AC] wlan service-template service1
```

4)　サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1] ssid service_dot1x
```

5)　サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1] cipher-suite ccmp
[AC-wlan-st-service1] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

6)　失敗許可機能を有効にします。

```
[AC-wlan-st-service1] fail-permit enable
```

7)　サービステンプレート service1 を有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

8)　バックアップの 802.1X 認証用サービステンプレートを作成します。

```
<AC> system-view
[AC] wlan service-template service1_bu
```

9)　サービステンプレートの SSID サービスを指定します。

```
[AC-wlan-st-service1_bu] ssid service_dot1x
```

10)　サービステンプレート service1 の WLAN セキュリティを設定します。

AKM モードとして 802.1X を設定します。

```
[AC-wlan-st-service1_bu] akm mode dot1x
```

cipher スイートとして CCMP を設定し、セキュリティ IE として RSN を設定します。

```
[AC-wlan-st-service1_bu] cipher-suite ccmp
[AC-wlan-st-service1_bu] security-ie rsn
```

802.1X 認証モードを設定します。

```
[AC-wlan-st-service1_bu] client-security authentication-mode dot1x
```

802.1X 認証ドメインとして dom1 を設定します。

```
[AC-wlan-st-service1_bu] dot1x domain dot1x
```

11)　クライアントの関連付けを AP に設定します。

```
[AC-wlan-st-service1_bu] client association-location ap
```

12) 認証装置を AP に指定します。

```
[AC-wlan-st-service1_bu] client-security authentication-location ap
```

13) バックアップ用に fail-permit template を設定します。

```
[AC-wlan-st-service1_bu] fail-permit template
```

14) サービステンプレート service1_bu を有効にします。

```
[AC-wlan-st-service1_bu] service-template enable
[AC-wlan-st-service1_bu] quit
```

15) RADIUS スキームを設定します。

RADIUS スキーム radius1 を作成し、RADIUS scheme view に移行します。

```
[AC] radius scheme radius1
```

プライマリ認証サーバ、アカウンティングサーバを指定します。

```
[AC-radius-radius1] primary authentication 10.1.1.3 1812
[AC-radius-radius1] primary accounting 10.1.1.3 1813
```

プレーンテキストで認証サーバ、アカウンティングサーバの共有鍵 12345 を設定します。

```
[AC-radius-radius1] key authentication simple 12345
[AC-radius-radius1] key accounting simple 12345
```

RADIUS サーバの設定にもとづいて、RADIUS サーバにユーザ名を送信するように設定します。

- RADIUS サーバに送信するユーザ名からドメイン名を除外します。

```
[Device-radius-rs1] user-name-format without-domain
[Device-radius-rs1] quit
```

- RADIUS サーバに送信するユーザ名にドメイン名を含めます。

```
[Device-radius-rs1] user-name-format with-domain
[Device-radius-rs1] quit
```

16) ISP ドメイン dom1 を作成し、ISP ドメインの RADIUS スキームを設定します。

```
[AC] domain dom1
[AC-isp-dom1] authentication lan-access radius-scheme radius1
[AC-isp-dom1] authorization lan-access radius-scheme radius1
[AC-isp-dom1] accounting lan-access radius-scheme radius1
[AC-isp-dom1] quit
```

17) AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

18) サービステンプレート service1 と service1_bu を AP の radio 1 に割り当て、radio 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
```

```
[AC-wlan-ap-ap1-radio-1] service-template service1
[AC-wlan-ap-ap1-radio-1] service-template service1_bu
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

19) 以下の設定を記述した“.mpcfg”形式のファイル“AP_RADIUS.mpcfg”を作成し、AC に格納する。

```
#
 dot1x authentication-method eap
#
radius scheme radius1
 primary authentication 10.1.1.3 1812
 primary accounting 10.1.1.3 1813
 key authentication simple 12345
 key accounting  simple 12345
#
domain dom1
 authentication default radius-scheme radius1
 authorization default radius-scheme radius1
 accounting default radius-scheme radius1
#
```

20) AP に“AP_RADIUS.mpcfg”を適用する。

```
[AC-wlan-ap-ap1] map-configuration flash:/AP_RADIUS.mpcfg
```

🕮 メモ：

AAA、RADIUS コマンドの詳細は、コマンドマニュアルのセクション 9 *セキュリティ“AAA”*を参照してください。

III. 設定の確認

クライアントが SSID に接続できることを確認します。（詳細は省略します。）

AP が AC と切断されてから、もしくは RADIUS サーバと切断されてから数分後、失敗許可機能が動作開始し、新規クライアントが 802.1X 認証で SSID に接続できることを確認します。（詳細は省略します。）

目次

8章 WIPSの設定 8-1
8.1 概要 8-1
8.2 攻撃検出 8-1
8.2.1 フラッドアタックの検出 8-1
8.2.2 不正パケットの検出 8-2
8.2.3 なりすまし攻撃の検出 8-4
8.2.4 Weak IVの検出 8-5
8.2.5 Omerta攻撃の検出 8-5
8.2.6 ブロードキャストアソシエーション解除/認証取り消し攻撃の検出 8-5
8.2.7 40MHzの帯域幅モードを使用禁止にしたクライアントの検出 8-5
8.2.8 パワーセーブ攻撃の検出 8-5
8.2.9 禁止チャネルの検出 8-6
8.2.10 ソフトAPの検出 8-6
8.2.11 Windowsブリッジの検出 8-6
8.2.12 未暗号化装置の検出 8-6
8.2.13 ホットスポット攻撃の検出 8-6
8.2.14 APなりすまし攻撃の検出 8-6
8.2.15 HT-グリーンフィールドAPの検出 8-7
8.2.16 ハニーポットAPの検出 8-7
8.2.17 MITM攻撃の検出 8-7
8.2.18 無線ブリッジの検出 8-7
8.2.19 アソシエーション/再アソシエーションDoS攻撃の検出 8-7
8.2.20 APフラッド攻撃の検出 8-8
8.2.21 装置エントリ攻撃の検出 8-8
8.2.22 シグネチャにもとづいたユーザ定義の攻撃の検出 8-8
8.3 装置の種別 8-8
8.3.1 APの種別 8-8
8.3.2 クライアント種別 8-12
8.4 対策 8-13
8.5 WIPS設定作業リスト 8-13
8.6 WIPS有効化 8-14
8.6.1 radio viewでのWIPSの有効化 8-14
8.6.2 AP group radio viewでのWIPSの有効化 8-15
8.7 無線攻撃検出の設定 8-15
8.7.1 フラッド攻撃検出の設定 8-15
8.7.2 不正パケット検出の設定 8-16
8.7.3 装置エントリ攻撃検出の設定 8-17
8.7.4 その他の攻撃に対する検出設定 8-18
8.7.5 攻撃検知ポリシーの適用 8-19
8.7.6 シグネチャにもとづいたユーザ定義攻撃検出の設定 8-20
8.7.7 アラーム無視装置リストの設定 8-21
8.8 装置種別の設定 8-21
8.8.1 分類ポリシーの設定 8-22
8.8.2 分類ポリシーの適用 8-23

8.9 対策の設定 8-24
8.9.1 対策ポリシーの設定 8-24
8.9.2 対策ポリシーの適用 8-25
8.10 WIPSの表示と維持 8-26
8.11 WIPS設定例 8-26
8.11.1 装置の分類の設定例 8-26
8.11.2 不正パケットとフラッド攻撃の検出例 8-29
8.11.3 シグネチャベースのユーザ定義攻撃検出設定例 8-34

8章 WIPS の設定

この章は WIPS の設定について記載します。

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

8.1 概要

無線侵入防止システム（WIPS）は、802.11 プロトコルに対応したレイヤ 2 プロトコルの検出および防御機能です。

WIPS はチャネルを監視し、分析データを処理することで、ネットワークの安全性を脅かす行為、サービスを妨害する行為、または性能に影響を与える無線機器や動作を検出します。さらに、不正な無線機器に対する対抗措置を提供し、無線ネットワークに包括的なセキュリティ対策を提供します。

WIPS は、センサと AC で構成されます。WIPS は以下の機能を提供します。

- WIPS 機能を有効にした AP をセンサと呼び。センサは無線チャネルを監視し、収集した情報を簡易処理した後、AC へ送信して総合分析を行います。
- AC は攻撃元を分析し、対抗措置を実施するとともに、ログを出力します。

8.2 攻撃検出

WIPS は、無線区間の 802.11 フレームを解析して攻撃を検出し、通知します。

8.2.1 フラッドアタックの検出

AP が、短期間に同じタイプのフレームを多数受信した場合、フラッドアタック攻撃を受けている可能性があります。AP の機能不全を防止するため、WIPS は周期的に受信パケット統計を調査し、フラッドアタックが疑われる場合には、アラームを発生します。WIPS は、以下のフラッドアタックを検出することができます。

- 認証要求フラッドアタック

多数のクライアントの認証要求を模倣することにより、AP の認証テーブルは、容量をオーバーします。

- プローブ要求/アソシエーション要求/再アソシエーション要求フラッドアタック

多数のクライアントのプローブ要求/アソシエーション要求/再アソシエーション要求を模倣することにより、AP のアソシエーションテーブルは、容量をオーバーします。

- EAPOL-Start フラッドアタック

多数のクライアントの IEEE802.1X で定義された EAPOL-start フレームを模倣することにより、AP のリソースを消費します。

- ブロードキャスト/ユニキャスト認証取り消し（Deauthentication）フラッドアタック

クライアントは、AP からのなりすまし認証取り消し（Deauthentication）フレームを受信すると、AP への接続を切断します。この攻撃で、急速に複数のクライアントの無線サービスを終わらせることができます。

- ブロードキャスト/ユニキャスト アソシエーション解除フラッドアタック

クライアントは、AP からのなりすましアソシエーション解除フレームを受信すると、AP への接続を切断します。この攻撃により、複数クライアントの無線サービスが急速に終了させられる恐れがあります。

- RTS/CTS フラッドアタック

大量の RTS/CTS フレームで RF 帯域を予約し、RF 帯域を共有する他の無線装置が送信を抑止するように強制します。この攻撃はバーチャルなキャリアメカニズムの脆弱性を利用します。

- ブロック ACK フラッドアタック

大量のブロック ACK フレームにより、ブロック ACK 動作を中断させます。

- ヌルデータ フラッドアタック

なりすましのヌルデータをクライアントから AP に送信します。AP は、クライアントがパワーセーブモードであると判断し、クライアントのためにフレームをバッファ処理します。バッファ処理されたフレームの保存時間が期限切れになった場合、AP はフレームを廃棄します。これにより、クライアントと AP との通信が中断されます。

- ビーコン フラッドアタック

多数の擬似 AP を模倣するビーコンフレームは、クライアントの関連付けを中断させます。

- EAPOL-logoff フラッドアタック

IEEE802.1X 標準は、LAN（EAPOL）上で拡張認証プロトコルを使って、認証プロトコルを定義します。クライアントは、APによってセッションを終わらせるためにEAPOL-logoffフレームを送る必要があります。EAPOL-logoff フレームは認証されておらず、攻撃者は、クライアントを分離するために EAPOL-logoff フレームを偽ることができます。

- EAP-success/failure フラッドアタック

802.1X 認証を使用している WLAN において、認証成功/失敗を通知するために、AP は EAP-success/EAP-failure フレームをクライアントに送信します。攻撃者は、認証プロセスを混乱させるために、AP の MAC アドレスに偽装した EAP-success/EAP-failure フレームをクライアントに送ることができます。

8.2.2 不正パケットの検出

WIPS は、フレームが表 8-1示した条件と一致している場合、不正フレームと判定し、アラームとログを発生します。WIPS は 16 種類の不正パケットを検出することができます。

表 8-1 不正フレーム条件

検出タイプ	適用フレーム	一致条件
無効なIE長検出	全管理フレーム	IE長が802.11プロトコルに準拠していません。
重複IE検出	全管理フレーム	重複IE。このタイプの検出はベンダで定義されたIEに適用可能ではありません。

検出タイプ	適用フレーム	一致条件
冗長IE検出	全管理フレーム	IEはフレームに必要なIEではなく、予約されたIEでもありません。
無効パケット長検出	全管理フレーム	パケットペイロードが解決された後の残IE長は、ゼロではありません。
異常なIBSSとESS設定検出	• ビーコンフレーム • プローブ応答フレーム	IBSSとESSの両方が1に設定されています。
不正な認証要求フレーム検出	認証要求フレーム	• 認証アルゴリズム番号が802.11プロトコルに対応せず、3より大きいです。 • 認証トランザクションシーケンス番号が1で且つ、ステータスコードが0ではありません。 • 認証トランザクションシーケンス番号が4より大きいです。
不正なアソシエーション要求フレーム検出	アソシエーション要求フレーム	フレーム長が0です。
不正なHT IE検出	• ビーコンフレーム • プローブ応答フレーム • アソシエーション応答フレーム • 再アソシエーション要求フレーム	• HT capabilities IEのSMパワーセーブ値が2です。 • HT capabilities IEの二次チャネルオフセット値が2です。
継続時間超過検出	• ユニキャスト管理フレーム • ユニキャストデータフレーム • RTS, CTS, ACK フレーム	パケットの継続時間の値が指定したしきい値を超えています。
不正なプローブ応答フレーム検出	プローブ応答フレーム	フレームはメッシュフレームではなく、そのSSID長が0です。
無効な認証取り消し（Deauthentication）コード検出	認証取り消し（Deauthentication）フレーム	理由コードが0、または、67～65535の範囲内にあります。
無効なアソシエーション解除コード検出	アソシエーション解除フレーム	理由コードが0、または、67～65535の範囲内にあります。
SSIDデータ長超過検出	• ビーコンフレーム • プローブ要求フレーム • プローブ応答フレーム • アソシエーション要求フレーム	SSIDデータ長が32より大きいです。
FATA-Jack 検出	認証フレーム	認証アルゴリズム番号が2です。

検出タイプ	適用フレーム	一致条件
無効ソースアドレス検出	全管理フレーム	• TO DSは1であり、フレームがクライアントによってAPに送信されたことを示しています。 • フレームのソースMACアドレスが、マルチキャストまたはブロードキャストアドレスです。
EAPOL key長超過検出	EAPOL-Keyフレーム	TO DSが1、かつ、キー長が0より大きいです。

8.2.3 なりすまし攻撃の検出

なりすまし攻撃では、攻撃者はネットワークを脅かすために別の装置になりすましてフレームを送ります。WIPS は以下のなりすまし攻撃の検出をサポートします。

- フレームなりすまし

偽 AP は、許可された AP になりすまして、ビーコン、または、プローブ応答フレームを送信し、クライアントが偽 AP に参加するよう誘導します。

- AP MAC アドレスなりすまし

許可された AP になりすましたクライアントは、認証取り消し（Deauthentication）、または、アソシエーション解除フレームを他のクライアントに送ります。

これにより、クライアントがオフラインになり、WLAN の正常な動作に影響を与える可能性があります。

- クライアント MAC アドレスなりすまし

偽 AP は、許可されたクライアントになりしまし、許可された AP に参加することができます。

I. フレームなりすまし攻撃の検出

WIPS は、フレーム受信時刻とタイムスタンプを使用して AP の起動時間を計算します。計算された AP の起動時間が WIPS に記録された起動時間と異なる場合、WIPS は、なりすまし攻撃であると判断します。

II. AP MAC アドレスなりすまし攻撃の検出

WIPS は、送信側の MAC アドレスを調査します。送信側の MAC アドレスが、すでに AP MAC アドレステーブルに存在している場合、WIPS は、なりすまし攻撃であると判断します。

III. クライアント MAC アドレスなりすまし攻撃の検出

WIPS は、送信側の MAC アドレスを調査します。送信側の MAC アドレスが、すでにクライアント MAC アドレステーブルに存在している場合、WIPS は、なりすまし攻撃であると判断します。

8.2.4 Weak IV の検出

WEP セキュリティプロトコルで使用されている RC4 暗号化アルゴリズムで特定の IV を使用する場合、WEP キーがクラックされる可能性が高くなります。この特定の IV を Weak IV といいます。WIPS は、各 WEP パケットの IV を検出することで、この種の攻撃を防ぎます。

8.2.5 Omerta 攻撃の検出

Omerta は 802.11 のプロトコルをベースにした DoS 攻撃ツールです。このツールは、クライアントを分離するために、理由コード 0x01 のアソシエーション解除フレームを送信します。理由コード 0x01 は、未知の分離理由です。WIPS は、各アソシエーション解除フレームの理由コードを検出することによって、Omerta 攻撃を検出します。

8.2.6 ブロードキャストアソシエーション解除/認証取り消し攻撃の検出

攻撃者は、全クライアントを正当な AP からログオフさせるためのブロードキャスト アソシエーション解除/認証取り消し（Deauthentication）フレームを送信するために、正当な AP になりすまします。

8.2.7 40MHz の帯域幅モードを使用禁止にしたクライアントの検出

複数の帯域幅を使用できるラジオにおいて、40MHz 帯域幅モードを使用禁止(40Mhz チャネル幅非互換)のクライアントが接続されて通信をしている場合、そのクライアントの通信が完了するまで、同じラジオに接続されている他のクライアントは通信を開始できず、ネットワークスループットと効率に影響を与えます。

WIPS は、クライアントが送信するプローブ要求フレームを検出することによって、そのようなクライアントを検出します。

8.2.8 パワーセーブ攻撃の検出

攻撃者は、クライアントの MAC アドレスになりすまして、パワーセーブのフレームを AP に送信します。AP はクライアントのフレームをキャッシュします。攻撃を受けたクライアントは、パワーセーブモードであると AP に判断されているため、データフレームを受信できません。キャッシングされたフレームのエージングタイムが満了すると、AP はフレームを破棄してしまいます。WIPS は、パワーセーブ ON フレームとパワーセーブ OFF フレームの比率を決定することでパワーセーブ攻撃を検出します。

8.2.9 禁止チャネルの検出

許可チャネルリストを設定し、禁止チャネル検出を有効にすると、WIPS は許可チャネルリストにないチャネルを禁止チャネルであると判断します。

8.2.10 ソフト AP の検出

ソフト AP とは、AP として機能し、無線サービスを提供するクライアントを指します。攻撃者は、ソフト AP を介して内部ネットワークにアクセスし、さらに攻撃を開始することができます。WIPS は、装置がクライアントと AP 間の役割を切り替える間隔を検出することにより、ソフト AP を検出します。WIPS は、接続していないクライアントのソフト AP 検出を実行しません。

8.2.11 Windows ブリッジの検出

有線ネットワークに接続された無線クライアントが有線 NIC を介して Windows ブリッジを確立すると、クライアントは外部 AP を内部ネットワークとブリッジすることができます。これにより、内部ネットワークにセキュリティ上の問題が発生する可能性があります。WIPS は、接続したクライアントから送信されるデータフレームを分析して、Windows ブリッジを検出します。

8.2.12 未暗号化装置の検出

暗号化していないフレームを送信する認証 AP またはクライアントは、セキュリティ問題をネットワークにもたらす可能性があります。WIPS は、認証 AP またはクライアントから送信されたフレームを分析することによって、暗号化していない装置を検出します。

8.2.13 ホットスポット攻撃の検出

攻撃者は、ホットスポットと同じ SSID を持つ不正な AP を設定して、クライアントが接続するよう誘導します。クライアントが不正な AP に接続した場合、攻撃者はクライアント情報を取得するためにさらに攻撃を開始します。

WIPS がホットスポット攻撃を検出できるように、ホットスポットファイルを設定できます。

8.2.14 AP なりすまし攻撃の検出

AP なりすまし攻撃では、正規 AP と同じ BSSID と ESSID を持つ悪意のある AP に、クライアントを接続するように誘導します。次に、このなりすまし AP は、ホットスポット攻撃を開始するか、検出システムをだまします。

WIPS は、AP が送信するビーコンフレーム間隔を検出することによって、AP なりすまし攻撃を検出します。

8.2.15 HT-グリーンフィールド AP の検出

HT-グリーンフィールドモードで動作する AP は、802.11a/b/g 装置と通信できないため、衝突、エラー、再送信を引き起こす可能性があります。 WIPS は、AP によって送信されたビーコンフレームまたはプローブ応答フレームを分析することによって HT-グリーンフィールド AP を検出します。

8.2.16 ハニーポット AP の検出

ハニーポット AP 攻撃では、攻撃者は悪意のある AP を設定してクライアントが接続するよう誘導します。 悪意のある AP の SSID は、正規 AP の SSID に似ています。 クライアントがハニーポット AP に接続した場合、ハニーポット AP は、ポートスキャンや偽認証などのさらなる攻撃を開始して、クライアント情報を取得します。

WIPS は外部 AP の SSID を検出してハニーポット AP を検出します。外部 AP の SSID と正規 AP の SSID との類似性が指定されたしきい値に達すると、WIPS はアラームを発生します。

8.2.17 MITM 攻撃の検出

MITM 攻撃では、攻撃者は不正 AP を設定し、クライアントが接続するように誘導します。次に、不正 AP は、許可 AP に接続するクライアントの MAC アドレスになりすまします。クライアントと認可 AP が通信するとき、不正 AP はクライアントと認可 AP の両方からパケットをキャプチャします。不正 AP はフレームを修正し、フレーム情報を取得する可能性があります。 WIPS は、許可 AP から切り離され、ハニーポット AP に接続したクライアントを検出することによって、MITM 攻撃を検出します。

8.2.18 無線ブリッジの検出

攻撃者は、無線ブリッジを経由して、内部のネットワークに侵入するかもしれません。WIPS は、無線ブリッジを検出するとアラームを発生します。無線ブリッジがメッシュネットワークにある場合、WIPS はメッシュリンクを記録します。

8.2.19 アソシエーション/再アソシエーション DoS 攻撃の検出

アソシエーション/再アソシエーション DoS 攻撃では、多くのクライアントになりすましたアソシエーション要求を AP に送信することにより、AP のアソシエーションテーブル

をオーバーさせます。テーブル登録が上限に達すると、AP は正規のクライアントの要求を処理することができません。

8.2.20 AP フラッド攻撃の検出

WIPS は WLAN 内の AP 数を検出し、AP 数が指定したしきい値を超えた場合、AP フラッド攻撃のアラームを発生します。

8.2.21 装置エントリ攻撃の検出

攻撃者は、無効なパケットを WIPS に送信して処理コストを増加させることができます。WIPS は学習された装置エントリを定期的に調べ、装置エントリの学習を制限するかどうかを決定します。指定した間隔内に学習された AP またはクライアントエントリの数がしきい値を超えると、WIPS はアラームを発生して新しいエントリの学習を停止します。

8.2.22 シグネチャにもとづいたユーザ定義の攻撃の検出

WIPS は、シグネチャにもとづいたユーザ定義の攻撃検出を提供します。シグネチャには、パケットの識別方法と、一致するパケットを取得するアクションが含まれています。センサは、検出されたパケットをシグネチャと照合し、パケットがシグネチャと一致した場合、シグネチャで定義されたアクションを実行します。

シグネチャには、フレームタイプ、MAC アドレス、シリアル ID、SSID 長、SSID、フレームパターンにもとづいて定義できる最大 6 つのサブシグネチャを含めることができます。 パケットは、シグネチャ内のすべてのサブシグネチャと一致する場合にのみ、シグネチャと一致したことになります。

8.3 装置の種別

8.3.1 AP の種別

表 8-2に示すように、WIPS はあらかじめ決められた分類ポリシーに応じて、検出された AP を分類します。

表 8-2 AP の種別

種別	説明	分類ルール
許可されたAP	WLANで許可されているAP	● 許可APとして設定されています ● 許可APリストに該当します ● 許可APとしてユーザ定義のAP分類ルールによって分類されます ● 無線サービスを提供し、禁止装置リストに該当しません
不正AP	WLANで使用できないAP	● 禁止装置リストに該当します ● OUIコンフィグファイルには該当しません。 ● 不正APとして設定されています ● ユーザ定義のAP分類ルールによって不正APに分類されます
設定ミスのAP	WLANで使用できるが誤ったコンフィグのAP	● 設定が誤っているAPとして設定されています ● ユーザ定義のAP分類ルールによって誤って設定されたAPとして分類されます
外部AP	隣接するWLANにあるAP	● 外部APとして設定されています ● ユーザ定義のAP分類ルールによって外部APとして分類されます
アドホック	アドホックモードで動作するAP。 WIPSはビーコンフレームを確認してアドホックAPを検出します。	－
メッシュAP	WLANメッシュネットワーク内のAP	WIPSはビーコンフレームを通じてメッシュAPを識別します。
潜在的な不正AP	不正APであると考えられるAP。	ワイヤレス設定が間違っていて、次のいずれのリストにも記載されていません。 ● 許可装置リスト。 ● 禁止装置リスト。 ● 信頼できるOUIリスト。 APの有線ポートがネットワークに接続されている場合、APは不正APです。

種別	説明	分類ルール
潜在的外部AP	外部APの可能性があるAP。	● ワイヤレスサービスの設定が間違っています。 ● 有線ポートがネットワークに接続されていません。 ● 次のリストには含まれていません。 1. 許可装置リスト。 2. 禁止装置リスト。 3. 信頼できる OUI リスト。
未分類AP	分類を特定できないPA	ー

検出された AP は以下の手順に従って分類されます。

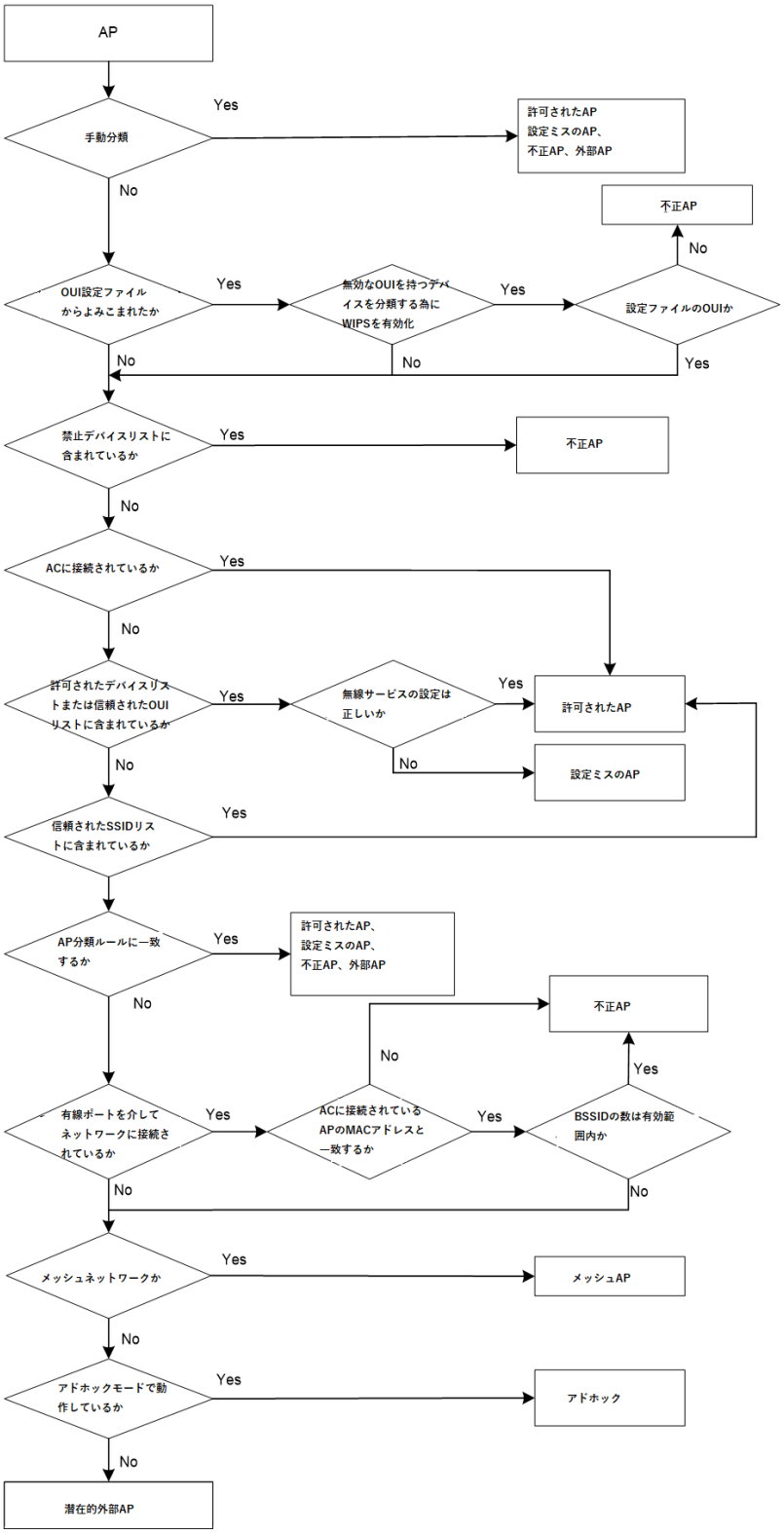


図 8-1 AP 分類フロー

8.3.2 クライアント種別

表 8-3に示すように、WIPS はあらかじめ決められた分類ポリシーに応じて、検出されたクラオアントを分類します。

表 8-3 クライアント種別

種別	説明	分類ルール
許可クライアント	WLANで許可されているクライアント	● 禁止装置リストに該当し、許可APに接続しています。 ● 認証に成功し、許可APに接続しています。
無許可クライアント	WLANで使用できないクライアント	● 禁止装置リストに該当します。 ● 不正APに接続しています。 ● OUIコンフィグファイルに該当しません。
関連付けが不正なクライアント	無許可APに接続しているクライアント	許可装置リストに該当するが、無許可APに接続しています。誤接続したクライアントは、セキュリティ脅威をネットワークにもたらす可能性があります。
未分類クライアント	種別を特定できないクライアント	―

検出されたクライアントは以下の手順に従って分類されます。

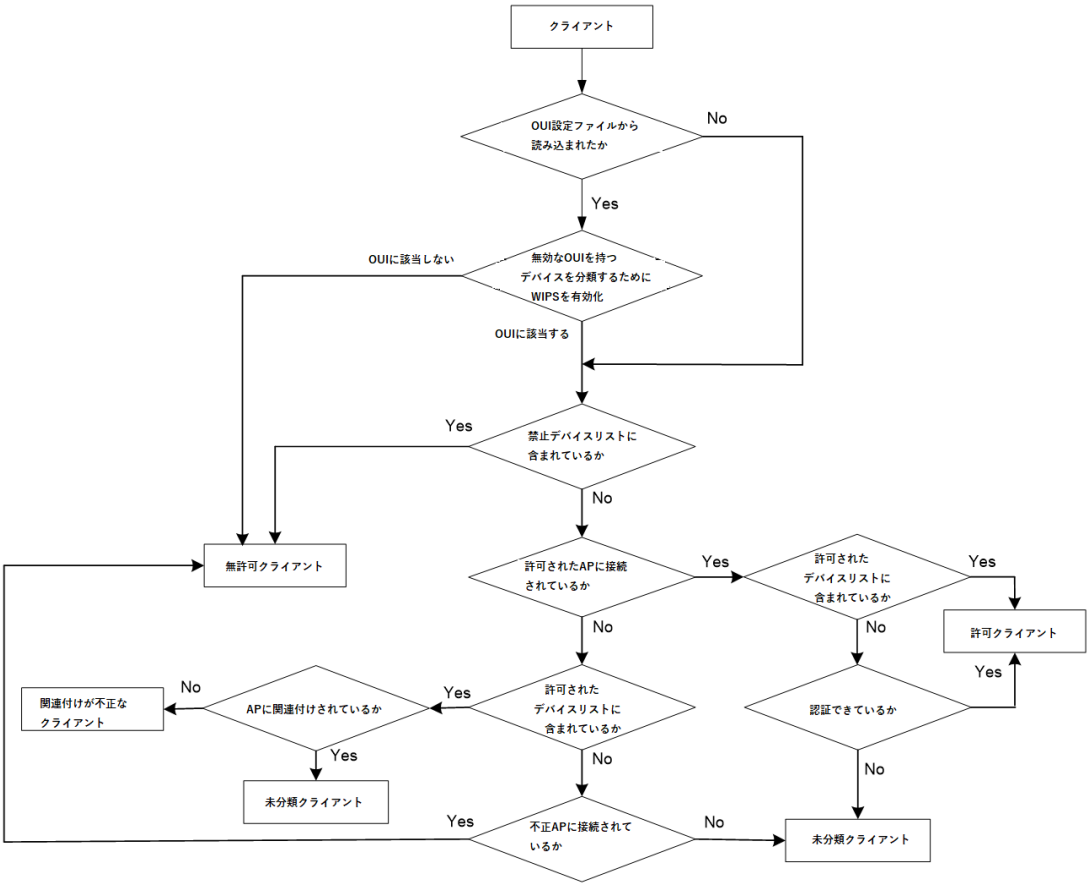


図 8-2 クライアントの分類フロー

8.4 対策

WLAN は不正装置からの攻撃の影響を受けやすく、攻撃によりセキュリティ上の問題が引き起こされる可能性があります。WIPS では、不正装置に対する対策を実行できます。

8.5 WIPS設定作業リスト

作業リスト
（必須設定項目）WIPSの有効化

作業リスト
（オプション設定項目）無線攻撃検出の設定 ● フラッド攻撃検出の設定 ● 不正パケット検出の設定 ● 装置エントリ攻撃検出の設定 ● その他の攻撃に対する検出設定 ● 攻撃検知ポリシーの適用 ● シグネチャにもとづいたユーザ定義攻撃検出の設定 ● アラーム無視装置リストの設定
（オプション設定項目）装置種別の設定 ● 分類ポリシーの設定 ● 分類ポリシーの適用 （オプション設定項目）対策の設定 ● 対策ポリシーの設定 ● 対策ポリシーの適用
（オプション設定項目）クライアントプロービングの有効化

8.6 WIPS有効化

🕮 **メモ：**

無線通信と WIPS センサは同じ Radio 上での併用をサポートしています。
無線通信と WIPS センサを併用している Radio の WIPS スキャンは、通信への影響を与えないために、端末との通信のないタイミングで行われます。
また、無線通信と WIPS センサが有効な Radio に対する通信、および端末の接続に対しては、通信を優先するため WIPS 検出はできません。

WIPS センサとして動作させるために、AP の radio で WIPS を有効にします。

WIPS は、ワイヤレスネットワークを複数の仮想セキュリティドメイン（VSD）に分割し、それぞれに異なるポリシーを適用することができます。

AP の radio で WIPS を有効化する前に、AP を VSD に追加する必要があります。

8.6.1 radio view での WIPS の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	APを作成するときは、モデル名を指定する必要があります。
3． AP を VSD に追加する	**wips virtual-security-domain** *vsd-name*	デフォルト：設定なし
4． radio view に移行する	**radio** *radio-id*	ー

操作	コマンド	補足
5． WIPS を有効にする	**wips enable**	デフォルト：無効

8.6.2 AP group radio view での WIPS の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP view に移行する	**wlan ap-group** *group-name*	―
3． AP を VSD に追加する	**wips virtual-security-domain** *vsd-name*	デフォルト：設定なし
4． AP model view に移行する	**ap-model** *ap-model*	―
5． radio view に移行する	**radio** *radio-id*	―
6． WIPS を有効にする	**wips enable**	デフォルト：無効

8.7 無線攻撃検出の設定

無線攻撃検出を設定する場合、最初に攻撃検出ポリシーを作成し、指定した攻撃検出を許可する必要があります。

8.7.1 フラッド攻撃検出の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． WIPS view に移行する	**wips**	―
3． 攻撃検出ポリシーを作成し、その view に移行する	**detect policy** *policy-name*	デフォルト：設定なし
4． アソシエーション要求用フラッド攻撃検出を設定する	**flood association-request** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
5． 認証要求用フラッド攻撃検出を設定する	**flood authentication** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
6． ビーコン用フラッド攻撃検出を設定する	**flood beacon** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
7． ブロック ACK 用フラッド攻撃検出を設定する	**flood block-ack** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
8． RTS 用フラッド攻撃検出を設定する	**flood rts** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
9． CTS 用フラッド攻撃検出を設定する	**flood cts** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効

操作	コマンド	補足
10．認証取り消し（Deauthentication）用フラッド攻撃検出を設定する	**flood deauthentication** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
11．アソシエーション解除用フラッド攻撃検出を設定する	**flood disassociation** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
12．EAPOL-start 用フラッド攻撃検出を設定する	**flood eapol-start** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
13．ヌルデータ用フラッド攻撃検出を設定する	**flood null data** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
14．プローブ要求用フラッド攻撃検出を設定する	**flood probe-request** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
15．再アソシエーション要求用フラッド攻撃検出を設定する	**flood reassociation-request** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
16．EAPOL-logoff 用フラッド攻撃検出を設定する	**flood eapol-logoff** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*]*	デフォルト：無効
17．EAP-failure 用フラッド攻撃検出を設定する	**flood eap-failure** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
18．EAPOL-success 用フラッド攻撃検出を設定する	**flood eap-success** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効

8.7.2 不正パケット検出の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． WIPS view に移行する	**wips**	―
3． 攻撃検出ポリシーを作成し、その view に移行する	**detect policy** *policy-name*	デフォルト：設定なし
4． 重複 IE 検出を設定する	**malformed duplicated-ie** [**quiet** *quiet-value*]	デフォルト：無効
5． FATA-Jack 検出を設定する	**malformed fata-jack** [**quiet** *quiet-value*]	デフォルト：無効
6． 異常な IBSS と ESS 設定検出を設定する	**malformed illegal-ibss-ess** [**quiet** *quiet-value*]	デフォルト：無効
7． 無効ソースアドレス検出を設定する	**malformed invalid-address-combination** [**quiet** *quiet-value*]	デフォルト：無効
8． 不正アソシエーション要求フレーム検出を設定する	**malformed invalid-assoc-req** [**quiet** *quiet-value*]	デフォルト：無効
9． 不正認証要求フレーム検出を設定する	**malformed invalid-auth** [**quiet** *quiet-value*]	デフォルト：無効

操作	コマンド	補足
10．無効な認証取り消し（Deauthentication）コード検出を設定する	**malformed invalid-deauth-code** [**quiet** *quiet-value*]	デフォルト：無効
11．無効なアソシエーション解除コード検出を設定する	**malformed invalid-disassoc-code** [**quiet** *quiet-value*]	デフォルト：無効
12．無効な IE 長検出を設定する	**malformed invalid-ie-length** [**quiet** *quiet-value*]	デフォルト：無効
13．不正な HT IE 検出を設定する	**malformed invalid-ht-ie** [**quiet** *quiet-value*]	デフォルト：無効
14．無効なパケット長検出を設定する	**malformed invalid-pkt-length** [**quiet** *quiet-value*]	デフォルト：無効
15．継続時間超過検出を設定する	**malformed large-duration** [**quiet** *quiet-value* | threshold value]	デフォルト：無効
16．不正なプローブ応答フレーム検出を設定する	**malformed null-probe-resp** [**quiet** *quiet-value*]	デフォルト：無効
17．EAPOL key 長超過検出を設定する	**malformed overflow-eapol-key** [**quiet** *quiet-value*]	デフォルト：無効
18．SSID データ長超過検出を設定する	**malformed overflow-ssid** [**quiet** *quiet-value*]	デフォルト：無効
19．冗長 IE 検出を設定する	**malformed redundant-ie** [**quiet** *quiet-value*]	デフォルト：無効

8.7.3 装置エントリ攻撃検出の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． WIPS view に移行する	**wips**	―
3． 攻撃検出ポリシーを作成し、その view に移行する	**detect policy** *policy-name*	デフォルト：設定なし
4． クライアントエントリの学習レートを設定する	**client-rate-limit** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：統計収集間隔は60秒、待機時間は1200秒、学習するクライアントエントリのしきい値は512です。
5． クライアントエントリタイマを設定する	**client-timer inactive** *inactive-value* **aging** *aging-value*	デフォルト：非アクティブ時間は300秒、エージングタイマは600秒です。 非アクティブ時間内にクライアントがパケットを送受信しない場合、WIPSはクライアントを非アクティブ状態に設定します。クライアントがエージングタイム内にフレームを送受信しない場合、WIPSはそのエントリを削除します。

操作	コマンド	補足
6. APエントリの学習レートを設定する	**ap-rate-limit** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：統計収集間隔は60秒、待機時間は1200秒、学習するAPエントリのしきい値は64です。
7. APエントリタイマを設定する	**ap-timer** [**inactive** *inactive-value* **aging** *aging-value*]	デフォルト：APの非アクティブ時間は300秒、エージングタイマは600秒です。 APが非アクティブ時間内にパケットを送受信しない場合、WIPSはAPを非アクティブ状態に設定します。 APがエージングタイム内にフレームを送受信しない場合、WIPSはそのエントリを削除します。

8.7.4 その他の攻撃に対する検出設定

操作	コマンド	補足
1. system viewに移行する	**system-view**	ー
2. WIPS viewに移行する	**wips**	ー
3. 攻撃検出ポリシーを作成し、そのviewに移行する	**detect policy** *policy-name*	デフォルト：設定なし
4. ライアントMACアドレスなりすまし攻撃検出を設定する	**client-spoofing** [**quiet** *quiet-value*]	デフォルト：無効
5. AP MACアドレスなりすまし攻撃検出を設定する	**ap-spoofing** [**quiet** *quiet-value*]	デフォルト：無効
6. weak IV検出を設定する	**weak-iv** [**quiet** *quiet-value*]	デフォルト：無効
7. Omerta攻撃検出を設定する	**omerta** [**quiet** *quiet-value*]	デフォルト：無効
8. ブロードキャストアソシエーション解除攻撃検出を設定する	**disassociation-broadcast** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
9. ブロードキャスト認証取り消し（Deauthentication）攻撃検出を設定する	**deauthentication-broadcast** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：無効
10. 40MHzの帯域幅モードを使用禁止にしたクライアント検出を設定する	**ht-40mhz-intolerance** [**quiet** *quiet-value*]	デフォルト：無効
11. パワーセーブ攻撃検出を設定する	**power-save** [**interval** *interval-value* | **minoffpacket** *packet-value* | **onoffpercent** *percent-value* | **quiet** *quiet-value*] *	デフォルト：無効
12. 許可チャネルリストを設定する	**permit-channel** *channel-id-list*	デフォルト：設定なし

操作	コマンド	補足
13．禁止チャネル検出を設定する	**prohibited-channel** [**quiet** *quiet-value*]	デフォルト：無効
14．Windows ブリッジ検出を設定する	**windows-bridge** [**quiet** *quiet-value*]	デフォルト：無効
15．未暗号許可 AP 検出を設定する	**unencrypted-authorized-ap** [**quiet** *quiet-value*]	デフォルト：無効
16．未暗号許可クライアント検出を設定する	**unencrypted-trust-client** [**quiet** *quiet-value*]	デフォルト：無効
17．ソフト AP 検出を設定する	**soft-ap** [**convert-time** *time-value*]	デフォルト：無効
18．AP なりすまし攻撃検出を設定する	**ap-impersonation** [**quiet** *quiet-value*]	デフォルトで：無効
19．HT-グリーンフィールドモード AP 検出を設定する	**ht-greenfield** [**quiet** *quiet-value*]	デフォルト：無効
20．アソシエーション/再アソシエーション DoS 攻撃検出を設定する	**association-table-overflow** [**quiet** *quiet-value*]	デフォルト：無効
21．無線ブリッジ検出を設定する	**wireless-bridge** [**quiet** *quiet-value*]	デフォルト：無効
22．AP フラッド攻撃検出を設定する	**ap-flood** [**apnum** *apnum-value* | **exceed** *exceed-value* | **quiet** *quiet-value*] *	デフォルト：無効
23．ハニーポット AP 検出を設定する	**honeypot-ap** [**similarity similarity-value** | **quiet** *quiet-value*] *	デフォルト：無効
24．MITM 攻撃検出を設定する	**man-in-the-middle** [**quiet** *quiet-value*]	デフォルト：無効
25．チャネル変更検出を設定する	**ap-channel-change** [**quiet** *quiet-value*]	デフォルト：無効
26．WIPS view に戻る	**quit**	ー
27．コンフィグファイルからホットスポット情報をインポートする	**import hotspot** *file-name*	デフォルト：ホットスポット情報はインポートされません。
28．攻撃検出ポリシーを作成し、その view に移行する	**detect policy** *policy-name*	デフォルト：設定なし
29．ホットスポット攻撃検出を設定する	**hotspot-attack** [**quiet** *quiet-value*]	デフォルト：無効

8.7.5 攻撃検知ポリシーの適用

操作	コマンド	補足
1．system view に移行する	**system-view**	ー
2．WIPS view に移行する	**wips**	ー
3．VSD を作成し、その view に移行する	**virtual-security-domain** *vsd-name*	デフォルト：設定なし

操作	コマンド	補足
4． VSD に攻撃検出ポリシーを適用する	**apply detect policy** *policy-name*	デフォルト：設定なし VSDに適用される攻撃検出ポリシーは、VSD内のすべての無線に適用されます。

8.7.6 シグネチャにもとづいたユーザ定義攻撃検出の設定

I. シグネチャ設定

WIPS は、検出されたパケットを設定済みシグネチャと昇順 ID で一致するまで照合します。

シグネチャに対して 1 つまたは複数のサブシグネチャを設定できます。 パケットは、シグネチャのすべてのサブシグネチャと一致する場合にのみ、シグニチャと一致したとみなします。

以下にシグネチャ設定をする手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． WIPS view に移行する	**wips**	―
3． シグネチャを作成し、その view に移行する	**signature rule** *rule-id*	デフォルト：設定なし
4． フレームのフレームタイプに一致するサブシグネチャを設定する	**frame-type** { **control** | **data** | **management** [**frame-subtype** { **association-request** | **association-response** | **authentication** | **beacon** | **deauthentication** | **disassociation** | **probe-request** }] }	デフォルト：設定なし
5． フレームの MAC アドレスに一致するサブシグネチャを設定する	**mac-address** { **bssid** | **destination** | **source** } *mac-address*	デフォルト：設定なし
6． フレームのシーケンス番号に一致するサブシグネチャを設定する	**seq-number** *seq-value1* [**to** *seq-value2*]	デフォルト：設定なし
7． フレームの SSID 長に一致するサブシグネチャを設定する	**ssid-length** *length-value1* [**to** *length-value2*]	デフォルト：設定なし
8． フレームの SSID に一致するサブシグネチャを設定する	**ssid** [**case-sensitive**] [**not**] { **equal** | **include** } *string*	デフォルト：設定なし
9． フレームの指定ビットに一致するサブシグネチャを設定する	**pattern** *pattern-number* **offset** *offset-value* **mask** *hex-value value1* [**to** *value2*] [**from-payload**]	デフォルト：設定なし

II. シグネチャの適用

シグネチャを適用するには、シグネチャをシグネチャポリシーに割り当てます。

以下にシグネチャの適用手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. シグネチャポリシーを作成し、その view に移行する	**signature policy** *policy-name*	デフォルト：設定なし
4. 指定シグネチャをシグネチャポリシーに割り当てる	**apply signature rule** *rule-id*	デフォルト：設定なし
5. WIPS でシグネチャに一致するパケットの検出を有効にする	**detect signature** [**interval** *interval-value* | **quiet** *quiet-value* | **threshold** *threshold-value*] *	デフォルト：有効 統計収集間隔は60秒、待機時間は600秒、学習するAPエントリのしきい値は50です。

III. シグネチャポリシーの適用

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. VSD を作成し、その view に移行する	**virtual-security-domain** *vsd-name*	デフォルト：設定なし
4. 指定シグネチャポリシーを VSD に適用する	**apply signature policy** *policy-name*	デフォルト：設定なし

8.7.7 アラーム無視装置リストの設定

アラーム無視装置リストに該当する無線装置の場合、WIPS は、監視のみを行い、アラームを発生しません。

以下にアラーム無視装置リストの設定手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. アラーム無視装置リストに MAC アドレスを追加する	**ignorelist mac-address** *mac-address*	デフォルト：設定なし

8.8 装置種別の設定

無線装置種別設定では、最初に分類ポリシーを作成し、指定装置の種別を設定しなければなりません。

8.8.1 分類ポリシーの設定

以下の方法のいずれかで、WIPS による装置の分類が可能です。

- **自動分類**－装置の MAC アドレス、OUI、SSID を指定リストに追加することにより、WIPS は自動的に装置を分類します。また、WIPS は、ユーザ定義の AP 分類ポリシーを使用して、AP を分類することもできます。
- **手動分類**－装置種別を手動で指定します。手動分類は AP のみ適用可能です。

自動分類と手動分類の両方を設定した場合、手動分類が有効になります。

🕮 **メモ：**

AP を指定する場合は、BSSID(無線の MAC アドレス)を指定してください。

I. 自動装置分類の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WIPS view に移行する	**wips**	―
3. OUI コンフィグファイルから OUI をインポートする	**import oui** *file-name*	デフォルト：設定なし
4. 分類ポリシーを作成し、その view に移行する	**classification policy** *policy-name*	デフォルト：設定なし
5. WIPS で無効 OUI 装置を悪意のある装置に分類する	**invalid-oui-classify illegal**	デフォルト：設定なし
6. 許可装置リストへ MAC アドレスを追加する	**trust mac-address** *mac-address*	デフォルト：設定なし
7. 許可 OUI リストへ OUI を追加する	**trust oui** *oui*	デフォルト：設定なし このコマンドは、APの分類のみに適用されます。
8. 許可 SSID リストへ SSID を追加する	**trust ssid** *ssid-name*	デフォルト：設定なし
9. スタティック禁止装置リストへ MAC アドレスを追加する	**block mac-address** *mac-address*	デフォルト：設定なし
10. 指定 AP 分類ルールを分類ポリシーに割り当てる	**apply ap-classification rule** *rule-id* { **authorized-ap** | { { **external-ap** | **misconfigured-ap** | **rogue-ap** } [**severity-level** *level*] } }	デフォルト：設定なし

II. AP 分類ルールの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WIPS view に移行する	**wips**	―

操作	コマンド	補足
3. AP 分類ルールを作成し、その view に移行する	**ap-classification rule** *rule-id*	デフォルト：設定なし
4. AP の RSSI と一致する AP 分類ルールを設定する	**rssi** *value1* [**to** *value2*]	デフォルト：設定なし
5. AP の無線サービスの SSID と一致する AP 分類ルールを設定する	**ssid** [**case-sensitive**] [**not**] { **equal** | **include** } *ssid-string*	デフォルト：設定なし
6. AP の動作時間と一致する AP 分類ルールを設定する	**up-duration** *value1* [**to** *value2*]	デフォルト：設定なし
7. AP の接続クライアント数と一致する AP 分類ルールを設定する	**client-online** *value1* [**to** *value2*]	デフォルト：設定なし
8. AP を検出するセンサ数と一致する AP 分類ルールを設定する	**discovered-ap** *value1* [**to** *value2*]	デフォルト：設定なし
9. AP が使用するセキュリティモードと一致する AP 分類ルールを設定する	**security** { **equal** | **include** } { **clear** | **wep** | **wpa** | **wpa2** }	デフォルト：設定なし
10. AP が使用する認証モードと一致する AP 分類ルールを設定する	**authentication** { **equal** | **include** } { **802.1x** | **none** | **other** | **psk** }	デフォルト：設定なし
11. AP の OUI 情報と一致する AP 分類ルールを設定する	**oui** *oui-info*	デフォルト：設定なし

III. 手動 AP 分類の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WIPS view に移行する	**wips**	―
3. 分類ポリシーを作成し、その view に移行する	**classification policy** *policy-name*	デフォルト：設定なし
4. 指定された AP カテゴリを設定する	**manual-classify mac-address** *mac-address* { **authorized-ap** | **external-ap** | **misconfigured-ap** | **rogue-ap** }	デフォルト：設定なし

8.8.2 分類ポリシーの適用

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. WIPS view に移行する	**wips**	―
3. VSD view に移行する	**virtual-security-domain** *vsd-name*	デフォルト：設定なし

操作	コマンド	補足
4. VSD に分類ポリシーを適用する	**apply classification policy** *policy-name*	デフォルト：設定なし VSDに適用される分類ポリシーは、VSD内のすべての無線に適用されます。

8.9 対策の設定

不正装置に対策を行うには、まず対策ポリシーを作成し、WIPS を有効にする必要があります。

8.9.1 対策ポリシーの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WIPS view に移行する	**wips**	ー
3. 対策ポリシーを作成し、その view に移行する	**countermeasure policy** *policy-name*	デフォルト：設定なし
4. WIPS の外部 AP 対策を有効にする	**countermeasure external-ap**	デフォルト：無効
5. WIPS の未設定 AP 対策を有効にする	**countermeasure misconfigured-ap**	デフォルト：無効
6. WIPS の誤接続クライアント対策を有効にする	**countermeasure misassociation-client**	デフォルト：無効
7. WIPS の潜在的外部 AP 対策を有効にする	**countermeasure potential-external-ap**	デフォルト：無効
8. WIPS の潜在的許可 AP 対策を有効にする	**countermeasure potential-authorized-ap**	デフォルト：無効
9. WIPS の潜在的不正 AP 対策を有効にする	**countermeasure potential-rogue-ap**	デフォルト：無効
10. WIPS の不正 AP 対策を有効にする	**countermeasure rogue-ap**	デフォルト：無効
11. WIPS の無許可クライアント対策を有効にする	**countermeasure unauthorized-client**	デフォルト：無効
12. WIPS の未分類 AP 対策を有効にする	**countermeasure uncategorized-ap**	デフォルト：無効
13. WIPS の未分類クライアント対策を有効にする	**countermeasure uncategorized-client**	デフォルト：無効
14. WIPS の指定装置対策を有効にする	**countermeasure mac-address** *mac-address*	デフォルト：無効
15. WIPS のアドホック装置対策を有効にする	**countermeasure adhoc**	デフォルト：無効
16. 認証取り消しアタックをブロードキャストする装置対策を有効にする	**countermeasure attack deauth-broadcast**	デフォルト：無効

操作	コマンド	補足
17．アソシエーション解除アタックをブロードキャストする装置対策を有効にする	**countermeasure attack disassoc-broadcast**	デフォルト：無効
18．WIPS のハニーポット AP 対策を有効にする	**countermeasure attack honeypot-ap**	デフォルト：無効
19．WIPS ホットスポット攻撃の対策を有効にする	**countermeasure attack hotspot-attack**	デフォルト：無効
20．40MHz 帯域幅モードが無効の装置対策を有効にする	**countermeasure attack ht-40-mhz-intolerance**	デフォルト：無効
21．不正パケットを送信する装置対策を有効にする	**countermeasure attack malformed-packet**	デフォルト：無効
22．WIPS の MITM 攻撃対策を有効にする	**countermeasure attack man-in-the-middle**	デフォルト：無効
23．WIPS の Omerta 攻撃対策を有効にする	**countermeasure attack omerta**	デフォルト：無効
24．WIPS のパワーセーブ攻撃対策を有効にする	**countermeasure attack power-save**	デフォルト：無効
25．WIPS のソフト AP 対策を有効にする	**countermeasure attack soft-ap**	デフォルト：無効
26．未暗号化のフレームを送信する許可クライアント対策を有効にする	**countermeasure attack unencrypted-trust-client**	デフォルト：無効
27．Weak IV を使用する装置対策を有効にする	**countermeasure attack weak-iv**	デフォルト：無効
28．Windows ブリッジ攻撃対策を有効にする	**countermeasure attack windows-bridge**	デフォルト：無効
29．WIPS の全検出攻撃対応対策を有効にする	**countermeasure attack all**	デフォルト：無効
30．WIPS の全攻撃検出用センサの攻撃対応対策を有効にする	**select sensor all**	デフォルト：最後に攻撃検出したセンサのみが、攻撃対策を行います。

8.9.2 対策ポリシーの適用

操作	コマンド	補足
1．　system view に移行する	**system-view**	―
2．　WIPS view に移行する	**wips**	―
3．　VSD を作成し、その view に移行する	**virtual-security-domain** *vsd-name*	デフォルト：設定なし
4．　VSD に対策ポリシーを適用する	**apply countermeasure policy** *policy-name*	デフォルト：設定なし VSDに適用される対策ポリシーは、VSD内のすべての無線に適用されます。

8.10 WIPSの表示と維持

すべての view で **display** コマンドを実行し、user view で **reset** コマンドを実行できます。

操作	コマンド
全センサに関する情報を表示する	**display wips sensor**
センサが収集した攻撃検出情報を表示する	**display wips statistics** [**receive** | **virtual-security-domain** *vsd-name*]
VSDで検出された無線装置情報を表示する	**display wips virtual-security-domain** *vsd-name* **device** [**ap** [**adhoc** | **authorized** | **external** | **misconfigured** | **potential-authorized** | **potential-external** | **potential-rogue** | **rogue**] | **client** [[**dissociative-client**] [**authorized** | **misassociation** | **unauthorized** | **uncategorized**]] | **mac-address** *mac-address*] [**verbose**]
検出したNAT設定クライアント情報を表示する	**display wlan nat-detect [mac-address** *mac-address* **]**
全センサ受信情報を削除する	**reset wips statistics**
VSDの学習されたAPエントリまたはクライアントエントリを削除する	**reset wips virtual-security-domain** *vsd-name* { **ap** { **all** | **mac-address** *mac-address* } | **client** { **all** | **mac-address** *mac-address* } | **all** }
検出したNAT設定気裏慰安と情報を消去する	**reset wlan nat-detect**

8.11 WIPS設定例

8.11.1 装置の分類の設定例

I. ネットワーク要件

図 8-3に示すように、センサはスイッチ経由で AC と接続します。AP1 と AP2 は SSID abc を設定してクライアントに無線サービスを提供します。以下のタスクを実行してください。

- Radio の通信状況の影響を受けずに WIPS 検出を行うためにセンサ用 AP を用意します。
- 無線装置種別を設定して、静的禁止装置リストに MAC アドレス 000f-1c35-12a5 を追加し、許可 SSID リストに SSID abc を追加します。

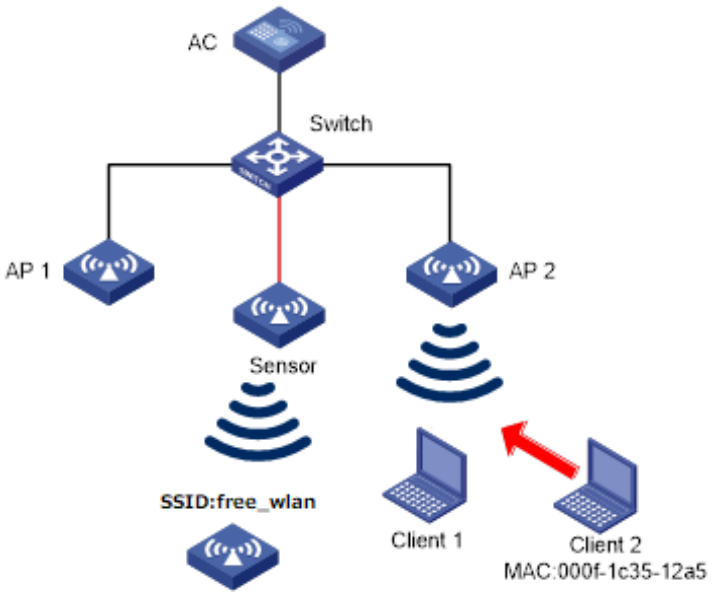


図 8-3 ネットワーク図

II. 設定手順

AC の無線サービスを設定します。（詳細は省略します。）

無線サービスの設定については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN アクセスの設定"* を参照してください。

VSD vsd1 を作成します。

```
<AC> system-view
[AC] wips
[AC-wips] virtual-security-domain vsd1
[AP-wips-vsd-vsd1] quit
[AC-wips] quit
```

AP Sensor を作成し、この AP 用 WIPS を有効にします。

```
[AC] wlan ap Sensor model QX-W1020
[AC-wlan-ap-Sensor] serial-id 210235A1GQB139000435
[AC-wlan-ap-Sensor] radio 1
[AC-wlan-ap-Sensor-radio-1] radio enable
[AC-wlan-ap-Sensor-radio-1] wips enable
[AC-wlan-ap-Sensor-radio-1] quit
```

AP Sensor を VSD vsd1 に追加します。

```
[AC-wlan-ap-Sensor] wips virtual-security-domain vsd1
```

```
[AC-wlan-ap-Sensor] quit
```

分類ポリシーclass1 を作成し、禁止装置リストにクライアント 2 の MAC アドレスを追加します。

```
[AC] wips
[AC-wips] classification policy class1
[AC-wips-cls-class1] block mac-address 000f-1c35-12a5
[AC-wips-cls-class1] trust ssid abc
[AC-wips-cls-class1] quit
```

分類ポリシーclass1 を VSD vsd1 に適用します。

```
[AC-wips] virtual-security-domain vsd1
[AC-wips-vsd-vsd1] apply classification policy class1
[AC-wips-vsd-vsd1] quit
```

対策ポリシーprotect を作成し、無許可クライアントや潜在的外部 AP 用対策を行うように WIPS を有効にします。

```
[AC-wips] countermeasure policy protect
[AC-wips-cms-protect] countermeasure unauthorized-client
[AC-wips-cms-protect] countermeasure potential-external-ap
[AC-wips-cms-protect] quit
```

対策ポリシーprotect を VSD vsd1 に適用します。

```
[AC-wips] virtual-security-domain vsd1
[AC-wips-vsd-vsd1] apply countermeasure policy protect
[AC-wips-vsd-vsd1] quit
[AC-wips] quit
```

III. 設定の確認

VSD vsd1 の無線装置分類情報を表示します。

```
[AC] display wips virtual-security-domain vsd1 device
Total 3 detected devices in virtual-security-domain vsd1

Class: Auth - authorization; Ext - extern; Mis - mistake;
       Unauth - unauthorized; Uncate - uncategorized;
       (A) - associate; (C) - config; (P) - potential

MAC address    Type   Class    Duration    Sensors Channel Status
000f-e200-5829 AP     Auth     00h 10m 24s 1       11      Active
000f-e228-2528 AP     Auth     00h 10m 04s 1       11      Active
000f-e223-1616 AP     Ext(P)   00h 10m 46s 1       11      Active
000f-1c35-12a5 Client Unauth   00h 10m 02s 1       11      Active
000f-e201-0102 Client Auth     00h 10m 02s 1       11      Active
```

この例は、MAC アドレス 000f-e223-1616 を持つ AP が潜在的外部 AP として分類され、MAC アドレス 000f-1c35-12a5 を持つクライアントが無許可クライアントとして分類されることを示します。

WIPS が装置に対して行った対策情報を表示します。

```
[AC] display wips virtual-security-domain vsd1 countermeasure record
Total 2 times countermeasure, current 2 countermeasure record in
virtual-security-domain vsd1

Class: Auth - authorization; Ext - extern; Mis - mistake;
       Unauth - unauthorized; Uncate - uncategorized;
       (A) - associate; (C) - config; (P) - potential

MAC address    Type   Class    Sensor name          Radio ID   Time
000f-e200-5829 AP     Auth     Sensor               1          2014-06-03/09:30:25
000f-e228-2528 AP     Auth     Sensor               1          2014-06-03/19:31:56
000f-e223-1616 AP     Ext(P)   Sensor               1          2014-06-03/10:30:36
000f-1c35-12a5 Client Unauth   Sensor               1          2014-06-03/09:13:26
000f-e201-0102 Client Auth     Sensor               1          2014-06-03/09:33:46
```

この例は、WIPS が MAC アドレス 000f-1c35-12a5 を持つ無許可クライアントと MAC アドレス 000f-e223-1616 を持つ潜在的外部 AP に対して対策を取ったことを示します。

8.11.2 不正パケットとフラッド攻撃の検出例

I. ネットワーク要件

図 8-4に示すように、センサとして 2 つの AP をスイッチ経由で AC と接続してください。センサ 1 とセンサ 2 を VSD VSD_1 に追加してください。重複 IE の不正パケット、または、ビーコンフラッド攻撃を検出した場合にアラームを発生するように、不正パケットとフラッド攻撃用 WIPS を有効にします。

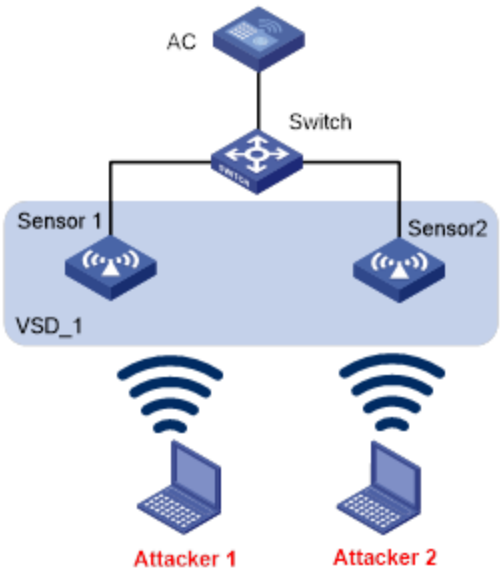


図 8-4 ネットワーク図

II. 設定手順

AC の無線サービスを設定します。（詳細は省略します。）

無線サービスの設定については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN アクセスの設定"* を参照してください。

AP sensor1 を作成し、この AP 用 WIPS を有効にします。

```
<AC> system-view
[AC] wlan ap sensor1 model QX-W1020
[AC-wlan-ap-sensor1] serial-id 210235A1GQB139000435
[AC-wlan-ap-sensor1] radio 1
[AC-wlan-ap-sensor1-radio-1] radio enable
[AC-wlan-ap-sensor1-radio-1] wips enable
[AC-wlan-ap-sensor1-radio-1] return
```

AP sensor2 を作成し、この AP 用 WIPS を有効化します。

```
<AC> system-view
[AC] wlan ap sensor2 model QX-W1020
[AC-wlan-ap-sensor2] serial-id 210235A1GQB139000436
[AC-wlan-ap-sensor2] radio 1
[AC-wlan-ap-sensor2-radio-1] radio enable
[AC-wlan-ap-sensor2-radio-1] wips enable
[AC-wlan-ap-sensor2-radio-1] quit
[AC-wlan-ap-sensor2] quit
```

VSD VSD_1 を作成します。

```
[AC] wips
[AC-wips] virtual-security-domain VSD_1
[AP-wips-vsd-VSD_1] quit
```

攻撃検出ポリシーdtc1 を作成します。

```
[AC-wips] detect policy dtc1
```

重複 IE の不正パケット検出を有効にし、待機時間を 50 秒に設定します。

```
[AC-wips-dtc-dtc1] malformed duplicated-ie quiet 50
```

ビーコンフラッド攻撃検出を有効にし、統計間隔、しきい値、待機時間を 100 秒、200、50 秒に設定します。

```
[AC-wips-dtc-dtc1] flood beacon interval 100 quiet 50 threshold 200
[AC-wips-dtc-dtc1] quit
```

攻撃検出ポリシーdtc1 を VSD VSD_1 に適用します。

```
[AC-wips] virtual-security-domain VSD_1
[AC-wips-vsd-VSD_1] apply detect policy dtc1
[AC-wips-vsd-VSD_1] quit
[AC-wips] quit
```

AP sensor1 を VSD VSD_1 に追加します。

```
[AC] wlan ap sensor1
[AC-wlan-ap-sensor1] wips virtual-security-domain VSD_1
[AC-wlan-ap-sensor1] quit
```

AP sensor2 を VSD VSD_1 に追加します。

```
[AC] wlan ap sensor2
[AC-wlan-ap-sensor2] wips virtual-security-domain VSD_1
[AC-wlan-ap-sensor2] return
```

III. 設定の確認

WIPS が、WLAN で何も攻撃を検出していない状態でパケット統計情報を表示してください。この例では、不正パケットもフラッド攻撃メッセージも存在していないことを示します。

```
<AC> display wips statistics receive
Information from sensor 1
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
```

```
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
Information from sensor 2
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
```

WIPS が、ビーコンフラッド攻撃と重複 IE の不正パケットを検出した状態でパケット統計を表示してください。この例では、重複 IE の不正パケット 28、ビーコンフラッド攻撃メッセージ 18 を検出したことを示します。

<AC> display wips statistics receive

```
Information from sensor 1
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 18
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
```

```
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
Information from sensor 2
Information about attack statistics:
Detected association-request flood messages: 0
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 28
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 0
```

8.11.3 シグネチャベースのユーザ定義攻撃検出設定例

I. ネットワーク要件

図 8-5に示すように、AP1 と AP2 に SSID abc を設定し、クライアントに無線サービスを提供します。SSID が abc ではないビーコンフレームを検出した場合、アラームを発生するシグネチャ設定を行ったセンサ用 WIPS を有効にします。

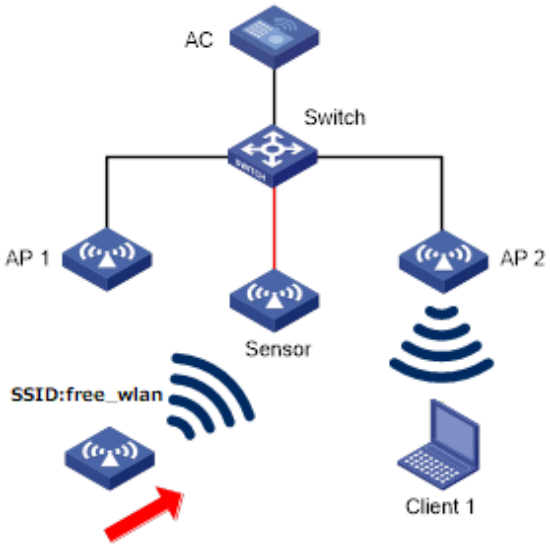


図 8-5 ネットワーク図

II. 設定手順

AC の無線サービスを設定します。（詳細は省略します。）

無線サービスの設定については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“WLAN アクセスの設定”* を参照してください。

AP sensor1 を作成し、この AP 用 WIPS を有効にします。

```
<AC> system-view
[AC] wlan ap sensor1 model QX-W1020
[AC-wlan-ap-sensor1] serial-id 210235A1GQB139000435
[AC-wlan-ap-sensor1] radio 1
[AC-wlan-ap-sensor1-radio-1] radio enable
[AC-wlan-ap-sensor1-radio-1] wips enable
[AC-wlan-ap-sensor1-radio-1] quit
[AC-wlan-ap-sensor1 ] quit
```

VSD vsd1 を作成します。

```
[AC] wips
```

```
[AC-wips] virtual-security-domain vsd1
[AC-wips] quit
```

AP sensor1 を VSD vsd1 に追加します。

```
[AC] wlan ap sensor1
[AC-wlan-ap-sensor1] wips virtual-security-domain vsd1
[AC-wlan-ap-sensor1] quit
```

シグネチャ 1 を作成し、ビーコンフレームでかつ SSID が abc ではないフレームと一致するというサブシグネチャを設定します。

```
[AC] wips
[AC-wips] signature rule 1
[AC-wips-sig-rule-1] frame-type management frame-subtype beacon
[AC-wips-sig-rule-1] ssid not equal abc
[AC-wips-sig-rule-1] quit
```

シグネチャポリシーsig1 を作成し、シグネチャ 1 をシグネチャポリシーsig1 に割り当てます。

```
[AC-wips] signature policy sig1
[AC-wips-sig-sig1] apply signature rule 1
```

シグネチャと一致したパケットを検出するように WIPS を有効にし、統計収集間隔、待機時間、アラームしきい値を、それぞれ 5 秒、60 秒、60 に設定します。

```
[AC-wips-sig-sig1] detect signature interval 5 quiet 60 threshold 60
[AC-wips-sig-sig1] quit
```

シグネチャポリシーsig1 を VSD vsd1 に適用します。

```
[AC] wips
[AC-wips] virtual-security-domain vsd1
[AP-wips-vsd-vsd1] apply signature policy sig1
[AP-wips-vsd-vsd1] quit
```

III. 設定の確認

センサが SSID free_wlan の無線サービスを検出したときに、AC がセンサからアラームを受信していることを確認します。

```
WIPS/5/WIPS_SIGNATURE: -VSD=vsd1-RuleID=1; Signature rule matched.
```

センサから収集した攻撃検出情報を表示してください。この例では、シグネチャと一致したパケットを 26 パケット検出したことを示します。

```
[AC] display wips statistics receive
Information from sensor
Information about attack statistics:
Detected association-request flood messages: 0
```

```
Detected authentication flood messages: 0
Detected beacon flood messages: 0
Detected block-ack flood messages: 0
Detected cts flood messages: 0
Detected deauthentication flood messages: 0
Detected disassociation flood messages: 0
Detected eapol-start flood messages: 0
Detected null-data flood messages: 0
Detected probe-request flood messages: 0
Detected reassociation-request flood messages: 0
Detected rts flood messages: 0
Detected duplicated-ie messages: 0
Detected fata-jack messages: 0
Detected illegal-ibss-ess messages: 0
Detected invalid-address-combination messages: 0
Detected invalid-assoc-req messages: 0
Detected invalid-auth messages: 0
Detected invalid-deauth-code messages: 0
Detected invalid-disassoc-code messages: 0
Detected invalid-ht-ie messages: 0
Detected invalid-ie-length messages: 0
Detected invalid-pkt-length messages: 0
Detected large-duration messages: 0
Detected null-probe-resp messages: 0
Detected overflow-eapol-key messages: 0
Detected overflow-ssid messages: 0
Detected redundant-ie messages: 0
Detected AP spoof AP messages: 0
Detected AP spoof client messages: 0
Detected AP spoof ad-hoc messages: 0
Detected ad-hoc spoof AP messages: 0
Detected client spoof AP messages: 0
Detected weak IV messages: 0
Detected excess AP messages: 0
Detected excess client messages: 0
Detected sig rule messages: 26
```

目次

9章 WLAN QoSの設定 9-1
9.1 概要 9-1
9.1.1 WMMプロトコル 9-1
9.1.2 帯域保証 9-3
9.1.3 クライアント帯域制限 9-3
9.1.4 プロトコルと標準 9-3
9.2 WMMの設定 9-3
9.2.1 WMMの有効化 9-3
9.2.2 EDCAパラメータの設定 9-4
9.2.3 クライアントのEDCAパラメータ設定（AC-BEまたはAC-BK） 9-5
9.2.4 クライアントのEDCAパラメータ設定（AC-VIまたはAC-VO） 9-6
9.2.5 MU EDCAパラメータの設定 9-6
9.2.6 トラストモードとポートプライオリティの設定 9-7
9.3 SVPマッピングの設定 9-8
9.4 帯域保証の設定 9-9
9.4.1 AP viewでの帯域保証の設定 9-9
9.4.2 AP group viewでの帯域保証の設定 9-9
9.5 クライアント帯域制限 9-10
9.5.1 サービステンプレートベースの帯域制限設定 9-10
9.5.2 無線ベースの帯域制限設定 9-11
9.5.3 クライアントタイプベースの帯域制限設定 9-11
9.6 U-APSDの設定 9-12
9.7 Air Time Fairnessの設定 9-12
9.8 WMMの表示および維持 9-13
9.9 WLAN QoSの設定例 9-14
9.9.1 基本的なWMMの設定例 9-14
9.9.2 トラフィック差別化の設定例 9-16
9.9.3 帯域保証の設定例 9-17
9.9.4 クライアント帯域制限の設定例 9-19
9.9.5 Air Time Fairnessの設定例 9-20

9章 WLAN QoS の設定

この章では、WLAN QoS の設定方法について説明します。

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

9.1 概要

802.11 ネットワークは、コンテンションベースのワイヤレスアクセスを提供します。アプリケーションに QoS サービスを提供するため、IEEE は 802.11 ベースの WLAN 向けに 802.11e を開発しました。

IEEE 802.11e は標準化されていますが、Wi-Fi Alliance は異なるベンダーの QoS 供給装置を相互運用させるために Wi-Fi マルチメディア（WMM）標準を定めました。WMM を使用することで、WLAN で QoS サービスを提供でき、オーディオおよびビデオアプリケーションのパフォーマンスが向上します。

9.1.1 WMM プロトコル

802.11 の DCF（Distributed Coordination Function）では、AP とクライアントが CSMA / CA（ carrier sense multiple access with collision avoidance）アクセスメカニズムを使用する必要があります。AP またはクライアントは、データを転送するためのチャネルを保持する前に、そのチャネルの使用状況を確認します。指定されたチャネルのアイドル時間がタイムアウトすると、AP またはクライアントはコンテンションウィンドウ内のバックオフスロットをランダムに選択してバックオフを実行します。最初にバックオフが終了したデバイスがチャネルを取得します。802.11 では、すべてのデバイスが同じアイドル時間とコンテンションウィンドウを持ちます。そのため、チャネルが競合する場合、すべての通信が平等に扱われることになります。

WMM では QoS サービスを提供するために、データ トラフィックを異なる優先度を持つ 4 つの AC に分割します。優先度の高い AC のトラフィックは、チャネルを使用できる可能性が高くなります。

I. 用語

- **Enhanced distributed channel access**－EDCA は、優先度が高いパケットを優先的に送信しより多くの帯域幅を割り当てる、WMM によって定義されたチャネル競合メカニズムです。
- **Access category**－WMM は、音声トラフィック用の AC-VO、ビデオトラフィック用の AC-VI、ベストエフォートトラフィック用の AC-BE、バックグラウンドトラフィック用の AC-BK の 4 つの AC を定義します。4 つの AC の優先度は降順です。
- **Unscheduled automatic power save delivery**－U-APSD は、クライアントの電力を節約するために WMM によって定義された節電方法です。

II. EDCA パラメータ

- **Arbitration inter-frame spacing number**－802.11 ベースの WLAN は、各クライアントで同じアイドル時間（DIFS）を持ちますが、WMM では AC ごとにアイドル時間を定義します。アイドル時間は、AIFSN が増加するにつれて増加します。
- **Exponent form of CWmin/Exponent form of Cwmax**－ECWmin と ECWmax の 2 つの値が増加するにつれて、バックオフスロットを増加します。
- **Transmission opportunity limit**－TXOP 制限は、競合が発生した後にクライアントがチャネルを保持できる最大時間を指定します。値が大きいほど時間が長くなります。値が 0 の場合、クライアントはチャネルを保持するたびに 1 つのパケットのみ送信することができます。

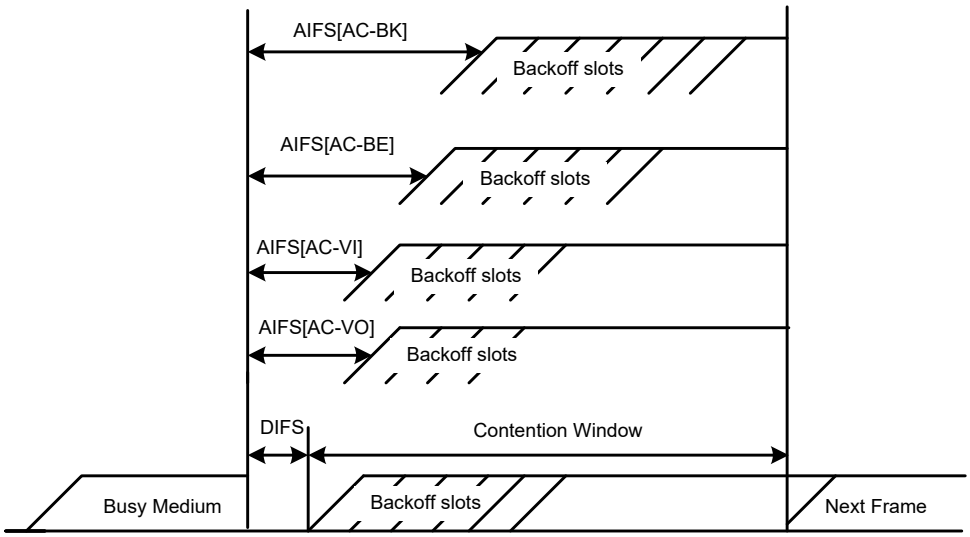


図 9-1 EDCA パラメータ

III. U-APSD 節電方法

U-APSD を使用すると、スリープモードのクライアントは、トリガーパケットを受信した後にのみ、指定された数のパケットを受信することができます。U-APSD は 802.11 APSD 節電方法を改善します。

U-APSD は、WMM を有効にすると自動的に有効になります。なお、ソフトウェアバージョン 7.2.42 を含む以降のソフトウェアでは、**undo u-apsd enable** コマンドにて U-APSD を無効にできます。

IV. ACK ポリシー

WMM では、次の ACK ポリシーが定義されています。

- Normal ACK－受信者は、受信した各ユニキャストパケットの確認応答を行います。
- No ACK－受信者は、無線パケット通信中に受信パケットの確認応答を行いません。このポリシーは、通信品質が高く干渉が弱い環境での伝送効率を向上させます。通信品質が悪化した場合、パケットロス率が増加する可能性があります。802.11n クライアントから送信された A-MPDU パケットの場合、No ACK ポリシーは有効になりません。

9.1.2 帯域保証

この機能は、以下の機能を提供します。

- ネットワークが輻輳していないときは、すべての BSS からのトラフィックが自由に通過できるようにします。
- ネットワークが輻輳しているときは、各 BSS が保証された帯域幅を確保できるようにします。

この機能により、帯域幅の効率化や、WLAN サービス間で帯域幅を公正に使用することができます。たとえば、SSID1、SSID2、SSID3 には、合計帯域幅の 25%、25%、50%を割り当てます。ネットワークが輻輳していない場合、SSID1 は保証された帯域幅に加えて、未使用な帯域幅も使用することができます。ネットワークが輻輳している場合、SSID1 は帯域幅の 25%が保証されます。

この機能は、AP からクライアントへのトラフィックにのみ適用されます。

9.1.3 クライアント帯域制限

この機能は、1 つのクライアントによる帯域幅の積極的な使用を防ぎ、同じ AP に関連づけられているクライアント間で帯域幅を公正に使用することを可能にします。

クライアント帯域制限には、次のいずれかのモードを設定することができます。

- **Dynamic mode**－すべてのクライアントで共有する総帯域幅を設定します。各クライアントの帯域制限は、総帯域幅をオンラインクライアントの数で割ったものとなります。たとえば、総帯域幅が 10Mbps で、5 つのクライアントがオンラインの場合、各クライアントのレート制限は 2Mbps です。
- **Static mode**－各クライアントで使用できる帯域幅を設定します。設定した帯域幅にクライアントの数を掛けた値が AP によって提供することのできる帯域幅を超えた場合、クライアントは設定された帯域幅を使用することができない可能性があります。

9.1.4 プロトコルと標準

- 802.11e-2005, *Amendment 8: Medium Access Control (MAC) Quality of Service Enhancements, IEEE Computer Society, 2005*
- Wi-Fi, *WMM Specification version 1.1, Wi-Fi Alliance, 2005*

9.2 WMMの設定

9.2.1 WMM の有効化

802.11n プロトコルでは、すべての 802.11n クライアントが WLAN QoS をサポートしている必要があります。802.11n クライアントが関連する AP と通信するには、無線が 802.11an または 802.11gn モードで動作しているときに WMM を有効にします。

I. AP view での WMM の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． WMM を有効にする	**wmm enable**	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での WMM の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—
5． WMM を有効にする	**wmm enable**	デフォルト：有効

9.2.2 EDCA パラメータの設定

I. AP view での EDCA パラメータ設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． EDCA パラメータを設定する	**edca radio** { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** } { **ack-policy** { **noack** | **normalack** } | **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での EDCA パラメータ設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—
5． WMM を有効にする	**edca radio** { **ac-be** | **ac-bk** | **ac-vi** | **ac-vo** } { **ack-policy** { **noack** | **normalack** } | **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	デフォルト：EDCAパラメータのデフォルトを表 9-1に示します。

表 9-1 EDCA パラメータのデフォルト値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	6	0
AC-VI	1	3	4	94
AC-VO	1	2	3	47

9.2.3 クライアントの EDCA パラメータ設定（AC-BE または AC-BK）

I. AP view でのクライアントの EDCA パラメータ設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． クライアントの AC-BE キューまたは AC-BK キューの EDCA パラメータを設定する	**edca client** { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	デフォルト：APはAP group viewの設定を使用します。

II. AP group view でのクライアントの EDCA パラメータ設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—
5． クライアントの AC-BE キューまたは AC-BK キューの EDCA パラメータを設定する	**edca client** { **ac-be** | **ac-bk** } { **aifsn** *aifsn-value* | **ecw ecwmin ecwmin-value ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	デフォルト：EDCAパラメータのデフォルトを表 9-2に示します。

表 9-2 クライアントの AC-BE キューまたは AC-BK キューの EDCA パラメータのデフォルト値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-BK	7	4	10	0
AC-BE	3	4	10	0

9.2.4 クライアントの EDCA パラメータ設定（AC-VI または AC-VO）

I. AP view でのクライアントの EDCA パラメータ設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. クライアントの AC-VI キューまたは AC-VO キューの EDCA パラメータを設定する	**edca client** { **ac-vi** | **ac-vo** } { **aifsn** *aifsn-value* | **cac** { **disable** | **enable** } | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	デフォルト：APはAP group viewの設定を使用します。

II. AP group view でのクライアントの EDCA パラメータ設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. クライアントの AC-VI キューまたは AC-VO キューの EDCA パラメータを設定	**edca client** { **ac-vi** | **ac-vo** } { **aifsn** *aifsn-value* | **cac** { **disable** | **enable** } | **ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* | **txoplimit** *txoplimit-value* } *	デフォルト：EDCAパラメータのデフォルトを表 9-3に示します。

表 9-3 クライアントの AC-BI キューまたは AC-VO キューの EDCA パラメータのデフォルト値

AC	AIFSN	ECWmin	ECWmax	TXOP Limit
AC-VI	2	3	4	94
AC-VO	2	2	3	47

9.2.5 MU EDCA パラメータの設定

メモ：

- この機能はソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。
- MU EDCA パラメータは、QX-W1100 シリーズの AP でのみサポートしています。

802.11ax 無線と非 802.11 ax 無線の両方が存在する場合に、クライアントは 802.11ax パケットに対して異なる EDCA パラメータセットを使用して、非 802.11 ax パケットの公平な伝送を保証できます。

MU EDCA パラメータを設定すると、関連付けられた AP が 802.11 ax クライアントをトリガーしてデータを送信するときに、クライアントは MU EDCA パラメータの使用を選択できます。EDCA パラメータと比較して、MU EDCA パラメータは、より大きな aifsn、ecwmin、および ecwmax 値が指定され、待機時間と平均バックオフ時間を増やして 802.11 ax パケットの優先度を下げます。

システムは MU EDCA パラメータを使用するためのタイマーを設定します。タイマーの期限が切れる前に AP がクライアントにデータを送信するようにトリガーすると、タイマーはリセットされます。タイマーの期限が切れると、MU EDCA パラメータの代わりに、EDCA パラメータが 802.11 ax パケットに再び使用されます。

I. AP view での MU EDCA パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. MU EDCA パラメータを設定する	**mu-edca client { ac-be | ac-bk | ac-vi | ac-vo } { aifsn** *aifsn-value* **| ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* **| muedcatimer** *muedcatimer-value* **} ***	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での MU EDCA パラメータの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. MU EDCA パラメータを設定	**mu-edca client { ac-be | ac-bk | ac-vi | ac-vo } { aifsn** *aifsn-value* **| ecw ecwmin** *ecwmin-value* **ecwmax** *ecwmax-value* **| muedcatimer** *muedcatimer-value* **} ***	デフォルト：MU EDCAパラメータは指定されていません

9.2.6 トラストモードとポートプライオリティの設定

以下のトラストモードをサポートしています。

- **Packet trust mode**－プライオリティマッピングには、転送を行うパケットの 802.11e プライオリティを使用します。
- **Port trust mode**－プライオリティマッピングには、設定されたポートプライオリティを使用します。

パケットトラストモードとポートトラストモードは、アップリンクパケットに適用することが可能です。

パケットトラストモードが有効な場合、ポートプライオリティは有効になりません。

I. トラストモードとポートプライオリティの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. パケットトラストモードを有効にする	**qos trust** { **dot11e** | **dscp** }	デフォルト：ポートプライオリティを信頼する
4. ポートプライオリティを設定する	**qos priority** *priority-value*	デフォルト： 0

9.3 SVPマッピングの設定

SVP マッピングは、WMM が設定されていないクライアントでのみ有効です。

この機能は、IP ヘッダーのプロトコル ID として 119 を持つパケットを AC-VI または AC-VO キューに割り当て、SVP パケットに指定された優先度を提供します。SVP は、SVP パケットのランダムバックオフを必要としません。そのため、AC-VI または AC-VO キューに SVP パケットのみがある場合、ECWmin と ECWmax の両方を 0 に設定できます。

SVP マッピングが無効の場合、SVP パケットは AC-BE キューに割り当てられます。

I. AP view での SVP マッピングの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. SVP マッピングを設定する	**svp map-ac** { **ac-vi** | **ac-vo** | **disable** }	デフォルト：APはAP group viewの設定を使用します。

II. AP group view での SVP マッピングの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. SVP マッピングを設定する	**svp map-ac** { **ac-vi** | **ac-vo** | **disable** }	デフォルト：無効

9.4 帯域保証の設定

9.4.1 AP view での帯域保証の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 指定した無線タイプの最大帯域幅を設定する	**wlan max-bandwidth** { **dot11a** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11g** | **dot1gac** | **dot11gn** } *bandwidth*	デフォルト：以下の設定が摘要されています。 ● dot11a、dot11g：30000Kbps ● dot11an、dot11gn、dot11gac：250000Kbps ● dot11ac、dot11ax：500000Kbps ● dot11b：7000Kbps
3. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
4. radio view に移行する	**radio** *radio-id*	—
5. 帯域保証を設定する	**bandwidth-guarantee** { **disable** | **enable** }	デフォルト：以下の設定が摘要されています。 ● AP group viewのサービステンプレートの設定が使用されている場合、APはAP group viewの設定を使用します。 ● サービステンプレートが手動で無線に関連づけられている場合、帯域幅の保証は無効になります。
6. 指定したサービステンプレートの帯域保証幅の割合を設定する	**bandwidth-guarantee service-template** *service-template-name* **percent** *percent*	デフォルト：以下の設定が摘要されています。 ● AP group viewのサービステンプレート設定が使用されている場合、APはAP group viewの設定を使用します。 ● サービステンプレートが手動で無線に関連づけられている場合、帯域保証幅の割合はサービステンプレートに設定されません。

9.4.2 AP group view での帯域保証の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2. 指定した無線タイプの最大帯域幅を設定する	**wlan max-bandwidth** { **dot11a** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11g** | **dot1gac** | **dot11gn** } *bandwidth*	デフォルト：以下の設定が摘要されています。 ● dot11a、dot11g：30000Kbps ● dot11an、dot11gn、dot11gac：250000Kbps ● dot11ac、dot11ax：500000Kbps ● dot11b：7000Kbps
3. AP group view に移行する	**wlan ap-group** *group-name*	—
4. AP model view に移行する	**ap-model** *ap-model*	—
5. radio view に移行する	**radio** *radio-id*	—
6. 帯域保証を設定する	**bandwidth-guarantee** { **disable** | **enable** }	デフォルト：無効
7. 指定したサービステンプレートの帯域保証幅の割合を設定する	**bandwidth-guarantee service-template** *service-template-name* **percent** *percent*	デフォルト：設定なし

9.5 クライアント帯域制限

サービステンプレートベース、無線ベース、クライアントタイプベースの方式でクライアント帯域制限を設定できます。帯域制限モードでは、クライアント帯域制限の動的モードまたは静的モードを構成できます。

複数の方式とモードが設定されている場合、すべての設定が有効になります。 クライアント帯域は、すべてのクライアント帯域制限設定の中で最小値に制限されます。

9.5.1 サービステンプレートベースの帯域制限設定

本設定は、同じサービステンプレートに関連づけられているすべてのクライアントに影響を与えます。

サービステンプレートベースのクライアント帯域制限を設定するには、次の手順を実行します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service-template view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートベースのクライアント帯域制限を有効化する	**client-rate-limit enable**	デフォルト：無効
4. サービステンプレートベースのクライアント帯域制限値を設定する	**client-rate-limit** { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*	デフォルト：設定なし

9.5.2 無線ベースの帯域制限設定

本設定は、同じ無線に関連づけられたすべてのクライアントに影響を与えます。

I. AP view での無線ベースのクライアント帯域制限設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. 無線ベースのクライアントレート制限を有効または無効にする	**client-rate-limit** { **disable** | **enable** }	デフォルト： APはAP group viewの設定を使用します。
5. 無線ベースのクライアント帯域制限値を設定する	**client-rate-limit** { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*	デフォルト： APはAP group viewの設定を使用します。

II. AP view での無線ベースのクライアント帯域制限設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. 無線ベースのクライアントレート制限を有効または無効にする	**client-rate-limit** { **disable** | **enable** }	デフォルト：無効
6. 無線ベースのクライアント帯域制限値を設定する	**client-rate-limit** { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*	デフォルト：設定なし

9.5.3 クライアントタイプベースの帯域制限設定

本設定は、指定されたプロトコルのすべてのクライアントに影響を与えます。

クライアントタイプベースのクライアント帯域制限を設定するには、次の手順を実行します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. クライアントタイプベースのクライアント帯域制限値を設定する	**wlan client-rate-limit** { **dot11a** | **dot11ac** | **dot11ax** | **dot11an** | **dot11b** | **dot11g** | **dot1gac** | **dot11gn** } { **inbound** | **outbound** } **cir** *cir* [**cbs** *cbs*]	デフォルト：設定なし

9.6 U-APSDの設定

🕮 **メモ：**

u-apsd enable コマンドはソフトウェアバージョン 7.2.42 を含む以降のソフトウェアからサポートしています。

I. 制限とガイドライン

U-APSD は、WMM を有効にすると自動的に有効になります。

クライアントが U-APSD をサポートしている場合、この機能を有効にして節電機能を向上させることを推奨します。

この機能を設定するにはサービステンプレートが無効になっていることを確認してください。

II. U-APSD の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． service-template view に移行する	**wlan service-template** *service-template-name*	—
3． U-APSD を有効にする	**u-apsd enable**	デフォルト：有効 U-APSDを無効にする場合、**undo u-apsd enable**コマンドを実行します。

9.7 Air Time Fairnessの設定

🕮 **メモ：**

atf コマンドはソフトウェアバージョン7.2.47 を含む以降のソフトウェアからサポートしています。
Air Time Fairness は QX-W1100 シリーズの AP でのみサポートしています。

Air Time Fairness は、すべてのクライアントが AP のカバレッジエリア内の通信時間に均等にアクセスできるようにします。この機能を使用すると、高速クライアントがワイヤレスリソースを使用する機会が増えます。これにより、ネットワーク全体の転送効率が向上します。

この機能を有効にすると、低速クライアントの転送効率が低下する可能性があります。

この機能を設定する場合は、アクセスクライアントの数と高速クライアントの転送効率を考慮してください。

この機能でネットワークの転送効率が向上するのは、AP からクライアント方向の通信のみです。

I. AP view での Air Time Fairness 設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． Air Time Fairness を設定する	**atf** { **disable** | **enable** }	デフォルト： APはAP group viewの設定を使用します。

II. AP group view での Air Time Fairness 設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—
5． Air Time Fairness を設定する	**atf** { **disable** | **enable** }	デフォルト：無効

9.8 WMMの表示および維持

すべての view で **display** コマンドを実行することができ、user view で **reset** コマンドを実行することができます。

操作	コマンド
無線のWMM統計情報を表示する	**display wlan wmm radio** { **all** | **ap** *ap-name* }
クライアントのWMM統計情報を表示する	**display wlan wmm client** { **all** | **ap** *ap-name* | **mac-address** *mac-address* }
無線のWMM統計情報をリセットする	**reset wlan wmm radio** { **all** | **ap** *ap-name* }
クライアントのWMM統計情報をリセットする	**reset wlan wmm client** { **all** | **ap** *ap-name* | **mac-address** *mac-address* }

9.9 WLAN QoSの設定例

9.9.1 基本的な WMM の設定例

I. ネットワーク要件

図 9-2に示すように、AC 上で WMM を有効にし、AP とクライアントがトラフィックに優先度を付けるようにします。

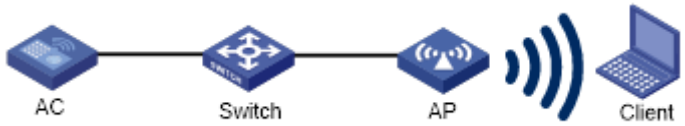


図 9-2 ネットワーク図

II. 設定手順

market という名前のサービステンプレートを作成し、SSID を market に設定し、サービステンプレートを有効にします。

```
<AC> system-view
[AC] wlan service-template market
[AC-wlan-st-market] ssid market
[AC-wlan-st-market] service-template enable
[AC-wlan-st-market] quit
```

ap1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

WMM を有効にし、サービステンプレート market を無線 1 に紐づけ、無線 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] wmm enable
[AC-wlan-ap-ap1-radio-1] service-template market
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

III. 設定の確認

無線の WMM 統計情報を表示します。

```
[AC] display wlan wmm radio
AP ID : 1   AP Name : 441a-fa25-4ef0

 Radio : 1
 Client EDCA updates : 0
 QoS mode   : WMM
 WMM status : Enabled
 Radio max AIFSN     : 15         Radio max ECWmin : 10
 Radio max TXOPLimit : 32767      Radio max ECWmax : 10
 CAC information
 Clients accepted                : 0
  Voice                          : 0
  Video                          : 0
 Total request medium time(μs)    : 0
  Voice(μs)                      : 0
  Video(μs)                      : 0
 Calls rejected due to insufficient resources  : 0
 Calls rejected due to invalid parameters      : 0
 Calls rejected due to invalid medium time      : 0
 Calls rejected due to invalid delay bound      : 0

 Radio : 2
 Client EDCA updates : 0
 QoS mode   : WMM
 WMM status : Enabled
 Radio max AIFSN     : 15         Radio max ECWmin : 10
 Radio max TXOPLimit : 32767      Radio max ECWmax : 10
 CAC information
 Clients accepted                : 0
  Voice                          : 0
  Video                          : 0
 Total request medium time(μs)    : 0
  Voice(μs)                      : 0
  Video(μs)                      : 0
 Calls rejected due to insufficient resources  : 0
 Calls rejected due to invalid parameters      : 0
 Calls rejected due to invalid medium time      : 0
 Calls rejected due to invalid delay bound      : 0

 Radio : 3
 Client EDCA updates : 0
 QoS mode   : WMM
 WMM status : Enabled
 Radio max AIFSN     : 15         Radio max ECWmin : 10
 Radio max TXOPLimit : 32767      Radio max ECWmax : 10
 CAC information
 Clients accepted                : 0
  Voice                          : 0
  Video                          : 0
 Total request medium time(μs)    : 0
  Voice(μs)                      : 0
  Video(μs)                      : 0
 Calls rejected due to insufficient resources  : 0
 Calls rejected due to invalid parameters      : 0
 Calls rejected due to invalid medium time      : 0
 Calls rejected due to invalid delay bound      : 0
```

9.9.2 トラフィック差別化の設定例

I. ネットワーク要件

図 9-3に示すように、クライアントから AC-VO キューに 802.11 パケットを追加するために、AC 上でプライオリティマッピングを設定します。

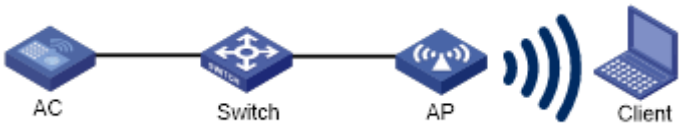


図 9-3 ネットワーク図

II. 設定手順

market という名前のサービステンプレートを作成し、SSID を market に設定します。以下は中央転送モード時の設定を示します。

```
<AC> system-view
[AC] wlan service-template market
[AC-wlan-st-market] client forwarding-location ac
[AC-wlan-st-market] qos trust dscp
[AC-wlan-st-market] ssid market
```

#プライオリティマッピングを設定し、サービステンプレートを有効にします。

```
[AC-wlan-st-market] qos priority 7
[AC-wlan-st-market] service-template enable
[AC-wlan-st-market] quit
```

ap1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

#WMM を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] wmm enable
```

#無線 1 にサービステンプレート market を紐づけ、無線 1 を有効にします。

```
[AC-wlan-ap-ap1-radio-1] service-template market
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

III. 設定の確認

#クライアントからのパケットが AC-VO キューに追加されていることを確認します。

```
[AC] display wlan statistics client
MAC address                    : 0015-005e-97cc
 AP name                       : ap1
 Radio ID                      : 1
 SSID                          : market
 BSSID                         : 5866-ba74-e570
 RSSI                          : 27 dB
 Sent frames:
   Back ground                 : 0/0 (frames/bytes)
   Best effort                 : 0/0 (frames/bytes)
   Video                       : 0/0 (frames/bytes)
   Voice                       : 14/1092 (frames/bytes)
 Received frames:
   Back ground                 : 0/0 (frames/bytes)
   Best effort                 : 66/8177 (frames/bytes)
   Video                       : 0/0 (frames/bytes)
   Voice                       : 0/0 (frames/bytes)
 Discarded frames:
   Back ground                 : 0/0 (frames/bytes)
   Best effort                 : 0/0 (frames/bytes)
   Video                       : 0/0 (frames/bytes)
   Voice                       : 0/0 (frames/bytes)
```

9.9.3 帯域保証の設定例

I. ネットワーク要件

図 9-4に示すように、クライアント 1、2、3 は、それぞれ SSID research、office、entertain を通じてネットワークにアクセスします。

ネットワークが正常に動作するためには、SSID office に帯域幅の 20%、research に 80% を保証し、entertain の帯域幅は保証を行わないようにする必要があります。

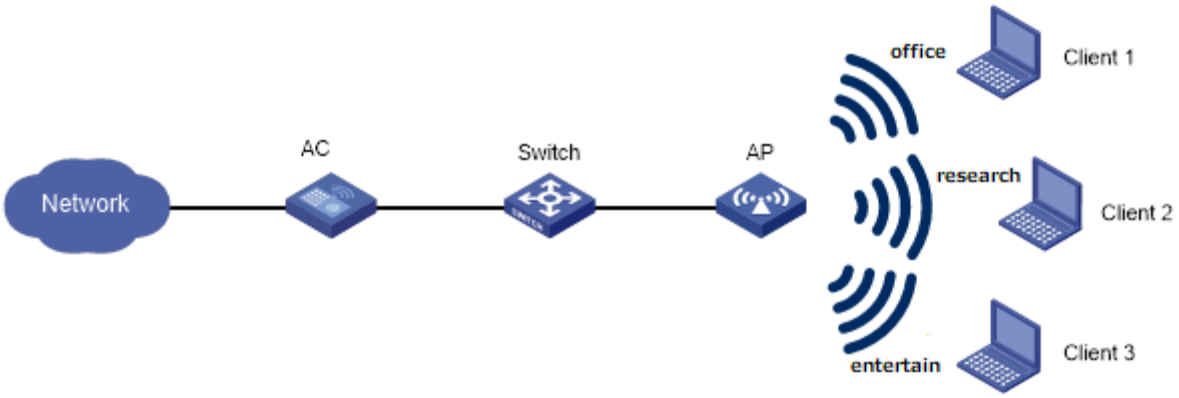


図 9-4 ネットワーク図

II. 設定手順

office という名前のサービステンプレートを作成し、SSID を office に設定し、サービステンプレートを有効にします。

```
<AC> system-view
[AC] wlan service-template office
[AC-wlan-st-office] ssid office
[AC-wlan-st-office] service-template enable
[AC-wlan-st-office] quit
```

research という名前のサービステンプレートを作成し、SSID を research に設定し、サービステンプレートを有効にします。

```
[AC] wlan service-template research
[AC-wlan-st-research] ssid research
[AC-wlan-st-research] service-template enable
[AC-wlan-st-research] quit
```

entertain という名前のサービステンプレートを作成し、SSID を entertain に設定し、サービステンプレートを有効にします。

```
[AC] wlan service-template entertain
[AC-wlan-st-entertain] ssid entertain
[AC-wlan-st-entertain] service-template enable
[AC-wlan-st-entertain] quit
```

802.11ac 無線の場合、最大帯域幅を 10000 Kbps に設定します。

```
[AC] wlan max-bandwidth dot11ac 10000
```

ap1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
```

無線 1 の場合は無線の種類を dot11ac に設定し、サービステンプレートの office、research、entertain を無線 1 に紐づけ、無線 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] type dot11ac
[AC-wlan-ap-ap1-radio-1] service-template office
[AC-wlan-ap-ap1-radio-1] service-template research
[AC-wlan-ap-ap1-radio-1] service-template entertain
[AC-wlan-ap-ap1-radio-1] radio enable
```

帯域保証を有効にします。

```
[AC-wlan-ap-ap1-radio-1] bandwidth-guarantee enable
```

帯域保証する割合をサービステンプレート office は 20%、research は 80%に設定します。

```
[AC-wlan-ap-ap1-radio-1] bandwidth-guarantee service-template office percent 20
[AC-wlan-ap-ap1-radio-1] bandwidth-guarantee service-template research percent 80
[AC-wlan-ap-ap1-radio-1] return
```

III. 設定の確認

#総トラフィックレートが 10000 Kbps 未満の場合、AP から任意のクライアントへのトラフィックのレートが制限されていないことを確認します。

#次の項目を確認するために、AP からクライアント 1 へ 2000Kbps 以上、クライアント 2 に 8000 Kbps 以上の速度でトラフィックを送信します。

- AP は 2000 Kbps でクライアント 1 にトラフィックを送信します。
- AP は 8000 Kbps でクライアント 2 にトラフィックを送信します。
- AP からクライアント 3 へのトラフィックの送信は制限されています。

9.9.4 クライアント帯域制限の設定例

I. ネットワーク要件

図 9-5に示すように、AC は AP と同じネットワークに存在します。AC 上で次の作業を実行します。

- static mode のクライアント帯域制限を設定して、着信クライアントトラフィックの帯域を制限します。
- dynamic mode のクライアント帯域制限を設定して、発信クライアントトラフィックの帯域を制限します。

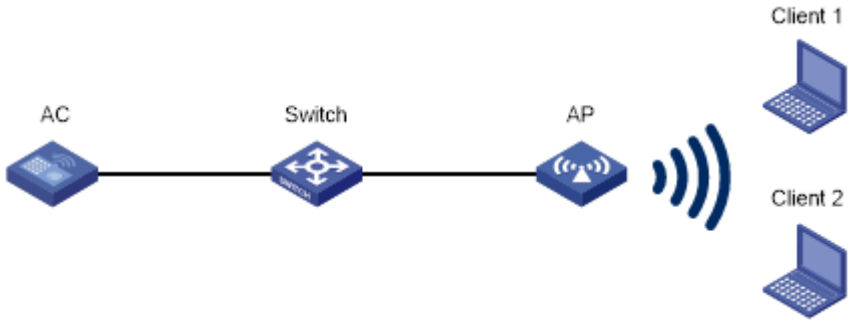


図 9-5 ネットワーク図

II. 設定手順

service という名前のサービステンプレートを作成し、SSID を service に設定し、サービステンプレートを有効にします。

```
<AC> system-view
[AC] wlan service-template service
[AC-wlan-st-service] ssid service
```

サービステンプレート service のクライアント帯域制限を有効にし、次のようにクライアント帯域制限を構成します。

- static mode で、受信トラフィックの帯域を 8000 Kbps に制限します。
- dynamic mode で、送信トラフィックの帯域を 8000Kbps に制限します。

```
[AC-wlan-st-service] client-rate-limit enable
[AC-wlan-st-service] client-rate-limit inbound mode static cir 8000
[AC-wlan-st-service] client-rate-limit outbound mode dynamic cir 8000
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

ap1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
```

無線 1 にサービステンプレート service を紐づけ、無線 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] return
```

9.9.5 Air Time Fairness の設定例

I. ネットワーク要件

図 9-6に示すように、AC は AP と同じネットワークに存在します。AC 上で次の作業を実行します。

- Client 1 は 802.11n に対応した低速クライアントです。
- Client 2 は 802.11ax に対応した高速クライアントです。Air Time Fairness を有効にして、Client 1 による通信速度の低下の影響を抑えます

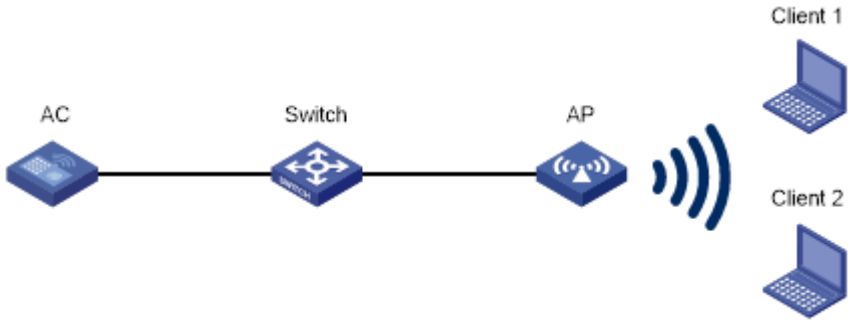


図 9-6 ネットワーク図

II. 設定手順

service という名前のサービステンプレートを作成し、SSID を service に設定し、サービステンプレートを有効にします。

```
<AC> system-view
[AC] wlan service-template service
[AC-wlan-st-service] ssid service
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

ap1 という名前の手動 AP を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1130
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
```

無線 1 にサービステンプレート service を紐づけ、無線 1 を有効にします。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] radio enable
```

無線 1 で Air Time Fairness を有効にします。

```
[AC-wlan-ap-ap1-radio-1] atf enable
```

目次

10章 WLANローミングの設定 10-1
10.1 概要 10-1
10.2 特殊な用語 10-1
10.3 WLANローミングメカニズム 10-1
10.3.1 AC内ローミング 10-1
10.3.2 AC間ローミング 10-2
10.4 設定の制限とガイドライン 10-4
10.5 WLANローミング用SNMP通知機能の有効化 10-4
10.6 802.11rの設定 10-4
10.6.1 802.11r 動作メカニズム 10-5
10.6.2 プロトコルと標準 10-6
10.6.3 802.11rの設定 10-6
10.6.4 モビリティドメインIDの設定 10-7
10.7 802.11vの設定 10-8
10.7.1 BTM (BSS移行管理) 10-8
10.7.2 BTMの設定 10-9
10.7.3 BTMアソシエーション解除の設定 10-9
10.7.4 クライアントanti-stickyの設定 10-10
10.8 802.11kの設定 10-11
10.9 WLANローミング設定例 10-11
10.9.1 AC内ローミング 10-11
10.9.2 AC間ローミング 10-13
10.10 802.11r設定例 10-18
10.10.1 Over-the-DS FTとPSK認証設定例 10-18
10.10.2 Over-the-air FTとPSK認証設定例 10-22
10.10.3 Over-the-DS FTと802.1X認証設定 10-25
10.10.4 Over-the-air FTと802.1X認証設定例 10-29
10.11 802.11v設定例 10-32
10.11.1 BTMとPSK認証設定 10-32
10.11.2 BTMと802.1X認証設定 10-36

10章 WLAN ローミングの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

10.1 概要

WLAN ローミングは、クライアントが、同一 ESS の AP ローミングプロセスの間で、IP アドレスと認可情報を保持してシームレスに移動することを可能にします。

QX シリーズの AC は、RSN + 802.1X を使用した再認証不要な AP 間の移動により、高速なローミングを提供します。

10.2 特殊な用語

- IACTP（Inter Access Controller Tunneling Protocol）

IACTP は、AC 間の安全な通信のための、一般的なパケットカプセル化と通信メカニズムで、QX 独自のプロトコルです。ローミング・サービスを提供している AC 間では、IACTP トンネル上で制御メッセージとクライアント情報を交換しています。

- Home AC

Home AC は、クライアントが最初に接続する AP を管理する AC です。

- Foreign AC

Foreign AC は、クライアントが相互 AC ローミングの後に接続する AC です。

- モビリティグループ

モビリティグループはクライアントがローミングできる複数の AP を管理する AC を含むグループです。

IACTP を使用するためには、モビリティグループを設定する必要があります。

10.3 WLANローミングメカニズム

クライアントは AC が管理する同じモビリティグループの AP 間で移動することができます。

10.3.1 AC 内ローミング

AC 内ローミングは、同じ AC によって管理される AP の間でクライアントが移動することを可能にします。

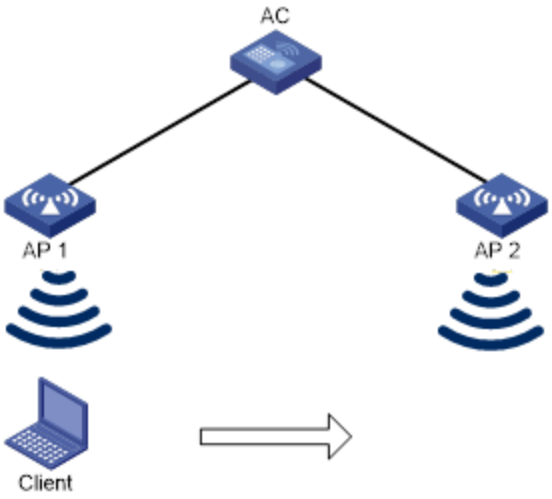


図 10-1 AC 内ローミング

図 10-1に示すように、AC 内ローミングは以下の処理を行います。

1) クライアントは AP 1 からオンラインになり、AC はクライアントのローミングエントリを作成します。
2) クライアントは AP 2 に移動します。AC はクライアントのローミングエントリを調査し、高速ローミング可能か決定します。クライアントが RSN + 802.1X クライアントなら、高速ローミングを使用し、再認証なしで AP 2 に移動します。RSN + 802.1X クライアントでない場合、クライアントは、AP 2 に接続するために再認証する必要があります。

10.3.2 AC 間ローミング

AC 間ローミングは、同じモビリティグループに所属する AC によって管理される AP の間でクライアントが移動することを可能にします。

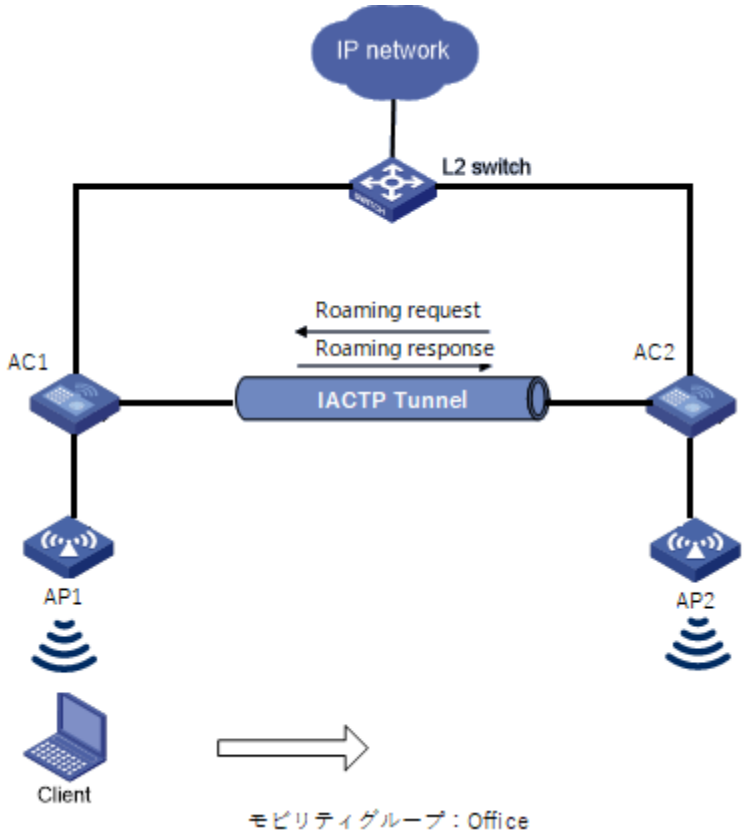


図 10-2 AC 間ローミング

図 10-2に示すように、AC 間ローミングは以下の処理を行います。

1) AC1 と AC2 はモビリティグループ office に所属しています。クライアントは AP 1 でオンラインになり、AC1 はクライアントのローミングエントリを作成します。
2) クライアントは AP 2 に移動します。AC2 はクライアントのローミングエントリを調査し、高速ローミング可能か決定します。クライアントが RSN + 802.1X クライアントなら、高速ローミングを使用し、再認証なしで AP2 に移動します。RSN + 802.1X クライアントでない場合、クライアントは、AP2 に接続するために再認証する必要があります。

I. AC 間ローミングの設定

🕮 **メモ：**

- モビリティグループの設定はソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
- AC 間でローミングする場合は、モビリティグループを設定してください。モビリティグループの設定をしていない場合の、AC 間ローミング動作は未サポートです。
- 異なる機種、異なるソフトウェアバージョンの組み合わせでのモビリティグループ動作は未サポートです。

AC 間でクライアントのローミングエントリをやり取りするために、AC にモビリティグループの設定をしてください。以下にモビリティグループを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. モビリティグループを作成し、その view に移行する	**wlan mobility group** *group-name*	デフォルト：設定なし
3. 送信元 IPv4 アドレスを指定する	**source ip** *ip-address*	デフォルト：設定なし
4. メンバ AP の IPv4 アドレスを指定する	**member ip** *ip-address*	デフォルト：設定なし
5. モビリティグループを有効にする	**group enable**	デフォルト：無効

10.4 設定の制限とガイドライン

WLAN ローミングを設定する際に、以下の制限とガイドラインに従ってください

- AP が認証するサービステンプレートではローミングをサポートしません。ローカルな転送の詳細については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN アクセスの設定"* を参照してください。
- AP をクライアント認証として設定するサービステンプレートは、本章ではサポートしません。クライアント認証の詳細については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN 認証の概要"*、*"WLAN 認証の設定"* を参照してください。

10.5 WLANローミング用SNMP通知機能の有効化

重大な WLAN ローミングイベントを NMS に通知するために、SNMP 通知機能の有効にしてください。WLAN ローミングイベントを正しく通知するために、QX-W1000/W1100 シリーズアクセスポイント オペレーションマニュアルのセクション 11 システム管理 *"SNMP"* に従って SNMP を設定してください。

以下に WLAN ローミング用 SNMP 通知機能を有効にする手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. WLAN ローミング用 SNMP 通知機能を有効にする	**snmp-agent trap enable wlan mobility**	デフォルト：無効

10.6 802.11rの設定

🕮 **メモ：**

802.11r の設定はソフトウェアバージョン 7.2.52 を含む以降のソフトウェアからサポートしています。

802.11r FT（fast BSS transition）により、クライアントが同一 ESS 内の別の BSS にローミングする際、遅延が短縮されます。802.11r FT では、クライアントはローミング先の AP とメッセージを交換する必要があります。FT は以下のメッセージ交換方法を提供します。

- **Over-the-air**－クライアントは事前ローミング認証のために、ローミング先の AP と直接通信します。
- **Over-the-DS**－クライアントは事前ローミング認証のために、現在接続している AP を介してローミング先の AP と通信します。

10.6.1 802.11r 動作メカニズム

I. Over-the-air FT を使用した AC 内ローミング

図 10-3に示すように、クライアントは AP1 に関連付いています。Over-the-air FT を使用した AC 内ローミングは以下の手順で実行されます。

1) クライアントは AP1 に関連付いています。
2) クライアントは AP2 に FT 認証要求を送信します。
3) AP2 は FT 認証応答をクライアントに送信します。
4) クライアントは AP2 に再関連付け要求を送信します。
5) AP2 はクライアントに再関連付け応答を送信します。
6) クライアントは AP2 にローミングします。

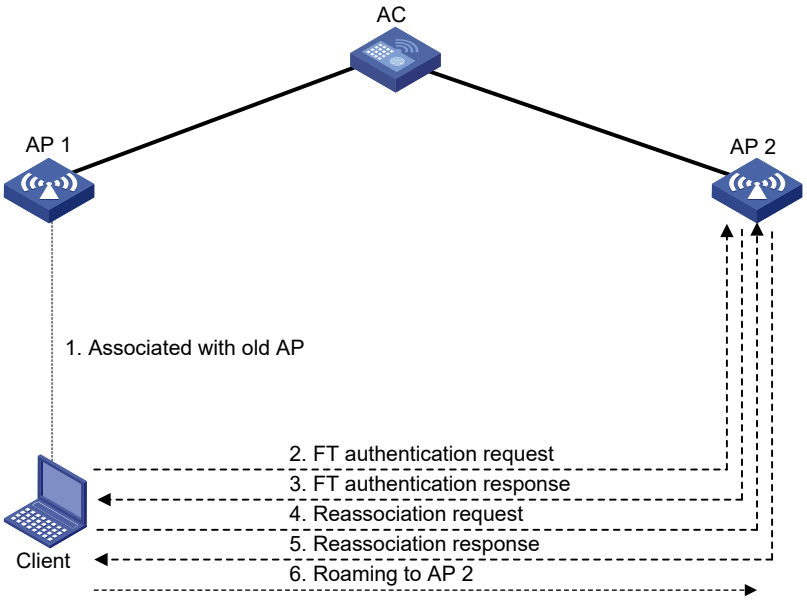


図 10-3 Over-the-air FT を使用した AC 内ローミング

II. Over-the-DS を使用した AC 内ローミング

図 10-4に示すように、クライアントは AP1 に関連付いています。Over-the-DS FT を使用した AC 内ローミングは以下の手順で実行されます。

1) クライアントは AP1 に関連付いています。
2) クライアントがオンラインになったあと、AC はクライアントのためのローミングエントリを作成し、保存します。
3) クライアントは FT 認証要求を AP1 に送信します。

4) AP1 は FT 認証応答をクライアントに送信します。
5) クライアントは再関連付け要求を AP2 に送信します。
6) AP2 は再関連付け応答をクライアントに送信します。
7) クライアントが AP2 にローミングします。

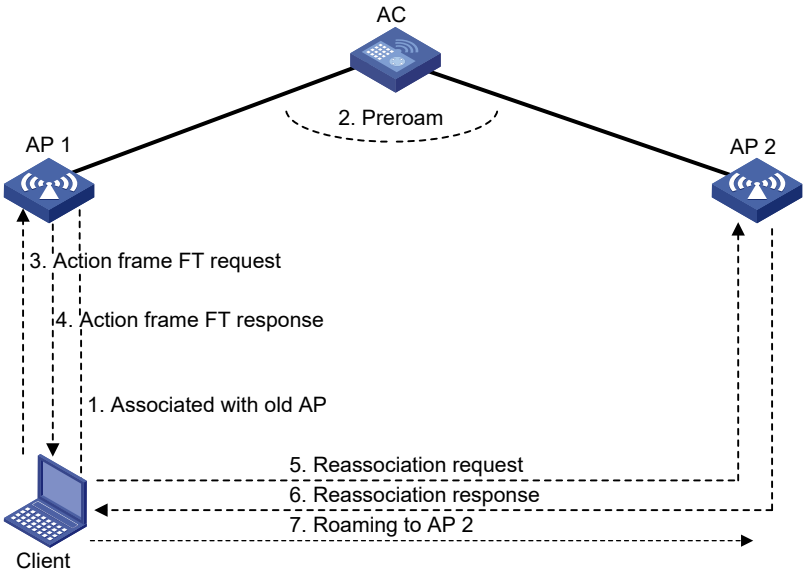


図 10-4 Over-the-DS FT を使用した AC 内ローミング

10.6.2 プロトコルと標準

802.11r IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements

10.6.3 802.11r の設定

802.11r を設定する際、以下の制限とガイドラインに従ってください。

- FT をサポートしていないクライアントが WLAN にアクセスできるようにするには、SSID 名が同じ 2 つのサービステンプレートを作成し、一方のサービステンプレートで FT を有効にし、もう一方では FT を無効にしてください。
- 定期的な再認証タイマが終了するたびにクライアントがオンラインになることを防ぐために、FT と定期的再認証を同じサービステンプレートに対して有効にしないでください。定期的再認証に関する詳細はオペレーションマニュアルのセクション 2 *WLAN “WLAN 認証の設定”* を参照してください。
- PTK アップデートは FT を使用して WLAN にアクセスしているクライアントにはサポートされません。PTK アップデートの詳細はオペレーションマニュアルのセクション 2 *WLAN “WLAN セキュリティ”* を参照してください。

802.11r の設定方法を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． Service template view に移行する	**wlan service-template** *service-template-name*	—
3． FT を有効にする	**ft enable**	デフォルト：無効 FTを有効にするサービステンプレートは、security-ie rsn、client association-location acを使用し、WPA3とenhanced-openが無効である必要があります。
4． （オプション設定項目）FT の方法を設定する	**ft method** { **over-the-air** | **over-the-ds** }	デフォルト：**over-the-air**
5． （オプション設定項目）再関連付けタイムアウトタイマを設定する	**ft reassociation-timeout** *timeout*	デフォルト：20秒 タイムアウトタイマが終了する前にクライアントが再関連付け要求を送信しない場合、ローミングプロセスは終了されます。

10.6.4 モビリティドメイン ID の設定

🕮 **メモ：**

モビリティドメインIDの設定はソフトウェアバージョン7.2.56を含む以降のソフトウェアからサポートしています。

クライアントが異なる AP 間を移動するときに、クライアントのアクセス時間を短縮するには、この機能を設定します。

この機能を設定すると、クライアントは、2 つの AP が同じモビリティドメイン ID を持つ場合に限り、802.11r FT(fast BSS transition) を介して異なる AP 間をローミングできます。

クライアントが、FT が有効なっていてもモビリティグループに含まれていない AP 間を移動する場合、クライアントは AP 間の FT ローミングを使用する場合があります。ただし、AP は同じモビリティグループに属していないため、ローミングは失敗します。次に、クライアントはアソシエーションを使用して新しい AP に切り替えます。

AP に異なるモビリティドメイン ID を設定することで、クライアントは AP 間の FT ローミングを試行せずに新しい AP に直接関連付けができるようになります。その結果、AP 間の FT ローミング処理が省略されるため、サービス切り替え時間が短縮されます。

サービステンプレートを有効にする前に、この機能を設定します。この機能は、FT が有効の場合にだけ有効です。

モビリティドメイン ID の設定方法を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Service template view に移行する	**wlan service-template** *service-template-name*	—

操作	コマンド	補足
3. モビリティドメイン ID を設定する	**ft mobility-domain-id** *mobility-domain-id*	デフォルト：設定なし

10.7 802.11vの設定

🕮 **メモ：**

802.11v の設定はソフトウェアバージョン 7.2.52 を含む以降のソフトウェアからサポートしています。

802.11v は、省電力、ロードバランシング、および BSS 移行管理(BTM) などの多数の拡張機能を定義した、ワイヤレスネットワーク管理の規格です。これにより、クライアントはネットワーク情報を交換し、常に最適な AP と関連付けることができるため、クライアントのバッテリ持続時間が長くなり、ユーザエクスペリエンスが向上します

10.7.1 BTM (BSS 移行管理)

BTM を使用すると、接続中の AP の信号強度が低い場合や、より信号強度の優れた AP が検出された場合に、クライアントは最適な AP にローミングできます。

図 10-5に示すように、クライアントは AP に関連付いています。この時 BSS 移行管理は、以下のように動作します。

1) AP または 802.11v クライアントが BSS 移行をトリガします。

- Unsolicited request： AP は、クライアントの RSSI が RSSI しきい値よりも低いことを検出すると、クライアントに BTM request を送信します。
- Solicited request： 現在関連付けられている AP の RSSI が低すぎるか、クライアントがより適切な AP を検出した場合、クライアントは関連付けられている AP に BTM query を送信します。BTM query を受信すると、AP は BTM request で応答します。

BTM request には、推奨される BSS に関する情報が含まれます。

2) BTM request を受信すると、クライアントは現在接続している AP から切断して推奨される AP にローミングするかどうかを決定します。

3) クライアントがローミングを実行することを決定すると、BTM response を AP に送信します。クライアントがアソシエーション解除タイマの期限内に現在の BSS から移行できない場合、AP はクライアントに Disassociation request を送信し、クライアントをログオフします。

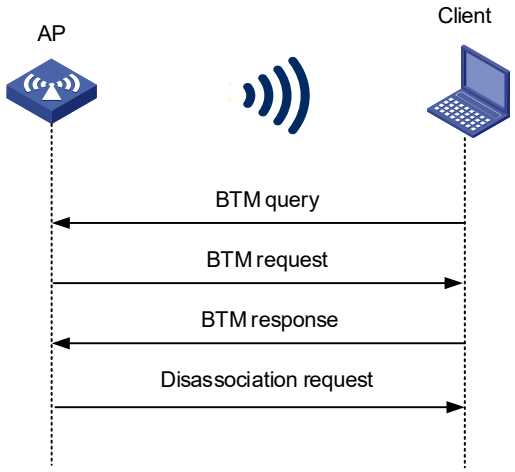


図 10-5 BSS 移行管理

10.7.2 BTM の設定

BTM を設定する際、以下の制限とガイドラインに従ってください。

- クライアント anti-sticky が無効の場合、AP はクライアントの信号強度がしきい値よりも低いかどうかを調べず、unsolicited BTM をトリガしません。
- この作業を行う前に、サービステンプレートが無効になっていることを確認してください。

BTM の設定方法を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Service template view に移行する	**wlan service-template** *service-template-name*	—
3. BTM を有効にする	**bss transition-management enable**	デフォルト：無効

10.7.3 BTM アソシエーション解除の設定

BTM アソシエーション解除が設定されている場合、AP はクライアントから BTM query を受信すると BTM request をクライアントに送信し、BSS 移行のためにクライアントを案内します。

- forced：アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はそのクライアントを強制的にログオフします。
- recommended： アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合、AP はクライアントを強制的にログオフしません。

bss transition-management disassociation forced を設定すると、アソシエーション解除タイマの期限が切れてもクライアントが AP とのアソシエーションを解除していない場合に、クライアントが強制的にログオフされます。この機能は慎重に使用してください。

BTM アソシエーション解除の設定方法を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． Service template view に移行する	**wlan service-template** *service-template-name*	―
3． BTM アソシエーション解除を設定する	**bss transition-management disassociation** { **forced** | **recommended** } [**timer** *time*]	デフォルト：無効

10.7.4 クライアント anti-sticky の設定

🕮 **メモ：**

forced-logoff のパラメータはソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。

クライアント anti-sticky を設定すると、AP は指定された間隔でクライアントの信号強度を調べることができます。802.11v クライアントの場合、クライアントの信号強度がしきい値より低いと、関連付けられた AP が BSS 移行をトリガして、クライアントをより適切な BSS に導きます。802.11v 以外のクライアントの場合、アクションは実行されません。

I. ap view でのクライアント anti-sticky の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ap view に移行する	**wlan ap** *ap-name*	―
3． radio view に移行する	**radio** *radio-id*	―
4． クライアント anti-sticky を設定する	**sacp anti-sticky** { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] [**forced-logoff**] }	デフォルト：AP group viewの設定を使用します。

II. ap group view でのクライアント anti-sticky の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． ap group view に移行する	**wlan ap** *ap-group-name*	―
3． ap model-view に移行する	**ap-model** *ap-model*	―
4． radio view に移行する	**radio** *radio-id*	―
5． クライアント anti-sticky を設定する	**sacp anti-sticky** { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] [**forced-logoff**] }	デフォルト：有効

10.8 802.11kの設定

QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの“*WLAN 無線リソースの計測の設定*”の“*802.11k 計測*”を参照してください。

10.9 WLANローミング設定例

10.9.1 AC 内ローミング

I. ネットワーク要件

図 10-6に示すように、クライアントが、同じ AC によって管理される AP1 から AP2 にローミングする内部 AC を設定します。

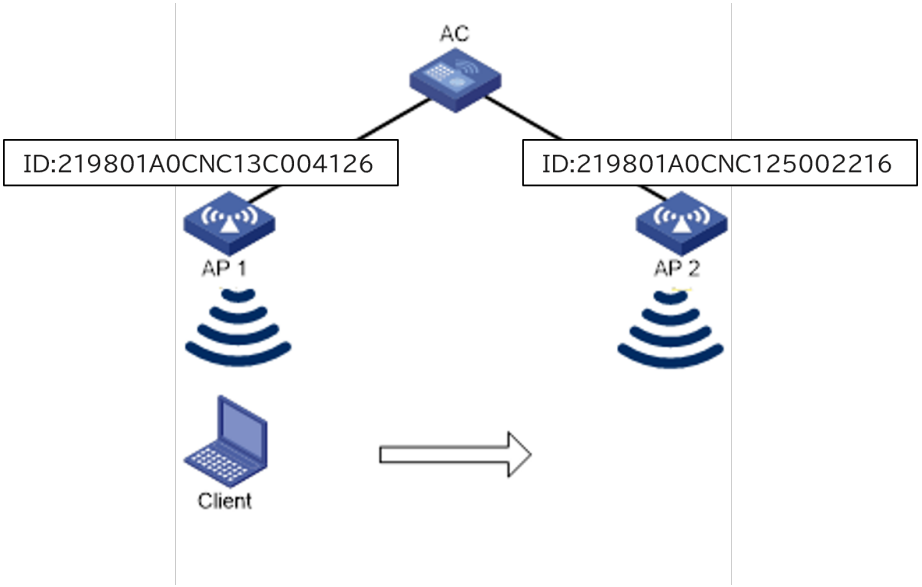


図 10-6 AC 内ローミング

II. 設定手順

サービステンプレート service を作成し、SSID を 1 に設定し、サービステンプレートを使用可能にします。

```
<AC> system-view
[AC] wlan service-template service
[AC-wlan-st-service] ssid 1
[AC-wlan-st-service] service-template enable
[AC-wlan-st-service] quit
```

手動 AP ap1 を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC13C004126
```

サービステンプレートを AP1 の radio1 と結合します。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] service-template service
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

#手動 AP ap2 を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
[AC-wlan-ap-ap2] serial-id 219801A0CNC125002216
```

サービステンプレートを AP2 の radio1 と結合します。

```
[AC-wlan-ap-ap2] radio 1
[AC-wlan-ap-ap2-radio-1] radio enable
[AC-wlan-ap-ap2-radio-1] service-template service
[AC-wlan-ap-ap2-radio-1] quit
[AC-wlan-ap-ap2] quit
```

III. 設定確認

クライアントを AP1 に参加させます。（詳細は省略します。）

クライアントが AP1 に参加しているが、ローミングステータスは N/A であることを確認します。これは、クライアントがローミングを行っていないことを示します。

```
[AC] display wlan client verbose
Total number of clients: 1

 MAC address                      : a60a-139e-6778
 IPv4 address                     : 10.1.1.114
 IPv6 address                     : N/A
 Username                         : N/A
 AP ID                            : 8
 AID                              : 1
 AP name                          : ap1
 Radio ID                         : 1
 SSID                             : 1
 BSSID                            : 000f-e200-4444
 VLAN ID                          : 1
 Power save mode                  : Active
 Wireless mode                    : 802.11a
 Supported rates                  : 6, 9, 12, 18, 24, 36,
                                    48, 54 Mbps
 QoS mode                         : N/A
 Listen interval                  : 10
 RSSI                             : 40
 Rx/Tx rate                       : 54/48
 Authentication method            : Open system
```

```
 Security mode                    : PRE-RSNA
 AKM mode                         : N/A
 Cipher suite                     : N/A
 User authentication mode         : Bypass
 Authorization ACL ID             : N/A
 Authorization user profile       : N/A
 Roam status                      : N/A
 Key derivation                   : N/A
 PMF status                       : N/A
 Forward policy                   : N/A
 Online time                      : 0hr 0min 31sec
 FT Status                        : Inactive
```

クライアントを AP2 にローミングします。（詳細は省略します。）

クライアントが AP2 に参加し、ローミングステータスが内部 AC ローミングであることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

 MAC address                      : a60a-139e-6778
 IPv4 address                     : 10.1.1.114
 IPv6 address                     : N/A
 Username                         : N/A
 AID                              : 1
 AP ID                            : 7
 AP name                          : ap2
 Radio ID                         : 1
 SSID                             : 1
 BSSID                            : 000f-e203-7777
 VLAN ID                          : 1
 Power save mode                  : Active
 Wireless mode                    : 802.11a
 Supported rates                  : 6, 9, 12, 18, 24, 36,
                                    48, 54 Mbps
 QoS mode                         : N/A
 Listen interval                  : 10
 RSSI                             : 0
 Rx/Tx rate                       : 0/0
 Authentication method            : Open system
 Security mode                    : PRE-RSNA
 AKM mode                         : N/A
 Cipher suite                     : N/A
 User authentication mode         : Bypass
 Authorization ACL ID             : N/A
 Authorization user profile       : N/A
 Roam status                      : Intra-AC roam
 Key derivation                   : N/A
 PMF status                       : N/A
 Forward policy                   : N/A
 Online time                      : 0hr 0min 43sec
 FT Status                        : Inactive
```

10.9.2 AC 間ローミング

I. ネットワーク要件

図 10-7に示すように、AC1 に管理されている AP1 と AC2 に管理されている AP2 の間でクライアントがローミングできるように、モビリティグループを設定します。AP1 と AP2 は同じ VLAN で利用します。

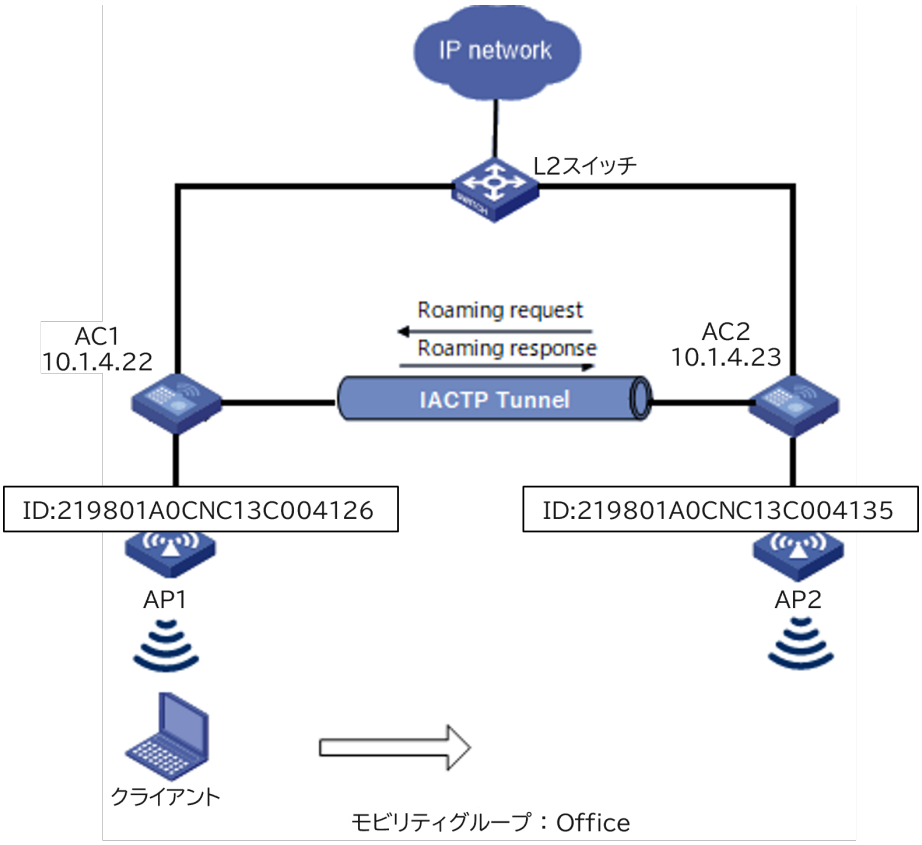


図 10-7 AC 間レイヤ 2 ローミング

II. 設定手順

AC1 でサービステンプレート service を作成し、SSID を 1 に設定し、サービステンプレートを使用可能にします。

```
<AC1> system-view
[AC1] wlan service-template service
[AC1-wlan-st-service] ssid 1
[AC1-wlan-st-service] service-template enable
[AC1-wlan-st-service] quit
```

手動 AP AP1 を作成し、AP モデルとシリアル ID を指定します。

```
[AC1] wlan ap AP1 model QX-W1020
[AC1-wlan-ap-AP1] serial-id 219801A0CNC13C004126
```

AP1 の radio1 に対してサービステンプレートを設定します。

```
[AC1-wlan-ap-AP1] radio 1
[AC1-wlan-ap-AP1-radio-1] radio enable
[AC1-wlan-ap-AP1-radio-1] service-template service
[AC1-wlan-ap-AP1-radio-1] quit
```

```
[AC1-wlan-ap-AP1] quit
```

AC1 でモビリティグループ office を作成します。

```
[AC1] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.22 を設定します。

```
[AC1-wlan-mg-office] source ip 10.1.4.22
```

メンバ IP 10.1.4.23 を設定します。

```
[AC1-wlan-mg-office] member ip 10.1.4.23
```

モビリティグループを有効化します。

```
[AC1-wlan-mg-office] group enable
```

AC2 でサービステンプレート service を作成し、SSID を 1 に設定し、サービステンプレートを使用可能にします。

```
<AC2> system-view
[AC2] wlan service-template service
[AC2-wlan-st-service] ssid 1
[AC2-wlan-st-service] service-template enable
[AC2-wlan-st-service] quit
```

手動 AP AP2 を作成し、AP モデルとシリアル ID を指定します。

```
[AC2] wlan ap AP2 model QX-W1020
[AC2-wlan-ap-AP2] serial-id 219801A0CNC13C004135
```

AP2 の radio1 に対してサービステンプレートを設定します。

```
[AC2-wlan-ap-AP2] radio 1
[AC2-wlan-ap-AP2-radio-1] radio enable
[AC2-wlan-ap-AP2-radio-1] service-template service
[AC2-wlan-ap-AP2-radio-1] quit
[AC2-wlan-ap-AP2] quit
```

モビリティグループ office を作成します。

```
[AC2] wlan mobility group office
```

モビリティトンネルの確立に使用する送信元 IP として 10.1.4.23 を設定します。

```
[AC2-wlan-mg-office] source ip 10.1.4.23
```

メンバ IP 10.1.4.23 を設定します。

```
[AC2-wlan-mg-office] member ip 10.1.4.22
```

モビリティグループを有効化します。

```
[AC2-wlan-mg-office] group enable
```

III. 設定確認

AC1 で display wlan mobility group コマンドを使用します

```
[AC1] display wlan mobility group
Mobility group name: office
 Tunnel type: IPv4
 Source IPv4: 10.1.4.22
 Source IPv6: Not configured
 Authentication method: Not configured
 Mobility group status: Enabled
 Member entries: 1
 IP address                              State          Online time
 10.1.4.23                               Up             00hr 00min 12sec
```

AC2 で、display wlan mobility group コマンドを使用します

```
[AC2] display wlan mobility group
Mobility group name: office
 Tunnel type: IPv4
 Source IPv4: 10.1.4.23
 Source IPv6: Not configured
 Authentication method: Not configured
Mobility group status: Enabled
 Member entries: 1
 IP address                              State          Online time
 10.1.4.22                               Up             00hr 00min 05sec
```

クライアントを AP1 に参加させます。（詳細は省略します。）

クライアントが AP1 に参加しているが、ローミングステータスは N/A であることを確認します。これは、クライアントがローミングを行っていないことを示します。

```
[AC1] display wlan client verbose
Total number of clients: 1

 MAC address                     : 0103-0184-cd1e
 IPv4 address                    : 192.168.1.21
 IPv6 address                    : N/A
 Username                        : N/A
 AID                             : 1
 AP name                         : AP1
 Radio ID                        : 1
 Channel                         : 36
 SSID                            : service
 BSSID                           : 782c-2979-7c80
 VLAN ID                         : 1
 Service VLAN ID                 : N/A
 Sleep count                     : 369
 Wireless mode                   : 802.11ac
 Channel bandwidth               : 80MHz
 SM power save                   : Disabled
 Short GI for 20MHz              : Supported
 Short GI for 40MHz              : Supported
 Short GI for 80MHz              : Supported
 Short GI for 160/80+80MHz       : Not supported
 STBC RX capability              : Not supported
 STBC TX capability              : Not supported
 LDPC RX capability              : Supported
 Beamformee STS capability       : N/A
 Number of Sounding Dimensions   : N/A
 SU beamformee capability        : Not supported
```

```
 MU beamformee capability          : Not supported
 Block Ack                         : TID 0  Both
                                     TID 1  In
                                     TID 5  In
 Supported VHT-MCS set             : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
                                     NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
 Supported HT MCS set              : 0, 1, 2, 3, 4, 5, 6, 7,
                                     8, 9, 10, 11, 12, 13, 14,
                                     15
 Supported rates                   : 6, 9, 12, 18, 24, 36,
                                     48, 54 Mbps
 QoS mode                          : WMM
 Listen interval                   : 20
 RSSI                              : 32
 Rx/Tx rate                        : 39/6 Mbps
 Speed                             : 4.320/1.112Kbps
 Authentication method             : Open system
 Security mode                     : RSN
 AKM mode                          : PSK
 Cipher suite                      : CCMP
 User authentication mode          : Bypass
 WPA3 status                       : Disabled
 Authorization CAR                 : N/A
 Authorization user group name     : N/A
 Authorization ACL ID              : N/A
 Authorization user profile        : N/A
 Roam status                       : N/A
 Key derivation                    : SHA256
 PMF status                        : N/A
 Forwarding policy name            : Not configured
 Online time                       : 0days 0hours 3minutes 24seconds
 FT status                         : Active
 BTM mode                          : Inactive
```

クライアントを AP2 にローミングします。（詳細は省略します。）

クライアントが AP2 に参加し、ローミングステータスが Inter-AC roam であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

 MAC address                       : 0103-0184-cd1e
 IPv4 address                      : 192.168.1.21
 IPv6 address                      : N/A
 Username                          : N/A
 AID                               : 1
 AP name                           : AP2
 Radio ID                          : 1
 Channel                           : 36
 SSID                              : service
 BSSID                             : 74ea-c8fd-bd70
 VLAN ID                           : 1
 Service VLAN ID                   : N/A
 Sleep count                       : 0
 Wireless mode                     : 802.11ac
 Channel bandwidth                 : 80MHz
 SM power save                     : Disabled
 Short GI for 20MHz                : Supported
 Short GI for 40MHz                : Supported
 Short GI for 80MHz                : Supported
 Short GI for 160/80+80MHz         : Not supported
 STBC RX capability                : Not supported
 STBC TX capability                : Not supported
 LDPC RX capability                : Supported
 Beamformee STS capability         : N/A
 Number of Sounding Dimensions     : N/A
 SU beamformee capability          : Not supported
 MU beamformee capability          : Not supported
```

```
Block Ack                          : TID 0  In
Supported VHT-MCS set              : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
                                     NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set               : 0, 1, 2, 3, 4, 5, 6, 7,
                                     8, 9, 10, 11, 12, 13, 14,
                                     15
Supported rates                    : 6, 9, 12, 18, 24, 36,
                                     48, 54 Mbps
QoS mode                           : WMM
Listen interval                    : 20
RSSI                               : 57
Rx/Tx rate                         : 780/6 Mbps
Speed                              : N/A
Authentication method              : FT
Security mode                      : RSN
AKM mode                           : PSK
Cipher suite                       : CCMP
User authentication mode           : Bypass
WPA3 status                        : Disabled
Authorization CAR                  : N/A
Authorization user group name      : N/A
Authorization ACL ID               : N/A
Authorization user profile         : N/A
Roam status                        : Inter-AC roam
Key derivation                     : SHA256
PMF status                         : N/A
Forwarding policy name             : Not configured
Online time                        : 0days 0hours 0minutes 4seconds
FT status                          : Active
BTM mode                           : Inactive
```

10.10 802.11r設定例

10.10.1 Over-the-DS FT と PSK 認証設定例

I. ネットワーク要件

図 10-8に示すように、クライアントが AP1 と AP2 間でローミングできるように Over-the-DS FT を使用した AC 内ローミングを設定します。akm(authentication and key management)モードを PSK に設定します。

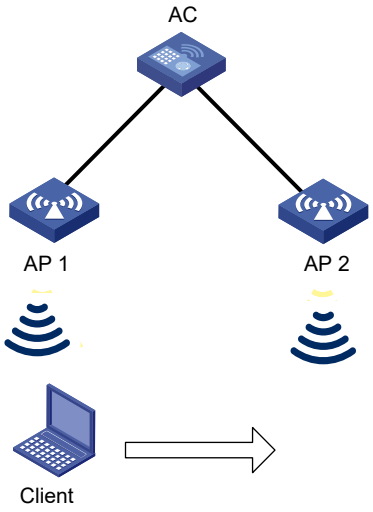


図 10-8 ネットワーク図

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

akm モードを PSK に設定し、事前共有鍵を 12345678 に設定します。

```
[AC-wlan-st-acstname] akm mode psk
[AC-wlan-st-acstname] preshared-key pass-phrase simple 12345678
```

cipher スイートを CCMP に設定し、セキュリティ IE を RSN に設定します。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

FT を有効にします。

```
[AC-wlan-st-acstname] ft enable
```

再関連付けタイムアウトタイマを 50 秒に設定します。

```
[AC-wlan-st-acstname] ft reassociation-timeout 50
```

FT の方法を Over-the-DS に設定します。

```
[AC-wlan-st-acstname] ft method over-the-ds
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
```

```
[AC-wlan-st-acstname] quit
```

AP1 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 1
[AC-wlan-ap-1] radio 2
[AC-wlan-ap-1-radio-2] service-template acstname
[AC-wlan-ap-1-radio-2] radio enable
[AC-wlan-ap-1-radio-2] quit
[AC-wlan-ap-1] quit
```

AP2 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 2
[AC-wlan-ap-2] radio 2
[AC-wlan-ap-2-radio-2] service-template acstname
[AC-wlan-ap-2-radio-2] radio enable
[AC-wlan-ap-2-radio-2] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

サービステンプレートが正しく設定されていることを確認します。

```
[AC] display wlan service-template acstname verbose
Service template name         : acstname
SSID                          : service
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Enabled
Maximum clients per BSS       : Not configured
Frame format                  : Dot3
Seamless-roam                 : Disabled
Seamless-roam RSSI threshold  : 50
Seamless-roam RSSI gap        : 20
VLAN ID                       : 1
AKM mode                      : PSK
Security IE                   : RSN
Cipher suite                  : CCMP
TKIP countermeasure time      : 0 sec
PTK lifetime                  : 43200 sec
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Disabled
User authentication mode      : Bypass
Intrusion protection          : Disabled
Intrusion protection mode     : Temporary-block
Temporary block time          : 180 sec
Temporary service stop time   : 20 sec
Fail VLAN ID                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : Not configured
MAC-auth domain               : Not configured
```

```
Max 802.1X users              : 4096
Max MAC-auth users            : 4096
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : SHA1
PMF status                    : Disabled
Hotspot policy number         : Not configured
Forward policy                : Not configured
Forwarder                     : AC
FT Status                     : Enable
FT Method                     : over-the-ds
FT Reassociation Deadline     : 50 sec
QoS trust                     : Port
QoS priority                  : 0
```

ローミング状態が N/A で、FT 状態が Active であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

MAC address                          : a60a-1303-8361
IPv4 address                         : 10.1.1.114
IPv6 address                         : N/A
Username                             : N/A
AID                                  : 1
AP ID                                : 1
AP name                              : 1
Radio ID                             : 2
SSID                                 : service
BSSID                                : 000f-e266-7788
VLAN ID                              : 1
Power save mode                      : Active
Wireless mode                        : 802.11gn
Channel bandwidth                    : 20MHz
SM power save                        : Enabled
SM power save mode                   : Static
Short GI for 20MHz                   : Not supported
Short GI for 40MHz                   : Not supported
STBC RX capability                   : Supported
STBC TX capability                   : Not supported
Support HT-MCS set                   : 0, 1, 2, 3, 4, 5, 6, 7
QoS mode                             : WMM
Listen interval                      : 20
RSSI                                 : 0
Rx/Tx rate                           : 65/65
Authentication method                : Open system
Security mode                        : RSN
AKM mode                             : PSK
Encryption cipher                    : CCMP
User authentication mode             : Bypass
Authorization ACL ID                 : N/A
Authorization user profile           : N/A
Roam status                          : N/A
Key derivation                       : SHA256
PMF status                           : N/A
Forward policy                       : N/A
Online time                          : 0hr 0min 41sec
FT status                            : Active
```

クライアントを AP2 にローミングさせます（詳細は省略します）。

認証方式が FT で、ローミング状態が Intra-AC roam であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

 MAC address                         : a60a-1303-8361
```

```
IPv4 address                    : 10.1.1.114
IPv6 address                    : N/A
Username                        : N/A
AID                             : 1
AP ID                           : 2
AP name                         : 2
Radio ID                        : 2
SSID                            : service
BSSID                           : 000f-e211-2233
VLAN ID                         : 1
Power save mode                 : Active
Wireless mode                   : 802.11gn
Channel bandwidth               : 20MHz
SM power save                   : Enabled
SM power save mode              : Static
Short GI for 20MHz              : Not supported
Short GI for 40MHz              : Not supported
STBC RX capability              : Supported
STBC TX capability              : Not supported
Support HT-MCS set              : 0, 1, 2, 3, 4, 5, 6, 7
QoS mode                        : WMM
Listen interval                 : 20
RSSI                            : 0
Rx/Tx rate                      : 0/0
Authentication method           : FT
Security mode                   : RSN
AKM mode                        : PSK
Encryption cipher               : CCMP
User authentication mode        : Bypass
Authorization ACL ID            : N/A
Authorization user profile      : N/A
Roam status                     : Intra-AC roam
Key derivation                  : SHA256
PMF status                      : N/A
Forward policy                  : N/A
Online time                     : 0hr 0min 27sec
FT status                       : Active
```

10.10.2 Over-the-air FT と PSK 認証設定例

I. ネットワーク要件

図 10-8に示すように、クライアントが AP1 と AP2 間でローミングできるように Over-the-air FT を使用した AC 内ローミングを設定します。akm モードを PSK に設定します。

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

akm モードを PSK に設定し、事前共有鍵を 12345678 に設定します。

```
[AC-wlan-st-acstname] akm mode psk
[AC-wlan-st-acstname] preshared-key pass-phrase simple 12345678
```

cipher スイートを CCMP に設定し、セキュリティ IE を RSN に設定します。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

FT を有効にします。

```
[AC-wlan-st-acstname] ft enable
```

再関連付けタイムアウトタイマを 50 秒に設定します。

```
[AC-wlan-st-acstname] ft reassociation-timeout 50
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

AP1 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 1
[AC-wlan-ap-1] radio 2
[AC-wlan-ap-1-radio-2] service-template acstname
[AC-wlan-ap-1-radio-2] radio enable
[AC-wlan-ap-1-radio-2] quit
[AC-wlan-ap-1] quit
```

AP2 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 2
[AC-wlan-ap-2] radio 2
[AC-wlan-ap-2-radio-2] service-template acstname
[AC-wlan-ap-2-radio-2] radio enable
[AC-wlan-ap-2-radio-2] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

以下の情報を確認します。

- RSN IE が有効。
- AKM モードが PSK。
- Cipher スイートが CCMP。
- FT 状態が Active。

```
[AC] display wlan client verbose
Total number of clients: 1
```

```
MAC address                          : a60a-1303-8361
IPv4 address                         : 10.1.1.114
IPv6 address                         : N/A
Username                             : N/A
AID                                  : 1
AP ID                                : 1
AP name                              : 1
Radio ID                             : 2
SSID                                 : service
BSSID                                : 000f-e266-7788
VLAN ID                              : 1
Power save mode                      : Active
Wireless mode                        : 802.11gn
Channel bandwidth                    : 20MHz
SM power save                        : Enabled
SM power save mode                   : Static
Short GI for 20MHz                   : Not supported
Short GI for 40MHz                   : Not supported
STBC RX capability                   : Supported
STBC TX capability                   : Not supported
Support HT-MCS set                   : 0, 1, 2, 3, 4, 5, 6, 7
QoS mode                             : WMM
Listen interval                      : 20
RSSI                                 : 0
Rx/Tx rate                           : 65/65
Authentication method                : Open system
Security mode                        : RSN
AKM mode                             : PSK
Encryption cipher                    : CCMP
User authentication mode             : Bypass
Authorization ACL ID                 : N/A
Authorization user profile           : N/A
Roam status                          : N/A
Key derivation                       : SHA256
PMF status                           : N/A
Forward policy                       : N/A
Online time                          : 0hr 0min 41sec
FT status                            : Active
```

クライアントを AP2 にローミングさせます（詳細は省略します）。

認証方式が FT で、ローミング状態が Intra-AC roam であることを確認します。

[AC] display wlan client verbose

```
Total number of clients: 1

 MAC address                         : a60a-1303-8361
 IPv4 address                        : 10.1.1.114
 IPv6 address                        : N/A
 Username                            : N/A
 AID                                 : 1
 AP ID                               : 2
 AP name                             : 2
 Radio ID                            : 2
 SSID                                : service
 BSSID                               : 000f-e211-2233
 VLAN ID                             : 1
 Power save mode                     : Active
 Wireless mode                       : 802.11gn
 Channel bandwidth                   : 20MHz
 SM power save                       : Enabled
 SM power save mode                  : Static
 Short GI for 20MHz                  : Not supported
 Short GI for 40MHz                  : Not supported
 STBC RX capability                  : Supported
 STBC TX capability                  : Not supported
 Support HT-MCS set                  : 0, 1, 2, 3, 4, 5, 6, 7
 QoS mode                            : WMM
```

```
Listen interval                  : 20
RSSI                             : 0
Rx/Tx rate                       : 0/0
Authentication method            : FT
Security mode                    : RSN
AKM mode                         : PSK
Encryption cipher                : CCMP
User authentication mode         : Bypass
Authorization ACL ID             : N/A
Authorization user profile       : N/A
Roam status                      : Intra-AC roam
Key derivation                   : SHA256
PMF status                       : N/A
Forward policy                    : N/A
Online time                      : 0hr 0min 27sec
FT status                        : Active
```

10.10.3 Over-the-DS FT と 802.1X 認証設定

I. ネットワーク要件

図 10-8に示すように、クライアントが AP1 と AP2 間でローミングできるように Over-the-DS FT を使用した AC 内ローミングを設定します。akm モードを 802.1X に設定します。

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

akm モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] akm mode dot1x
```

cipher スイートを CCMP に設定し、セキュリティ IE を RSN に設定します。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

クライアントに対する認証モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] client-security authentication-mode dot1x
[AC-wlan-st-acstname] dot1x domain imc
```

FT を有効にします。

```
[AC-wlan-st-acstname] ft enable
```

FT の方法を Over-the-DS に設定します。

```
[AC-wlan-st-acstname] ft method over-the-ds
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

802.1X 認証モードを EAP に設定します。

```
[AC] dot1x authentication-method eap
```

RADIUS スキーム **imcc** を作成します。

```
[AC] radius scheme imcc
```

プライマリ認証とアカウンティングサーバの IP アドレスを **10.1.1.3** に設定します。

```
[AC-radius-imcc] primary authentication 10.1.1.3
[AC-radius-imcc] primary accounting 10.1.1.3
```

認証とアカウンティングサーバとパケットを交換できるように、AC に共有鍵 **12345678** を設定します。

```
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
```

RADIUS サーバに送信するユーザ名から ISP ドメイン名を外すように設定します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

ISP ドメイン **imc** を作成し、RADIUS スキーム **imcc** を認証、許可、アカウンティングに使用するためにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

AP1 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 1
[AC-wlan-ap-1] radio 2
[AC-wlan-ap-1-radio-2] service-template acstname
[AC-wlan-ap-1-radio-2] radio enable
[AC-wlan-ap-1-radio-2] quit
[AC-wlan-ap-1] quit
```

AP2 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 2
```

```
[AC-wlan-ap-2] radio 2
[AC-wlan-ap-2-radio-2] service-template acstname
[AC-wlan-ap-2-radio-2] radio enable
[AC-wlan-ap-2-radio-2] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

サービステンプレートが正しく設定されたことを確認します。

```
[AC] display wlan service-template acstname verbose
Service template name         : stname
SSID                          : service
SSID-hide                     : Disabled
User-isolation                : Disabled
Service template status       : Enabled
Maximum clients per BSS       : Not configured
Frame format                  : Dot3
Seamless-roam                 : Disabled
Seamless-roam RSSI threshold  : 50
Seamless-roam RSSI gap        : 20
VLAN ID                       : 1
AKM mode                      : 802.1X
Security IE                   : RSN
Cipher suite                  : CCMP
TKIP countermeasure time      : 0 sec
PTK lifetime                  : 43200 sec
GTK rekey                     : Enabled
GTK rekey method              : Time-based
GTK rekey time                : 86400 sec
GTK rekey client-offline      : Disabled
User authentication mode      : 802.1X
Intrusion protection          : Disabled
Intrusion protection mode     : Temporary-block
Temporary block time          : 180 sec
Temporary service stop time   : 20 sec
Fail VLAN ID                  : Not configured
802.1X handshake              : Disabled
802.1X handshake secure       : Disabled
802.1X domain                 : imc
MAC-auth domain               : Not configured
Max 802.1X users              : 4096
Max MAC-auth users            : 4096
802.1X re-authenticate        : Disabled
Authorization fail mode       : Online
Accounting fail mode          : Online
Authorization                 : Permitted
Key derivation                : SHA1
PMF status                    : Disabled
Hotspot policy number         : Not configured
Forward policy                : Not configured
Forwarder                     : AC
FT Status                     : Enable
FT Method                     : over-the-ds
FT Reassociation Deadline     : 20 sec
QoS trust                     : Port
QoS priority                  : 0
```

ローミング状態が N/A で、FT 状態が Active であることを確認します。

```
[AC] display wlan client verbose
```

```
Total number of clients: 1

MAC address                          : a60a-1303-8361
IPv4 address                         : 10.1.1.114
IPv6 address                         : N/A
Username                             : w2
AID                                  : 1
AP ID                                : 1
AP name                              : 1
Radio ID                             : 2
SSID                                 : service
BSSID                                : 000f-e266-7788
VLAN ID                              : 1
Power save mode                      : Active
Wireless mode                        : 802.11gn
Channel bandwidth                    : 20MHz
SM power save                        : Enabled
SM power save mode                   : Static
Short GI for 20MHz                   : Not supported
Short GI for 40MHz                   : Not supported
STBC RX capability                   : Supported
STBC TX capability                   : Not supported
Support HT-MCS set                   : 0, 1, 2, 3, 4, 5, 6, 7
QoS mode                             : WMM
Listen interval                      : 20
RSSI                                 : 0
Rx/Tx rate                           : 0/0
Authentication method                : Open system
Security mode                        : RSN
AKM mode                             : 802.1X
Encryption cipher                    : CCMP
User authentication mode             : 802.1X
Authorization ACL ID                 : N/A
Authorization user profile           : N/A
Roam status                          : N/A
Key derivation                       : SHA256
PMF status                           : N/A
Forward policy                       : N/A
Online time                          : 0hr 0min 7sec
FT status                            : Active
```

クライアントを AP2 にローミングします（詳細は省略します）。

認証方法が FT で、ローミング状態が Intra-AC roam であることを確認します。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                          : a60a-1303-8361
IPv4 address                         : 10.1.1.114
IPv6 address                         : N/A
Username                             : w2
AID                                  : 1
AP ID                                : 2
AP name                              : 2
Radio ID                             : 2
SSID                                 : service
BSSID                                : 000f-e211-2233
VLAN ID                              : 1
Power save mode                      : Active
Wireless mode                        : 802.11gn
Channel bandwidth                    : 20MHz
SM power save                        : Enabled
SM power save mode                   : Static
Short GI for 20MHz                   : Not supported
Short GI for 40MHz                   : Not supported
STBC RX capability                   : Supported
STBC TX capability                   : Not supported
Support HT-MCS set                   : 0, 1, 2, 3, 4, 5, 6, 7
```

```
QoS mode                          : WMM
Listen interval                   : 20
RSSI                              : 0
Rx/Tx rate                        : 0/0
Authentication method             : FT
Security mode                     : RSN
AKM mode                          : 802.1X
Encryption cipher                 : CCMP
User authentication mode          : 802.1X
Authorization ACL ID              : N/A
Authorization user profile        : N/A
Roam status                       : Intra-AC roam
Key derivation                    : SHA256
PMF status                        : N/A
Forward policy                    : N/A
Online time                       : 0hr 0min 7sec
FT status                         : Active
```

10.10.4 Over-the-air FT と 802.1X 認証設定例

I. ネットワーク要件

図 10-8に示すように、クライアントが AP1 と AP2 間でローミングできるように Over-the-air FT を使用した AC 内ローミングを設定します。akm モードを 802.1X に設定します。

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

akm モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] akm mode dot1x
```

cipher スイートを CCMP に設定し、セキュリティ IE を RSN に設定します。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

クライアントに対する認証モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] client-security authentication-mode dot1x
[AC-wlan-st-acstname] dot1x domain imc
```

FT を有効にします。

```
[AC-wlan-st-acstname] ft enable
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

802.1X 認証モードを EAP に設定します。

```
[AC] dot1x authentication-method eap
```

RADIUS スキーム **imcc** を作成します。

```
[AC] radius scheme imcc
```

プライマリ認証とアカウンティングサーバの IP アドレスを **10.1.1.3** に設定します。

```
[AC-radius-imcc] primary authentication 10.1.1.3
[AC-radius-imcc] primary accounting 10.1.1.3
```

認証とアカウンティングサーバとパケットを交換できるように、AC に共有鍵 **12345678** を設定します。

```
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
```

RADIUS サーバに送信するユーザ名から ISP ドメイン名を外すように設定します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

ISP ドメイン **imc** を作成し、RADIUS スキーム **imcc** を認証、許可、アカウンティングに使用するためにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

AP1 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 1
[AC-wlan-ap-1] radio 2
[AC-wlan-ap-1-radio-2] service-template acstname
[AC-wlan-ap-1-radio-2] radio enable
[AC-wlan-ap-1-radio-2] quit
[AC-wlan-ap-1] quit
```

AP2 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC] wlan ap 2
[AC-wlan-ap-2] radio 2
[AC-wlan-ap-2-radio-2] service-template acstname
```

```
[AC-wlan-ap-2-radio-2] radio enable
[AC-wlan-ap-2-radio-2] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

以下の情報を確認します。

- RSN IE が有効。
- AKM モードが 802.1X。
- Cipher スイートが CCMP。
- FT 状態が Active。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                          : a60a-1303-8361
IPv4 address                         : 10.1.1.114
IPv6 address                         : N/A
Username                             : w2
AID                                  : 1
AP ID                                : 1
AP name                              : 1
Radio ID                             : 2
SSID                                 : service
BSSID                                : 000f-e266-7788
VLAN ID                              : 1
Power save mode                      : Active
Wireless mode                        : 802.11gn
Channel bandwidth                    : 20MHz
SM power save                        : Enabled
SM power save mode                   : Static
Short GI for 20MHz                   : Not supported
Short GI for 40MHz                   : Not supported
STBC RX capability                   : Supported
STBC TX capability                   : Not supported
Support HT-MCS set                   : 0, 1, 2, 3, 4, 5, 6, 7
QoS mode                             : WMM
Listen interval                      : 20
RSSI                                 : 0
Rx/Tx rate                           : 0/0
Authentication method                : Open system
Security mode                        : RSN
AKM mode                             : 802.1X
Encryption cipher                    : CCMP
User authentication mode             : 802.1X
Authorization ACL ID                 : N/A
Authorization user profile           : N/A
Roam status                          : N/A
Key derivation                       : SHA256
PMF status                           : N/A
Forward policy                       : N/A
Online time                          : 0hr 0min 19sec
FT status                            : Active
```

クライアントを AP2 にローミングします（詳細は省略します）。

認証方法が FT で、ローミング状態が Intra-AC roam であることを確認します。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                          : a60a-1303-8361
```

```
IPv4 address                    : 10.1.1.114
IPv6 address                    : N/A
Username                        : w2
AID                             : 1
AP ID                           : 2
AP name                         : 2
Radio ID                        : 2
SSID                            : service
BSSID                           : 000f-e211-2233
VLAN ID                         : 1
Power save mode                 : Active
Wireless mode                   : 802.11gn
Channel bandwidth               : 20MHz
SM power save                   : Enabled
SM power save mode              : Static
Short GI for 20MHz              : Not supported
Short GI for 40MHz              : Not supported
STBC RX capability              : Supported
STBC TX capability              : Not supported
Support HT-MCS set              : 0, 1, 2, 3, 4, 5, 6, 7
QoS mode                        : WMM
Listen interval                 : 20
RSSI                            : 0
Rx/Tx rate                      : 0/0
Authentication method           : FT
Security mode                   : RSN
AKM mode                        : 802.1X
Encryption cipher               : CCMP
User authentication mode        : 802.1X
Authorization ACL ID            : N/A
Authorization user profile      : N/A
Roam status                     : Intra-AC roam
Key derivation                  : SHA256
PMF status                      : N/A
Forward policy                  : N/A
Online time                     : 0hr 0min 7sec
FT status                       : Active
```

10.11 802.11v設定例

🕮 **メモ：**

- 802.11v の設定は V7.2.52 を含む以降のバージョンからサポートしています。
- 802.11v の設定は、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。

10.11.1 BTM と PSK 認証設定

I. ネットワーク要件

図 10-9に示すように、クライアントが AP1 から AP2 の方向へ移動するとき、より適切な AP にクライアントの接続先を誘導する為、BTM、BTM アソシエーション解除(forced)を設定します。クライアント anti-sticky を設定し、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。akm(authentication and key management)モードを PSK に設定します。

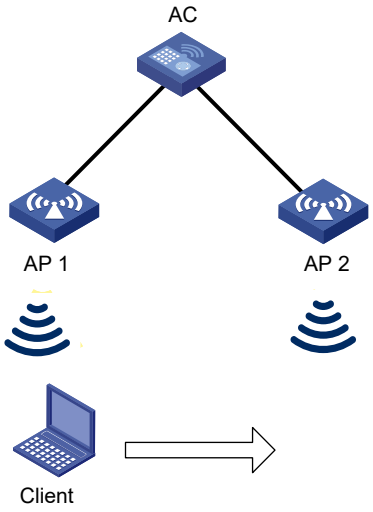


図 10-9 ネットワーク図

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

akm モードを PSK に設定し、事前共有鍵を 12345678 に設定します。

```
[AC-wlan-st-acstname] akm mode psk
[AC-wlan-st-acstname] preshared-key pass-phrase simple 12345678
```

cipher スイートを CCMP に設定し、セキュリティ IE を RSN に設定します。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

BTM を有効にします。

```
[AC-wlan-st-acstname] bss transition-management enable
```

BTM アソシエーション解除を forced で設定し、タイマを 90 秒に設定します。

```
[AC-wlan-st-acstname] bss transition-management disassociation forced timer 90
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

AP1 の radio2 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出価格を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。

```
[AC] wlan ap 1
[AC-wlan-ap-1] radio 2
[AC-wlan-ap-1-radio-2] sacp anti-sticky enable rssi 30 interval 5 forced-logoff
```

AP1 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC-wlan-ap-1-radio-2] service-template acstname
[AC-wlan-ap-1-radio-2] radio enable
[AC-wlan-ap-1-radio-2] quit
[AC-wlan-ap-1] quit
```

AP2 の radio2 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。

```
[AC] wlan ap2
[AC-wlan-ap-2] radio 2
[AC-wlan-ap-1-radio-2] sacp anti-sticky enable rssi 30 interval 5 forced-logoff
[AC-wlan-ap-2-radio-2] radio enable
```

AP2 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC-wlan-ap-2-radio-2] service-template acstname
[AC-wlan-ap-2-radio-2] radio enable
[AC-wlan-ap-2-radio-2] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

サービステンプレートが正しく設定されていることを確認します。

- RSN IE が有効。
- AKM モードが PSK。
- Cipher スイートが CCMP。
- BTM status が Active。

```
[AC] display wlan service-template acstname verbose
Service template name                          : acstname
Description                                    : Not configured
SSID                                           : service
SSID-hide                                      : Disabled
User-isolation                                 : Disabled
Service template status                        : Enabled
Maximum clients per BSS                        : Not configured
Frame format                                   : Dot3
Seamless roam status                           : Disabled
Seamless roam RSSI threshold                   : 50
Seamless roam RSSI gap                         : 20
VLAN ID                                        : 1
Service VLAN ID                                : N/A
Service VLAN TPID                              : dot1q
AKM mode                                       : PSK
Security IE                                    : RSN
Cipher suite                                   : CCMP
```

```
TKIP countermeasure time                              : 0 sec
PTK lifetime                                          : 43200 sec
PTK rekey                                             : Enabled
GTK rekey                                             : Enabled
GTK rekey method                                      : Time-based
GTK rekey time                                        : 86400 sec
GTK rekey client-offline                              : Disabled
WPA3 status                                           : Disabled
PPSK                                                  : Disabled
PPSK Fail Permit                                      : Enabled
Enhance-open status                                   : Disabled
Enhanced-open transition-mode service-template        : N/A
User authentication mode                              : Bypass
Intrusion protection                                  : Disabled
Intrusion protection mode                             : Temporary-block
Temporary block time                                  : 180 sec
Temporary service stop time                           : 20 sec
Fail VLAN ID                                          : Not configured
802.1X handshake                                      : Disabled
802.1X handshake secure                               : Disabled
802.1X domain                                         : Not configured
MAC-auth domain                                       : Not configured
Max 802.1X users per BSS                              : 512
Max MAC-auth users per BSS                            : 512
802.1X re-authenticate                                : Disabled
Authorization fail mode                               : Online
Accounting fail mode                                  : Online
Authorization                                         : Permitted
Key derivation                                        : SHA1
PMF status                                            : Disabled
Hotspot policy number                                 : Not configured
Forwarding policy status                              : Disabled
Forwarding policy name                                : Not configured
Forwarder                                             : AP
FT status                                             : Disabled
QoS trust                                             : Port
QoS priority                                          : 0
QoS U-APSD mode                                       : 1
BTM status                                            : Enabled
```

#802.11v 対応クライアントを AP1 に接続します。(詳細は省略します)

クライアントの情報で、BTM mode が Active となっていることを確認します。

```
[AC-wlan-st-acstname]display wlan client verbose
Total number of clients: 1

MAC address                       : a601-13af-8cc3
IPv4 address                      : N/A
IPv6 address                      : N/A
Username                          : N/A
AID                               : 1
AP ID                             : 1
AP name                           : 1
Radio ID                          : 2
Channel                           : 100
SSID                              : service
BSSID                             : 882a-5e6c-5fb0
VLAN ID                           : 1
Service VLAN ID                   : N/A
Sleep count                       : 0
Wireless mode                     : 802.11ac
Channel bandwidth                 : 80MHz
SM power save                     : Disabled
Short GI for 20MHz                : Supported
Short GI for 40MHz                : Supported
Short GI for 80MHz                : Supported
Short GI for 160/80+80MHz         : Not supported
STBC RX capability                : Supported
STBC TX capability                : Supported
```

```
LDPC RX capability                : Supported
Beamformee STS capability         : N/A
Number of Sounding Dimensions     : N/A
SU beamformee capability          : Not supported
MU beamformee capability          : Not supported
Block Ack                         : N/A
Supported VHT-MCS set             : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
                                    NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set              : 0, 1, 2, 3, 4, 5, 6, 7,
                                    8, 9, 10, 11, 12, 13, 14,
                                    15
Supported rates                   : 6, 9, 12, 18, 24, 36,
                                    48, 54 Mbps
QoS mode                          : WMM
Listen interval                   : 250
RSSI                              : 0
Rx/Tx rate                        : 0/0 Mbps
Speed                             : N/A
Authentication method             : Open system
Security mode                     : RSN
AKM mode                          : PSK
Cipher suite                      : CCMP
User authentication mode          : Bypass
WPA3 status                       : Disabled
Authorization CAR                 : N/A
Authorization ACL ID              : N/A
Authorization user profile        : N/A
Roam status                       : N/A
Key derivation                    : SHA1
PMF status                        : N/A
Forwarding policy name            : Not configured
Online time                       : 0days 0hours 0minutes 35seconds
FT status                         : Inactive
BTM mode                          : Active
```

10.11.2 BTM と 802.1X 認証設定

I. ネットワーク要件

図 10-9に示すように、クライアントが AP1 から AP2 の方向へ移動するとき、より適切な AP にクライアントの接続先を誘導する為、BTM、BTM アソシエーション解除 (recommended)、クライアント anti-sticky を設定し、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。akm モードを 802.1X に設定します。

II. 設定手順

サービステンプレート **acstname** を作成します。

```
<AC> system-view
[AC] wlan service-template acstname
```

SSID を **service** に設定します。

```
[AC-wlan-st-acstname] ssid service
```

akm モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] akm mode dot1x
```

cipher スイートを CCMP に設定し、セキュリティ IE を RSN に設定します。

```
[AC-wlan-st-acstname] cipher-suite ccmp
[AC-wlan-st-acstname] security-ie rsn
```

クライアントに対する認証モードを 802.1X に設定します。

```
[AC-wlan-st-acstname] client-security authentication-mode dot1x
[AC-wlan-st-acstname] dot1x domain imc
```

BTM を有効にします。

```
[AC-wlan-st-acstname] bss transition-management enable
```

BTM アソシエーション解除を recommended で設定し、タイマを 90 秒に設定します。

```
[AC-wlan-st-acstname] bss transition-management disassociation recommended timer 90
```

サービステンプレートを有効にします。

```
[AC-wlan-st-acstname] service-template enable
[AC-wlan-st-acstname] quit
```

802.1X 認証モードを EAP に設定します。

```
[AC] dot1x authentication-method eap
```

RADIUS スキーム **imcc** を作成します。

```
[AC] radius scheme imcc
```

プライマリ認証とアカウンティングサーバの IP アドレスを **10.1.1.3** に設定します。

```
[AC-radius-imcc] primary authentication 10.1.1.3
[AC-radius-imcc] primary accounting 10.1.1.3
```

認証とアカウンティングサーバとパケットを交換できるように、AC に共有鍵 **12345678** を設定します。

```
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
```

RADIUS サーバに送信するユーザ名から ISP ドメイン名を外すように設定します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

ISP ドメイン **imc** を作成し、RADIUS スキーム **imcc** を認証、許可、アカウンティングに使用するためにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
```

```
[AC-isp-imc] quit
```

AP1 の radio2 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出価格を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。

```
[AC] wlan ap 1
[AC-wlan-ap-1] radio 2
[AC-wlan-ap-1-radio-2] sacp anti-sticky enable rssi 30 interval 5 forced-logoff
```

AP1 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC-wlan-ap-1-radio-2] service-template acstname
[AC-wlan-ap-1-radio-2] radio enable
[AC-wlan-ap-1-radio-2] quit
[AC-wlan-ap-1] quit
```

AP2 の radio2 でクライアント anti-sticky を有効にし、RSSI しきい値を 30 に設定し、検出間隔を 5 秒に設定し、非 802.11v クライアントの強制ログオフを有効にします。

```
[AC] wlan ap2
[AC-wlan-ap-2] radio 2
[AC-wlan-ap-1-radio-2] sacp anti-sticky enable rssi 30 interval 5 forced-logoff
[AC-wlan-ap-2-radio-2] radio enable
```

AP2 の radio2 に対してサービステンプレート **acstname** を設定します。

```
[AC-wlan-ap-2-radio-2] service-template acstname
[AC-wlan-ap-2-radio-2] radio enable
[AC-wlan-ap-2-radio-2] quit
[AC-wlan-ap-2] quit
```

III. 設定確認

サービステンプレートが正しく設定されたことを確認します。

- RSN IE が有効。
- AKM モードが 802.1X。
- Cipher スイートが CCMP。
- BTM status が Enabled。

```
[AC] display wlan service-template acstname verbose
Service template name                          : acstname
Description                                    : Not configured
SSID                                           : service
SSID-hide                                      : Disabled
User-isolation                                 : Disabled
Service template status                        : Enabled
Maximum clients per BSS                        : Not configured
Frame format                                   : Dot3
Seamless roam status                           : Disabled
Seamless roam RSSI threshold                   : 50
Seamless roam RSSI gap                         : 20
```

```
VLAN ID                                          : 1
Service VLAN ID                                  : N/A
Service VLAN TPID                                : dot1q
AKM mode                                         : 802.1X
Security IE                                      : RSN
Cipher suite                                     : CCMP
TKIP countermeasure time                         : 0 sec
PTK lifetime                                     : 43200 sec
PTK rekey                                        : Enabled
GTK rekey                                        : Enabled
GTK rekey method                                 : Time-based
GTK rekey time                                   : 86400 sec
GTK rekey client-offline                         : Disabled
WPA3 status                                      : Disabled
PPSK                                             : Disabled
PPSK Fail Permit                                 : Enabled
Enhance-open status                              : Disabled
Enhanced-open transition-mode service-template   : N/A
User authentication mode                         : 802.1X
Intrusion protection                             : Disabled
Intrusion protection mode                        : Temporary-block
Temporary block time                             : 180 sec
Temporary service stop time                      : 20 sec
Fail VLAN ID                                     : Not configured
802.1X handshake                                 : Disabled
802.1X handshake secure                          : Disabled
802.1X domain                                    : imc
MAC-auth domain                                  : Not configured
Max 802.1X users per BSS                         : 512
Max MAC-auth users per BSS                       : 512
802.1X re-authenticate                           : Disabled
Authorization fail mode                          : Online
Accounting fail mode                             : Online
Authorization                                    : Permitted
Key derivation                                   : SHA1
PMF status                                       : Disabled
Hotspot policy number                            : Not configured
Forwarding policy status                         : Disabled
Forwarding policy name                           : Not configured
Forwarder                                        : AP
FT status                                        : Disabled
QoS trust                                        : Port
QoS priority                                     : 0
QoS U-APSD mode                                  : 1
BTM status                                       : Enabled
```

#802.11v 対応クライアントを AP1 に接続します。(詳細は省略します)

#クライアントの情報で、BTM mode が Active となっていることを確認します。

[AC]display wlan client verbose

```
Total number of clients: 1

 MAC address                    : 0908-37af-8cc3
 IPv4 address                   : N/A
 IPv6 address                   : N/A
 Username                       : tester
 AID                            : 1
 AP ID                          : 1
 AP name                        : 1
 Radio ID                       : 2
 Channel                        : 100
 SSID                           : service
 BSSID                          : 882a-5e6c-5fb0
 VLAN ID                        : 1
 Service VLAN ID                : N/A
 Sleep count                    : 0
 Wireless mode                  : 802.11ac
 Channel bandwidth              : 80MHz
```

```
SM power save                       : Disabled
Short GI for 20MHz                  : Supported
Short GI for 40MHz                  : Supported
Short GI for 80MHz                  : Supported
Short GI for 160/80+80MHz           : Not supported
STBC RX capability                  : Supported
STBC TX capability                  : Supported
LDPC RX capability                  : Supported
Beamformee STS capability           : N/A
Number of Sounding Dimensions       : N/A
SU beamformee capability            : Not supported
MU beamformee capability            : Not supported
Block Ack                           : N/A
Supported VHT-MCS set               : NSS1 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
                                      NSS2 0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Supported HT MCS set                : 0, 1, 2, 3, 4, 5, 6, 7,
                                      8, 9, 10, 11, 12, 13, 14,
                                      15
Supported rates                     : 6, 9, 12, 18, 24, 36,
                                      48, 54 Mbps
QoS mode                            : WMM
Listen interval                     : 250
RSSI                                : 0
Rx/Tx rate                          : 0/0 Mbps
Speed                               : N/A
Authentication method               : Open system
Security mode                       : RSN
AKM mode                            : 802.1X
Cipher suite                        : CCMP
User authentication mode            : 802.1X
WPA3 status                         : Disabled
Authorization CAR                   : N/A
Authorization ACL ID                : N/A
Authorization user profile          : N/A
Roam status                         : N/A
Key derivation                      : SHA1
PMF status                          : N/A
Forwarding policy name              : Not configured
Online time                         : 0days 0hours 0minutes 12seconds
FT status                           : Inactive
BTM mode                            : Active
```

目次

11 章 WLAN ロードバランスの設定 11-1
11.1 概要 11-1
11.1.1 実行必須条件 11-1
11.1.2 動作メカニズム 11-2
11.1.3 ロードバランスモード 11-2
11.1.4 ロードバランスタイプ 11-4
11.2 設定作業リスト 11-4
11.3 WLAN ロードバランスの設定 11-5
11.3.1 WLAN ロードバランスの有効化 11-5
11.3.2 ロードバランスモードの設定 11-5
11.3.3 ロードバランスグループの設定 11-5
11.3.4 ロードバランスパラメータの設定 11-6
11.4 WLAN ロードバランスに対する SNMP 通知の有効化 11-6
11.5 WLAN ロードバランスの表示と維持 11-7
11.6 無線ベース WLAN ロードバランスの設定例 11-7
11.6.1 セッションモードロードバランスの設定 11-7
11.6.2 トラフィックモードロードバランスの設定 11-9
11.6.3 帯域幅モードロードバランスの設定 11-11
11.7 ロードバランスグループベース WLAN ロードバランスの設定例 11-13
11.7.1 セッションモードロードバランスの設定 11-13
11.7.2 トラフィックモードロードバランスの設定 11-16
11.7.3 帯域幅モードロードバランスの設定 11-18

11章 WLAN ロードバランスの設定

本章では、AP は有効な無線をひとつだけ持つと仮定します。

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

11.1 概要

WLAN ロードバランス機能は、密集した WLAN において無線サービスの品質とクライアントの帯域幅を保証するため、AP を経由したクライアントの負荷を動的に分散させます。

11.1.1 実行必須条件

WLAN ロードバランスを特定の AP 間で実行するために、AP は同じ AC に管理されなければなりません。同じ AC で管理することで、クライアントは AP を検出することができます。図 11-1 に示すように、ロードバランスは、同じ AC で管理された AP 1、AP 2、AP 3 上で有効化されます。AP 3 は最大ロードに達します。Client 5 が AP 3 と関連づけようとしたとき、AC はそのアソシエーション要求を拒否します。しかし、Client 5 が AP 3 しか発見できない場合、Client 5 は AP 3 に対してアソシエーション要求を送信し続けます。AP 3 が Client 5 を拒否する回数が、指定した拒絶の最大数に達した場合、AP 3 は Client 5 のアソシエーション要求を承認します。

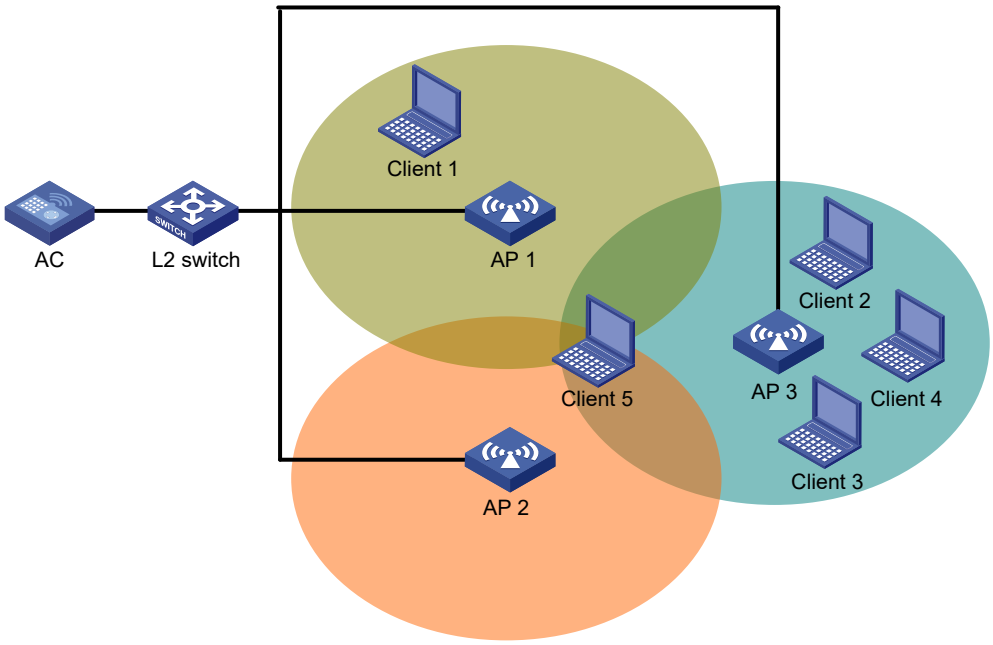


図 11-1 実行必須条件

11.1.2 動作メカニズム

AC は、以下の条件が満たされたときロードバランスを実行します。

- AP の負荷がしきい値に到達した場合、ロードバランスを実行します。
- AP と最も軽い負荷の AP との間の負荷のギャップが、しきい値に到達した場合、ロードバランスを実行します。

負荷と AP に対する負荷のギャップがそれぞれのしきい値に達すると、AP はクライアントのアソシエーション要求を拒否します。AP がクライアントを拒否する回数が、指定した拒絶の最大数に達した場合、AP はクライアントのアソシエーション要求を承認します。

11.1.3 ロードバランスモード

AC は、セッションモード、トラフィックモード、帯域幅モードロードバランスをサポートします。以下の条件が満たされたとき、AC は特定のモードのロードバランスを実行します。

- 指定したセッション/トラフィック/帯域幅しきい値に達する場合、ロードバランスを実行します。
- 指定したセッション/トラフィック/帯域幅ギャップしきい値に達する場合、ロードバランスを実行します。

I. セッションモードロードバランス

図 11-2 に示すように、Client 1 は AP 1 に関連づき、Client 2～Client 4 は AP 2 に関連づいています。セッションしきい値とセッションギャップしきい値を、それぞれ 3 と 2 に設定したと仮定します。Client 5 が AP 2 と関連づけようとしたとき、セッションしきい値とセッションギャップしきい値がともに最大値に達するため、AP 2 はその要求を拒否します。

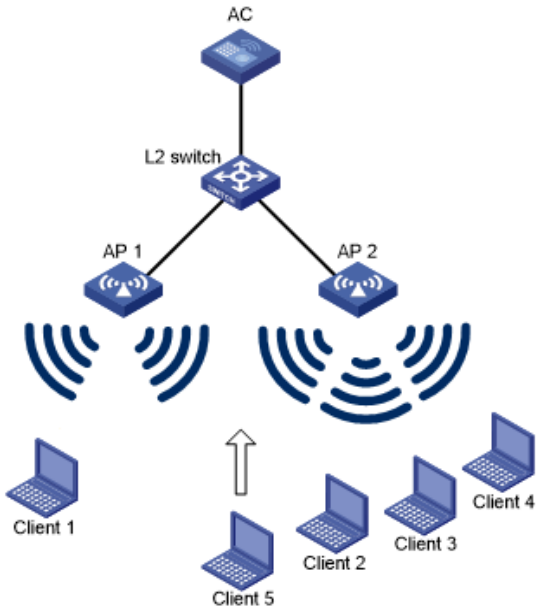


図 11-2 セッションモードロードバランス

II. トラフィックモードロードバランス

図 11-3 に示すように、Client 1 は AP 1 に関連付き、Client 2 は AP 2 に関連付いています。AP 1 のトラフィックと、AP1 と AP 2 のトラフィックギャップが、それぞれのしきい値に達するとき、AP 1 は Client 3 からのアソシエーション要求を拒否します。

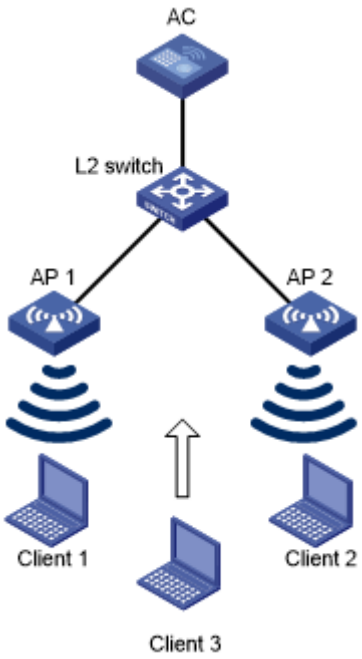


図 11-3　トラフィックモードロードバランス

III. 帯域幅モードロードバランス

図 11-4 に示すように、Client 1 は AP 1 に関連付き、Client 2 は AP 2 に関連付いています。AP 1 の帯域幅と、AP 1 と AP 2 の帯域幅ギャップが、それぞれのしきい値に達するとき、AP 1 は Client 3 からの要求を拒否します。

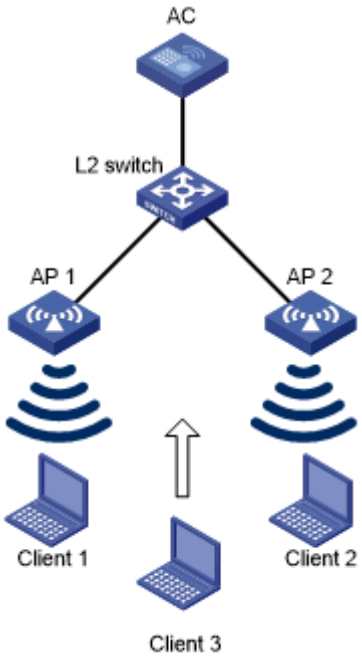


図 11-4 帯域幅モードロードバランス

11.1.4 ロードバランスタイプ

AC は以下のロードバランスタイプをサポートします。

- **無線ベース**－AC は、AP の隣接レポートに基づいたロードバランスに参加する AP を決定します。AP の隣接レポートは、AP に検出された各クライアントの MAC アドレスと RSSI 値を記録します。AC は、以下の条件のいずれかが満たされたときに、AP がロードバランスに参加すると決定します。
  - □ クライアントが AP とのアソシエーションを要求し、クライアントの RSSI が RSSI しきい値より低いと AP が検出した場合。
  - □ クライアントの RSSI が RSSI しきい値に達するが、クライアントは AP とのアソシエーションを要求しないと AP が検出した場合。
- **ロードバランスグループベース**－要求した AP の無線をロードバランスグループに追加します。AC は、ロードバランスグループに属さない無線上ではロードバランスを実行しません。

11.2 設定作業リスト

作業リスト	補足
（必須設定項目） WLANロードバランスの有効化	—
（必須設定項目） ロードバランスモードの設定	—
（オプション設定項目） ロードバランスグループの設定	ロードバランスグループを作成しない場合、ACは無線ベースロードバランスを実行します。

作業リスト	補足
（オプション設定項目） ロードバランスパラメータの設定	—
（オプション設定項目） WLANロードバランスに対するSNMP通知の有効化	—

11.3 WLANロードバランスの設定

ロードバランスの設定をする前に、クイックアソシエーション機能が無効であることを確認してください。クイックアソシエーションに関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN アクセスの設定"* を参照してください。

11.3.1 WLAN ロードバランスの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． WLAN ロードバランスを有効にする	**wlan load-balance enable**	デフォルト：無効

11.3.2 ロードバランスモードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． ロードバランスモードを設定にする	• セッションモードロードバランスを設定する：**wlan load-balance mode session** *value* [**gap** *gap-value*] • トラフィックモードロードバランスを設定する：**wlan load-balance mode traffic** *value* [**gap** *gap-value*] • 帯域幅モードロードバランスを設定する：**wlan load-balance mode bandwidth** *value* [**gap** *gap-value*]	デフォルト：セッションモードロードバランスが使用されます。

11.3.3 ロードバランスグループの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． ロードバランスグループを作成し、load balancing group view に移行する	**wlan load-balance group** *group-id*	デフォルト：設定なし
3． AP の無線をロードバランスグループに追加する	**ap name** *ap-name* **radio** *radio-id*	デフォルト：設定なし
4． （オプション設定項目） ロードバランスグループに対して記述を設定する	**description** *text*	デフォルト：設定なし

11.3.4 ロードバランスパラメータの設定

以下のパラメータはロードバランスの計算に影響を与えます。

- **ロードバランス RSSI しきい値**ークライアントの RSSI が、指定した RSSI しきい値より低いと AP が検出した場合、AP は以下のいずれかの操作を実行します。
  - 複数の AP がクライアントを検出できる場合、AP はクライアントがアソシエーションを要求したときのみロードバランスに参加します。
  - 単独の AP のみがクライアントを検出できる場合、クライアントが AP と関連付く機会をよりもてるように拒絶最大数を 1 まで小さくします。
- **アソシエーション要求に対する拒絶最大数**－AP がクライアントを拒否する回数が、指定した拒絶最大数に達する場合、AP はクライアントにアソシエーション要求を承認します。

ロードバランスパラメータの設定手順は以下のとおりです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． RSSI しきい値を設定する	**wlan load-balance rssi-threshold** *rssi-threshold*	デフォルト： 25
3． アソシエーション要求に対する拒絶最大数を設定する	**wlan load-balance access-denial** *access-denial*	デフォルト：10

11.4 WLANロードバランスに対するSNMP通知の有効化

NMS に WLAN ロードバランスの重要なイベントを報告するために、SNMP 通知を WLAN ロードバランスに対して有効にします。WLAN ロードバランスイベント通知が正確に送信されるためには、QX-W1000/W1100 シリーズアクセスポイント オペレーションマニュアルのセクション 11 システム管理 の *“SNMP”* に記述されるように、SNMP の設定もしなければなりません。

SNMP 通知を WLAN ロードバランスに対して有効にする手順は以下のとおりです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． WLAN ロードバランスに対して SNMP 通知を有効にする	**snmp-agent trap enable wlan load-balance**	デフォルト：無効

11.5 WLANロードバランスの表示と維持

すべての view で **display** コマンドを実行できます。

操作	コマンド
ロードバランスグループ情報を表示する	**display wlan load-balance group** { *group-id* | **all** }
サービステンプレートにバインドされたラジオのロードバランス情報を表示する	**display wlan load-balance status service-template** *template-name* { **client** *mac-address* | **group** *group-id* }

11.6 無線ベースWLANロードバランスの設定例

11.6.1 セッションモードロードバランスの設定

I. ネットワーク要件

図 11-5 に示すように、AP 1 と AP 2 は AC により管理され、クライアントは AP を検出できます。

以下の条件が満たされたとき、AC が AP 1 と AP 2 上でセッションモードロードバランスを実行するように設定します。

- 1 つの AP 上のセッション数が 3 に達する場合。
- AP 間のセッションギャップが 2 に達する場合。

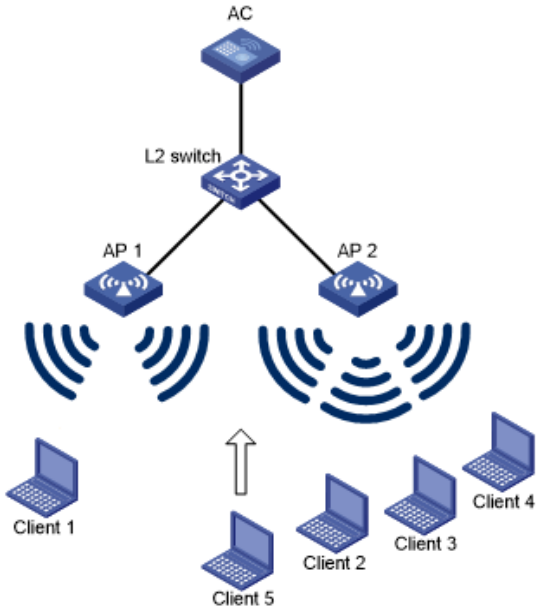


図 11-5 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を session-balance に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid session-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

AP template ap2 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
```

```
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

ロードバランスモードをセッションモードに設定し、セッションしきい値とセッションギャップしきい値をそれぞれ 3 と 2 に設定します。

```
[AC] wlan load-balance mode session 3 gap 2
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

以下の条件が満たされるとき、AC が AP 1 と AP 2 に対してセッションモードロードバランスを実行することを確認します。

- 1 つの AP 上でのセッション数が 3 に達する場合。
- AP 間のセッションギャップが 2 に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

11.6.2 トラフィックモードロードバランスの設定

I. ネットワーク要件

図 11-6 に示すように、AP 1 と AP 2 は AC により管理され、クライアントは AP を検出できます。各 AP に対する最大帯域幅は 150Mbps です。

以下の条件が満たされたとき、AC が AP 1 と AP 2 上でトラフィックモードロードバランスを実行するように設定します。

- 1 つの AP のトラフィックが 30Mbps（最大帯域幅の 20%）に達する場合。
- AP 間のトラフィックギャップが 15Mbps（最大帯域幅の 10%）に達する場合。

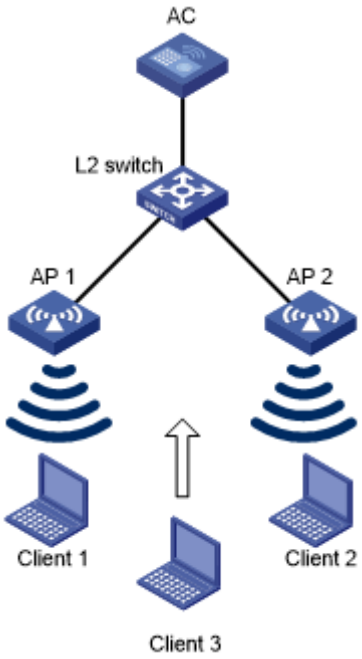


図 11-6 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を traffic-balance に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid traffic-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
```

```
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

ロードバランスモードをトラフィックモードに設定し、トラフィックしきい値とトラフィックギャップしきい値をそれぞれ 20%と 10%に設定します。

```
[AC] wlan load-balance mode traffic 20 gap 10
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

以下の条件が満たされるとき、AC が AP 1 と AP 2 に対してトラフィックモードロードバランスを実行することを確認します。

- 1 つの AP のトラフィックが 30Mbps に達する場合。
- AP 間のトラフィックギャップが 15Mbps に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

11.6.3 帯域幅モードロードバランスの設定

I. ネットワーク要件

図 11-7 に示すように、AP 1 と AP 2 は AC により管理され、クライアントは AP を発見できます。

以下の条件が満たされたとき、AC が AP 1 と AP 2 上で帯域幅モードロードバランスを実行するように設定します。

- 1 つの AP の帯域幅が 12Mbps に達する場合。
- AP 間の帯域幅ギャップが 3Mbps に達する場合。

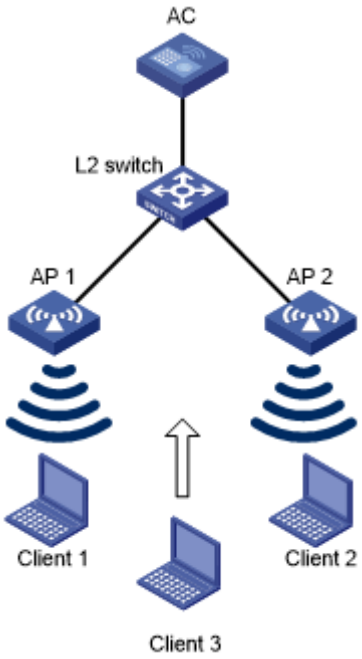


図 11-7 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を bandwidth-balance に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid bandwidth-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
```

```
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

ロードバランスモードを帯域幅モードに設定し、帯域幅しきい値と帯域幅ギャップしきい値をそれぞれ 12 Mbps と 3 Mbps に設定します。

```
[AC] wlan load-balance mode bandwidth 12 gap 3
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

以下の条件が満たされるとき、AC が AP 1 と AP 2 に対して帯域幅モードロードバランスを実行することを確認します。

- 1 つの AP の帯域幅が 12 Mbps に達する場合。
- AP 間の帯域幅ギャップが 3 Mbps に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

11.7 ロードバランスグループベースWLANロードバランスの設定例

11.7.1 セッションモードロードバランスの設定

I. ネットワーク要件

図 11-8 に示すように、AP 1、AP 2、AP 3 は AC により管理され、クライアントは AP を発見できます。

以下の条件が満たされたとき、AC が AP 1 の radio 2 と AP 2 の radio 2 上でセッションモードロードバランスを実行するように設定します。

- 1 つの無線上のセッション数が 3 に達する場合。
- 無線間のセッションギャップが 2 に達する場合。

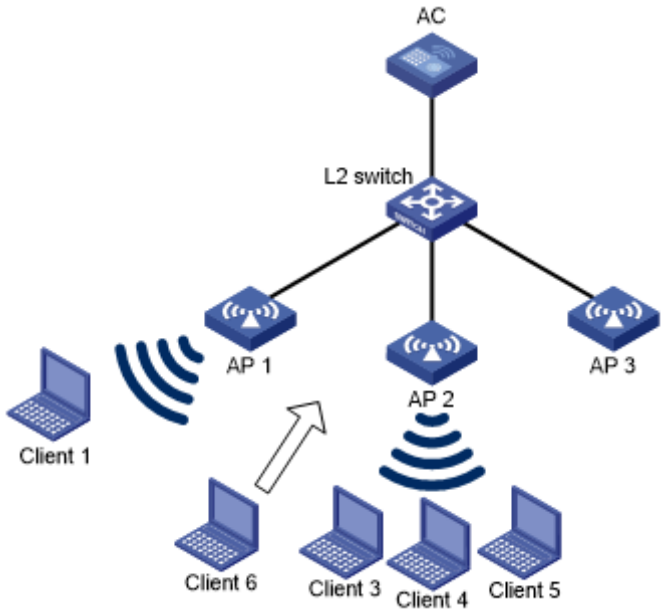


図 11-8 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を session-balance に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid session-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、model と serial ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
```

```
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

AP template ap3 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap3 model QX-W1020
[AC-wlan-ap-ap3] serial-id 210235A29G007C000022
```

サービステンプレート 1 を AP 3 の radio 2 に設定します。

```
[AC-wlan-ap-ap3] radio 2
[AC-wlan-ap-ap3-radio-2] service-template 1
[AC-wlan-ap-ap3-radio-2] radio enable
[AC-wlan-ap-ap3-radio-2] quit
[AC-wlan-ap-ap3] quit
```

ロードバランスモードをセッションモードに設定し、セッションしきい値とセッションギャップしきい値をそれぞれ 3 と 2 に設定します。

```
[AC] wlan load-balance mode session 3 gap 2
```

load balancing group 1 を作成します。

```
[AC] wlan load-balance group 1
```

AP 1 の radio 2 と AP 2 の radio 2 をロードバランスグループ 1 に追加します。

```
[AC-wlan-lb-group-1] ap name ap1 radio 2
[AC-wlan-lb-group-1] ap name ap2 radio 2
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

以下の条件が満たされるとき、AC が AP 1 の radio 2 と AP 2 の radio 2 に対してセッションモードロードバランスを実行することを確認します。

- 1 つの無線上でのセッション数が 3 に達する場合。
- 無線間のセッションギャップが 2 に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

11.7.2 トラフィックモードロードバランスの設定

I. ネットワーク要件

図 11-9 に示すように、AP 1、AP 2、AP 3 は AC により管理され、クライアントは AP を検出できます。

以下の条件が満たされたとき、AC が AP 1 の radio 2 と AP 2 の radio 2 上でトラフィックモードロードバランスを実行するように設定します。

- 1 つの無線のトラフィックが 30Mbps（最大帯域幅の 20%）に達する場合。
- 無線間のトラフィックギャップが 15Mbps（最大帯域幅の 10%）に達する場合。

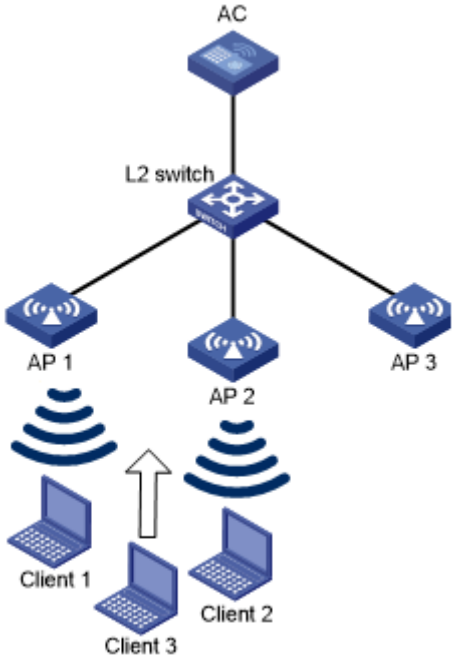


図 11-9 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を traffic-balance に設定します。

```
<AC> system
[AC] wlan service-template 1
[AC-wlan-st-1] ssid traffic-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、model と serial ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

AP template ap3 を作成し、model と serial ID を指定します。

```
<AC> system-view
[AC] wlan ap ap3 model QX-W1020
[AC-wlan-ap-ap3] serial-id 210235A29G007C000022
```

サービステンプレート 1 を AP 3 の radio 2 に設定します。

```
[AC-wlan-ap-ap3] radio 2
[AC-wlan-ap-ap3-radio-2] service-template 1
[AC-wlan-ap-ap3-radio-2] radio enable
[AC-wlan-ap-ap3-radio-2] quit
[AC-wlan-ap-ap3] quit
```

#ロードバランスモードをトラフィックモードに設定し、トラフィックしきい値とトラフィックギャップしきい値をそれぞれ 20%と 10%に設定します。

```
[AC] wlan load-balance mode traffic 20 gap 10
```

load balancing group 1 を作成します。

```
[AC] wlan load-balance group 1
```

AP 1 の radio 2 と AP 2 の radio 2 をロードバランスグループ 1 に追加します。

```
[AC-wlan-lb-group-1] ap name ap1 radio 2
[AC-wlan-lb-group-1] ap name ap2 radio 2
[AC-wlan-lb-group-1] quit
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

#以下の条件が満たされるとき、AC が AP 1 の radio 2 と AP 2 の radio 2 に対してトラフィックモードロードバランスを実行することを確認します。

- 1 つの無線でのトラフィックが 30Mbps に達する場合。
- 無線間のトラフィックギャップが 15Mbps に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

11.7.3 帯域幅モードロードバランスの設定

I. ネットワーク要件

図 11-10 に示すように、AP 1、AP 2、AP 3 は AC により管理され、クライアントは AP を発見できます。

以下の条件が満たされたとき、AC が AP 1 の radio 2 と AP 2 の radio 2 上で帯域幅モードロードバランスを実行するように設定します。

- 1 つの無線の帯域幅が 12Mbps に達する場合。
- 無線間の帯域幅ギャップが 3Mbps に達する場合。

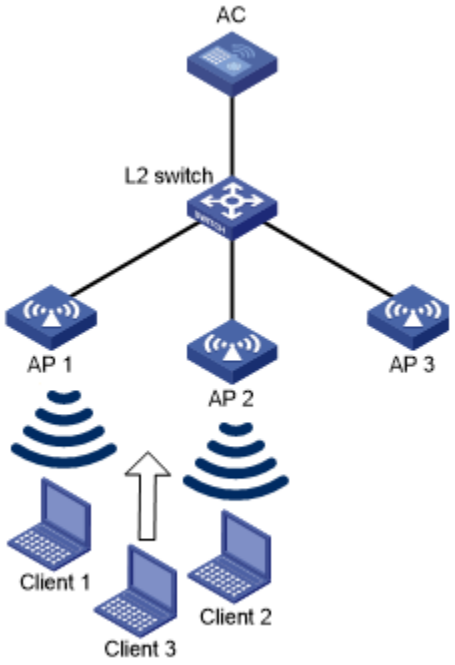


図 11-10 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を bandwidth-balance に設定します。

```
<AC> system
[AC] wlan service-template 1
[AC-wlan-st-1] ssid bandwidth-balance
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

サービステンプレート 1 を AP 1 の radio 2 に設定します。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

AP template ap2 を作成し、model と serial ID を指定します。

```
[AC] wlan ap ap2 model QX-W1020
[AC-wlan-ap-ap2] serial-id 210235A29G007C000021
```

サービステンプレート 1 を AP 2 の radio 2 に設定します。

```
[AC-wlan-ap-ap2] radio 2
[AC-wlan-ap-ap2-radio-2] service-template 1
[AC-wlan-ap-ap2-radio-2] radio enable
[AC-wlan-ap-ap2-radio-2] quit
[AC-wlan-ap-ap2] quit
```

AP template ap3 を作成し、model と serial ID を指定します。

```
[AC] wlan ap ap3 model QX-W1020
[AC-wlan-ap-ap3] serial-id 210235A29G007C000022
```

サービステンプレート 1 を AP 3 の radio 2 に設定します。

```
[AC-wlan-ap-ap3] radio 2
[AC-wlan-ap-ap3-radio-2] service-template 1
[AC-wlan-ap-ap3-radio-2] radio enable
[AC-wlan-ap-ap3-radio-2] quit
```

```
[AC-wlan-ap-ap3] quit
```

ロードバランスモードを帯域幅モードに設定し、帯域幅しきい値と帯域幅ギャップしきい値をそれぞれ 12 Mbps と 3 Mbps に設定します。

```
[AC] wlan load-balance mode bandwidth 12 gap 3
```

#ロードバランスグループ 1 を作成します。

```
[AC] wlan load-balance group 1
```

AP 1 の radio 2 と AP 2 の radio 2 をロードバランスグループ 1 に追加します。

```
[AC-wlan-lb-group-1] ap name ap1 radio 2
[AC-wlan-lb-group-1] ap name ap2 radio 2
[AC-wlan-lb-group-1] quit
```

WLAN ロードバランスを有効にします。

```
[AC] wlan load-balance enable
```

III. 設定の確認

#以下の条件が満たされるとき、AC が AP 1 の radio 2 と AP 2 の radio 2 に対して帯域幅モードロードバランスを実行することを確認します。

- 1 つの無線の帯域幅が 12 Mbps に達する場合。
- 無線間の帯域幅ギャップが 3 Mbps に達する場合。（詳細は省略します。）

display wlan client コマンドを使用し、AP 1 と AP 2 がロードバランスされるか確認します。（詳細は省略します。）

目次

12 章 WLAN 無線リソースの計測の設定.....12-1
12.1 概要.....12-1
12.1.1 802.11h 計測.....12-1
12.1.2 802.11k 計測.....12-2
12.2 設定作業リスト.....12-2
12.3 無線リソース計測の有効化.....12-3
12.3.1 radio view での無線リソース計測の有効化.....12-3
12.3.2 AP group radio view での無線リソース計測の有効化.....12-3
12.4 計測期間と計測間隔の設定.....12-4
12.4.1 radio view での計測期間と計測間隔の設定.....12-4
12.4.2 AP group radio view での計測期間と計測間隔の設定.....12-4
12.5 クライアント無線リソース計測性能に対するマッチモードの設定.....12-5
12.5.1 radio view でのクライアント無線リソース計測性能に対するマッチモードの設定12-5
12.5.2 AP group radio view でのクライアント無線リソース計測性能に対するマッチモードの設定.....12-5
12.6 WLAN 無線リソース計測の表示と維持.....12-5
12.7 無線リソース計測の設定例.....12-6
12.7.1 ネットワーク要件.....12-6
12.7.2 設定手順.....12-6
12.7.3 設定の確認.....12-7

12章 WLAN 無線リソースの計測の設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

12.1 概要

WLAN 無線リソース計測は、チャネル品質と無線性能を計測します。WLAN 無線リソース計測により、クライアントと AP は無線環境を学習可能になり、また、スペクトル、電力、帯域幅などの無線リソースをより効果的に使用可能になります。

12.1.1 802.11h 計測

802.11h 計測は、5GHz 帯のチャネルを計測します。表 12-1 は、802.11h 計測がサポートする計測の一覧です。

表 12-1 802.11h 計測

タイプ		内容
スペクトル管理計測	Basic	クライアントが以下のいずれかを検出したかを計測します。 ● 別のBSSからのパケット ● OFDMプリアンブル ● レーダ信号 ● 未知の信号
	CCA（Clear Channel Assessment）	計測時間の総和に対するチャネルのビジー時間の割合を計測します。
	RPI（Receive Power Indication）	計測時間の総和に対する異なるRPI範囲の時間の割合を計測します。
TPC（Transmit Power Control）計測		リンク冗長性とクライアントに対する伝送電力を計測します。

802.11h 計測は、以下の手順で作動します。

1) AP は、802.11h 計測要求を送信できるとクライアントに通知するために、ビーコン、プローブ応答、アソシエーション応答、または再アソシエーション応答内でスペクトル計測フィールドを 1 に設定します。
2) クライアントから計測要求を受信すると、AP は要求された計測を実行し、クライアントにレポートを送信します。

12.1.2 802.11k 計測

802.11k 計測は、2.4GHz 帯と 5GHz 帯の両方のチャネルを計測します。表 12-2 は、802.11k 計測がサポートする計測の一覧です。

表 12-2 802.11k 計測

タイプ		内容
無線計測	Beacon	ビーコン、計測パイロットパケット、プローブ応答のRCPI（Received Channel Power Indicator）とRSNI（Received Signal to Noise Indicator）を計測します。
	Frame	伝送されたフレームの数と伝送されたフレームに対する平均RCPIを計測します。
	Station statistics	送受信されたフラグメント総計、マルチキャストフレーム総計、失敗総計、リトライ総計、ACK失敗総計を計測します。
	Transmit stream	特定の伝送ストリームのフレームを計測します。
	Channel load	チャネル使用を計測します。
	Location	要求者と要求されたものの相対的な位置を計測します。
	Noise histogram	異なるデシベル範囲での雑音分布を計測します。
Link measurement		リンク冗長性とクライアントに対する伝送電力を計測します。
Neighbor measurement		チャネルとネイバAPのBSSIDを計測します。

802.11k 計測は、以下の手順で作動します。

1) AP は、802.11k 計測要求を送信できるとクライアントに通知するために、ビーコン、プローブ応答、アソシエーション応答、または再アソシエーション応答内で無線計測フィールドを 1 に設定します。
これらの応答フレームは、AP がサポートする計測タイプのクライアントに通知するために、AP の計測性能も運びます。
AP は、クライアントがすばやく AP を検出できるように、計測パイロットフレームを定期的に送信します。計測パイロットフレームはビーコンよりも頻繁に送信され、運ぶ情報はより少ないです。
2) クライアントから計測要求を受信すると、AP は要求された計測を実行し、クライアントにレポートを送信します。
AP は、クライアントに定期的に計測要求を送信し、クライアントから計測報告を収集することもできます。

12.2 設定作業リスト

作業リスト
（必須設定項目） 無線リソース計測の有効化
（オプション設定項目） 計測期間と計測間隔の設定
（オプション設定項目） クライアント無線リソース計測性能に対するマッチモードの設定

12.3 無線リソース計測の有効化

12.3.1 radio view での無線リソース計測の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． 無線リソース計測を有効にする	**resource-measure enable**	デフォルト：AP group view内の設定が使用されます。 リンク計測、ネイバ計測、無線計測を有効にする場合、無線リソース計測を有効にしなければなりません。
5． スペクトル管理を有効にする	**spectrum-management enable**	デフォルト：AP group view内の設定が使用されます。 スペクトル計測またはTPC計測は、スペクトル管理を有効にしたあとにのみ適用されます。 このコマンドに関する詳細はQX-W1000/W1100シリーズアクセスポイント Anchor-AC コマンドマニュアルの *"WLAN RRM"* を参照してください。
6． 計測タイプを有効にする	**measure** { **all** | **link** | **neighbor** | **radio** | **spectrum** | **tpc** } { **enable** | **disable** }	デフォルト：AP group view内の設定が使用されます。 **spectrum**、**tpc**パラメータは5GHz帯のみサポートします。

12.3.2 AP group radio view での無線リソース計測の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． AP group radio view に移行する	**radio** *radio-id*	—
5． 無線リソース計測を有効にする	**resource-measure enable**	デフォルト：無効 リンク計測、ネイバ計測、無線計測を有効にする場合、無線リソース計測を有効にしなければなりません。

操作	コマンド	補足
6. スペクトル管理を有効にする	**spectrum-management enable**	デフォルト：無効 スペクトル計測またはTPC計測は、スペクトル管理を有効にしたあとにのみ適用されます。 このコマンドに関する詳細はQX-W1000/W1100シリーズアクセスポイント Anchor-AC コマンドマニュアルの *"WLAN RRM"* を参照してください。
7. 計測タイプを有効にする	**measure** { **all** | **link** | **neighbor** | **radio** | **spectrum** | **tpc** } { **enable** | **disable** }	デフォルト：無効 **spectrum**、**tpc**パラメータは5GHz帯のみサポートします。

12.4 計測期間と計測間隔の設定

無線リソース計測が AP に対して有効なとき、AP は計測期間の情報を運ぶ計測要求を、指定された間隔でクライアントに送信します。

12.4.1 radio view での計測期間と計測間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. radio view に移行する	**radio** *radio-id*	—
4. 計測期間を設定する	**measure-duration** *time*	デフォルト：AP group view内の設定が使用されます。
5. 計測間隔を設定する	**measure-interval** *value*	デフォルト：AP group view内の設定が使用されます。

12.4.2 AP group radio view での計測期間と計測間隔の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. AP group radio view に移行する	**radio** *radio-id*	—
5. 計測期間を設定する	**measure-duration** *time*	デフォルト： 500TU
6. 計測間隔を設定する	**measure-interval** *value*	デフォルト：30秒

12.5 クライアント無線リソース計測性能に対するマッチモードの設定

本機能により、クライアントは事前に定義されたマッチ基準に基づいて AP と関連付けることができます。無線リソース計測性能は、AP とクライアントにサポートされた無線リソース計測タイプに言及します。装置は、クライアントの無線リソース計測性能に対して以下のマッチモードをサポートします。

- **ALL**－クライアントは、すべての無線リソース計測性能が AP の無線リソース計測性能と一致する場合に限り、AP とのアソシエーションが許可されます。
- **None**－クライアントの無線リソース計測性能はチェックされません。
- **Partial**－クライアントは、無線リソース計測性能の 1 つが AP の任意の無線リソース計測性能と一致する場合に限り、AP とのアソシエーションが許可されます。

12.5.1 radio view でのクライアント無線リソース計測性能に対するマッチモードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． クライアントの無線リソース計測性能に対してマッチモードを設定する	**rm-capability mode** { **all** | **none** | **partial** }	デフォルト：AP group view内の設定が使用されます。

12.5.2 AP group radio view でのクライアント無線リソース計測性能に対するマッチモードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． AP group radio view に移行する	**radio** *radio-id*	—
5． クライアントの無線リソース計測性能に対してマッチモードを設定する	**rm-capability mode** { **all** | **none** | **partial** }	デフォルト：none

12.6 WLAN無線リソース計測の表示と維持

すべての view で **display** コマンドを実行します。

操作	コマンド
クライアント計測報告を表示する	**display wlan measure-report ap** *ap-name* **radio** *radio-id* [**client mac-address** *mac-address*]

12.7 無線リソース計測の設定例

12.7.1 ネットワーク要件

図 12-1 に示すように、以下の条件を満たすように無線リソース計測を設定します。

- クライアントは、すべての無線リソース計測性能が AP の無線リソース計測性能と一致したときのみオンラインになります。
- クライアントはすべてのタイプの計測を実行できます。



図 12-1 ネットワーク図

12.7.2 設定手順

サービステンプレート 1 を作成します。

```
<AC> system-view
[AC] wlan service-template 1
```

SSID resource-measure を設定し、サービステンプレート 1 を有効にします。

```
[AC-wlan-st-1] ssid resource-measure
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

手動 AP ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 219801A0CNC138011454
```

radio 1 の radio view に移行します.

```
[AC-wlan-ap-ap1] radio 1
```

スペクトル管理を有効にします。

```
[AC-wlan-ap-ap1-radio-1] spectrum-management enable
```

無線リソース計測を有効にします。

```
[AC-wlan-ap-ap1-radio-1] resource-measure enable
```

すべての計測機能を有効にします。

```
[AC-wlan-ap-ap1-radio-1] measure all enable
```

クライアントの無線リソース計測性能に対するマッチモードを All に設定します。

```
[AC-wlan-ap-ap1-radio-1] rm-capability mode all
```

radio 1 にサービステンプレートを設定し、無線を有効にします。

```
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

12.7.3 設定の確認

クライアントがオンラインになることを検証します。

```
[AC] display wlan client
Total number of clients: 1

MAC address       Username             APID/RID  IP address          VLAN ID
00ee-bd44-557f      N/A                   1/1    1.1.1.1              1
```

#クライアントからの計測報告を表示します。

```
[AC] display wlan measure-report ap ap1 radio 1
Total number of clients: 1

Client MAC address                          : 00ee-bd44-557f
Link measurement:
  Link margin                               : 2 dBm
  RCPI                                      : -85 dBm
  RSNI                                      : 53 dBm
Noise histogram:
  Antenna ID                                : 3
  ANPI                                      : -56 dBm
  IPI0 to IPI10 density                     : 5 12 16 13 8 5 5 15 17 1 3
Spectrum measurement:
  Transmit power                            : 20 dBm
  BSS                                       : Detected
  OFDM preamble                             : Detected
  Radar                                     : Detected
  Unidentified signal                       : Undetected
  CCA busy fraction                         : 60
  RPI0 to RPI7 density                      : 3 7 11 19 15 23 15 7
Frame report entry:
  BSSID                                     : a072-2351-e253
  PHY type                                  : fhss
  Average RCPI                              : -10 dBm
  Last RSNI                                 : 2 dBm
  Last RCPI                                 : -20 dBm
  Frames                                    : 1
Dot11BSSAverageAccessDelay group:
  Average access delay                      : 32 ms
  BestEffort average access delay           : 1 ms
  Background average access delay           : 1 ms
```

```
  Video average access delay                : 1 ms
  Voice average access delay                : 1 ms
  Clients                                   : 32
  Channel utilization rate                  : 11
Transmit stream:
  Traffic ID                                : 0
  Sent MSDUs                                : 60
  Discarded MSDUs                           : 5
  Failed MSDUs                              : 3
  MSDUs resent multiple times               : 3
  Lost QoS CF-Polls                         : 2
  Average queue delay                       : 2 ms
  Average transmit delay                    : 1 ms
  Bin0 range                                : 0 to 10 ms
  Bin0 to Bin5                              : 5 10 10 5 10 10
```

目次

13 章 チャネルスキャンの設定 13-1
13.1 概要.....13-1
13.1.1 基本概念 13-1
13.1.2 動作メカニズム 13-1
13.2 チャネルスキャンの設定.....13-2
13.2.1 スキャン期間の設定.....13-2
13.2.2 最大サービス期間の設定.....13-2
13.2.3 サービスアイドルタイムアウトの設定.....13-3
13.2.4 チャネルスキャンブラックリスト・ホワイトリストの設定.....13-4
13.2.5 作動チャネルのみのスキャン 13-5
13.3 チャネルスキャンの設定例 13-5
13.3.1 相対的な優先転送の設定例.....13-5
13.3.2 絶対的な優先転送の設定例.....13-6

13章 チャネルスキャンの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

13.1 概要

チャネルスキャンにより、AP はチャネルをスキャンし無線パケットをキャプチャすることができます。AC は、インタフェース、エラービットレート、無線信号強度などの無線サービス情報を得るために、キャプチャした無線パケットを分析します。チャネルスキャンにより、WLAN RRM と WIDS に対してデータが提供され、無線サービス品質が向上します。

13.1.1 基本概念

- **スキャン期間**－AP は、スキャン期間内でチャネルのスキャンのみ行い、無線サービスは提供しません。
- **サービス期間**－AP は、サービス期間内で以下の方法のいずれかで動作します。
  - □ AP は無線サービスの提供のみを行い、チャネルのスキャンはしません。
  - □ AP は、スキャン期間と同じ期間、動作チャネルのスキャンと無線サービスの提供を同時に行います。その後、AP は無線サービスの提供のみ行います。

13.1.2 動作メカニズム

AP は、AP が無線サービスを提供するかどうかにかかわらず、スキャン期間の間にチャネルスキャンリスト上の各チャネルを順番にスキャンします。AP が無線サービスを提供しない場合、AP はスキャン期間を継続的に開始します。AP が無線サービスを提供する場合、AP はサービス期間とスキャン期間のどちらか一方を開始します。

たとえば図 13-1 は、AP がチャネル 6 で動作し、チャネルスキャンリストがチャネル 1、6、11 を含むときのチャネルスキャンの仕組みを示します。

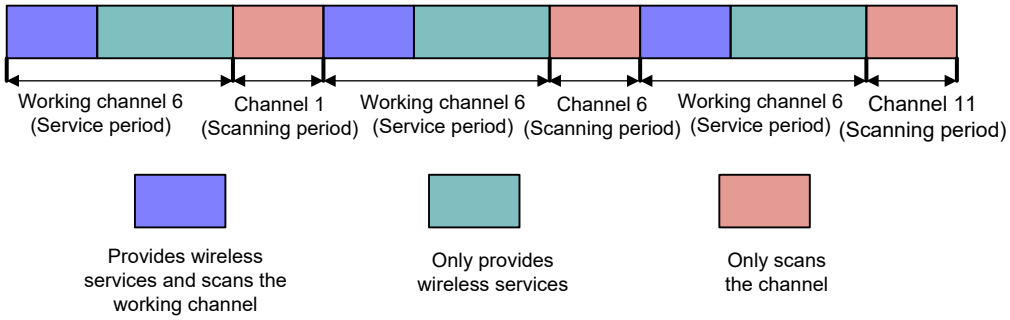


図 13-1 チャネルスキャンメカニズム

13.2 チャネルスキャンの設定

最大サービス期間よりスキャン期間の値が小さいことを確認してください。

13.2.1 スキャン期間の設定

I. radio view でのスキャン期間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. スキャン期間を設定する	**scan scan-time** *scan-time*	デフォルト： AP group radio viewの設定を使用します。

II. AP group view でのスキャン期間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. スキャン期間を設定する	**scan scan-time** *scan-time*	デフォルト： 100ミリ秒

13.2.2 最大サービス期間の設定

スキャン品質とサービス品質の両方を保証するために、最大サービス期間を設定できます。最大サービス期間に達すると、AP は転送するトラフィックの有無に関わらずスキャン期

間を開始します。無線サービス品質を保証するため、AP がサービス期間を制限しないように設定できます。AP はサービスアイドルタイムアウトが終了するまでスキャン期間を開始しません。

I. radio view での最大サービス期間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. 最大サービス期間を設定する	**scan max-service-time** { *max-service-time* | **no-limit**}	デフォルト： AP group radio viewの設定を使用します。

II. AP group view での最大サービス期間の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. スキャン期間を設定する	**scan max-service-time** { *max-service-time* | **no-limit**}	デフォルト： ソフトウェアバージョンにより異なります。 ソフトウェアバージョン7.2.19を含む以前のソフトウェアでは5000ミリ秒です。 ソフトウェアバージョン7.2.21を含む以降のソフトウェアではno-limitです。

13.2.3 サービスアイドルタイムアウトの設定

サービス期間の間、たとえ指定されたサービスアイドルタイムアウトが終了しても、現在のサービス期間がスキャン期間を超過するまで、AP は新たなスキャン期間を開始しません。

I. radio view でのサービスアイドルタイムアウトの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. サービスアイドルタイムアウトを設定する	**scan idle-time** *idle-time*	デフォルト： AP group radio viewの設定を使用します。 サービスアイドルタイムアウトは最大サービス期間よりも大きくすることはできません。

II. AP group view でのービスアイドルタイムアウトの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. スキャン期間を設定する	**scan idle-time** *idle-time*	デフォルト： 100ミリ秒

13.2.4 チャネルスキャンブラックリスト・ホワイトリストの設定

ブラックリストのチャネルをスキャンしない、あるいはホワイトリストのチャネルのみをスキャンするようにAP を設定します。ブラックリストとホワイトリストの両方を同じAP に設定することはできません。

I. radio view でのブラックリスト・ホワイトリストの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. 特定のチャネルをブラックリストに指定する	**scan channel blacklist** *channel-list*	デフォルト： AP group radio viewの設定を使用します。
5. 特定のチャネルをホワイトリストに指定する	**scan channel whitelist** *channel-list*	デフォルト： AP group radio viewの設定を使用します。

II. AP group radio view でのブラックリスト・ホワイトリストの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. 特定のチャネルをブラックリストに指定する	**scan channel blacklist** *channel-list*	デフォルト： 設定なし
6. 特定のチャネルをホワイトリストに指定する	**scan channel whitelist** *channel-list*	デフォルト： 設定なし

13.2.5 作動チャネルのみのスキャン

注意：
この機能はデュアルバンド無線にのみ適用可能です。

2.4GHz チャネルあるいは 5GHz チャネルを、指定した間隔でスキャンします。

I. radio view での作動チャネルのみのスキャン

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. 作動チャネルのみのスキャンを有効にする	**scan work-channel-only** { **disable** | **enable** }	デフォルト： AP group radio viewの設定を使用します。

II. AP group radio view での作動チャネルのみのスキャン

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. radio view に移行する	**radio** *radio-id*	—
5. 作動チャネルのみのスキャンを有効にする	**scan work-channel-only** { **disable** | **enable** }	デフォルト：サポートされたチャネルを順番にスキャンします。

13.3 チャネルスキャンの設定例

13.3.1 相対的な優先転送の設定例

I. ネットワーク要件

図 13-2 に示すように、チャネルスキャンを設定し、チャネルスキャンと無線サービス品質を保証するために AP 1 に最大サービス期間を設定します。

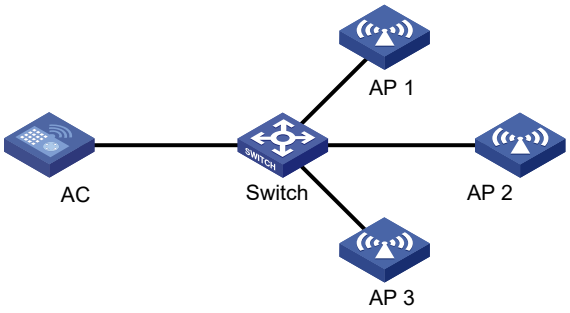


図 13-2 ネットワーク図

II. 設定手順

手動 AP を作成し、AP モデル名とシリアル ID を指定します。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1]  serial-id 219801A0CNC138011454
```

radio 1 の radio view を有効にします。

```
[AC-wlan-ap-ap1]  radio 1
```

スキャン期間を 200 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1]  scan scan-time 200
```

最大サービス期間を 5000 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1]  scan max-service-time  5000
```

サービスアイドルタイムアウトを 100 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1]  scan idle-time 100
```

13.3.2 絶対的な優先転送の設定例

I. ネットワーク要件

図 13-3 に示すように、チャネルスキャンを設定し、無線サービス品質を保証するために AP 1 に対してサービス期間を制限しないようにします。

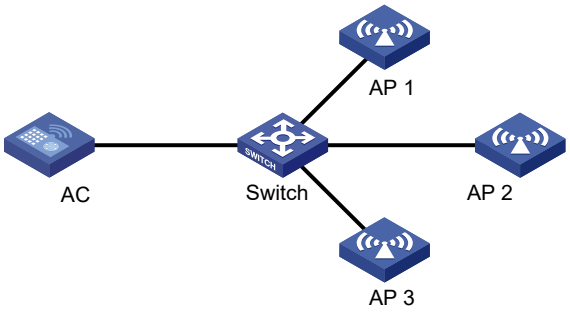


図 13-3 ネットワーク図

II. 設定手順

手動 AP を作成し、AP モデル名とシリアル ID を指定します。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1]  serial-id 219801A0CNC138011454
```

radio 1 の radio view を有効にします。

```
[AC-wlan-ap-ap1]  radio 1
```

スキャン期間を 100 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1]  scan scan-time 100
```

無線がサービス期間を制限しないように設定します。

```
[AC-wlan-ap-ap1-radio-1]  scan max-service-time  no-limit
```

サービスアイドルタイムアウトを 100 ミリ秒に設定します。

```
[AC-wlan-ap-ap1-radio-1]  scan idle-time 100
```

目次

14 章 バンドナビゲーションの設定.....14-1
14.1 概要.....14-1
14.2 設定作業リスト.....14-1
14.3 設定必須要件.....14-2
14.4 バンドナビゲーションの設定.....14-2
14.4.1 グローバルでのバンドナビゲーションの有効化.....14-2
14.4.2 AP に対するバンドナビゲーションの有効化.....14-2
14.4.3 バンドナビゲーションに対するロードバランスの設定.....14-3
14.4.4 バンドナビゲーションパラメータの設定.....14-3
14.5 バンドナビゲーションの設定例.....14-4

14章 バンドナビゲーションの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

14.1 概要

AP は、バンドナビゲーションを行うことで、デュアルバンド（2.4GHz と 5GHz）クライアントの優先的な 5GHz 無線使用を可能にします。これにより、混雑しやすい 2.4GHz バンドでの無線負荷を分散でき、ネットワーク性能が向上します。

図 14-1に示すように、バンドナビゲーションは WLAN 内で有効化されます。Client 1 は 5GHz 無線に関連づけられ、Client 2 は 2.4GHz 無線に関連づけられます。デュアルバンドクライアントの Client 3 が 2.4GHz 無線への関連づけを要求したとき、AP は Client 3 を拒否し、5GHz 無線を使用するように暗示します。

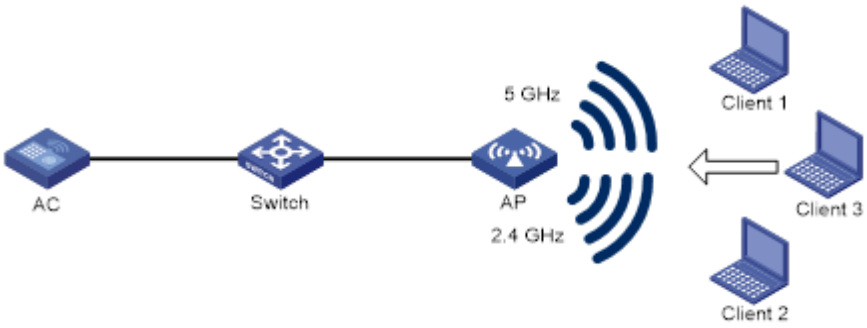


図 14-1 バンドナビゲーション

14.2 設定作業リスト

作業リスト
バンドナビゲーションの設定 • （必須設定項目） グローバルでのバンドナビゲーションの有効化 • （必須設定項目） APに対するバンドナビゲーションの有効化 • （オプション設定項目） バンドナビゲーションに対するロードバランスの設定 • （オプション設定項目） バンドナビゲーションパラメータの設定

14.3 設定必須要件

クイックアソシエーションが無線サービスに対して無効にされていることを確認してください。クイックアソシエーションに関する詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN アクセスの設定"* を参照してください。

5GHz 無線と 2.4GHz 無線の両方が有効化され、無線が同じサービステンプレートに設定されていることを確認してください。

14.4 バンドナビゲーションの設定

WLAN 内の大半のクライアントが 2.4GHz バンドしかサポートしていない場合、またはトラフィック遅延に敏感なWLAN内ではバンドナビゲーションを有効にしないでください。

14.4.1 グローバルでのバンドナビゲーションの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. バンドナビゲーションをグローバルに有効化する	**wlan band-navigation enable**	デフォルト：無効

14.4.2 AP に対するバンドナビゲーションの有効化

バンドナビゲーションは、グローバルおよび AP の両者に有効なときにのみ、AP に対して適用します。

I. AP に対するバンドナビゲーションの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap ap-name** [**model** *model-name*]	—
3. AP に対してバンドナビゲーションを有効にする	**band-navigation enable**	デフォルト：APはAP group viewの設定を使用します。

II. AP group に対するバンドナビゲーションの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—

操作	コマンド	補足
3． APに対してバンドナビゲーションを有効にする	**band-navigation enable**	デフォルト：有効

14.4.3 バンドナビゲーションに対するロードバランスの設定

AP は、以下の条件が満たされるとき、クライアントの 5GHz のアソシエーション要求を拒否します。

- 5GHz 無線のクライアント数が、指定したしきい値に達した場合。
- 5GHz 無線と、関連づけられたクライアント数が最小の無線とのクライアント数のギャップが、指定したしきい値に達した場合。

バンドナビゲーションに対するロードバランスの設定手順は以下のとおりです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． バンドナビゲーションに対してロードバランスを設定する	**wlan band-navigation balance session** *session* [**gap** *gap*]	デフォルト：無効

14.4.4 バンドナビゲーションパラメータの設定

以下のパラメータはバンドナビゲーションに影響を与えます。

- **5GHz アソシエーション要求に対する拒絶の最大数**－5GHz 無線がクライアントを拒否する回数が、指定した最大数に達した場合、無線はクライアントのアソシエーション要求を承認します。
- **バンドナビゲーション RSSI しきい値**－クライアントは複数の無線に検出される可能性があります。クライアントの RSSI がバンドナビゲーション RSSI しきい値より小さい場合、5GHz 無線はクライアントのアソシエーション要求を拒否します。
- **クライアント情報エージングタイマ**－AP は、クライアントからアソシエーション要求を受信すると、クライアントの情報を記録し、クライアント情報エージングタイマを開始します。エージングタイマが終了する前に AP がクライアントからプローブ要求やアソシエーション要求を受信しない場合、AP はクライアントの情報を削除します。

クライアントのアソシエーションとシステムリソースの効率の両方を保証するために、適切なクライアント情報エージングタイマを設定してください。

バンドナビゲーションパラメータの設定手順は以下のとおりです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． 5GHz アソシエーション要求に対する拒絶の最大数を設定する	**wlan band-navigation balance access-denial** *access-denial*	デフォルト：APは5GHzアソシエーション要求を拒否しません。
3． バンドナビゲーション RSSI しきい値を設定する	**wlan band-navigation rssi-threshold** *rssi-threshold*	デフォルト：15

操作	コマンド	補足
4． クライアント情報エージングタイマを設定する	**wlan band-navigation aging-time** *aging-time*	デフォルト： 180秒

14.5 バンドナビゲーションの設定例

I. ネットワーク要件

図 14-2に示すように、5GHz 無線と 2.4GHz 無線の両方が AP 上で有効化されています。バンドナビゲーションを設定し、無線の負荷を分散させるためにとロードバランスを設定します。

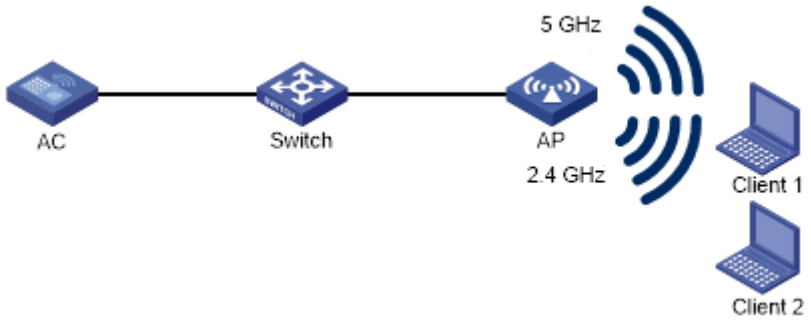


図 14-2 ネットワーク図

II. 設定手順

サービステンプレート 1 を作成し、SSID を band-navigation に設定します。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid band-navigation
[AC-wlan-st-1] service-template enable
[AC-wlan-st-1] quit
```

AP template ap1 を作成し、AP モデル名とシリアル ID を指定します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] serial-id 210235A29G007C000020
```

radio 1 の radio view に移行し、radio 1 が 802.11n （5 GHz）モード内で作動するように設定します。

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] type dot11an
```

サービステンプレート 1 を AP 1 の radio 1 に設定し、radio 1 を有効にします。

```
[AC-wlan-ap-ap1-radio-1] service-template 1
[AC-wlan-ap-ap1-radio-1] radio enable
[AC-wlan-ap-ap1-radio-1] quit
```

radio 3 の radio view に移行し、radio 3 は 802.11n （2.4 GHz） モード内で作動するように設定します。

```
[AC-wlan-ap-ap1] radio 3
[AC-wlan-ap-ap1-radio-3] type dot11gn
```

サービステンプレート 1 を AP 1 の radio 3 に設定し、radio 3 を有効にします。

```
[AC-wlan-ap-ap1-radio-3] service-template 1
[AC-wlan-ap-ap1-radio-3] radio enable
[AC-wlan-ap-ap1-radio-3] quit
[AC-wlan-ap-ap1] quit
```

バンドナビゲーションをグローバルに有効化します。

```
[AC] wlan band-navigation enable
```

AP 1 に対してバンドナビゲーションを有効化します。

```
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] band-navigation enable
[AC-wlan-ap-ap1] quit
```

バンドナビゲーションに対してロードバランスを有効化し、クライアント数のしきい値とクライアント数のギャップしきい値をそれぞれ 5 と 2 に設定します。

```
[AC] wlan band-navigation balance session 5 gap 2
```

5GHz アソシエーション要求に対する拒絶の最大数を 3 に設定します。

```
[AC] wlan band-navigation balance access-denial 3
```

#バンドナビゲーション RSSI しきい値を 30 に設定します。

```
[AC] wlan band-navigation rssi-threshold 30
```

クライアント情報エージングタイマ 160 秒に設定します。

```
[AC] wlan band-navigation aging-time 160
```

III. 設定の確認

1) デュアルバンドクライアントが AP に関連づけを要求したときに、5GHz 無線に関連付くことを確認します。
2) 以下の条件を満たすとき、デュアルバンドクライアントが 2.4GHz 無線に関連付くことを確認します。

- 5GHz 無線上のクライアント数が 5 に達した場合。（詳細は省略します。）

- 5GHz 無線と 2.4GHz 無線とのクライアント数ギャップが 2 に達した場合。（詳細は省略します。）

目次

15章 WLAN最適化 15-1
15.1 概要 15-1
15.2 制限事項とガイドライン:WLAN最適化設定 15-1
15.3 APトリガのクライアント再関連付けの設定 15-1
15.4 隠れ端末保護の設定 15-2
15.5 ブロードキャストおよびマルチキャストパケット制御の設定 15-3
15.6 ブロードキャストおよびマルチキャストのパケットレート制御の設定 15-4
15.7 クライアント高速キープアライブの設定 15-5

15章 WLAN 最適化

15.1 概要

WLAN 導入時の適切なチャネル選択と送信パワー制御は、良好なパフォーマンスのために重要です。しかし、通常の WLAN ネットワークでは、重複しないチャネル数に対し、WLAN デバイス数は常に増加するため、チャネル重複,衝突,干渉は容易に発生します。

WLAN 最適化機能は、WLAN の品質と安定性の向上に役立ちます。

15.2 制限事項とガイドライン:WLAN最適化設定

特定の WLAN を最適化するために固定された組み合わせはありません。

コマンドの効果と WLAN のパフォーマンスに基づいて機能を選択し調整する必要があります。

WLAN の全体的なパフォーマンスは、ネットワークアーキテクチャ、チャネルと送信パワーによって決まります。従って、WLAN 最適化機能は WLAN の性能を著しく向上させることはできません。

15.3 APトリガのクライアント再関連付けの設定

I. AP トリガのクライアント再関連付けについて

クライアントは、クライアントのメーカーが定義した信号強度より低い場合にのみ、別の AP にローミングを行います。そのため、クライアントは良好なネットワークとサービス品質を得ることができません。

この機能を使用すると、クライアントの信号強度が指定された RSSI しきい値よりも低い場合に、AP は、認証解除フレームをクライアントに送信します。その後、クライアントは AP と再接続するか、別の AP にローミングします。

II. 設定手順

radio view での AP トリガのクライアント再関連付けの設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP を作成し、その view に移行する	**wlan ap** *ap-name*	―
3. radio view に移行する	**radio** *radio-id*	―

操作	コマンド	補足
4. APトリガのクライアント再関連付けを設定する	**option client reconnect** { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] }	デフォルト：AP group viewの設定を使用します。

AP group radio view での AP トリガのクライアント再関連付けの設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	―
3. AP model view に移行する	**ap-model** *ap-model*	―
4. radio view に移行する	**radio** *radio-id*	―
5. APトリガのクライアント再関連付けを設定する	**option client reconnect** { **disable** | **enable** [**rssi** *rssi-value*] [**interval** *interval*] }	デフォルト：無効

15.4 隠れ端末保護の設定

I. 隠れ端末保護について

この機能を使用すると、クライアントは隠れ端末からの干渉を避けるために、フレームを転送する前に RTS/CTS フレームを送信します。

本機能によって複数端末の通信衝突を軽減させることが可能です。

II. 制限とガイドライン

この機能は 802.11g、802.11n、802.11ac、802.11ax のクライアントにのみ適用できます。

III. 設定手順

radio view での隠れたノード保護の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP を作成し、その view に移行する	**wlan ap** *ap-name*	―
3. radio view に移行する	**radio** *radio-id*	―
4. 隠れ端末保護を設定する	**option client hide-node-protection** { **disable** | **enable** }	デフォルト：AP group viewの設定を使用します。

AP group radio view での AP トリガのクライアント再関連付けの設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―

操作	コマンド	補足
2． AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	―
3． AP model view に移行する	**ap-model** *ap-model*	―
4． radio view に移行する	**radio** *radio-id*	―
5． 隠れ端末保護を設定する	**option client hide-node-protection** { **disable** | **enable** }	デフォルト：無効

15.5 ブロードキャストおよびマルチキャストパケット制御の設定

🕮 **メモ：**

- ブロードキャストおよびマルチキャストパケット制御の設定はソフトウェアバージョン 7.2.46 を含む以降のソフトウェアからサポートしています。
- ブロードキャストおよびマルチキャストパケット制御の設定は Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。QX-W1030 Anchor-AC/Anchor-FIT ではサポートしていません。

I. ブロードキャストおよびマルチキャストパケット制御について

無線リソースを節約し、転送パフォーマンスを向上させるには、次の作業を実行します。

IPv4 ネットワークで基本的なブロードキャストおよびマルチキャストパケットを制御します。本機能を有効にすると、AP は ARP ブロードキャストパケットに応答し、DHCP ブロードキャストパケットを廃棄し、他のパケットを正常に処理します。

II. 設定手順

AP view でのブロードキャストおよびマルチキャストパケット制御の設定方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP を作成し、その view に移行する	**wlan ap** *ap-name*	―
3． ブロードキャストおよびマルチキャストパケットのパケット制御を設定する	**rrop anti-bmc network { disable | ipv4-simple enable }**	デフォルト：AP group viewの設定を使用します。

AP group view でのブロードキャストおよびマルチキャストパケット制御の設定方法を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	―

操作	コマンド	補足
3. ブロードキャストおよびマルチキャストパケットのパケット制御を設定する	**rrop anti-bmc network { disable | ipv4-simple enable }**	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン7.2.50を含む以前のソフトウェアでは有効です。 ソフトウェアバージョン7.2.52を含む以降のバージョンでは無効です。

15.6 ブロードキャストおよびマルチキャストのパケットレート制御の設定

🕮 **メモ：**

- ブロードキャストおよびマルチキャストのパケットレート制御の設定はソフトウェアバージョン 7.2.50 を含む以降のソフトウェアからサポートしています。
- ブロードキャストおよびマルチキャストのパケットレート制御の設定は Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。QX-W1030 Anchor-AC/Anchor-FIT ではサポートしていません。

I. ブロードキャストおよびマルチキャストのパケットレート制御について

無線リソースを節約し、転送パフォーマンスを向上させるには、次の作業を実行します。

AP は、ブロードキャストまたはマルチキャストパケットを無線インタフェース経由で転送するレートを制限します。

II. 設定手順

AP view でのブロードキャスト、マルチキャストのパケットレート制限の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP を作成し、その view に移行する	**wlan ap** *ap-name*	—
3. ブロードキャストまたはマルチキャストパケットのパケットレート制限を有効化する	**rrop anti-bmc { broadcast | multicast } rate-limit { disable | enable }**	デフォルト：AP group viewの設定を使用します。
4. ブロードキャストまたはマルチキャストパケットのパケットレート制限値を設定する	**rrop anti-bmc { broadcast | multicast } rate-limit pps** *max-pps*	デフォルト：AP group viewの設定を使用します。

AP group view でのブロードキャスト、マルチキャストのパケットレート制限の設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	―
3. ブロードキャストまたはマルチキャストパケットのパケットレート制限を有効化する	**rrop anti-bmc { broadcast | multicast } rate-limit { disable | enable }**	デフォルト：無効
4. ブロードキャストまたはマルチキャストパケットのパケットレート制限値を設定する	**rrop anti-bmc { broadcast | multicast } rate-limit pps** *max-pps*	ブロードキャスト：無制限 マルチキャスト：無制限

15.7 クライアント高速キープアライブの設定

🕮 **メモ：**

- クライアント高速キープアライブの設定は、ソフトウェアバージョン 7.2.85a を含む以降のソフトウェアからサポートしています。ソフトウェアバージョン 7.2.85a より前では本機能がデフォルトのパラメータ値で動作しており、無効にすることはできません。
- クライアント高速キープアライブの設定は、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。QX-W1030 Anchor-AC ではサポートしていません。

I. クライアント高速キープアライブの設定について

この機能により、AP は、クライアントに送信されたユニキャストパケットの確認応答状態に基づいて、クライアントがまだオンラインであるかどうかを確認できます。AP はユーザーデータを 3 つのグループに分けて個別にカウントします。キープアライブ間隔 (*interval-value* パラメータで設定) 中に、3 グループのユニキャストパケットの確認応答が受信されなかった場合、AP はクライアントがオフラインであると判断し、クライアントへの接続を終了します。これにより、無線リソースの使用率が向上します。グループ内のユニキャストパケットの数は、*count-value* パラメータで設定します。

この機能は、クライアントの移動性が高いシナリオに適用できます。ネットワーク品質が悪い場合は、キープアライブカウントを減らすか、キープアライブ間隔を短くする必要があります。

II. 設定手順

AP view でのクライアント高速キープアライブの設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. AP を作成し、その view に移行する	**wlan ap** *ap-name*	―
3. クライアント高速キープアライブを設定する	**rrop client fast-keep-alive** { **disable** | **enable** [**count** *count-value*] [**interval** *interval-value*]}	デフォルト : AP group radio view の設定を使用します。

AP group view でのクライアント高速キープアライブの設定方法を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	ー
2. AP グループを作成し、その view に移行する	**wlan ap-group** *group-name*	ー
3. AP モデル view に移行する	**ap-model** *ap-model*	ー
4. Radio view に移行する	**radio** *radio-id*	ー
5. クライアント高速キープアライブを設定する	**rrop client fast-keep-alive** { **disable** | **enable** [**count** *count-value*] [**interval** *interval-value*]}	デフォルト：有効 (count 1024、interval 10)

目次

16 章 WLAN IP スヌーピング 16-1
16.1 概要 16-1
16.1.1 クライアント IPv4 アドレスの学習 16-1
16.2 WLAN IP スヌーピングの設定作業リスト 16-1
16.3 ARP パケットスヌーピングの無効化 16-1
16.4 WLAN IP スヌーピングの設定例 16-2
16.4.1 ネットワーク要件 16-2
16.4.2 設定手順 16-2

16章 WLAN IP スヌーピング

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

16.1 概要

WLAN IP snooping は AP が ARP snooping、DHCP snooping を使用してクライアントの IP アドレスを学習することを有効にします。IP アドレス、MAC アドレス、学習方式を記録した snooping エントリを生成します。エントリはクライアントにパケットを転送するかどうかを決定する IP ソースガードに使用されます。IP ソースガードの詳細は QX-W1000/W1100 シリーズ アクセスポイントオペレーションマニュアルのセクション 9 *セキュリティの "IP ソースガード"* を参照してください。

16.1.1 クライアント IPv4 アドレスの学習

AP は以下の方法を使用してクライアントの IPv4 アドレスを学習することができます。

- クライアントとサーバ間で交換される DHCPv4 パケットを確認します。

DHCP についての詳細は QX-W1000/W1100 シリーズ アクセスポイントオペレーションマニュアルのセクション 5 *IP サービス*を参照してください。

- クライアントによって送信される ARP パケットを確認します。

ARP についての詳細は QX-W1000/W1100 シリーズ アクセスポイントオペレーションマニュアルのセクション 5 *IP サービス "ARP"* を参照してください。

IP アドレスを学習する優先度は DHCPv4 パケット、ARP パケットの順番で行われます。

16.2 WLAN IP スヌーピングの設定作業リスト

作業リスト
（オプション設定項目）ARPパケットのsnoopingの無効化

16.3 ARPパケットスヌーピングの無効化

I. ARP パケットのスヌーピング

AP はデフォルトで ARP パケットと DHCPv4 パケットによってクライアントの IPv4 アドレスを学習します。

この設定を行うことによって ARP パケットからクライアントの IPv4 のアドレスの学習を無効にします。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． サービステンプレートを作成し、その view に移行する	**wlan service-template** *service-template-name*	―
3． ARP パケットの snooping を無効にする	**undo client ipv4-snooping arp-learning enable**	デフォルト：有効

16.4 WLAN IP スヌーピングの設定例

16.4.1 ネットワーク要件

図 16-1に示すように、AP が DHCPv4 パケットからクライアントの IPv4 アドレスを学習するように設定します。

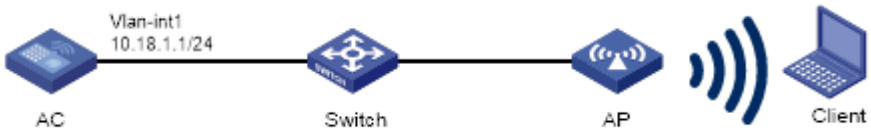


図 16-1 ネットワーク図

16.4.2 設定手順

無線サービスを設定します。（詳細は省略します。）

詳細は QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“AP 管理”*、*“WLAN アクセスの設定”* を参照してください。

ARP パケットの snooping を無効にします。

```
<AC> system-view
[AC] wlan service-template service
[AC-wlan-st-service] undo client ipv4-snooping arp-learning enable
```

目次

17 章 WLAN RRM の設定 17-1
17.1 概要 17-1
17.1.1 動的周波数選択（DFS） 17-1
17.1.2 送信電力制御（TPC） 17-2
17.1.3 スペクトル管理 17-3
17.1.4 帯域幅自動調整 17-3
17.2 WLAN RRM 設定作業リスト 17-4
17.3 DFS の設定 17-4
17.3.1 設定の制限とガイドライン 17-5
17.3.2 DFS トリガーパラメータの設定 17-5
17.3.3 定期 auto-DFS の設定 17-6
17.3.4 スケジュール auto-DFS の実行 17-7
17.3.5 オンデマンド DFS の設定 17-9
17.3.6 RRM 抑制グループの設定 17-9
17.4 TPC の設定 17-10
17.4.1 設定の制限とガイドライン 17-10
17.4.2 TPC モードの設定 17-10
17.4.3 TPC トリガーパラメータの設定 17-11
17.4.4 最小送信電力の設定 17-12
17.4.5 最大送信電力の設定 17-13
17.4.6 定期 auto-TPC の設定 17-13
17.4.7 オンデマンド TPC の実行 17-14
17.4.8 死角検出の設定 17-14
17.4.9 RRM 抑制グループの設定 17-16
17.5 スペクトル管理の設定 17-17
17.5.1 スペクトル管理の有効化 17-17
17.5.2 電力制約モードの設定 17-17
17.5.3 チャネルスイッチモードの設定 17-19
17.5.4 送信電力機能一致モードの設定 17-19
17.5.5 チャネル機能一致モードの設定 17-20
17.6 帯域幅自動調整の設定 17-21
17.6.1 帯域幅自動調整の有効化 17-21
17.6.2 帯域幅自動調整間隔の設定 17-22
17.7 無線ベースラインの設定 17-22
17.8 無線スキャニングの有効化 17-23
17.9 WLAN RRM の SNMP 通知の有効化 17-24
17.10 WLAN RRM の表示および管理 17-24
17.11 WLAN RRM の設定例 17-25
17.11.1 定期 auto-DFS の設定例 17-25
17.11.2 スケジュール auto-DFS の設定例 17-26
17.11.3 定期 TPC の設定例 17-28
17.11.4 スペクトル管理の設定例 17-30
17.11.5 帯域幅自動調整の設定例 17-31

17章 WLAN RRM の設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

17.1 概要

WLAN RRM（Radio Resource Management）は、インテリジェントで拡張性のある無線管理機能を提供します。RRM により、AC は関連する無線を監視し、無線リソースの監視、動的周波数選択（DFS）、送信電力制御（TPC）を実行できます。これにより、WLAN が環境変化に適応し、最適な無線リソース状態を維持することができます。

17.1.1 動的周波数選択（DFS）

同じチャネル上の 2 つの隣接する無線が信号の衝突を引き起こす、またレーダー信号や電子レンジなどの他の無線発信源が無線の動作を妨害する可能性があります。DFS はこれらの問題を解決することができます。

DFS を使用することで、AC は同一チャネルの干渉および他の無線発信源からの干渉を回避するために、リアルタイムで各無線に最適なチャネルを選択します。

DFS を決定する要因は以下の通りです。

- **エラーコード等級**－物理層エラーコード等級および CRC エラーです。
- **干渉**－すべての無線信号が無線サービスに及ぼす影響です。
- **再送信**－AC からの ACK メッセージを受信しない場合の無線によるデータ再送信です。
- **レーダー信号**－現在のチャネルで検出されたレーダー信号です。この場合、AC は新しいチャネルを選択し、直ちにその動作チャネルを変更するように無線に通知します。

AC は、以下のプロセスを使用し新しい無線チャネルを選択します。

1) 現在のチャネルを検出し、DFS のいずれかのしきい値に達した場合に最適なチャネルを選択します。
2) 古いチャネルと新しいチャネルとの品質を比較します。新しいチャネルと古いチャネルとの間の品質ギャップが許容レベルを超えるまで、無線では新しいチャネルを使用しません。

図 17-1に DFS の例を示します。BSS1、BSS3、および BSS5 のチャネルの品質が DFS しきい値に達すると、AC はそれらについて新しいチャネルを選択します。これにより、ワイヤレスサービスの品質が保証されます。

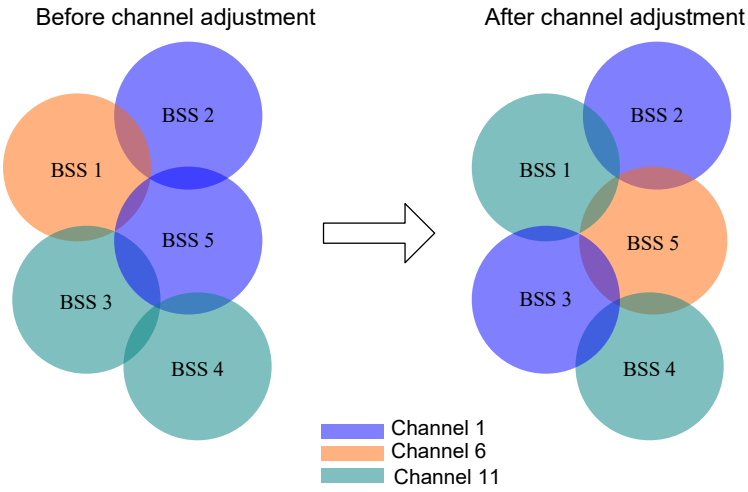


図 17-1 動的周波数選択（DFS）

17.1.2 送信電力制御（TPC）

TPC により、AC はリアルタイム WLAN 条件に基づいてアクセスポイントの送信電力を動的に制御できます。これは、無線間のチャネル干渉を回避しながら、要求された RF の適用範囲を達成することができます。

TPC を決定する要因は以下の通りです。

- **隣接番号しきい値**
- **電力検出用無線機**ー電力検出を実行する近隣無線機
- **電力調整しきい値**

1) TPC が有効になると、無線機は送信電力を次のように調整します。
- 無線の隣接数のしきい値に達すると、無線はその送信電力を次のように調整します。
- 無線の隣接番号しきい値に達していない場合、無線は最大送信電力を使用します。

2) ほかの無線の隣接通知に記録されている無線の RSSI を降順でランク付けます。
3) 近接要因によって指定された RSSI を電力調整しきい値と比較し、以下のアクションの 1 つを実行します。
- RSSI がしきい値を超過した場合、無線の送信電力を減少させます。
- RSSI がしきい値を下回った場合、無線の送信電力を増加させます。

図 17-2に示すように、各 AP は 1 つの無線のみが有効になっています。AP4 が加入すると、AP1 のデフォルトの最大近隣番号である 3 に達します。AP1 のすべての隣接者の中で、AP4 の信号強度が 3 番目であるため、AP4 が電力検出用 AP になります。AP1 の電力がデフォルト電力調整しきい値よりも低いことを AP4 が検出すると、AP1 はその送信電力を増加させます。AP1 の電力がデフォルト電力調整しきい値より高いことを AP4 が検出すると、AP1 は送信電力を減少させます。

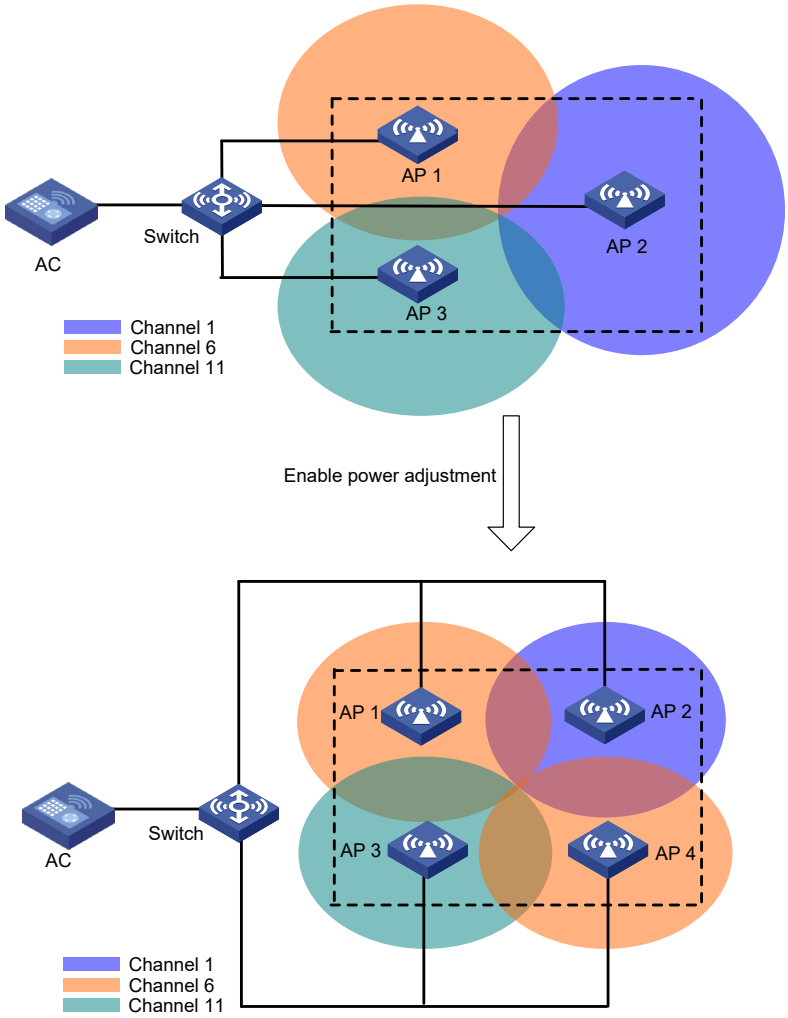


図 17-2 送信電力制御

17.1.3 スペクトル管理

802.11h で定義されているスペクトル管理は、5GHz 帯での運用の規制要件を満たすために 5GHz WLAN に適用されます。802.11h では、5GHz 帯で動作するクライアントは他の無線デバイスの干渉を避けるために送信電力を制御する必要があります。スペクトル管理により、無線機は関連するクライアントに許可された最大送信電力を通知し、その電力およびチャネルが規制上の要件を満たさない場合には、関連付けを拒否することができます。

17.1.4 帯域幅自動調整

帯域幅自動調整が有効の場合、AC は帯域幅自動調整間隔に達するとチャネル品質検出を開始し、帯域幅調整を実行するかどうかを決定します。周辺 AP の数が多い場合は干渉を減らすために無線の帯域幅を減らし、数が少ない場合は伝送レートを増やすために帯域幅を増やします。

17.2 WLAN RRM設定作業リスト

作業リスト
DFSの設定 （オプション設定項目）DFSトリガーパラメータの設定 （必須設定項目）次のいずれかのタスクを選んでください。 • 定期auto-DFSの設定 • スケジュールauto-DFSの実行 • オンデマンドDFSの設定 （オプション設定項目）RRM抑制グループの設定
TPCの設定 （オプション設定項目）定期auto-DFSの設定 （オプション設定項目）DFSトリガーパラメータの設定 （オプション設定項目）最小送信電力の設定 （オプション設定項目）最大送信電力の設定 （必須設定項目）次のいずれかのタスクを選んでください。 • スケジュールauto-DFSの実行 • RRM抑制グループの設定 （オプション設定項目）死角検出の設定 （オプション設定項目）RRM抑制グループの設定
スペクトル管理の設定 • （必須設定項目）スペクトル管理の有効化 • （オプション設定項目）電力制約モードの設定 • （オプション設定項目）チャネルスイッチモードの設定 • （オプション設定項目）送信電力機能一致モードの設定 • （オプション設定項目）チャネル機能一致モードの設定
帯域幅自動調整の設定 • （必須設定項目）帯域幅自動調整の有効化 • （オプション設定項目）帯域幅自動調整間隔の設定
（オプション設定項目）無線ベースラインの設定
（オプション設定項目）無線スキャニングの有効化
（オプション設定項目） WLAN RRMのSNMP通知の有効化

17.3 DFSの設定

AC は以下の DFS 方式をサポートします。

- **定期 auto-DFS**－AC は自動的にチャネルキャリブレーション間隔で無線の DFS を実行します。
- **スケジュール auto-DFS**－AC は時間範囲の指定した時間で DFS を実行します。干渉が大きい時、動作中の無線サービスへの影響を避ける場合、この方式を使用します。
- **オンデマンド DFS**－AC はチャネルキャリブレーション間隔時間を待った後、すべての無線の DFS を実行します。AC で無線の DFS を実行する際に、この方式を行う必要があります。

17.3.1 設定の制限とガイドライン

DFS を設定する際は、次の制限とガイドラインに従ってください。

DFS を動作させるには、無線のチャネルを自動で選択し、**channel auto unlock** コマンドを使用して、チャネルのロックを解除してください。

17.3.2 DFS トリガーパラメータの設定

注意：
正確なチャネル調整のため、DFS が有効になっているすべての無線で同じ DFS トリガーパラメータを設定することを推奨します。

I. RRM view での DFS トリガーパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． RRM view に移行する	**rrm**	—
5． CRC エラーしきい値を設定する	**crc-error-threshold** *percent*	デフォルト：AP group viewの設定が使用されます。
6． 干渉しきい値を設定する	**interference-threshold** *percent*	デフォルト：AP group viewの設定が使用されます。
7． 許容レベルを設定する	**tolerance-level** *percent*	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view での DFS トリガーパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—
6． CRC エラーしきい値を設定する	**crc-error-threshold** *percent*	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.21を含む以前のソフトウェアでは20%です。 ソフトウェアバージョン 7.2.27を含む以降のソフトウェアでは0%です。

操作	コマンド	補足
7. 干渉しきい値を設定する	**interference-threshold** *percent*	デフォルト : ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.21を含む以前のソフトウェアでは50%です。 ソフトウェアバージョン 7.2.27を含む以降のソフトウェアでは70%です。
8. 許容レベルを設定する	**tolerance-level** *percent*	デフォルト : ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.21を含む以前のソフトウェアでは20%です。 ソフトウェアバージョン 7.2.27を含む以降のソフトウェアでは1%です。

17.3.3 定期 auto-DFS の設定

I. RRM view での auto-DFS の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. （オプション設定項目）チャネルキャリブレーションを設定する	**wlan rrm calibration-channel interval** *minutes*	デフォルト : ソフトウェアバージョン 7.2.21 を含む以前のソフトウェアでは8分です。 ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでは23分です。
3. AP を作成し、AP view へ移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
4. radio view に移行する	**radio** *radio-id*	—
5. RRM view に移行する	**rrm**	—
6. auto-DFS を有効にする	**calibrate-channel self-decisive enable**	デフォルト：AP group viewの設定が使用されます。
7. 定期的に auto-DFS を実行するように設定する	**calibrate-channel mode periodic**	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view での auto-DFS の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. （オプション設定項目）チャネルキャリブレーション間隔を設定する	**wlan rrm calibration-channel interval** *minutes*	デフォルト : ソフトウェアバージョン 7.2.21 を含む以前のソフトウェアでは8分です。 ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアでは23分です。
3. AP group view に移行する	**wlan ap-group** *group-name*	—

操作	コマンド	補足
4． AP model view に移行する	**ap-model** *model-name*	—
5． radio view に移行する	**radio** *radio-id*	—
6． RRM view に移行する	**rrm**	—
7． auto-DFS を有効にする	**calibrate-channel self-decisive enable**	デフォルト：無効
8． 定期的に auto-DFS を実行するように設定する	**calibrate-channel mode periodic**	デフォルト：有効

17.3.4 スケジュール auto-DFS の実行

スケジュール auto-DFS を設定する場合、チャネルレポート、ネイバレポートを生成するため統計情報を取得するタイムレンジを設定する必要があります。

I. RRM view でのスケジュール auto-DFS の実行方法

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． タイムレンジを設定する	**time-range** *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }	デフォルト：設定なし
3． スケジュール自動実行機能の job を作成する	**scheduler job** *job-name*	デフォルト：設定なし
4． job にコマンドを割り当てる	**command 1 system-view** **command 2 wlan ap** *ap-name* [**model** *model-name*] **command 3 radio** *radio-id* **command 4 rrm** **command 5 calibrate-channel pronto**	デフォルト：設定なし
5． system view に戻る	**quit**	ー
6． スケジュール自動実行機能のスケジュールを作成し、schedule view に移行する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
7． スケジュールに job を割り当てる	**job** *job-name*	デフォルト：設定なし
8． スケジュールにユーザロールを割り当てる	**user-role** *role-name*	デフォルト：スケジュールの作成者がスケジュールに割り当てられています。
9． 1 回のみのスケジュール自動実行機能の実行日と時間を指定する	**time at** *time date*	いずれかの1つを設定します。 デフォルト：設定なし
10．1 回のみのスケジュール自動実行機能の複数の実行日と時間を指定する	**time once at** *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]	
11．スケジュール自動実行機能の実行日と時間を指定する	**time once delay** *time*	

操作	コマンド	補足
12．system view に戻る	**quit**	—
13．AP view に移行する	**wlan ap** *ap-name*	—
14．radio view に移行する	**radio** *radio-id*	—
15．RRM view に移行する	**rrm**	—
16．auto-DFS を有効にする	**calibrate-channel self-decisive enable**	デフォルト：AP group RRM viewの設定が使用されます。
17．スケジュール auto-DFS を設定する	**calibrate-channel mode scheduled**	デフォルト：AP group RRM viewの設定が使用されます。
18．チャネルモニタリングのタイムレンジを指定する	**calibrate-channel monitoring time-range** *time-range-name*	デフォルト：AP group RRM viewの設定が使用されます。

II. AP group RRM view でのスケジュール auto-DFS の実行方法

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． タイムレンジを設定する	**time-range** *time-range-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }	デフォルト：設定なし
3． スケジュール自動実行機能の job を作成する	**scheduler job** *job-name*	デフォルト：設定なし
4． job にコマンドを割り当てる	**command 1 system-view** **command 2 wlan ap** *ap-name* [**model** *model-name*] **command 3 radio** *radio-id* **command 4 rrm** **command 5 calibrate-channel pronto**	デフォルト：設定なし
5． system view に戻る	**quit**	ー
6． スケジュール自動実行機能のスケジュールを作成し、schedule view に移行する	**scheduler schedule** *schedule-name*	デフォルト：設定なし
7． スケジュールに job を割り当てる	**job** *job-name*	デフォルト：設定なし
8． スケジュールにユーザロールを割り当てる	**user-role** *role-name*	デフォルト：スケジュールの作成者がスケジュールに割り当てられています。
9． 1 回のみのスケジュール自動実行機能の実行日と時間を指定する	**time at** *time date*	いずれかの1つを設定します。 デフォルト：設定なし
10．1 回のみのスケジュール自動実行機能の複数の実行日と時間を指定する	**time once at** *time* [**month-date** *month-day* | **week-day** *week-day*&<1-7>]	
11．スケジュール自動実行機能の実行日と時間を指定する	**time once delay** *time*	
12．system view に戻る	**quit**	—
13．AP group view に移行する	**wlan ap-group** *group-name*	—

操作	コマンド	補足
14．AP model view に移行する	**ap-model** *model-name*	—
15．radio view に移行する	**radio** *radio-id*	—
16．RRM view に移行する	**rrm**	—
17．auto-DFS を有効にする	**calibrate-channel self-decisive enable**	デフォルト：無効
18．スケジュール auto-DFS を設定する	**calibrate-channel mode scheduled**	デフォルト：periodic
19．チャネルモニタリングのタイムレンジを指定する	**calibrate-channel monitoring time-range** *time-range-name*	デフォルト：指定なし

17.3.5 オンデマンド DFS の設定

注意：
この機能はシステムリソースを消費します。慎重に使用してください。

以下にオンデマンド DFS を設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． すべての AP の無線に対してワンタイム DFS を実行する	**wlan calibrate-channel pronto ap all**	—
3． （オプション設定項目）キャリブレーション間隔を設定する	**wlan rrm-calibration-interval** *minutes*	デフォルト：8分

17.3.6 RRM 抑制グループの設定

頻繁なチャネルまたは電力の調整が無線サービスに影響しないようにする場合、指定した無線を RRM 抑制グループに追加します。RRM 抑制グループ内の無線機に関する、チャネルまたは電力の変更が行われるたびに、チャネルまたは電力抑制タイマを開始します。チャネルまたは電力抑制タイマの時間が切れるまでは、無線のチャネルまたは電力は変更されません。

オンデマンド DFS を実行すると、チャネルタイマの時間切れに関係なく、キャリブレーション間隔が終了すると DFS が実行されます。

以下に RRM 抑制グループを設定する手順を示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． RRM 抑制グループを作成し、RRM holddown group view に移行する	**wlan rrm-calibration-group** *group-id*	デフォルト：設定なし
3． （オプション設定項目）RRM 抑制グループの説明を設定する	**description** *text*	デフォルト：設定なし
4． 無線を RRM グループに追加する	**ap name** *ap-name* **radio** *radio-id*	デフォルト：設定なし
5． （オプション設定項目）チャネル抑制タイマを設定する	**channel holddown-time** *minutes*	デフォルト： 720分

17.4 TPCの設定

AC は以下の DFS 方式をサポートします。

- **定期 auto-TPC**－AC は自動的に電力キャリブレーション間隔で無線の TPC を実行します。
- **オンデマンド TPC**－AC は電力キャリブレーション間隔時間を待った後、すべての無線の TPC を実行します。AC で無線の TPC を実行する際に、この方式を行う必要があります。

17.4.1 設定の制限とガイドライン

TPC を有効にする前に **power-lock enable** コマンドを設定して電力がロックされていないことを確認してください。電力ロックの詳細については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“無線管理の設定”* を参照してください。

17.4.2 TPC モードの設定

AC は density、coverage、custom の TPC モードをサポートします。AP 間の影響を避ける場合、density モードを使用してください。信号の適用範囲を増加させる場合、coverage モードを使用してください。density、coverage の 2 つのネットワーク要件に適合しない場合、電力調整の設定をカスタマイズさせるため、custom モードを使用してください。

density、coverage の 2 つのモードでは、電力調整の設定を変更することができません。

I. RRM view での TPC モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． RRM view に移行する	**rrm**	—

操作	コマンド	補足
5． TPC モードを設定する	**calibrate-power mode** { **coverage** | **custom** | **density** }	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view での TPC モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—
6． TPC モードを設定する	**calibrate-power mode** { **coverage** | **custom** | **density** }	デフォルト：custom

17.4.3 TPC トリガーパラメータの設定

注意：
正確な電力調整のために、TPC が有効になっているすべての無線で同じ TPC パラメータを設定することを推奨します。

近接ファクタ、電力調整しきい値によって無線の TPC が決まります。近接ファクタは検出された無線の品質を定義し、電力調整しきい値との比較に使用される RSSI のランク付けに使われます。必要に応じて近接ファクタを設定してください。

I. RRM view での TPC トリガーパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． RRM view に移行する	**rrm**	—
5． 隣接番号のしきい値を設定し、電力検出用無線機を指定する	**adjacency-factor** *neighbor*	デフォルト：AP group viewの設定が使用されます。
6． 電力調整のしきい値を設定する	**calibrate-power threshold** *value*	デフォルト：AP group RRM viewの設定が使用されます。

II. AP group RRM view での TPC トリガーパラメータの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—
6． 隣接番号のしきい値を設定し、電力検出用無線機を指定する	**adjacency-factor** *neighbor*	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.21を含む以前のソフトウェアでは3です。 ソフトウェアバージョン 7.2.27を含む以降のソフトウェアでは1です。
7． 電力調整のしきい値を設定する	**calibrate-power threshold** *value*	デフォルト：ソフトウェアバージョンにより異なります。 ソフトウェアバージョン 7.2.21を含む以前のソフトウェアでは65dBmです。 ソフトウェアバージョン 7.2.27を含む以降のソフトウェアでは75dBmです。

17.4.4 最小送信電力の設定

この機能を使用することにより、TPC が実行された後も無線を検出することができます。

I. RRM view での最小送信電力の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． RRM view に移行する	**rrm**	—
5． 最小送信電力を設定する	**calibrate-power min** *tx-power*	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view での最小送信電力の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—

操作	コマンド	補足
6. 最小送信電力を設定する	**calibrate-power min** *tx-power*	デフォルト：11dBm(ソフトウェアバージョン7.2.16) 1dBm(ソフトウェアバージョン7.2.19と7.2.21) 6dBm(ソフトウェアバージョン7.2.27を含む以降)

17.4.5 最大送信電力の設定

🕮 **メモ：**

最大送信電力の設定は、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

auto-TPC で設定できる無線の最大送信電力を調整することができます。

最大送信電力は、最小送信電力の設定値よりも小さくすることはできません。

以下に、最大送信電力を設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. global configuration view に移行する	**wlan global-configuration**	—
3. 2.4GHz 無線の最大送信電力を設定する	**calibrate-power 2.4g max** *tx-power*	デフォルト：2.4GHz無線でサポートされる最大電力
4. 5GHz 無線の最大送信電力を設定する	**calibrate-power 5g max** *tx-power*	デフォルト：5GHz無線でサポートされる最大電力

17.4.6 定期 auto-TPC の設定

I. RRM view での auto-TPC の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. （オプション設定項目）電力キャリブレーション間隔を設定する	**wlan rrm-calibration-interval** *minutes*	デフォルト：8分
3. AP view へ移行する	**wlan ap** *ap-name*	—
4. radio view に移行する	**radio** *radio-id*	—
5. RRM view に移行する	**rrm**	—
6. auto-TPC を有効にする	**calibrate-power self-decisive enable**	デフォルト：AP group viewの設定が使用されます。

II. AP group RRM view での auto-TPC の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. （オプション設定項目）電力キャリブレーション間隔を設定する	**wlan rrm-calibration-interval** *minutes*	デフォルト：8分
3. AP group view に移行する	**wlan ap-group** *group-name*	—
4. AP model view に移行する	**ap-model** *model-name*	—
5. radio view に移行する	**radio** *radio-id*	—
6. RRM view に移行する	**rrm**	—
7. auto-TPC を有効にする	**calibrate-power self-decisive enable**	デフォルト：無効

17.4.7 オンデマンド TPC の実行

注意：
この機能はシステムリソースを消費します。慎重に使用してください。

I. オンデマンド TPC の実行方法

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. すべての AP の無線に対してワンタイム TPC を実行する	**wlan calibrate-power pronto ap all**	—
3. （オプション設定項目）電力キャリブレーション間隔の設定する	**wlan rrm calibration-power interval** *minutes*	デフォルト：8分

17.4.8 死角検出の設定

メモ：
AP 死角検出の設定は、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。

この機能により、AC は無線信号カバレッジに死角 (または弱い信号領域) が存在するかどうかを判断できます。死角が検出された場合、AC は auto-TPC を実行するときに対応する AP の送信電力を増加させます。

AC は、次の条件を満たす場合に、無線のカバレッジに死角があると判断します。

- 無線に関連付けられた弱い信号クライアントの数が、しきい値に達するか、または超えている場合。
- 無線に関連付けられた弱い信号クライアントの割合がしきい値に達するか、それを超えている場合。

AC は、次の条件が満たされた場合に、クライアントが弱信号クライアントであると判断します。

- クライアントの弱信号パケット数がしきい値に達するか、またはしきい値を超えた場合。
- クライアントの弱信号パケットの割合がしきい値に達するか、それを超えた場合。

パケットの RSSI が RSSI しきい値より低い場合、そのパケットは弱い信号パケットと見なされます。

I. radio View での死角検出の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． 死角検出を有効にする	**calibrate-power coverage { disable | enable }**	デフォルト：AP group viewの設定が使用されます。

II. AP group radio View での死角検出の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． 死角検出を有効にする	**calibrate-power coverage { disable | enable }**	デフォルト： Global configuration viewの設定が使用されます。

III. global configuration View での死角検出の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan global-configuration**	—
3． 死角検出を有効にする	**calibrate-power coverage enable { 2.4g | 5g | all }**	デフォルト：無効
4． （オプション設定項目）2.4GHz 無線の弱信号クライアント数のしきい値を設定する	**calibrate-power 2.4g coverage weak-signal-client threshold** *counts*	デフォルト：3
5． （オプション設定項目）5GHz 無線の弱信号クライアント数のしきい値を設定する	**calibrate-power 5g coverage weak-signal-client threshold** *counts*	デフォルト：3

操作	コマンド	補足
6.　（オプション設定項目）2.4GHz 無線の弱信号クライアント割合のしきい値を設定する。	**calibrate-power 2.4g coverage weak-signal-client ratio** *percent*	デフォルト：25%
7.　（オプション設定項目）5GHz 無線の弱信号クライアント割合のしきい値を設定する。	**calibrate-power 5g coverage weak-signal-client ratio** *percent*	デフォルト：25%
8.　（オプション設定項目）2.4GHz 無線の弱信号パケット数のしきい値を設定する	**calibrate-power 2.4g coverage weak-signal-packet threshold** *packets*	デフォルト：5
9.　（オプション設定項目）5GHz 無線の弱信号パケット数のしきい値を設定する	**calibrate-power 5g coverage weak-signal-packet threshold** *packets*	デフォルト：5
10.　（オプション設定項目）2.4GHz 無線の弱信号パケット割合のしきい値を設定する	**calibrate-power 2.4g coverage weak-signal-packet ratio** *percent*	デフォルト：20%
11.　（オプション設定項目）5GHz 無線の弱信号パケット割合のしきい値を設定する	**calibrate-power 5g coverage weak-signal-packet ratio** *percent*	デフォルト：20%
12.　（オプション設定項目）2.4GHz 無線の弱信号パケットと判別する RSSI しきい値を設定する	**calibrate-power 2.4g coverage rssi-threshold** *rssi*	デフォルト：20
13.　（オプション設定項目）5GHz 無線の弱信号パケットと判別する RSSI しきい値を設定する	**calibrate-power 5g coverage rssi-threshold** *rssi*	デフォルト：25

17.4.9 RRM 抑制グループの設定

頻繁なチャネルまたは電力の調整が無線サービスに影響しないようにする場合、指定した無線を RRM 抑制グループに追加します。RRM 抑制グループ内の無線機に関する、チャネルまたは電力の変更が行われるたびに、チャネルまたは電力抑制タイマを開始します。チャネルまたは電力抑制タイマの時間が切れるまでは、無線のチャネルまたは電力は変更されません。

オンデマンド TPC を実行すると、電力抑制タイマの時間切れに関係なく、キャリブレーション間隔が終了すると TPC が実行されます。

I. RRM 抑制グループの設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—

操作	コマンド	補足
2． RRM 抑制グループを作成し、RRM holddown group view に移行する	**wlan rrm-calibration-group** *group-id*	デフォルト：設定なし
3． （オプション設定項目）RRM 抑制グループの説明を設定する	**description** *text*	デフォルト：設定なし
4． 無線を RRM グループに追加する	**ap name** *ap-name* **radio** *radio-id*	デフォルト：設定なし
5． （オプション設定項目）電力抑制タイマを設定する	**power holddown-time** *minutes*	デフォルト： 60分

17.5 スペクトル管理の設定

17.5.1 スペクトル管理の有効化

スペクトル管理機能は 5GHz 帯でのみ有効です。

I. radio view でのスペクトル管理の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． スペクトル管理を有効にする	**spectrum-management enable**	デフォルト：AP group viewの設定が使用されます。

II. AP group radio view でのスペクトル管理の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． スペクトル管理を有効にする	**spectrum-management enable**	デフォルト：無効

17.5.2 電力制約モードの設定

電力制約モードの設定は 5GHz 帯でのみ有効です。

この機能を使用することで、無線が関連するクライアントの送信電力を制限して、他の無線デバイスへの干渉を回避できます。無線からの電力制約値を含むビーコンフレームまた

はプローブ応答を受信すると、クライアントはその新しいローカル最大送信電力を使用してトラフィックを送信します。新しいローカル最大送信電力は、チャネルに対して指定された最大送信電力レベルから電力制約値を差し引いたものとなります。

無線には次の電力制約モードを設定できます。

- **Manual**－電力制約値を指定します。
- **Auto**－自動的に電力制約値を計算します。

I. radio view での電力制約モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． 電力制約モードを設定する	**power-constraint mode** { **auto** [**anpi-interval** *anpi-interval-value*] | **manual** *power-constraint* }	デフォルト：AP group viewの設定が使用されます。 電力制約モードは、スペクトル管理または無線リソース測定を有効にする場合にのみ利用することができます。 無線リソース管理の詳細については、QX-W1000/W1100シリーズ アクセスポイント Anchor-AC コマンドマニュアルの *"WLAN無線リソースの計測の設定"* を参照してください。

II. AP group radio view での電力制約モードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． 電力制約モードを設定する	**power-constraint mode** { **auto** [**anpi-interval** *anpi-interval-value*] | **manual** *power-constraint* }	デフォルト：Auto 電力制約モードは、スペクトル管理または無線リソース測定を有効にする場合にのみ利用することができます。 無線リソース管理の詳細については、QX-W1000/W1100シリーズ アクセスポイント Anchor-AC コマンドマニュアルの *"WLAN無線リソースの計測の設定"* を参照してください。

17.5.3 チャネルスイッチモードの設定

この機能を使用することにより、無線が新しいチャネルに変更されたときに、無線が関連付けられたクライアントにチャネルスイッチアナウンスメントを送信することができます。アナウンスメントには、新しいチャネル番号と、クライアントがフレームの送信を続行できるかどうかに関する情報が含まれています。

I. radio view でのチャネルスイッチモードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． チャネルスイッチモードを設定する	**channel-switch mode** { **continuous** | **suspend** }	デフォルト：AP group viewの設定が使用されます。

II. AP group radio view でのチャネルスイッチモードの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． チャネルスイッチモードを設定する	**channel-switch mode** { **continuous** | **suspend** }	デフォルト： suspend オンラインクライアントは、チャネル切り替え中にフレームの送信を停止します。

17.5.4 送信電力機能一致モードの設定

この機能を使用することにより、クライアントは定義済みの一致基準に基づいて無線に関連付けることができます。送信電力機能は、クライアントおよび無線機が現在のチャネルでフレームを送信できる最小電力および最大電力を指します。

デバイスは、次のクライアント電力機能の一致モードをサポートしています。

- **All**－クライアントは、それぞれの送信電力機能が各無線の送信電力機能と一致する場合にのみ、無線に関連付けることができます。
- **None**－クライアントの送信電力機能はチェックされません。
- **Partial**－クライアントは、その送信電力機能の 1 つが無線機の送信電力機能と一致する限り、無線機に関連付けることができます。

I. radio view での送信電力機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—

操作	コマンド	補足
3． radio view に移行する	**radio** *radio-id*	—
4． 送信電力機能一致モードを設定する	**power-capability mode** { **all** | **none** | **partial** }	デフォルト：AP group viewの設定が使用されます。 送信電力機能一致モードは、スペクトル管理または無線リソース測定を有効にした場合にのみ利用することができます。無線リソース管理の詳細については QX-W1000/W1100シリーズ アクセスポイント Anchor-AC コマンドマニュアルの *"WLAN 無線リソースの計測の設定"* を参照してください。

II. AP group radio view での送信電力機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． 送信電力機能一致モードを設定する	**power-capability mode** { **all** | **none** | **partial** }	デフォルト：設定なし 送信電力機能一致モードは、スペクトル管理または無線リソース測定を有効にした場合にのみ利用することができます。無線リソース管理の詳細については、QX-W1000/W1100シリーズ アクセスポイント Anchor-AC コマンドマニュアルの *"WLAN 無線リソースの計測の設定"* を参照してください。

17.5.5 チャネル機能一致モードの設定

この機能を使用することにより、クライアントは定義済みの一致基準に基づいて無線に関連付けることができます。チャネル機能は、クライアントおよび無線がそれぞれサポートするチャネルを指します。

このデバイスは、次のクライアントチャネル機能一致モードを提供します。

- **All**－クライアントは、サポートされている各チャネルが無線でサポートされているチャネルのそれぞれと一致する場合にのみ、無線に関連付けることができます。
- **None**－チャネル機能のチェックはされません。
- **Partial**－サポートされているチャネルのいずれかがサポートされているラジオのチャネルと一致する限り、クライアントはラジオに関連付けることができます。

I. radio view でのクライアントチャネル機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． radio view に移行する	**radio** *radio-id*	—
4． クライアントチャネル機能一致モードを設定する	**channel-capability mode** { **all** | **none** | **partial** }	デフォルト：AP group viewの設定が使用されます。

II. AP group radio view でのクライアントチャネル機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． チャネル機能一致モードを設定する	**channel-capability mode** { **all** | **none** | **partial** }	デフォルト：設定なし

17.6 帯域幅自動調整の設定

メモ：

この機能はソフトウェアバージョン 7.2.55 を含む以降のソフトウェアからサポートしています。

17.6.1 帯域幅自動調整の有効化

帯域幅自動調整機能は 5GHz 帯でのみ有効です。

I. radio view での帯域幅自動調整の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP を作成し、AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． rrm view に移行する	**rrm**	—
5． 帯域幅自動調整を有効にする	**calibrate-bandwidth self-decisive enable**	デフォルト：AP group viewの設定が使用されます。

II. AP group radio view での帯域幅自動調整の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． rrm view に移行する	**rrm**	—
6． 帯域幅自動調整を有効にする	**calibrate-bandwidth self-decisive enable**	デフォルト：Global configuration viewの設定が使用されます。

III. Global configuration view での帯域幅自動調整の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan global-configuration**	—
3． 帯域幅自動調整を有効にする	**calibrate-bandwidth self-decisive enable**	デフォルト：無効

17.6.2 帯域幅自動調整間隔の設定

帯域幅自動調整が有効の場合、AC は帯域幅自動調整間隔に達するとチャネル品質検出を開始し、帯域幅調整を実行するかどうかを決定します。

I. 帯域幅自動調整間隔の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． （オプション設定項目）帯域幅自動調整間隔を設定する	**wlan rrm-calibration-bandwidth interval** *minutes*	デフォルト：13分

17.7 無線ベースラインの設定

無線ベースラインは無線の動作チャネル、転送レートやほかの無線属性を保存します。

現在の無線の設定を保存することで無線ベースラインを作成し、必要な設定を使用するためのベースラインを適用することができます。

無線ベースラインは AC のファイルシステムに“.csv”ファイルで保存されます。

以下のいずれかの状態の場合、無線ベースラインを無線に適用することができません。

- 無線がダウンしています。
- サービステンプレートが無煙に関連付けられていません。あるいはサービステンプレートが無効です。

- ベースラインのチャネルが不正です。
- 無線が手動で指定されたチャネルを使用しています。
- 無線の動作チャネル、送信電力がロックされています。
- 無線のチャネル、電力抑制タイマが終了していません。
- ベースラインのチャネルが指定したチャネルギャップに一致していません。
- 無線のベースラインの送信電力が指定した最小送信電力より小さいです。
- 無線のベースラインの送信電力が指定した最大送信電力より大きいです。
- ベースラインの無線モード、ロケーション識別子、帯域幅が無線の無線モード、ロケーション識別子、帯域幅に一致していません。

以下に無線ベースラインを設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 現在の無線の設定を保存するベースラインを作成する	**wlan rrm baseline save name** *baseline-name* { **ap** *ap-name* **radio** *radio-id* | **ap-group** *group-name* **ap-model** *ap-model* **radio** *radio-id* | **global** }	—
3. ベースラインを適用する	**wlan rrm baseline apply name** *baseline-name*	—
4. （オプション設定項目）無線ベースラインを削除する	**wlan rrm baseline remove name** *baseline-name*	—

17.8 無線スキャニングの有効化

この機能は、WLAN 環境をスキャンするため、AP で有効にします。指定した間隔で AC に収集した統計情報を通知します。AC はチャネルレポートと隣接レポートを作成するため、統計情報を使用します。

チャネルレポートと隣接レポートを表示する場合、**display wlan rrm-status ap** コマンドを使用します。

定期 auto-DFS、スケジュール auto-DFS、定期 auto-TPC、スケジュール auto-TPC が設定されている場合、この機能を有効にする必要がありません。

I. RRM view でのクライアントチャネル機能一致モード設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. RRM view に移行する	**rrm**	—
5. 無線スキャニングを有効にする	**scan-only enable**	デフォルト：AP group RRM viewの設定が使用されます。

II. AP group RRM view でのクライアントチャネル機能一致モード設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *model-name*	—
4． radio view に移行する	**radio** *radio-id*	—
5． RRM view に移行する	**rrm**	—
6． 無線スキャニングを有効にする	**scan-only enable**	デフォルト：無効

17.9 WLAN RRMのSNMP通知の有効化

重要な WLAN RRM イベントを NMS に報告するには、WLAN RRM の SNMP 通知を有効にする必要があります。WLAN RRM イベント通知を正しく送信するには、SNMP を設定する必要があります。SNMP の詳細は QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 11 *システム管理 “SNMP”* を参照してください。

I. WLAN RRM の SNMP 通知有効化設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． WLAN RRM の SNMP 通知を有効にする	**snmp-agent trap enable wlan rrm**	デフォルト：無効

17.10 WLAN RRMの表示および管理

すべての view で **display** コマンドを実行できます

操作	コマンド
無線ベースラインの情報を表示する	**display wlan rrm baseline** { **all** | **name** *baseline-name* } [**verbose**]
無線ベースラインのアプリケーション履歴を表示する	**display wlan rrm baseline apply-history** [**verbose**]
チャネルと電力調整履歴を表示する	**display wlan rrm-history ap** { **all** | **name** *ap-name* }
WLAN RRMを情報表示する	**display wlan rrm-status ap** { **all** | **name** *ap-name* }
RRM抑制グループの情報を表示する	**display wlan rrm-calibration-group** { **all** | *group-id* }

17.11 WLAN RRMの設定例

17.11.1 定期 auto-DFS の設定例

I. ネットワーク要件

図 17-3に示すように、チャネル調整トリガー条件が満たされたときに AP の無線用のチャネルを調整するように auto-DFS を設定します。頻繁なチャネル調整を避けるために、AP1 の無線 1 を RRM 抑制グループに追加します。

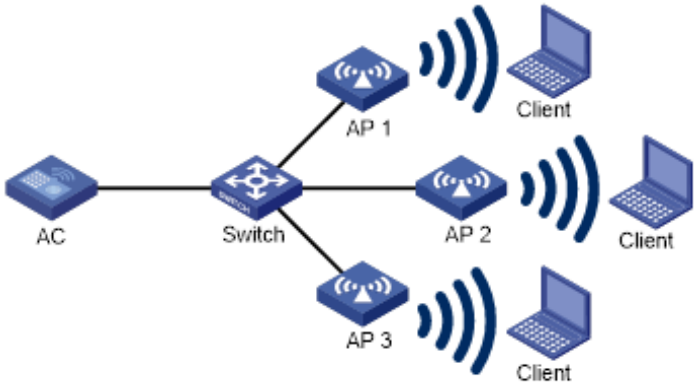


図 17-3 ネットワーク図

II. 設定手順

AC と各 AP の間に CAPWAP トンネルを確立します。詳細については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"AP 管理"* を参照してください。（詳細は省略します。）

AP1 で auto-DFS を有効にします。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] rrm
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable
```

DFS トリガーパラメータを設定します。

```
[AC-wlan-ap-ap1-radio-1-rrm] crc-error-threshold 20
[AC-wlan-ap-ap1-radio-1-rrm] interference-threshold 50
[AC-wlan-ap-ap1-radio-1-rrm] tolerance-level 20
[AC-wlan-ap-ap1-radio-1-rrm] quit
[AC-wlan-ap-ap1-radio-1] quit
```

```
[AC-wlan-ap-ap1] quit
```

RRM 抑制グループ 10 を作成します。

```
[AC] wlan rrm-calibration-group 10
```

AP1 の無線 1 を RRM 抑制グループ 10 に追加します。

```
[AC-wlan-rc-group-10] ap name ap1 radio 1
```

チャネル抑制タイマを 600 分に設定します。

```
[AC-wlan-rc-group-10] channel holddown-time 600
```

AP 1 と同じ方法で、AP 2 と AP 3 の auto-DFS を設定します。（詳細は省略します。）

III. 設定の確認

display wlan rrm-status ap all コマンドを実行します。チャネル調整トリガー条件を満たし較正間隔に達することで、AP の無線用のチャネルが変更されることを確認します。（詳細は省略します。）

display wlan rrm-history ap all コマンドを使用して、チャネル調整の理由を表示します。（詳細は省略します）

最初の DFS から 600 分以内に、AP 1 の無線 1 のチャネルが変更されていないことを確認します。（詳細は省略します）

17.11.2 スケジュール auto-DFS の設定例

I. ネットワーク要件

図 17-4に示すように、チャネル調整トリガー条件が満たされたときに AP の無線用のチャネルを調整するようにスケジュール auto-DFS を設定します。

0:05～23:50 の測定結果を使用して翌日の 5:00 にチャネル設定を行います。

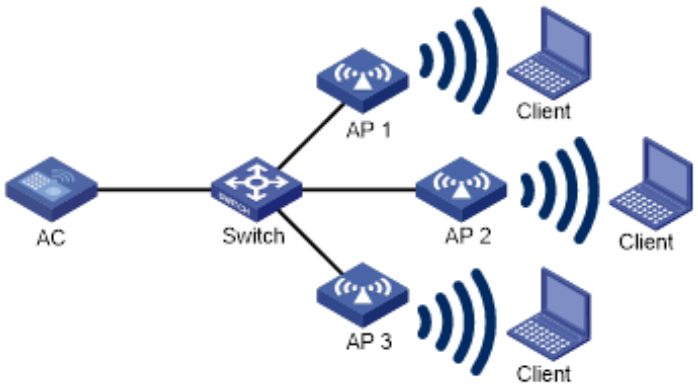


図 17-4 ネットワーク図

II. 設定手順

AC と各 AP の間に CAPWAP トンネルを確立します。詳細については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"AP 管理"* を参照してください。（詳細は省略します。）

タイムレンジを作成します。

```
<AC> system-view
[AC] time-range time1 from 0:05 to 23:50 daily
```

job を作成し、job にコマンドを割り当てます。

```
[AC] scheduler job calibratechannel
[AC-job-calibratechannel] command 1 system-view
[AC-job-calibratechannel] command 2 wlan ap ap1
[AC-job-calibratechannel] command 3 radio 1
[AC-job-calibratechannel] command 4 rrm
[AC-job-calibratechannel] command 5 calibrate-channel pronto
[AC-job-calibratechannel] quit
```

スケジュールを作成し、スケジュールに job を割り当てます。

```
[AC] scheduler schedule schedule1
[AC-schedule-schedule1] job calibratechannel
```

スケジュールに実行日時(毎日 5 時)を設定します。

```
[AC-schedule-schedule1] time repeating at 5:00
[AC-schedule-schedule1] quit
```

AP1 で auto-DFS を有効にし、スケジュール auto-DFS を設定します。

```
[AC] wlan ap ap1
```

```
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] rrm
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel self-decisive enable
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel mode scheduled
```

ap1 にタイムレンジ time1 の間、チャネルのモニタリングを実行するように設定します。

```
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-channel monitoring time-range time1
```

auto-DFS の属性は変更せず初期値を使用します。

III. 設定の確認

display wlan rrm-status ap all コマンドを実行します。チャネル調整トリガー条件を満たし較正間隔に達することで、AP の無線用のチャネルが変更されることを確認します。（詳細は省略します。）

display wlan rrm-history ap all コマンドを使用して、チャネル調整の理由を表示します。（詳細は省略します）

17.11.3 定期 TPC の設定例

I. ネットワーク要件

図 17-5に示すように、auto-TPC を設定し、隣接番号のしきい値を 3 に設定すると、AP 4 が参加したときに AC が auto-TPC を実行できるようになります。頻繁な電力調整を避けるために、AP1 の無線 1 を RRM 抑制グループに追加します。

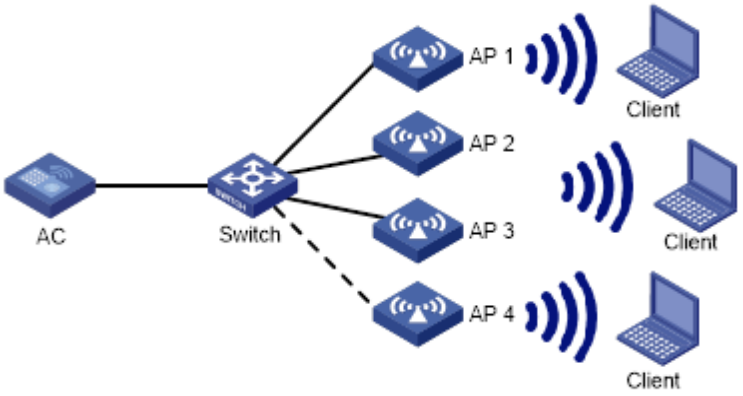


図 17-5 ネットワーク図

II. 設定手順

#AC と各 AP の間に CAPWAP トンネルを確立します。詳細については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"AP 管理"* を参照してください。（詳細は省略します。）

AP1 で auto-TPC を有効にします。

```
<AC> system-view
[AC] wlan ap ap1 model QX-W1020
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] rrm
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power self-decisive enable
```

TPC トリガーパラメータを設定します。

```
[AC-wlan-ap-ap1-radio-1-rrm] adjacency-factor 3
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power threshold 80
[AC-wlan-ap-ap1-radio-1-rrm] calibrate-power min 1
[AC-wlan-ap-ap1-radio-1-rrm] quit
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

RRM 抑制グループ 10 を作成します。

```
[AC] wlan rrm-calibration-group 10
```

AP1 の無線 1 を RRM 抑制グループ 10 に追加します。

```
[AC-wlan-rc-group-10] ap name ap1 radio 1
```

電力抑制タイマを 100 分に設定します。

```
[AC-wlan-rc-group-10] power holddown-time 100
```

AP 1 と同じ方法で、AP 2、AP 3、および AP 4 に auto-TPC を設定します。（詳細は省略します）

III. 設定の確認

AP4 の無線機が電力検出用無線機であり、このステップで AP の名前を使用してその無線機を参照すると仮定します。

次の情報を確認するには、**display wlan rrm-status ap all** コマンドを使用します。

- AP1 の電力が電力調整しきい値よりも低いことを AP4 が検出すると、AP1 は送信電力を増加させることを確認します。
- AP1 の電力が電力調整しきい値より高いことを AP4 が検出すると、AP1 は送信電力を減少させることを確認します。
- AP1 の調整された電力は、最小送信電力（この例では 1dBm）より低くはないことを確認します。

最初の TPC から 100 分以内に、AP1 の無線 1 の電力が変更されないことを確認します。

17.11.4 スペクトル管理の設定例

I. ネットワーク要求

図 17-6に示すように、スペクトル管理を設定してクライアントの送信電力を制限し、チャネル切り替え中にクライアントがフレームを送信し続けるようにします。



図 17-6 ネットワーク図

II. 設定手順

スペクトル管理を有効にします。

```
<AC> system-view
[AC] wlan ap officeap model QX-W1020
[AC-wlan-ap-officeap] radio 1
[AC-wlan-ap-officeap-radio-1] spectrum-management enable
```

チャネル機能一致モードを all に設定します。

```
[AC-wlan-ap-officeap-radio-1] channel-capability mode all
```

送信電力機能一致モードを all に設定します。

```
[AC-wlan-ap-officeap-radio-1] power-capability mode all
```

電力制約モードを手動に設定し、電力制約値を 5 dBm に設定します。

```
[AC-wlan-ap-officeap-radio-1] power-constraint mode manual 5
```

チャネルスイッチモードを continuous に設定します。

```
[AC-wlan-ap-officeap-radio-1] channel-switch mode continuous
```

III. 設定の確認

display wlan client コマンドを実行して、クライアントが正常に無線と関連付けられていることを確認します。（詳細は省略します）

17.11.5 帯域幅自動調整の設定例

I. ネットワーク要求

図 17-7に示すように、帯域幅自動調整を設定して周辺 AP の数に応じて、自動的に帯域幅が調整されるようにします。

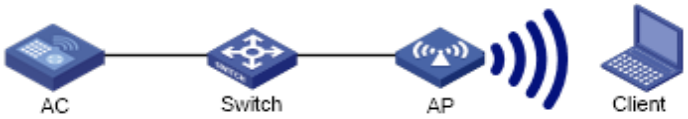


図 17-7 ネットワーク図

II. 設定手順

帯域幅自動調整を有効にします。

```
<AC> system-view
[AC] wlan ap officeap model QX-W1020
[AC-wlan-ap-officeap] radio 1
[AC-wlan-ap-officeap-radio-1] rrm
[AC-wlan-ap-officeap-radio-1-rrm] calibrate-bandwidth self-decisive enable
```

帯域幅自動調整間隔を 10 分に設定します。

```
[AC] wlan rrm calibration-bandwidth interval 10
```

III. 設定の確認

display wlan rrm-history ap all コマンドを使用して、帯域幅自動調整の履歴を表示します。（詳細は省略します）

目次

18 章 WLAN 無線ロードバランス 18-1
18.1 概要 18-1
18.1.1 ネットワークスキーム 18-1
18.1.2 無線ロードバランスのモードとタイプ 18-1
18.2 制限とガイドライン 18-2
18.3 5GHz 無線ロードバランス機能 18-2

18章 WLAN 無線ロードバランス

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

18.1 概要

WLAN 無線ロードバランスは、同じ AC で管理されている AP 上の無線間でクライアントの負荷を動的に分散します。これにより、高密度 WLAN のクライアントに対してワイヤレスサービス品質と適切な帯域幅が保証されます。

18.1.1 ネットワークスキーム

図 18-1 に示すように同じ AP の Radio1 と Radio2 が有効になっています。2 つの 5GHz 無線で同じ SSID を使用している場合、WLAN 無線ロードバランスを使用することで、Client4 が Radio1 に接続するのを避け、Radio2 への接続に誘導します。

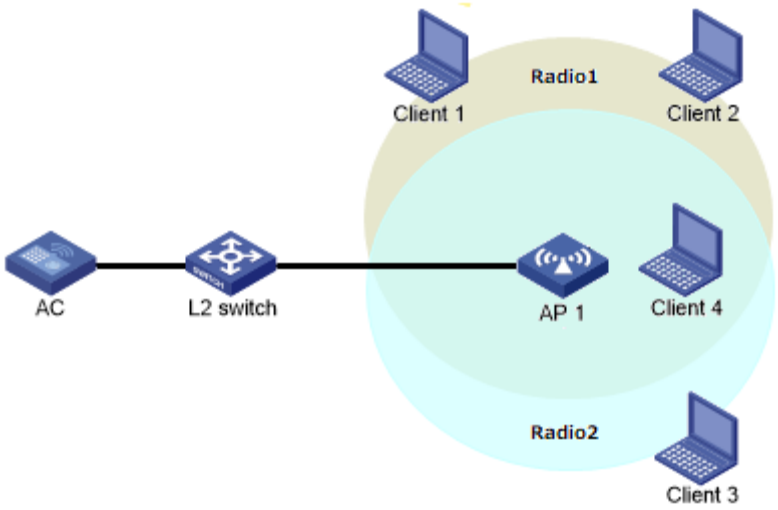


図 18-1 ネットワーク図

18.1.2 無線ロードバランスのモードとタイプ

装置は、セッションモードの無線ロードバランスと次の無線ロードバランスタイプをサポートしています。

- **セッションギャップしきい値ベース**－装置は、次の条件が満たされた場合に無線ロードバランスを実行します。
  - 無線に関連付けられたクライアントの数が、セッションしきい値に達した場合

□　クライアント数が最も少ない無線と無線の間のセッションギャップが、セッションギャップしきい値に達した場合

⚠ **注意：**
クライアントのネイバ無線は、クライアントから要求を受信するすべての無線を指します。

18.2 制限とガイドライン

クライアントが WLAN へのアクセスを要求すると、システムは同じ AC によって管理され、クライアントによって検出可能な AP の無線間でのみ無線ロードバランスを実行します。

WLAN 無線ロードバランスと WLAN ロードバランスまたはバンドナビゲーションは、互いに排他的です。WLAN ロードバランスとバンドナビゲーションの詳細は、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *"WLAN ロードバランス"*、*"バンドナビゲーションの設定"* を参照してください。

18.3 5GHz無線ロードバランス機能

🕮 **メモ：**
- この機能はソフトウェアバージョン 7.2.19 を含む以降のソフトウェアからサポートしています。
- この機能は、QX-W1110 および QX-W1010 では利用できません。

この機能を有効にすると、5GHz 無線は次の 2 つの条件が満たされた場合に、ビーコンフレームの SSID を非表示にします。

- 5GHz 無線に関連付けられたクライアントの数が、しきい値に達した場合
- 同じ AP 内の 2 つの 5GHz 無線の間のセッションギャップが、しきい値に達した場合

5GHz 無線に関連付けられているクライアントの数がセッションしきい値を下回ると、5GHz 無線はビーコンフレームの SSID の非表示を停止します。

2 つの 5GHz 無線で同一の SSID で動作させる環境で、ネットワークに多数のクライアントが存在する場合は、この機能を有効にすることを推奨します。

SSID を非表示にするための過負荷状態の 5GHz 無線の設定手順は以下のとおりです。

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP view または AP group view に移行する	• AP viewに移行する **wlan ap** *ap-name* • AP group viewに移行する **wlan ap-group** *group-name*	—

操作	コマンド	補足
3． 5 GHz 無線ロードバランスを有効にする	**wlan radio-load-balance overload-5g ssid-hide** [**session** *value* [**gap** *gap-value*]] } [**force-logoff**]	デフォルト： AP viewでは、APはAP group viewの設定を使用します。 AP group viewでは、 v7.2.21を含む以前は有効 v7.2.19は無効です。

目次

19 章 デュアルリンクバックアップの設定 19-1
19.1 概要 19-1
19.2 デュアルリンクバックアップの設定作業リスト 19-2
19.3 設定要件 19-2
19.4 AC 維持機能の設定 19-2
19.5 バックアップ AC の指定 19-3
19.6 マスタ CAPWAP トンネルの優先接続の設定 19-3
19.6.1 AP に対するマスタ CAPWAP トンネルの優先接続の設定 19-3
19.6.2 AP group に対するマスタ CAPWAP トンネルの優先接続の設定 19-4
19.6.3 グローバル マスタ CAPWAP トンネルの優先接続の設定 19-4
19.7 デュアルリンクバックアップモード設定例 19-4

19章 デュアルリンクバックアップの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

⚠ **注意**：

- デュアルリンクバックアップを使用する AC は、同一のソフトウェアバージョンを使用してください。
- デュアルリンクアップを使用する AC は、自動で選択されたチャネル情報を AC 間で引き継ぎません。デュアルリンクバックアップを使用する場合はチャネルを手動設定して使用することを推奨します。
- マスタ AC とバックアップ AC のコンフィグ同期はできません。
- バックアップ AC として動作する Anchor-AC が提供する無線 AP 機能は、マスタ AC で管理することができません。

🕮 **メモ**：

- デュアルリンクバックアップの設定は V7.2.52 を含む以降のバージョンからサポートしています。
- デュアルリンクバックアップの設定は、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。
- AC 選出機能と同時に設定した場合は、マスタ AC とバックアップ AC 両方がダウンしたときに AC 選出機能が動作します。

19.1 概要

デュアルリンクバックアップは 2 台の AC を互いにバックアップすることを可能にします。これにより、AC1 台時に発生するサービス停止のリスクを低減します。

デュアルリンクバックアップは AP に 2 つのアップリンク接続を提供します。AP は、マスタ AC、バックアップ AC それぞれと CAPWAP トンネルを接続します。マスタとバックアップ AC はリアルタイムで互いのリンク状態を検出することができません。マスタ AC 障害時に、バックアップ AC がトラフィック転送を引き継ぎますが一時的な通信中断が発生します。故障したマスタ AC が回復したとき、マスタ CAPWAP トンネルの優先機能により、AP 接続の優先度にもとづいて、マスタ CAPWAP トンネルを決定します。

デュアルリンクバックアップは、サービス連続性が不要なネットワークに適用できます。

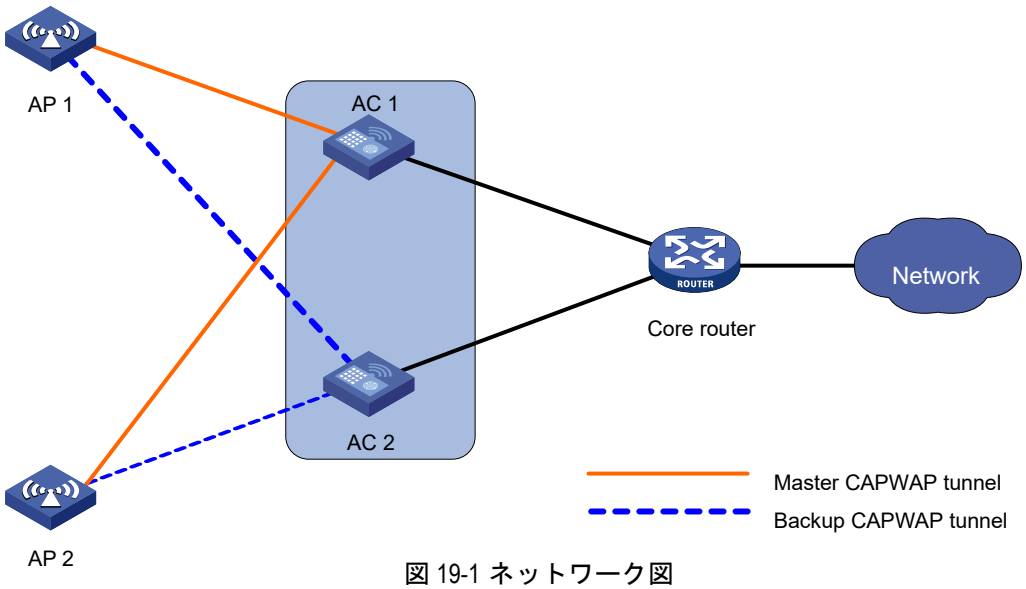


図 19-1 ネットワーク図

19.2 デュアルリンクバックアップの設定作業リスト

作業リスト
（必須設定項目）AC維持機能の設定
（必須設定項目）バックアップACの指定
（オプション設定項目）マスタCAPWAPトンネルの優先順位の設定

19.3 設定要件

2 台の AC それぞれでオート AP またはマニュアル AP の設定してください。マニュアル AP コンフィグレーションは 2 台の AC で同一でなければなりません。詳細については、QX-W1000/W1100 シリーズ アクセスポイント Anchor-AC オペレーションマニュアルの *“2 章 AP 管理”* を参照してください。

19.4 AC維持機能の設定

🕮 **メモ：**

- デュアルリンクバックアップを使用する場合は、事前に AC 維持機能を設定してからネットワークに接続してください。

2 台の AC それぞれで AC 維持機能を設定してください。詳細については、オペレーションマニュアルの *“1 章 Anchor-AC の設定”* の *“AC 維持機能の設定”* 参照してください。

19.5 バックアップACの指定

AP がマスタ AC と CAPWAP トンネルを確立した後、AP は指定したバックアップ AC とバックアップの CAPWAP トンネルを確立します。

AP が最初にマスタ AC と関連付けられるように、マスタ AC の AP 接続優先度をもっとも高く設定することを推奨します。

I. AP 用バックアップ AC の指定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	―
3． AP 接続のプライオリティを設定する	**priority** *priority*	デフォルト：APはAPグループviewの設定を使用します。
4． バックアップ AC を設定する	**backup-ac ip** *ipv4-address*	デフォルト：APはAPグループviewの設定を使用します。

II. AP グループ用バックアップ AC の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP group view に移行する	**wlan ap-group** *group-name*	―
3． AP 接続のプライオリティを設定する	**priority** *priority*	デフォルト：4
4． バックアップ AC を設定する	**backup-ac ip** *ipv4-address*|	デフォルト：設定なし

19.6 マスタCAPWAPトンネルの優先接続の設定

デュアルリンクバックアップを利用している環境において、優先度の高い AP との CAPWAP トンネルが切断されバックアップ AP との CAPWAP トンネルがマスタに切り替わった後、再度優先度の高い AP との CAPWAP トンネルが復旧した場合の動作を設定します。

この機能が有効な場合、高優先の AP との CAPWAP トンネルが復旧した際、マスタに接続が切り戻ります。

この機能が無効な場合、高優先の AP との CAPWAP トンネルが復旧しても、マスタに接続は切り戻りません。

19.6.1 AP に対するマスタ CAPWAP トンネルの優先接続の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． AP view に移行する	**wlan ap** *ap-name*	―
3． マスタ CAPWAP トンネルの強制排除を設定する	**wlan tunnel-preempt** { **disable** | **enable** }	デフォルト：AP group viewの設定を使用します。

19.6.2 AP group に対するマスタ CAPWAP トンネルの優先接続の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． AP group view に移行する	**wlan ap-group** *groupname*	―
3． マスタ CAPWAP トンネルの強制排除を設定する	**wlan tunnel-preempt** { **disable** | **enable** }	デフォルト：global configuration viewの設定を使用します。

19.6.3 グローバル マスタ CAPWAP トンネルの優先接続の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． global configuration view に移行する	**wlan global-configuration**	―
3． マスタ CAPWAP トンネルの強制排除を設定する	**wlan tunnel-preempt** { **disable** | **enable** }	デフォルト：無効

19.7 デュアルリンクバックアップモード設定例

I. ネットワーク要件

図 20-2 に示すように、AC1 をマスタ AC,AC2 をバックアップ AC とします。AC1 故障時 AC2 が処理を引き継ぎ AP は AC2 を使用して通信ができます。AC1 復旧時、AP は AC1 をマスタ AC として再接続するようにマスタ CAPWAP トンネルの優先接続設定を行います。

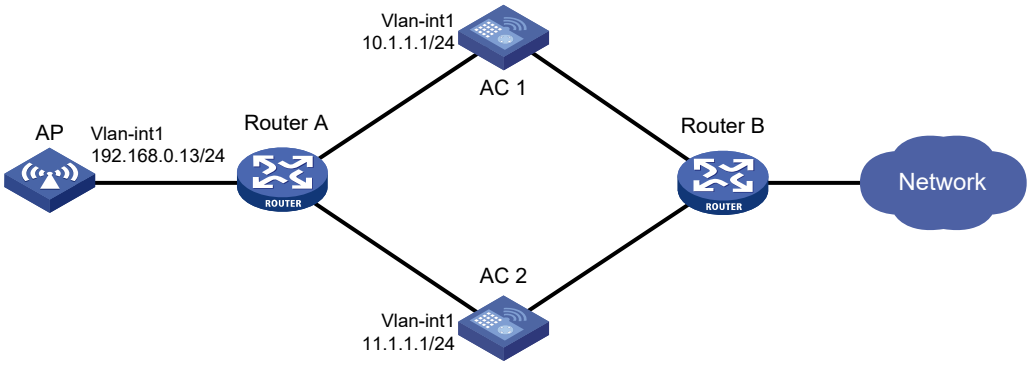


図 19-2 ネットワーク図

II. 設定手順

1)　AC1 を設定します。

AC 維持機能を有効にします。

```
<AC1> system-view
[AC1] wlan anchor-ap persistent-mode ac
```

VLAN インタフェース 1 を作成し、IP アドレスを設定します。

```
 [AC1] interface vlan-interface 1
[AC1-Vlan-interface1] ip address 10.1.1.1 24
[AC1-Vlan-interface1] quit
```

AP ap1 を作成し、AP モデルとシリアル ID を指定します。AP 接続プライオリティを 7 に設定します。

```
[AC1] wlan ap ap1 model QX-W1020
[AC1-wlan-ap-ap1] serial-id 210235A1BSC123000050
[AC1-wlan-ap-ap1] priority 7
```

バックアップ AC の IPv4 を指定します。

```
[AC1-wlan-ap-ap1] backup-ac ip  11.1.1.1
```

マスタ CAPWAP トンネル優先接続を有効にします。

```
[AC1-wlan-ap-ap1] wlan tunnel-preempt enable
```

2)　AC2 を設定します。

AC 維持機能を有効にします。

```
<AC2> system-view
[AC2] wlan anchor-ap persistent-mode ac
```

VLAN インタフェース 1 を作成し、IP アドレスを設定します。

```
[AC2] interface Vlan-interface 1
[AC2-Vlan-interface1] ip address 11.1.1.1 24
[AC2-Vlan-interface1] quit
```

AP ap1 を作成し、AP モデルとシリアル ID を指定します。AP 接続プライオリティを 5 に設定します。

```
[AC2] wlan ap ap1 model QX-W1020
[AC2-wlan-ap-ap1] serial-id 210235A1BSC123000050
[AC2-wlan-ap-ap1] priority 5
```

バックアップ AC の IPv4 を指定します。

```
[AC2-wlan-ap-ap1] backup-ac ip  10.1.1.1
```

マスタ CAPWAP トンネル優先接続を有効にします。

```
[AC2-wlan-ap-ap1] wlan tunnel-preempt enable
```

III. 設定の確認

#AP をオンラインにします。（詳細は省略します。）

#AC1 の VLAN インタフェース 1 をシャットダウンし、サービス中断が発生するまで 3 分程度待ちます。（詳細は省略します。）

#AP は AC2 と接続し、AC2 の AP 状態が R/M になるのを確認します。（詳細は省略します。）

#AC1 の VLAN インタフェース 1 をアップします。（詳細は省略します。）

#AP は AC1 と再接続し、AC1 の AP 状態が R/B になるのを確認します。

AC1 が安定動作していることを確認する為の監視時間(約 10 分)が経過後に、AC1 の AP 状態が R/M に、AC2 の AP 状態が R/B になるのを確認します。（詳細は省略します。）

目次

20 章 WLAN アップリンクの検出設定 20-1
20.1 概要 20-1
20.2 WLAN アップリンクの検出設定 20-1
20.3 WLAN アップリンク検出の設定例 20-2

20章 WLAN アップリンクの検出設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

20.1 概要

AC のアップリンク通信が失敗する場合、クライアントは、AC に接続された AP を通して外部のネットワークにアクセスすることができません。

WLAN アップリンク検出は、AC のアップリンク状態を、接続された AP の無線状態に関連づけます。アップリンクが失敗する場合、AC は AP の無線を使用不可にします。アップリンクが回復した場合、AC は AP の無線を使用可能にします。

アソシエーションは、AC のアップリンクに障害が発生した場合に、クライアントが別の AC に接続されている AP にアソシエートできることを保証します。

この機能は、検出モジュールとトラックモジュールと連携して機能します。

- トラックエントリがポジティブ状態の場合、AC は接続された AP の無線を使用可能にします。
- トラックエントリがネガティブ状態の場合、AC は接続された AP の無線を使用不可にします。
- トラックエントリが無効状態の場合、AC は接続された AP の無線状態を変更しません。

トラックモジュールの詳細については、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 10 *高可用性 “Track”* を参照してください。

20.2 WLANアップリンクの検出設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. 検出モジュールがアップリンクの状態を検出、および、検出モジュールにトラックエントリを結合する	検出モジュールとトラックの関連づけの詳細については、QX-W1000/W1100シリーズ アクセスポイント オペレーションマニュアルのセクション10 *高可用性 “Track”* を参照してください。	―
3. トラックエントリを WLAN アップリンク検出機能に結合する	**wlan uplink track** *track-entry-number*	デフォルト：設定なし

20.3 WLANアップリンク検出の設定例

I. ネットワーク要件

図 20-1 に示すように、各 AC のアップリンク接続性を確認するテストには、NQA 操作を使用します。AC のアップリンク送信の失敗時に、クライアントが、正常な別の AC 上の AP と接続することができるように、各 AC に WLAN アップリンク検出設定を行います。

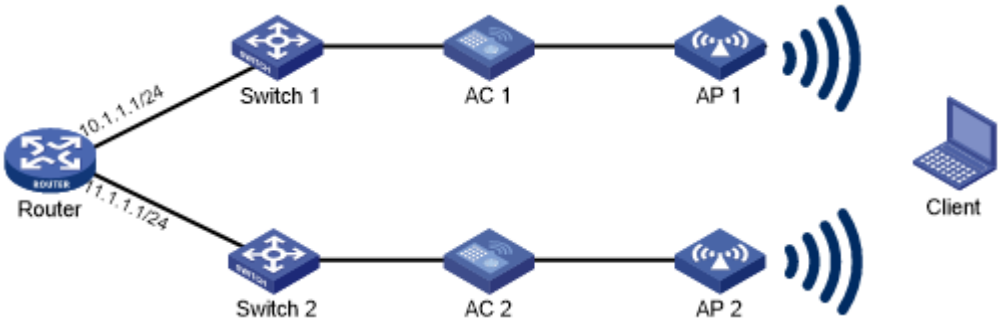


図 20-1 ネットワーク図

II. 設定手順

1)　AC1 を設定します。

ICMP エコーオペレーションを作成します。

```
<AC1> system-view
[AC1] nqa entry admin test
[AC1-nqa-admin-test] type icmp-echo
```

#ICMP エコー要求の宛先 IP アドレスとして 10.1.1.1 を指定します。

```
[AC1-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

#10000 ミリ秒ごとに繰り返すように ICMP エコー操作を設定します。

```
[AC1-nqa-admin-test-icmp-echo] frequency 10000
```

reaction entry 1 を作成します。調査失敗の数が連続 5 になると切り替えを行います。

```
[AC1-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
[AC1-nqa-admin-test-icmp-echo] quit
```

ICMP エコーを開始します。

```
[AC1] nqa schedule admin test start-time now lifetime forever
```

track entry 1 を reaction entry 1 の NQA 操作（管理者 admin、タグテスト）に結合します。

```
[AC1] track 1 nqa entry admin test reaction 1
```

track entry 1 を WLAN アップリンク検出に結合します。

```
[AC1] wlan uplink track 1
[AC1] quit
```

2)　AC2 を設定します。

ICMP エコーオペレーションを作成します。

```
<AC2> system-view
[AC2] nqa entry admin test
[AC2-nqa-admin-test] type icmp-echo
```

ICMP エコー要求の宛先 IP アドレスとして 11.1.1.1 を指定します。

```
[AC2-nqa-admin-test-icmp-echo] destination ip 11.1.1.1
```

reaction entry 1 を作成します。調査失敗の数が連続 5 になると切り替えを行います。

```
[AC2-nqa-admin-test-icmp-echo] reaction 1 checked-element probe-fail threshold-type consecutive 5 action-type trigger-only
[AC2-nqa-admin-test-icmp-echo] quit
```

#ICMP エコーを開始します。

```
[AC2] nqa schedule admin test start-time now lifetime forever
```

track entry 1 を reaction entry 1 の NQA 操作（管理者 admin、タグテスト）に結合します。

```
[AC2] track 1 nqa entry admin test reaction 1
```

track entry 1 を WLAN アップリンク検出に結合します。

```
[AC2] wlan uplink track 1
[AC2] quit
```

III. 設定の確認

本例では、設定確認するために AC1 を使用します。

1)　トラックエントリ 1 の状態がポジティブな場合、AP1 の無線がアップ状態にあることを確認します。

#トラックエントリ 1 の状態を表示します。

```
<AC1> display track 1
Track ID: 1
  State: Positive
  Duration: 0 days 1 hours 5 minutes 48 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
```

ap1 の詳細情報を表示します。

```
<AC1> display wlan ap name ap1 verbose
AP name                         : ap1
```

```
AP ID                          : 1
AP group name                  : default-group
State                          : Run
Online time                    : 0 days 2 hours 25 minutes 12 seconds
System up time                 : 0 days 1 hours 22 minutes 12 seconds
Model                          : QX-W1020
Region code                    : US
Region code lock               : Disable
Serial ID                      : 210235A1BSC123000050
MAC address                    : 83D5-AB43-67FF
IP address                     : 1.1.1.2
H/W version                    : Ver.C
S/W version                    : V700R001B62D001
Boot version                   : 1.01
Description                    : wtp1
Priority                       : 4
Echo interval                  : 10 seconds
Statistics report interval     : 50 seconds
Jumbo frame value              : Disabled
MAC type                       : Local MAC & Split MAC
Tunnel mode                    : Local Bridging & 802.3 Frame & Native Frame
Discovery type                 : DHCP
Retransmission count           : 3
Retransmission interval        : 5 seconds
Firmware upgrade               : Enabled
Sent control packets           : 1
Received control packets       : 1
Connection count               : 1
Backup Ipv4                    : Not configured
Backup Ipv6                    : Not configured
Tunnel encryption              : Disabled
LED mode                       : Normal
Radio 1:
    Basic BSSID                : N/A
    Admin state                : Up
    Radio type                 : 802.11n(5GHz)
    Antenna type               : internal
    Client dot11ac-only        : Disabled
    Client dot11n-only         : Disabled
    Channel band-width         : 20/40MHz
    Secondary channel offset   : SCB
    Short GI for 20MHz         : Supported
    Short GI for 40MHz         : Supported
    A-MSDU                     : Enabled
    A-MPDU                     : Enabled
    LDPC                       : Not Supported
    STBC                       : Supported
    Operational HT MCS Set:
        Mandatory              : Not configured
        Supported              : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                 10, 11, 12, 13, 14, 15
        Multicast              : Not configured
    Channel                    : 64(auto)
    Max power                  : 13 dBm
    Operational rate:
        Mandatory              : 6, 12, 24 Mbps
        Supported              : 9, 18, 36, 48, 54 Mbps
        Multicast              : 24 Mbps
        Disabled               : Not configured
    Distance                   : 1 km
    ANI                        : Enabled
    Fragmentation threshold    : 2346 bytes
    Beacon interval            : 100 TU
    Protection threshold       : 2346 bytes
    Long retry threshold       : 4
    Short retry threshold      : 7
    Maximum rx duration        : 2000 ms
    Noise Floor                : 0 dBm
    Smart antenna              : Enabled
    Smart antenna policy       : Auto
```

```
Radio 2:
    Basic BSSID               : N/A
    Admin state               : Up
    Radio type                : 802.11b
    Antenna type              : internal
    Channel                   : 5(auto)
    Max power                 : 20 dBm
    Preamble type             : Short
    Operational rate:
        Mandatory             : 1, 2 Mbps
        Multicast             : Auto
        Supported             : 5.5, 11 Mbps
        Disabled              : Not configured
    Distance                  : 1 km
    ANI                       : Enabled
    Fragmentation threshold   : 2346 bytes
    Beacon interval           : 100 TU
    Protection threshold      : 2346 bytes
    Long retry threshold      : 4
    Short retry threshold     : 7
    Maximum rx duration       : 2000 ms
    Noise Floor               : 0 dBm
```

2) トラックエントリ 1 の状態がネガティブな場合、AP1 の無線がダウン状態にあることを確認します。

トラックエントリ 1 の状態を表示します。

```
<AC1> display track 1
Track ID: 1
  State: Negative
  Duration: 0 days 2 hours 5 minutes 48 seconds
  Notification delay: Positive 0, Negative 0 (in seconds)
  Tracked object:
    NQA entry: admin test
    Reaction: 1
```

ap1 の詳細情報を表示します。

```
<AC1> display wlan ap name ap1 verbose
AP name                         : ap1
AP ID                           : 1
AP group name                   : default-group
State                           : Run
Online time                     : 0 days 3 hours 25 minutes 12 seconds
System up time                  : 0 days 2 hours 22 minutes 12 seconds
Model                           : QX-W1020
Region code                     : US
Region code lock                : Disable
Serial ID                       : 210235A1BSC123000050
MAC address                     : 83D5-AB43-67FF
IP address                      : 1.1.1.2
H/W version                     : Ver.C
S/W version                     : V700R001B62D001
Boot version                    : 1.01
Description                     : wtp1
Priority                        : 4
Echo interval                   : 10 seconds
Statistics report interval      : 50 seconds
Jumbo frame value               : Disabled
MAC type                        : Local MAC & Split MAC
Tunnel mode                     : Local Bridging & 802.3 Frame & Native Frame
Discovery type                  : DHCP
Retransmission count            : 3
Retransmission interval         : 5 seconds
Firmware upgrade                : Enabled
Sent control packets            : 1
Received control packets        : 1
Connection count                : 1
Backup Ipv4                     : Not configured
```

```
Backup Ipv6                     : Not configured
Tunnel encryption               : Disabled
LED mode                        : Normal
Radio 1:
    Basic BSSID                 : N/A
    Admin state                 : Down
    Radio type                  : 802.11n(5GHz)
    Antenna type                : internal
    Client dot11ac-only         : Disabled
    Client dot11n-only          : Disabled
    Channel band-width          : 20/40MHz
    Secondary channel offset    : SCB
    Short GI for 20MHz          : Supported
    Short GI for 40MHz          : Supported
    A-MSDU                      : Enabled
    A-MPDU                      : Enabled
    LDPC                        : Not Supported
    STBC                        : Supported
    Operational HT MCS Set:
        Mandatory               : Not configured
        Supported               : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
                                  10, 11, 12, 13, 14, 15
        Multicast               : Not configured
    Channel                     : 64(auto)
    Max power                   : 13 dBm
    Operational rate:
        Mandatory               : 6, 12, 24 Mbps
        Supported               : 9, 18, 36, 48, 54 Mbps
        Multicast               : 24 Mbps
        Disabled                : Not configured
    Distance                    : 1 km
    ANI                         : Enabled
    Fragmentation threshold     : 2346 bytes
    Beacon interval             : 100 TU
    Protection threshold        : 2346 bytes
    Long retry threshold        : 4
    Short retry threshold       : 7
    Maximum rx duration         : 2000 ms
    Noise Floor                 : 0 dBm
    Smart antenna               : Enabled
    Smart antenna policy        : Auto
Radio 2:
    Basic BSSID                 : N/A
    Admin state                 : Down
    Radio type                  : 802.11b
    Antenna type                : internal
    Channel                     : 5(auto)
    Max power                   : 20 dBm
    Preamble type               : Short
    Operational rate:
        Mandatory               : 1, 2 Mbps
        Multicast               : Auto
        Supported               : 5.5, 11 Mbps
        Disabled                : Not configured
    Distance                    : 1 km
    ANI                         : Enabled
    Fragmentation threshold     : 2346 bytes
    Beacon interval             : 100 TU
    Protection threshold        : 2346 bytes
    Long retry threshold        : 4
    Short retry threshold       : 7
    Maximum rx duration         : 2000 ms
    Noise Floor                 : 0 dBm
```

目次

21 章 WLAN メッシュの設定 21-1
21.1 概要 21-1
21.1.1 WLAN メッシュネットワーク 21-1
21.1.2 メッシュプロファイル 21-2
21.1.3 ネイバ検出とメッシュリンク確立 21-3
21.1.4 無線配置システム 21-4
21.1.5 メッシュピアブラックリスト、ホワイトリスト 21-5
21.1.6 プロトコルと標準 21-5
21.2 WLAN メッシュ設定の制限とガイドライン 21-6
21.3 WLAN メッシュ設定作業リスト 21-6
21.4 メッシュプロファイルの設定 21-6
21.5 無線へのメッシュプロファイルのバインド 21-7
21.6 メッシュポリシーの設定 21-8
21.7 無線へのメッシュポリシーのバインド 21-9
21.8 MPP のプローブ要求送信無効化 21-9
21.9 同一 AC に関連付く MPP がメッシュピアになることの有効化 21-10
21.10 メッシュピアブラックリスト・ホワイトリストの設定 21-11
21.11 メッシュインタフェースの設定 21-11
21.11.1 メッシュインタフェースの作成 21-11
21.11.2 メッシュインタフェースへのアクセスポート属性の設定 21-12
21.11.3 メッシュインタフェースへのトランクポート属性の設定 21-13
21.11.4 メッシュインタフェースへのハイブリッドポート属性の設定 21-14
21.11.5 無線へのメッシュインタフェースのバインド 21-15
21.12 WLAN メッシュのための表示と保守コマンド 21-16
21.13 WLAN メッシュ設定例 21-16
21.13.1 WLAN メッシュの設定例 21-16
21.13.2 WLAN メッシュリンクへの STP の設定例 21-19
21.13.3 WLAN メッシュネットワークの VLAN 設定の設定例 21-23

21章 WLAN メッシュの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

🕮 **メモ：**

- WLAN メッシュの設定は、ソフトウェアバージョン 7.2.27 を含む以降のソフトウェアからサポートしています。
- QX-W1100 シリーズの AP は、ソフトウェアバージョン 7.2.50 を含む以降のソフトウェアから WLAN メッシュ機能をサポートしています。
- Anchor-AC 自身で WLAN メッシュ機能を使用することはできません。
- WLAN メッシュ機能は、同じシリーズ、かつ、同じソフトウェアバージョンの装置同士の接続のみサポートしています。(QX-W1000 シリーズと QX-W1100 シリーズは別シリーズです。)
- WLAN メッシュ機能を設定した Radio には、RRM 機能および WIPS 機能を設定しないことを推奨します。

21.1 概要

WLAN メッシュにより、AP 同士が無線で接続できます。WLAN メッシュネットワーク上の AP が直接、あるいは複数の AP を介して接続できます。1 台の AP で障害が発生したとき、残りの AP が互いに通信を継続します。

21.1.1 WLAN メッシュネットワーク

図 21-1 に WLAN メッシュネットワークを示します。

WLAN メッシュネットワークの AP はメッシュポイント（MP）です。MP は以下の役割を担います。

- シングルパーパス MP－メッシュサービスのみ提供します。
- メッシュアクセスポイント（MAP）－メッシュサービスとアクセスサービスを提供します。
- メッシュポータルポイント（MPP）－有線ネットワークに有線接続を提供します。

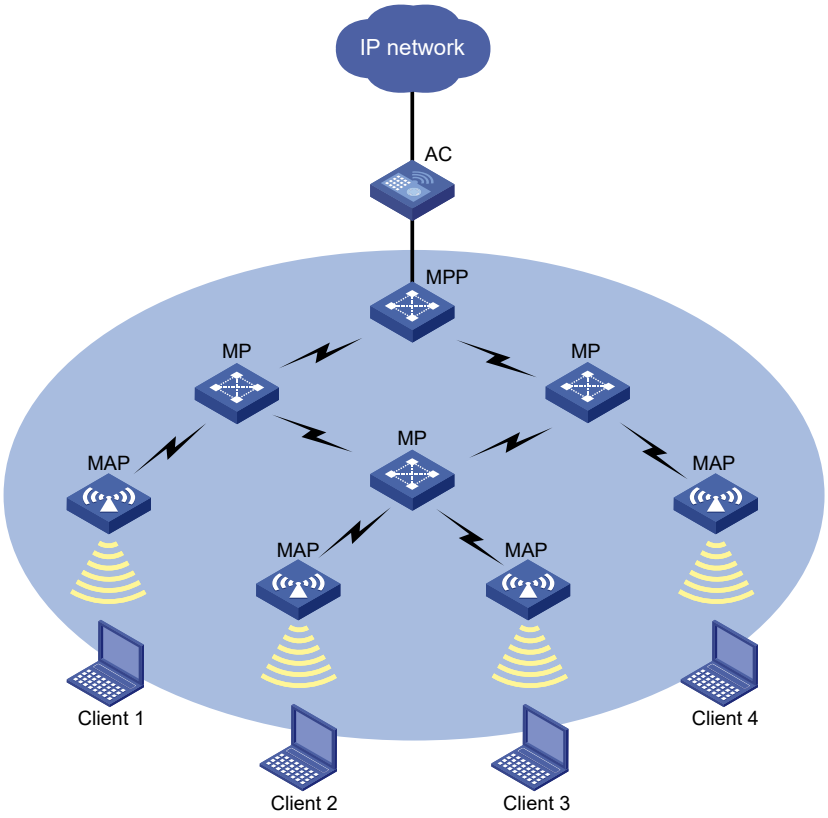


図21-1 WLAN メッシュネットワーク図

21.1.2 メッシュプロファイル

メッシュプロファイルは、メッシュネットワークを運用するためのメッシュプロトコルの集まりです。メッシュプロファイルには以下の属性が含まれます。

- メッシュ IDーメッシュネットワークを識別します。
- メッシュセキュリティー認証、鍵管理モード、事前共有鍵などネイバ認証のための設定を含みます。
- Keepalive 間隔ーメッシュリンク内に Keepalive パケットを送信する間隔を指定します。MAC アドレスの大きい MP は Keepalive 間隔で Keepalive パケットを終端まで送信します。Keepalive パケットを送信した MP は、3 回連続の Keepalive 間隔以内に応答を受信しない場合、メッシュリンクを切断します。Keepalive パケットを受信する MP が 3 回連続の Keepalive 間隔以内に Keepalive パケットを受信しない場合、メッシュリンクを切断します。リンク状態を正確に検出するために、送信端の Keepalive 間隔は受信端の Keepalive 間隔の 3 倍以下に設定してください。

メッシュネットワークを形成するために、AP は同じメッシュ ID とメッシュセキュリティ設定にする必要があります。

21.1.3 ネイバ検出とメッシュリンク確立

MP は、互いに検出できるように同じラジオとチャネルで動作する必要があります。MP は、互いに検出した後メッシュリンクを確立できます。

利用可能な検出方法は以下の通りです。

- **アクティブスキャニング**－MP はネイバを検出し、メッシュリンクを確立するためにプローブ要求フレームを送信します。
- **パッシブスキャニング**－MP は他の MP の情報を収集するためビーコンフレームを受信します。ネイバが存在する場合、AP はメッシュリンクを確立するためプローブ要求フレームを送信します。

この章では、アクティブスキャニングでのネイバ検出およびメッシュリンク確立のプロセスを説明します。

図 21-2 に示すように、MP はプローブ要求フレームとプローブ応答フレーム内のメッシュプロファイルを交換することでメッシュリンクを確立します。

以下の条件が満たされると、MP は別の MP をメッシュピアとして追加します。

- MP のメッシュプロファイルが一致する。
- 受信した要求もしくは応答内にピアリンクを承認するビットが設定されている。

MP 同士は互いにリンクオープン要求を送信することでメッシュリンクを確立します。メッシュリンクは、MP 同士が互いのリンクオープン要求を認識したあとに確立されます。

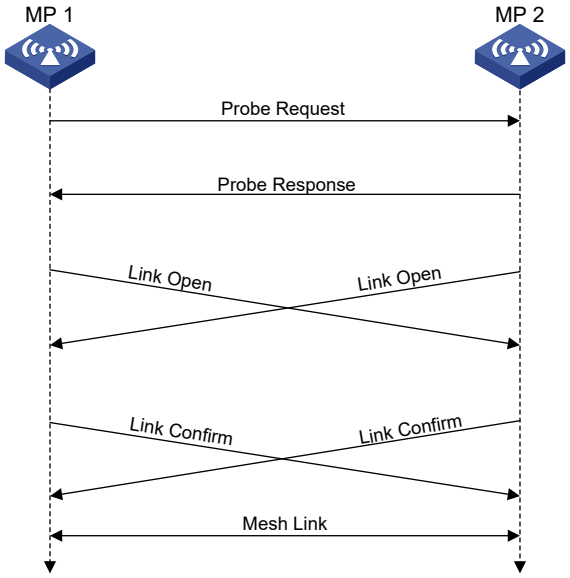


図21-2 ネイバ検出と WLAN メッシュネットワークでのメッシュリンク確立

AP は、メッシュリンクを確立するために AC からメッシュプロファイルを取得する必要があります。AP はメッシュリンク確立前に以下のタスクを実行します。

1) AC を発見するため、最初に検出した WLAN メッシュネットワークと一時的なメッシュリンク（テンポラリリンク）を確立します。テンポラリリンクではコンフィグレーションデータのみ転送できます。
2) メッシュプロファイルを含むコンフィグレーションを取得するため、AC との CAPWAP トンネル確立を試行します。

3) コンフィグレーションを取得後、テンポラリリンクを切断します。（テンポラリリンクは 2 分程度で切断されます。）

上記タスク実行後、AP はネイバ検出を実行し、WLAN メッシュネットワークに参加するためメッシュリンクを確立します。

AP が AC との CAPWAP トンネル確立に失敗した場合、AP は検出した他のメッシュネットワーク 1 つ 1 つに対してメッシュリンクの確立を試行します。

21.1.4 無線配置システム

無線配置システム（WDS）は WLAN メッシュのアプリケーションです。WDS は、各所に配置された LAN を接続するために AP 間のメッシュリンクを使用します。AP は、LAN からきた 802.3 フレームを、802.11s フレームとしてメッシュリンクに転送します。

管理上選択した AP 間でメッシュリンクを確立させることで、point-to-point トポロジもしくはスタートポロジでの WDS を作成できます。もしくは、自動ネイバ検出により、AP が自動的に作成したトポロジを使用できます。メッシュピアホワイトリストを設定しないことで、自動ネイバ検出が可能です。

- Point-to-point トポロジ

図 21-3 に示すように、2 つの LAN を接続するために 2 台の AP 間でメッシュリンクを設定できます。



図21-3 WDS point-to-point トポロジ

- スタートポロジ

図 21-4 に示すように、1 台の中心となる AP と複数の AP 間でメッシュリンクを設定し、複数の LAN を接続できます。

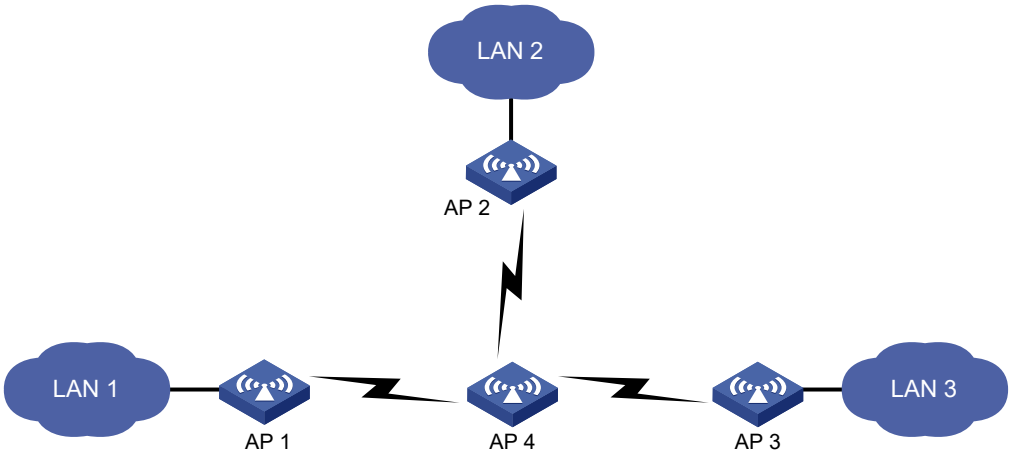


図21-4 スタートポロジ

- 管理なしで作成されたトポロジ

接続する AP を指定しない場合、WDS トポロジは AP 間の自動ネイバ検出とメッシュリンク確立に依存します。

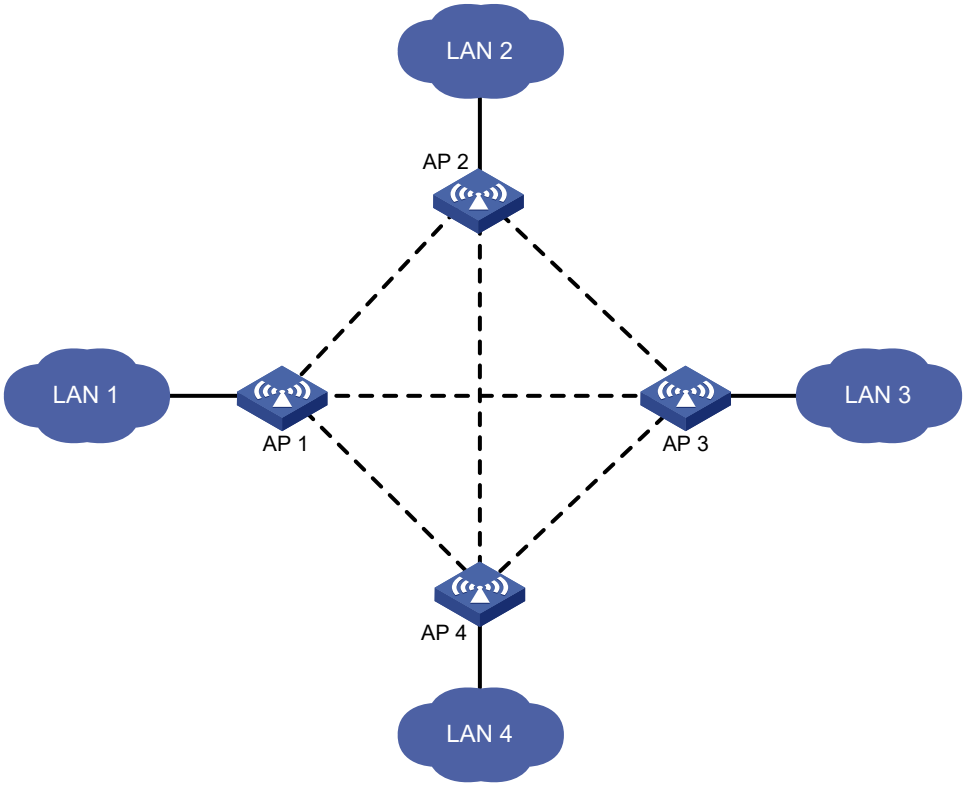


図21-5 自動トポロジ設定

21.1.5 メッシュピアブラックリスト、ホワイトリスト

ネイバ MP がローカル MP とメッシュリンクを確立できるかどうかをコントロールするため、ブラックリストもしくはホワイトリストを設定できます。

ブラックリストとホワイトリストの両方を設定した場合、ホワイトリストのみ適用されます。つまり、ホワイトリスト内のネイバ MP のみローカル MP とメッシュリンクを確立できます。また、ブラックリストのみ設定した場合、ブラックリスト内のネイバ MP はローカル MP とメッシュリンクを確立できません。

21.1.6 プロトコルと標準

- Draft P802.11s_D1.06
- ANSI/IEEE Std 802.11, 1999 Edition
- IEEE Std 802.11a
- IEEE Std 802.11b
- IEEE Std 802.11g

- IEEE Std 802.11i
- IEEE Std 802.11s
- IEEE Std 802.11-2004
- draft-ohara-capwap-lwapp-03

21.2 WLANメッシュ設定の制限とガイドライン

以下の方法により AP を設定できます。

- AP view で 1 台ずつ AP を設定します。
- AP を AP グループ view に割り当て、AP グループ view にて設定します。
- global configuration view ですべての AP を設定します。

AP view、AP group view、global configuration view に同様の設定をした場合、AP view、AP group view、global configuration view の順に設定が適用されます。

🕮 **メモ：**

レーダ検出時のチャネル移動において、メッシュ AP 間でチャネルを同じにする機能はありません。メッシュ接続にはレーダ検出が必要なチャネルの使用は推奨しません。

21.3 WLAN メッシュ設定作業リスト

作業リスト	補足
（必須設定項目）メッシュプロファイルの設定	ー
（必須設定項目）ラジオへのメッシュプロファイルのバインド	ー
（オプション設定項目）メッシュポリシーの設定	メッシュリンクの設定調整や保守のためにこの作業を実施します。
（オプション設定項目）ラジオへのメッシュポリシーのバインド	ー
（オプション設定項目）MPPのプローブ要求送信無効化	ー
（オプション設定項目）メッシュピアになるために同一ACに関連付くMPPの有効化	ー
（オプション設定項目）メッシュピアブラックリスト/ホワイトリストの設定	MPが適切なネイバMPとメッシュリンクを確立することを保証するためにこの作業を実施します。
（オプション設定項目）メッシュインタフェースの設定	ー

21.4 メッシュプロファイルの設定

I. 制限とガイドライン

同一メッシュネットワーク内の MP は、メッシュ ID とメッシュセキュリティ設定を同一にする必要があります。

リンク状態を正確に検出するために、送信端の keepalive 間隔は受信端の keepalive 間隔の 3 倍以下に設定して下さい。

II. 設定手順

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. メッシュプロファイルを作成し、view に移行する	**wlan mesh-profile** *mesh-profile-number*	デフォルト：設定なし
3. メッシュ ID を指定する	**mesh-id** *mesh-id*	デフォルト：設定なし
4. （オプション設定項目）メッシュセキュリティを設定する	a. SAE認証と鍵管理モードを有効にする事前 **akm mode sae** b. 事前共有鍵を設定する **preshared-key** { **pass-phrase** | **raw-key** } { **cipher** | **simple** } *string*	デフォルト：設定なし
5. （オプション設定項目）メッシュリンク keepalive 間隔を設定する	**link-keepalive** *keepalive-interval*	デフォルト：2秒
6. メッシュプロファイルを有効にする	**mesh-profile enable**	デフォルト：無効

21.5 無線へのメッシュプロファイルのバインド

I. メッシュプロファイルバインディング

AP がメッシュネットワークに参加するためには、AP の無線にメッシュプロファイルをバインドする必要があります。AP が異なるメッシュネットワークに参加できるように、無線インタフェースに異なるメッシュプロファイルをバインドできます。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. radio view に移行する	**radio** *radio-id*	—
4. 無線インタフェースにメッシュプロファイルをバインドする	**mesh-profile** *mesh-profile-number*	デフォルト：AP group radio viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—

操作	コマンド	補足
4． radio view に移行する	**radio** *radio-id*	—
5． 無線インタフェースにメッシュプロファイルをバインドする	**mesh-profile** *mesh-profile-number*	デフォルト：バインドされていません。

21.6 メッシュポリシーの設定

I. メッシュポリシー

メッシュポリシーはメッシュリンクの設定と保守の役割を含みます。

メモ：

ホップ数（ネットワーク内のメッシュリンクの最長経路）が増加するにつれてスループットは低下します。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． メッシュポリシーを作成し、view に移行する	**wlan mesh-policy** *policy-name*	デフォルト：システム定義のメッシュポリシーが存在します。そのポリシー名は **default_mesh_policy**です。
3． （オプション設定項目）リンク開始を有効にする	**link-initiation enable**	デフォルト：有効
4． （オプション設定項目）メッシュリンクの最大数を設定する	**link-maximum-number** *max-link-number*	デフォルト：2
5． （オプション設定項目）プローブ要求間隔を設定する	**probe-request-interval** *interval-value*	デフォルト：1000ms
6． （オプション設定項目）リンクレートモードを設定する	**link-rate-mode** { **fixed** | **real-time** }	デフォルト：fixedモード fixedモード：メッシュリンクのインタフェースレートは、無線インタフェースレートの現在の設定の最大値で固定されます。 real-timeモード：メッシュリンクのインタフェースレートは、自動でRSSIに適応します。
7． （オプション設定項目）メッシュリンクホールド RSSI（メッシュリンクを保持する最小信号強度）を設定する	**link-hold-rssi** *value*	デフォルト：15dBm

21.7 無線へのメッシュポリシーのバインド

I. メッシュポリシーバインディング

デフォルトでは、システム定義のメッシュポリシーが各無線にバインドされています。このシステム定義のメッシュポリシーは削除または修正できません。無線のリンク設定と保守設定を変更するには、ユーザ定義のメッシュポリシーを無線インタフェースにバインドし、システム定義のメッシュポリシーと置き換える必要があります。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． 無線インタフェースにメッシュポリシーをバインドする	**mesh-policy name** *policy-name*	デフォルト：AP groupのRadio viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—
5． 無線インタフェースにメッシュポリシーをバインドする	**mesh-policy name** *policy-name*	デフォルト：APグループのRadio viewにはシステム定義のメッシュポリシー **default_mesh_policy**がバインドされています。

21.8 MPPのプローブ要求送信無効化

I. プローブ要求送信無効化について

WLAN メッシュネットワークを有線ネットワークに接続する際、MPP は多くのメッシュリンクを確立しなければならない可能性があります。MPP のパフォーマンスを維持するため、MPP がネイバ検出のためにプローブ要求を送信するのを無効にすることができます。MPP は他の MP からのプローブ要求にのみ応答します。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． MPP のプローブ要求送信を無効にする	**portal-service enable**	デフォルト：AP group viewの設定を使用します。AP group viewに設定がない場合、global configuration viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． MPP のプローブ要求送信を無効にする	**portal-service enable**	デフォルト： global configuration viewの設定を使用します。

global configuration view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan global configuration**	—
3． MPP のプローブ要求送信を無効にする	**portal-service enable**	デフォルト： MPPはプローブ要求を送信できます。

21.9 同一ACに関連付くMPPがメッシュピアになることの有効化

I. 同一 AC に関連付くメッシュピアについて

ループを避けるため、同一 AC に関連付く MPP 同士はデフォルトではメッシュピアになることはできません。同一 AC に関連付いた MPP 同士がメッシュピアになるためには、本機を有効にしてください。同一 AC に関連付いた MPP が VLAN1 に属さないことを確認してください。また、ループを防ぐため、すべての装置に STP を設定してください。

II. 設定手順

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan global configuration**	—

操作	コマンド	補足
3． 同一 AC の MPP がメッシュピアになることを有効にする	**mesh-peer intra-ac-mpp enable**	デフォルト： ループを防ぐため、同一ACに関連付いたMPPはメッシュピアになれません。

21.10 メッシュピアブラックリスト・ホワイトリストの設定

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name*	—
3． radio view に移行する	**radio** *radio-id*	—
4． MP の MAC アドレスをメッシュピアブラックリストもしくはホワイトリストに追加する	**mesh peer-mac-address** [**blacklist**] *mac-address*	デフォルト：AP group viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—
5． MP の MAC アドレスをメッシュピアブラックリストもしくはホワイトリストに追加する	**mesh peer-mac-address** [**blacklist**] *mac-address*	デフォルト：設定なし ブラックリスト（ホワイトリスト）にMAのMACアドレスを追加するにはこの操作を繰り返します。 同一のMACアドレスを追加しようとした場合、最後の設定が適用されます。

21.11 メッシュインタフェースの設定

21.11.1 メッシュインタフェースの作成

I. メッシュインタフェースの作成について

MP がメッシュネットワークの同一 VLAN で互いに通信できるようにメッシュインタフェースを作成します。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし

21.11.2 メッシュインタフェースへのアクセスポート属性の設定

I. アクセスポートについて

アクセスポートでは 1 つの VLAN のみ許可します。

II. 制限とガイドライン

メッシュインタフェースにアクセスポートを設定する前に VLAN が存在することを確認してください。

III. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをアクセスに設定する	**mesh-port link-type access**	デフォルト：アクセスポート
5. アクセスタイプのメッシュインタフェースに VLAN を割り当てる	**mesh-port access vlan** *vlan-id*	デフォルト：VLAN 1

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをアクセスに設定する	**mesh-port link-type access**	デフォルト：アクセスポート
5. アクセスタイプのメッシュインタフェースに VLAN を割り当てる	**mesh-port access vlan** *vlan-id*	デフォルト：VLAN 1

21.11.3 メッシュインタフェースへのトランクポート属性の設定

I. トランクポートについて

トランクポートでは複数の VLAN を許可します。

II. 制限とガイドライン

ポートのリンクタイプをトランクとハイブリッド間で変更する場合、一度リンクタイプをアクセスに設定してください。

存在しない VLAN をトランクポートのポート VLAN として指定できます。

トランクポートがポート VLAN からパケットを転送できるようにするには、ポート VLAN にトランクポートを割り当てる必要があります。

III. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをトランクに設定する	**mesh-port link-type trunk**	デフォルト：アクセスポート
5. トランクポートに PVID を設定する	**mesh-port trunk pvid vlan** *vlan-id*	デフォルト：VLAN 1
6. トランクタイプのメッシュインタフェースに VLAN を割り当てる	**mesh-port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：VLAN1のみ

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをトランクに設定する	**mesh-port link-type trunk**	デフォルト：アクセスポート
5. トランクポートに PVID を設定する	**mesh-port trunk pvid vlan** *vlan-id*	デフォルト：VLAN 1
6. トランクタイプのメッシュインタフェースに VLAN を割り当てる	**mesh-port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：VLAN1のみ

21.11.4 メッシュインタフェースへのハイブリッドポート属性の設定

I. ハイブリッドポートについて

ハイブリッドポートでは複数の VLAN を許可します。

II. 制限とガイドライン

ポートのリンクタイプをトランクとハイブリッド間で変更する場合、一度リンクタイプをアクセスに設定してください。

存在しない VLAN をハイブリッドポートのポート VLAN として指定できます。

すでに存在している VLLAN にハイブリッドポートを割り当てていることを確認してください。

ハイブリッドポートがポート VLAN からパケットを転送できるようにするには、ポート VLAN にハイブリッドポートを割り当てる必要があります。

III. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをハイブリッドに設定する	**mesh-port link-type hybrid**	デフォルト：アクセスポート

操作	コマンド	補足
5. ハイブリッドポートに PVID を設定する	**mesh-port hybrid pvid vlan** *vlan-id*	デフォルト：ハイブリッドポートのPVIDは、リンクタイプがアクセスであるときにポートが所属しているVLANのIDです。
6. ハイブリッドタイプのメッシュインタフェースに VLAN を指定する	**mesh-port hybrid permit vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：ハイブリッドポートは、リンクタイプがアクセスであるときにポートが所属しているVLANのタグなしメンバです。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. メッシュインタフェースを作成し、その view に移行する	**interface wlan-mesh** *interface-number*	デフォルト：設定なし
4. メッシュインタフェースのリンクタイプをハイブリッドに設定する	**mesh-port link-type hybrid**	デフォルト：アクセスポート
5. ハイブリッドポートに PVID を設定する	**mesh-port hybrid pvid vlan** *vlan-id*	デフォルト：ハイブリッドポートのPVIDは、リンクタイプがアクセスであるときにポートが所属しているVLANのIDです。
6. ハイブリッドタイプのメッシュインタフェースに VLAN を指定する	**mesh-port hybrid permit vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：ハイブリッドポートは、リンクタイプがアクセスであるときにポートが所属しているVLANのタグなしメンバです。

21.11.5 無線へのメッシュインタフェースのバインド

I. 制限とガイドライン

AP view で作成されたメッシュインタフェースは、radio view 内のラジオにのみバインドできます。AP group view で作成されたメッシュインタフェースは radio view と AP group radio view のどちらのラジオにもバインドできます。

1 つのラジオに対して 1 つのメッシュインタフェースをバインドできます。

II. 設定手順

AP view での設定方法は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—

操作	コマンド	補足
3． radio view に移行する	**radio** *radio-id*	—
4． 無線インタフェースにメッシュインタフェースをバインドする	**mesh-interface** *interface-number*	デフォルト：AP group radio viewの設定を使用します。

AP group view での設定方法は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． radio view に移行する	**radio** *radio-id*	—
5． ラジオにメッシュインタフェースをバインドする	**mesh-interface** *interface-number*	デフォルト：設定なし

21.12 WLANメッシュのための表示と保守コマンド

display コマンドはすべての view で実行できます。

操作	コマンド
メッシュリンク情報を表示する	**display wlan mesh-link ap** [**name** *ap-name*] [**verbose]**
メッシュプロファイル情報を表示する	**display wlan mesh-profile** [*mesh-profile-number*]
メッシュポリシー情報を表示する	**display wlan mesh-policy** [*mesh-policy-name*]

21.13 WLANメッシュ設定例

21.13.1 WLAN メッシュの設定例

I. ネットワーク設定

図 21-6 に示すように、クライアントにネットワークアクセスを提供するために 802.11n 5GHz WLAN メッシュネットワークを確立します。チャネル 36 でメッシュリンクを確立するために、MP と MAP を設定します。

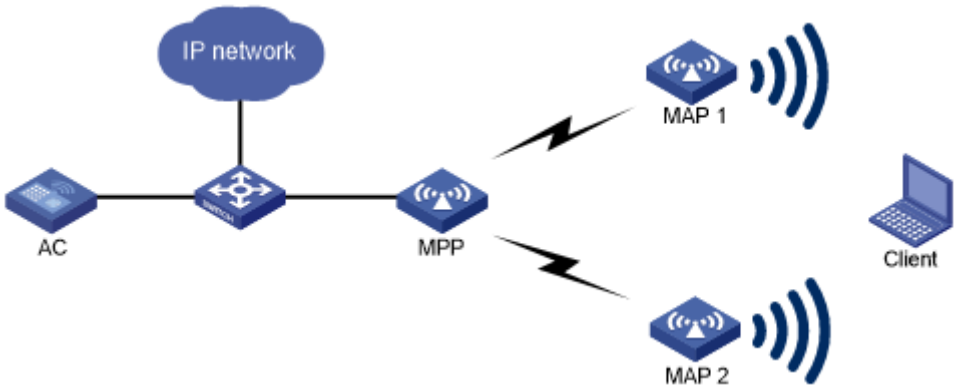


図21-6 ネットワーク図

II. 設定手順

1)　MPP を設定します。

メッシュプロファイルを設定します。

```
AC> system-view
[AC] wlan mesh-profile 1
```

メッシュ ID を 1 に設定します。

```
[AC-wlan-mesh-profile-1] mesh-id 1
```

認証と鍵管理に対して SAE を有効にします。

```
[AC-wlan-mesh-profile-1] akm mode sae
```

事前共有鍵を設定します。

```
[AC-wlan-mesh-profile-1] preshared-key pass-phrase simple 12345678
```

メッシュプロファイルを有効にします。

```
[AC-wlan-mesh-profile-1] mesh-profile enable
[AC-wlan-mesh-profile-1] quit
```

2)　サービステンプレートを設定します。

```
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid mesh-network
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

3)　MPP の設定を行います。

MPP に対して AP view を作成します。適切な AP モデル、シリアル ID を選択、指定していることを確認してください。

```
[AC] wlan ap mpp1 model QX-W1030
[AC-wlan-ap-mpp1] serial-id 219801A1K0917BG0000S
```

メッシュプロファイルを MPP のラジオ 1 にバインドします。

```
[AC-wlan-ap-mpp] radio 1
[AC-wlan-ap-mpp-radio-1] mesh-profile 1
```

MPP のラジオ 1 の無線タイプを 802.11n(5GHz)に設定します。

```
[AC-wlan-ap-mpp-radio-1] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[AC-wlan-ap-mpp-radio-1] channel 36
```

ラジオを有効にします。

```
[AC-wlan-ap-mpp-radio-1] radio enable
[AC-wlan-ap-mpp-radio-1] quit
```

4) MAP を設定します。

MAP1 の AP view を作成します。適切な AP モデル、シリアル ID を選択、指定していることを確認してください。

```
[AC] wlan ap map1 model QX-W1030
[AC-wlan-ap-map1] serial-id 219801A1K0917BG0000B
```

MAP のラジオ 1 にメッシュプロファイルをバインドします。

```
[AC-wlan-ap-map1] radio 1
[AC-wlan-ap-map1-radio-1] mesh-profile 1
```

MAP のラジオ 1 にサービステンプレートをバインドします。

```
[AC-wlan-ap-map1-radio-1] service-template service1
```

MAP のラジオ 1 の無線タイプを 802.11n(5GHz)に設定します。

```
[AC-wlan-ap-map1-radio-1] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[AC-wlan-ap-map1-radio-1] channel 36
```

ループを防ぐために MPP の MAC アドレスをメッシュピアホワイトリストに追加します。MAP1 は MPP とのみメッシュリンクを確立できます。

```
[AC-wlan-ap-map1-radio-1] mesh peer-mac-address 77a2-c25d-e316
```

ラジオを有効にします。

```
[AC-wlan-ap-map1-radio-1] radio enable
[AC-wlan-ap-map1-radio-1] quit
[AC-wlan-ap-map1] quit
```

MAP2 に対して MAP1 と同様に設定します。

```
[AC] wlan ap map2 model QX-W1030
[AC-wlan-ap-map2] serial-id 210235A29G007C000090
```

```
[AC-wlan-ap-map2] radio 1
[AC-wlan-ap-map2-radio-1] mesh-profile 1
[AC-wlan-ap-map2-radio-1] service-template service1
[AC-wlan-ap-map2-radio-1] type dot11an
[AC-wlan-ap-map2-radio-1] channel 36
[AC-wlan-ap-map2-radio-1] mesh peer-mac-address 77a2-c25d-e316
[AC-wlan-ap-map2-radio-1] radio enable
[AC-wlan-ap-map2-radio-1] quit
[AC-wlan-ap-map2] quit
[AC] quit
```

III. 設定の確認

MPP が MAP とメッシュリンクを確立することを確認します。

```
<AC> display wlan mesh-link ap
 AP Name: mpp
 Peer           Local          Status     RSSI Packets(Rx/Tx)
 4a9b-c5bb-e43f 77a2-c25d-e316 Forwarding 22   6058/1900
 a6b5-1c5a-22ff 77a2-c25d-e316 Forwarding 35   5354/1900

AP Name: map1
 Peer           Local          Status     RSSI Packets(Rx/Tx)
 77a2-c25d-e316 4a9b-c5bb-e43f Forwarding 22   1900/6058

AP Name: map2
 Peer           Local          Status     RSSI Packets(Rx/Tx)
 77a2-c25d-e316 a6b5-1c5a-22ff Forwarding 35   1900/5354
```

クライアントが AP と関連付いたことを確認します。

```
<AC> display wlan client
 Total number of clients: 1

MAC address     Username              AP name                 R IP address
VLAN
000f-e265-6400 N/A                map1                  1 1.1.1.1        300
```

21.13.2 WLAN メッシュリンクへの STP の設定例

I. ネットワーク要件

図 21-7 に示すように、クライアントにネットワークアクセスを提供するために 802.11n 5GHz WLAN メッシュネットワークを確立します。チャネル 36 でメッシュリンクを確立するために、MPP と MAP1 と MAP2 を設定します。メッシュリンクに STP を設定します。

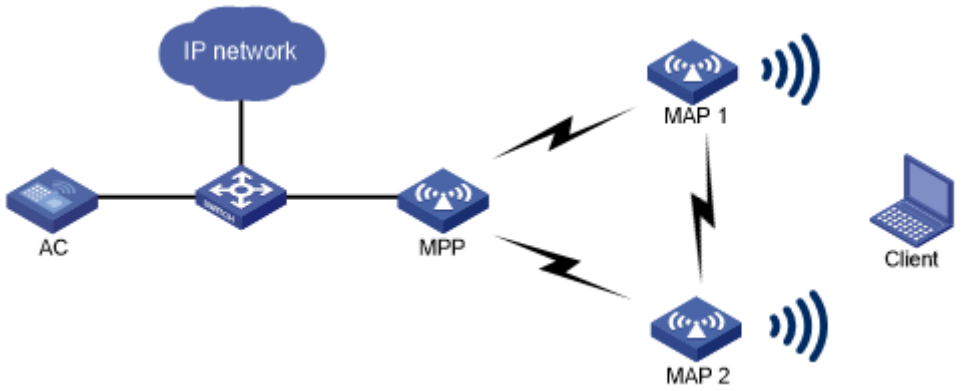


図21-7 ネットワーク図

II. 設定手順

1)　MPP を設定します。

メッシュプロファイルを設定します。

```
<AC> system-view
[AC] wlan mesh-profile 1
```

メッシュ ID を 1 に設定します。

```
[AC-wlan-mesh-profile-1] mesh-id 1
```

認証と鍵管理に対して SAE を有効にします。

```
[AC-wlan-mesh-profile-1] akm mode sae
```

事前共有鍵を設定します。

```
[AC-wlan-mesh-profile-1] preshared-key pass-phrase simple 12345678
```

メッシュプロファイルを有効にします。

```
[AC-wlan-mesh-profile-1] mesh-profile enable
[AC-wlan-mesh-profile-1] quit
```

2)　サービステンプレートを設定します。

```
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid mesh-network
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

3)　MPP の設定を行います。

MPP に対して AP view を作成します。適切な AP モデル、シリアル ID を選択、指定していることを確認してください。

```
[AC] wlan ap mpp model QX-W1030
[AC-wlan-ap-mpp] serial-id 219801A1K0917BG0000S
```

メッシュインタフェース 1 を作成します。

```
[AC-wlan-ap-mpp] interface wlan-mesh 1
[AC-wlan-ap-mpp-wlan-mesh-1] quit
```

MPP のラジオ 1 にメッシュプロファイルをバインドします。

```
[AC-wlan-ap-mpp] radio 1
[AC-wlan-ap-mpp-radio-1] mesh-profile 1
```

MPP のラジオ 1 にメッシュインタフェースをバインドします。

```
[AC-wlan-ap-mpp-radio-1] mesh-interface 1
```

MPP のラジオ 1 の無線タイプを 802.11n(5GHz)に設定します。

```
[AC-wlan-ap-mpp-radio-1] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[AC-wlan-ap-mpp-radio-1] channel 36
```

ラジオを有効にします。

```
AC-wlan-ap-mpp-radio-1] radio enable
[AC-wlan-ap-mpp-radio-1] quit
```

#以下の設定を記述した“.mpcfg”形式のファイル“stp-mesh.mpcfg”を作成し、AC に格納します。

```
system-view
stp global enable
interface WLAN-Mesh 1
stp enable
```

MPP に”stp-mesh.mpcfg”を適用します。

```
[AC-wlan-ap-mpp] map-configuration flash:/stp-mesh.mpcfg
[AC-wlan-ap-mpp] return
```

4) MAP を設定します。

MAP1 の AP view を作成します。適切な AP モデル、シリアル ID を選択、指定していることを確認してください。

```
[AC] wlan ap map1 model QX-W1030
[AC-wlan-ap-map1] serial-id 219801A1K0917BG0000B
```

メッシュインタフェース 1 を作成します。

```
[AC-wlan-ap-map1] interface wlan-mesh 1
[AC-wlan-ap-map1-wlan-mesh-1] quit
```

MAP1 のラジオ 1 にメッシュプロファイルをバインドします。

```
[AC-wlan-ap-map1] radio 1
[AC-wlan-ap-map1-radio-1] mesh-profile 1
```

MAP1 のラジオ 1 にメッシュインタフェースをバインドします。

```
[AC-wlan-ap-mpp-radio-1] mesh-interface 1
```

MAP のラジオ 1 にサービステンプレートをバインドします。

```
[AC-wlan-ap-map1-radio-1] service-template service1
```

MAP のラジオ 1 の無線タイプを 802.11n(5GHz)に設定します。

```
[AC-wlan-ap-map1-radio-1] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[AC-wlan-ap-map1-radio-1] channel 36
```

ラジオを有効にします。

```
[AC-wlan-ap-map1-radio-1] radio enable
[AC-wlan-ap-map1-radio-1] quit
```

MAP1 に”stp-mesh.mpcfg”を適用します。

```
AC-wlan-ap-map1] map-configuration flash:/stp-mesh.mpcfg
[AC-wlan-ap-map1] quit
```

MAP2 に対して MAP1 と同様に設定します。

```
[AC] wlan ap map2 model QX-W1030
[AC-wlan-ap-map2] serial-id 210235A29G007C000090
[AC-wlan-ap-map2] interface wlan-mesh 1
[AC-wlan-ap-map2-wlan-mesh-1] quit
[AC-wlan-ap-map2] radio 1
[AC-wlan-ap-map2-radio-1] mesh-profile 1
[AC-wlan-ap-map2-radio-1] mesh-interface 1
[AC-wlan-ap-map2-radio-1] service-template service1
[AC-wlan-ap-map2-radio-1] type dot11an
[AC-wlan-ap-map2-radio-1] channel 36
[AC-wlan-ap-map2-radio-1] radio enable
[AC-wlan-ap-map2-radio-1] quit
[AC-wlan-ap-map2] map-configuration flash:/stp-mesh.mpcfg
[AC-wlan-ap-map2] return
<AC>
```

III. 設定の確認

MPP が MAP とメッシュリンクを確立することを確認します。

```
<AC> display wlan mesh-link ap
AP name: mpp
 Peer Name     Peer Mac       Local Mac      Status     RSSI Packets(Rx/Tx)
 map1          4a9b-c5bb-e43f 77a2-c25d-e316 Forwarding 60   449/882464
 map2          a6b5-1c5a-22ff 77a2-c25d-e316 Forwarding 49   684730/155096

AP name: map1
 Peer Name     Peer Mac       Local Mac      Status     RSSI Packets(Rx/Tx)
 mpp           77a2-c25d-e316 4a9b-c5bb-e43f Forwarding 57   687001/639160
 map2          a6b5-1c5a-22ff 4a9b-c5bb-e43f Forwarding 57   155109/1182108

AP name: map2
 Peer Name     Peer Mac       Local Mac      Status     RSSI Packets(Rx/Tx)
 mpp           77a2-c25d-e316 a6b5-1c5a-22ff Forwarding 68   536370/455
 map1          a6b5-1c5a-22ff a6b5-1c5a-22ff Forwarding 59   487223/686931
```

クライアントが AP と関連付いたことを確認します。

```
<AC> display wlan client
 Total number of clients: 1

MAC address     Username              AP name                  R IP address
VLAN
000f-e265-6400 N/A                map1                  1 1.1.1.1        300
```

21.13.3 WLAN メッシュネットワークの VLAN 設定の設定例

I. ネットワーク設定

図 21-8 に示すように、LAN1 と LAN2 は VLAN2 に属しています。チャネル 36 でメッシュリンクを確立し、VLAN2 からのトラフィックを許可するように MPP1 と MPP2 を設定します。

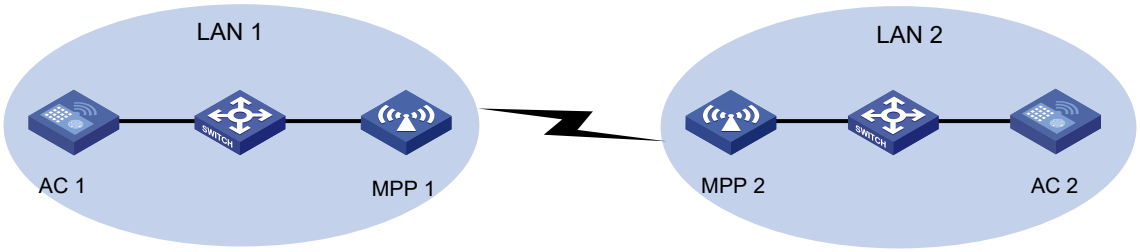


図21-8 ネットワーク図

II. 設定手順

1)　AP1 を設定します。

メッシュプロファイルを作成します。

```
<AC1> system-view
[AC1] wlan mesh-profile 1
```

メッシュ ID を 1 に設定します。

```
[AC1-wlan-mesh-profile-1] mesh-id 1
```

認証と鍵管理に対して SAE を有効にします。

```
[AC1-wlan-mesh-profile-1] akm mode sae
```

事前共有鍵を設定します。

```
[AC1-wlan-mesh-profile-1] preshared-key pass-phrase simple 12345678
```

メッシュプロファイルを有効にする。

```
[AC1-wlan-mesh-profile-1] mesh-profile enable
[AC1-wlan-mesh-profile-1] quit
```

2) サービステンプレートを設定します。

```
[AC] wlan service-template service1
[AC-wlan-st-service1] ssid mesh-network
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

3) MPP を設定します。

MPP の AP view を作成します。適切な AP モデル、シリアル ID を選択、指定していることを確認してください。

```
[AC] wlan ap map1 model QX-W1030
[AC-wlan-ap-map1] serial-id 219801A1K0917BG0000B
```

MAP のラジオ 1 にメッシュプロファイルをバインドします。

```
[AC-wlan-ap-map1] radio 1
[AC-wlan-ap-map1-radio-1] mesh-profile 1
```

MPP のラジオ 1 の無線タイプを 802.11n(5GHz)に設定します。

```
[AC-wlan-ap-mpp-radio-1] type dot11an
```

無線の作動チャネルを 36 に設定します。

```
[AC-wlan-ap-mpp-radio-1] channel 36
```

ラジオを有効にします。

```
[AC-wlan-ap-mpp-radio-1] radio enable
[AC-wlan-ap-mpp-radio-1] quit
```

4) メッシュインタフェースを設定します。

メッシュインタフェースを作成します。

```
[AC1-wlan-ap-mpp1] interface wlan-mesh 1
```

```
[AC1-wlan-ap-mpp1-wlan-mesh-1] quit
```

MPP のラジオ 1 にメッシュインタフェースをバインドします。

```
[AC1-wlan-ap-mpp1] radio 1
[AC1-wlan-ap-mpp1-radio-1] mesh-interface 1
[AC1-wlan-ap-mpp1-radio-1] quit
```

リンクタイプをトランクに設定します。

```
[AC1-wlan-ap-mpp1] interface wlan-mesh 1
[AC1-wlan-ap-mpp1-wlan-mesh-1] mesh-port link-type trunk
```

トランクポートを VLAN2 に割り当てます。

```
[AC1-wlan-ap-mpp1-wlan-mesh-1] mesh-port trunk permit vlan 2
[AC1-wlan-ap-mpp1-wlan-mesh-1] quit
```

remote-configuration を有効にします。

```
[AC1-wlan-ap-mpp1] remote-configuration enable
```

5)　AC1 と同様に AC2 を設定します。（詳細は省略します。）

III. 設定の確認

VLAN インタフェース 2 を設定し、AC1 と AC2 が互いに ping 通信できることを確認してください。

目次

22 章 コンフィグレーションプロファイルの設定 22-1
22.1 概要 22-1
22.2 設定作業リスト 22-1
22.3 コンフィグレーションプロファイルの作成 22-1
22.4 コンフィグレーションプロファイルの関連付け 22-2
22.5 コンフィグレーションプロファイルの設定 22-3
22.5.1 コンソールポートからのログイン設定 22-3
22.5.2 装置の Telnet ログインの設定 22-4
22.5.3 Ethernet インタフェースの設定 22-6
22.5.4 ポートアイソレーションの設定 22-7
22.5.5 リンクアグリゲーションの設定 22-7
22.5.6 VLAN の設定 22-8
22.5.7 IP アドレスの設定 22-10
22.5.8 DHCP クライアントの設定 22-11
22.5.9 DHCP サーバの設定 22-11
22.5.10 DHCP リレーエージェントの設定 22-13
22.5.11 NAT の設定 22-14
22.5.12 スタティックルーティングの設定 22-16
22.5.13 ACL の設定 22-17
22.5.14 QoS の設定 22-19
22.5.15 ローカルユーザの設定 22-20
22.6 設定例 22-21
22.6.1 コンフィグレーションプロファイルの設定例 22-21

22章 コンフィグレーションプロファイルの設定

本マニュアルに登場する「AC」という用語は、特に断りがない場合、Anchor-AC モードで動作する AP のことを示します。

🕮 **メモ：**

- コンフィグレーションプロファイルの設定は、ソフトウェアバージョン 7.2.58 を含む以降のソフトウェアからサポートしています。
- コンフィグレーションプロファイルの設定は、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。

22.1 概要

コンフィグレーションプロファイルは、AC のコンフィグレーションプロファイルで指定された設定を、AP または AP グループ内の AP がオンラインになったときに展開します。

22.2 設定作業リスト

操作
（必須設定項目）コンフィグレーションプロファイルの作成
（必須設定項目）コンフィグレーションプロファイルとAPまたはAPグループの関連付け
（オプション設定項目）CLIによるログインの設定
（オプション設定項目）Ethernetインタフェースの設定
（オプション設定項目）ポートアイソレーションの設定
（オプション設定項目）リンクアグリゲーションの設定
（オプション設定項目）VLANの設定
（オプション設定項目）IPアドレスの設定
（オプション設定項目）DHCPクライアントの設定
（オプション設定項目）DHCPサーバの設定
（オプション設定項目）NATの設定
（オプション設定項目）スタティックルーティングの設定
（オプション設定項目）ACLの設定
（オプション設定項目）QoSの設定
（オプション設定項目）ローカルユーザの設定

22.3 コンフィグレーションプロファイルの作成

I. 概要

AC でコンフィグレーションプロファイルを作成し、プロファイルを 1 つまたは複数の AP に関連付けることができます。その後、AC はプロファイルで指定された設定を、関連付けられた AP がオンラインになったときに自動的に展開します。

コンフィグレーションプロファイルを作成するときは、AP モデル名を指定する必要があります。AC は、AP モデルに基づいてプロファイルのデフォルト設定を生成します。

II. 設定手順

以下にコンフィグレーションプロファイルの作成手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし

22.4 コンフィグレーションプロファイルの関連付け

メモ：

- **configuration-profile** と **remote-configuration** を同じ AP に対して設定しないでください。
- コンフィグレーションプロファイルで設定できないコマンドを設定したい場合に限り、**map-configuration** の併用をご検討ください。また、**configuration-profile** と **map-configuration** の両方に同じ機能を有するコマンド設定がある場合、AP へのコンフィグ適用が正常におこなわれません。

既存のコンフィグレーションプロファイルと AP または AP グループの関連付ける場合、**configuration-profile** コマンドを使用します。AP または AP グループ内の AP がオンラインになると、AC はプロファイル内の設定を AP に自動的に展開します。

コンフィグレーションプロファイルと AP または AP グループの関連付けを解除するには、**undo configuration-profile** コマンドを実行します。また、**undo configuration-profile** コマンドを実行すると、AP または AP グループ内の AP の設定が工場出荷時のデフォルトに復元されます。

I. AP view でのコンフィグレーションプロファイルの関連付け

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name*	—
3. コンフィグレーションプロファイルを関連付ける	**configuration-profile** *profile-name* [**model** *model-name*]	設定なし

II. AP group view でのコンフィグレーションプロファイルの関連付け

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *group-name*	—

操作	コマンド	補足
4. コンフィグレーションプロファイルを関連付ける	**configuration-profile** *profile-name* [**model** *model-name*]	設定なし

22.5 コンフィグレーションプロファイルの設定

22.5.1 コンソールポートからのログイン設定

コンソールポートからのログイン設定の詳細は、QX-W1000/W1000 シリーズ アクセスポイント オペレーションマニュアルのセクション 1 *はじめに "CLI によるログイン" の "コンソールポートからのローカルログイン"* を参照してください。

コンフィグレーションプロファイル View での、コンソールポートからのログイン設定の手順を以下に示します。

I. None 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. console line view あるいは class view に移行する	• console line viewに移行する： **line console** *first-number* [*last-number*] • console line class viewに移行する： **line class console**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4. None 認証モードを有効にする	**authentication-mode** *none*	デフォルト：製品モデルにより異なります。 QX-W1000シリーズは**none**。 QX-W1100シリーズは**password**。

II. Password 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし

操作	コマンド	備考
3． console line view あるいは class view に移行する	● console line viewに移行する： **line console** *first-number* [*last-number*] ● console line class viewに移行する： **line class console**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4． Password 認証モードを有効にする	**authentication-mode password**	デフォルト：**none**
5． password を設定する	**set authentication password** { **hash** | **simple** } *password*	デフォルト：製品モデルにより異なります。 QX-W1000シリーズはパスワード設定なし。 QX-W1100シリーズはqx_admin。

III. Scheme 認証の設定

操作	コマンド	備考
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． console line view あるいは class view に移行する	● console line viewに移行する： **line console** *first-number* [*last-number*] ● console line class viewに移行する： **line class console**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4． Scheme 認証を有効にする	**authentication-mode** *scheme*	デフォルト：製品モデルにより異なります。 QX-W1000シリーズは**none**。 QX-W1100シリーズは**password**。

22.5.2 装置の Telnet ログインの設定

装置の Telnet ログイン設定の詳細は、QX-W1000/W1000 シリーズ アクセスポイント オペレーションマニュアルのセクション 1 *はじめに "CLI によるログイン" の "Telnet からのログイン"* を参照してください。

コンフィグレーションプロファイル View での、Telnet ログイン設定の手順を以下に示します。

I. Telnet サーバの有効化

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. Telnet サーバを有効化する	**telnet server enable**	デフォルト：無効

II. None 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. VTY line view または VTY line class view に移行する	● VTY line viewに移行する： **line vty** *first-number* [*last-number*] ● VTY line class viewに移行する： **line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4. None 認証モードを有効にする	**authentication-mode none**	デフォルト：**password**

III. Password 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. VTY line view または VTY line class view に移行する	● VTY line viewに移行する： **line vty** *first-number* [*last-number*] ● VTY line class viewに移行する： **line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4. Password 認証モードを有効にする	**authentication-mode password**	デフォルト：**password**

操作	コマンド	備考
5. password の設定	**set authentication password** { **hash** | **simple** } *password*	デフォルト：製品モデルにより異なります。 QX-W1000シリーズはパスワード設定なし。 QX-W1100シリーズはqx_admin。

IV. Scheme 認証の設定

操作	コマンド	備考
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. VTY line view または VTY line class view に移行する	● VTY line viewに移行する：**line vty** *first-number* [*last-number*] ● VTY line class viewに移行する：**line class vty**	どちらか一方を使用します。 User line viewでの設定はユーザラインのみ適用されます。 User line class viewでの設定はclassのすべてのユーザに適用されます。
4. Scheme 認証を有効にする	**authentication-mode scheme**	デフォルト：**password**

22.5.3 Ethernet インタフェースの設定

Ethernet インタフェースの詳細は、QX-W1000/W1000 シリーズ アクセスポイント オペレーションマニュアルのセクション 3 *インタフェース "Ethernet インタフェース"* を参照してください。

コンフィグレーションプロファイル View での Ethernet インタフェースの設定手順を以下に示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. Ethernet interface view に移行する	**interface** *interface-type interface-number*	―
4. Ethernet インタフェースを有効にする	**undo shutdown**	デフォルト：有効

22.5.4 ポートアイソレーションの設定

ポートアイソレーションの詳細は、オペレーションマニュアルの *“AP 管理”* の *“ポートアイソレーションの設定”* を参照してください。

コンフィグレーションプロファイル View での、ポートアイソレーション設定の手順を以下に示します。

I. Ethernet インタフェースのポートアイソレーションの設定

操作	コマンド	備考
1. system view に移行する	**system-view**	—
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. Ethernet interface view に移行する	**interface** interface-type interface-number	—
4. ポートアイソレーションを有効にする	**port-isolate enable**	デフォルト：有効

II. アグリゲートインタフェースのポートアイソレーション設定

操作	コマンド	備考
1. system view に移行する	**system-view**	—
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	—
4. ポートアイソレーションを有効にする	**port-isolate enable**	デフォルト：無効

22.5.5 リンクアグリゲーションの設定

リンクアグリゲーションの詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 4 *アクセス “リンクアグリゲーション”* を参照してください。

コンフィグレーションプロファイル View での、リンクアグリゲーション設定の手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． アグリゲートインタフェースを作成し、aggregate interface view に移行する	**interface bridge-aggregation** *interface-number*	アグリゲートインタフェースを作成すると、スタティックアグリゲーショングループ番号が、自動的に同一番号で作成されます。
4． system view へ戻る	**quit**	―
5． 指定されたアグリゲーショングループにインタフェースを割り当てる	6． Ethernet interface view に移行する：**interface** *interface-type interface-number* 7． 指定されたアグリゲーショングループにインタフェースを割り当てる：**port link-aggregation group** *group-id*	アグリゲーショングループに複数のインタフェースを割り当てる場合、このステップを繰り返してください。

22.5.6 VLAN の設定

VLAN の詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 4 *アクセス “VLAN”* を参照してください。

コンフィグレーションプロファイル View での、VLAN 設定の手順を以下に示します。

I. VLAN の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． VLAN を作成し、view へ移行あるいは VLAN リストを作成する	**vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }	デフォルト： デフォルト VLAN（VLAN1）のみ
4． VLAN view に移行する	**vlan** *vlan-id*	VLANリストを作成した後、指定したVLANを設定するには、この操作を実行してください。

II. VLAN インタフェースの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *interface-number*	デフォルト：設定なし VLANが存在する場合、直接そのviewに移行します。
4． VLAN インタフェースを有効にする	**undo shutdown**	デフォルト：有効

III. interface view でのアクセス VLAN の設定方法

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	● Ethernet interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	ー
4． リンクタイプをアクセスに設定する	**port link-type access**	デフォルト：アクセス
5． アクセスポートを VLAN に割り当てる	**port access vlan** *vlan-id*	デフォルト：VLAN1に属します。

IV. トランクポート VLAN の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	● interface viewに移行する： **interface** *interface-type interface-number* ● aggregate interface viewに移行する： **interface bridge-aggregation** *interface-number*	ー

操作	コマンド	補足
4． リンクタイプをトランクに設定する	● **port link-type trunk**	デフォルト：アクセス
5． トランクポートで許可する VLAN を設定する	● **port trunk permit vlan** { *vlan-id-list* | **all** }	デフォルト：vlan1のみ許可
6． トランクポートの PVID を設定する	● **port trunk pvid vlan** *vlan-id*	デフォルト： VLAN 1

V. ハイブリッドポート VLAN の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	● interface viewに移行する：**interface** *interface-type interface-number* ● aggregate interface viewに移行する：**interface bridge-aggregation** *interface-number*	ー
4． リンクタイプをハイブリッドに設定する	**port link-type hybrid**	デフォルト：アクセス
5． ハイブリッドポートで許可する VLAN を設定する	**port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }	デフォルト：リンクタイプがアクセスであるとき、ハイブリッドポートのPVIDはポートが所属しているVLANのIDです。
6． ハイブリッドポートの PVID を設定する	**port hybrid pvid vlan** *vlan-id*	デフォルト：リンクタイプがアクセスであるとき、ハイブリッドポートはポートが所属しているVLANのタグなしメンバです。

22.5.7 IP アドレスの設定

コンフィグレーションプロファイル View での､IP アドレス設定の手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *interface-number*	デフォルト：設定なし VLANが存在する場合、直接そのviewに移行します。

操作	コマンド	補足
4． VLAN インタフェースに IP アドレスを割り当てる	**ip address** *ip-address* { *mask* | *mask-length* } [sub]	デフォルト：設定なし

22.5.8 DHCP クライアントの設定

DHCP クライアントの詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 5 *IP サービス　"DHCP クライアント"* を参照してください。

コンフィグレーションプロファイル View での、DHCP クライアント設定の手順を以下に示します。

I. インタフェースでの DHCP クライアントの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． VLAN インタフェースを作成し、VLAN interface view に移行する	**interface vlan-interface** *interface-number*	デフォルト：設定なし VLANが存在する場合、直接そのviewに移行します。
4． VLAN インタフェースに IP アドレスを割り当てる	**ip address dhcp-alloc**	デフォルト：無効

22.5.9 DHCP サーバの設定

DHCP サーバの詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 5 *IP サービス　"DHCP サーバ"* を参照してください。

コンフィグレーションプロファイル View での、DHCP サーバ設定の手順を以下に示します。

I. DHCP アドレスプールの作成

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

II. DHCP アドレスプールの IP アドレス範囲の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし
4. プライマリサブネットを設定する	**network** *network-address* [*mask-length* | **mask** *mask*]	デフォルト：設定なし
5. （オプション設定項目） ゲートウェイを設定する	**gateway-list** *ip-address*&<1-64>	デフォルト：設定なし
6. DNS サーバを設定する	**dns-list** *ip-address*&<1-8>	デフォルト：設定なし
7. （オプション設定項目） アドレスのリース期間を設定する	**expired** { **day** *day* [**hour** *hour* [**minute** *minute* [**second** *second*]]] | **unlimited** }	デフォルト：1日
8. （オプション設定項目）アドレスプールの動的割り当てから設定された IP アドレスを除外する	**forbidden-ip** *ip-address*&<1-8>	デフォルト：DHCPアドレスプールすべてのアドレスが割り当て可能です。 複数のアドレス範囲を除外する場合、このステップを繰り返します。

III. DHCP の有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. DHCP を有効にする	**dhcp enable**	デフォルト：無効

IV. インタフェースでの DHCP サーバの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	―

操作	コマンド	補足
4． インタフェースで DHCP サーバを有効にする	**dhcp select server**	デフォルト：有効

V. インタフェースでのアドレスプールの適用

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． インタフェースにアドレスプールを適用する	**dhcp server apply ip-pool** *pool-name*	デフォルト：適用されていません。

22.5.10 DHCP リレーエージェントの設定

DHCP リレーエージェントの詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 5 *IP サービス “DHCP リレー”*を参照してください。

コンフィグレーションプロファイル View での、DHCP リレーエージェント設定の手順を以下に示します。

I. DHCP の有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． DHCP アドレスプールを作成し、その view に移行する	**dhcp server ip-pool** *pool-name*	デフォルト：設定なし

II. インタフェースでの DHCP リレーエージェントの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	―
4. DHCP リレーエージェントを有効にする	**dhcp select relay**	デフォルト：DHCPが有効にされたとき、インタフェースはDHCPサーバモードで動作します。

III. リレーエージェントの DHCP サーバの指定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. interface view に移行する	**interface** *interface-type interface-number*	―
4. リレーエージェントに DHCP サーバアドレスを指定する	**dhcp relay server-address** *ip-address*	デフォルト：指定なし

22.5.11 NAT の設定

NAT の詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 5 *IP サービス　"NAT の設定"* を参照してください。

コンフィグレーションプロファイル View での、NAT 設定の手順を以下に示します。

I. 送信ダイナミック NAT の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. NAT アドレスグループを作成し、そのビューに移行する	**nat address-group** *group-id* [**name** *group-name*]	
4. アドレスグループにアドレス範囲を追加する	**address** *start-address end-address*	1つのアドレスグループに複数のアドレス範囲を追加できます。 アドレス範囲は重複してはいけません。

操作	コマンド	補足
5. コンフィグレーションプロファイル View に戻る	**quit**	―
6. interface view に移行する	**interface** *interface-type interface-number*	―
7. 受信ダイナミック NAT を設定する	**nat inbound** { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** { *group-id* | **name** *group-name* } [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]	1つのインタフェースに複数の送信ダイナミックNATルールを設定できます。 **no-pat reversible**: これらのキーワードを指定すると、逆アドレス変換が有効になります。逆アドレス変換では、既存のNO-PATエントリを使用して、外部ネットワークからアクティブに開始された接続の宛先アドレスを内部ネットワークに変換します。宛先アドレスは、一致するNO-PATエントリ内のプライベートIPアドレスに変換されます。 **add-route**: このキーワードを使用すると、受信ダイナミックNATルールが一致したときに、プライベートアドレス宛てのルートを装置が自ダイナミックに追加できます。出力インタフェースはNATインタフェースで、ネクストホップは変換前の送信元アドレスです。 このキーワードを指定しない場合は、ルートを手動で追加する必要があります。

II. 受信ダイナミック NAT の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	―
2. コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3. NAT アドレスグループを作成し、そのビューに移行する	**nat address-group** *group-id* [**name** *group-name*]	
4. アドレスグループにアドレス範囲を追加する	**address** *start-address end-address*	1つのアドレスグループに複数のアドレス範囲を追加できます。 アドレス範囲は重複してはいけません。

操作	コマンド	補足
5． コンフィグレーションプロファイル view に戻る	**quit**	―
6． interface view に移行する	**interface** *interface-type interface-number*	―
7． 受信ダイナミック NAT を設定する	**nat inbound** { *ipv4-acl-number* | **name** *ipv4-acl-name* } **address-group** { *group-id* | **name** *group-name* } [**no-pat** [**reversible**] [**add-route**]] [**rule** *rule-name*] [**priority** *priority*] [**disable**] [**description** *text*] [**counting**]	1つのインタフェースに複数の送信ダイナミックNATルールを設定できます。 **no-pat reversible**: これらのキーワードを指定すると、逆アドレス変換が有効になります。逆アドレス変換では、既存のNO-PATエントリを使用して、外部ネットワークからアクティブに開始された接続の宛先アドレスを内部ネットワークに変換します。宛先アドレスは、一致するNO-PATエントリ内のプライベートIPアドレスに変換されます。 **add-route**: このキーワードを使用すると、受信ダイナミックNATルールが一致したときに、プライベートアドレス宛てのルートを装置が自ダイナミックに追加できます。出力インタフェースはNATインタフェースで、ネクストホップは変換前の送信元アドレスです。 このキーワードを指定しない場合は、ルートを手動で追加する必要があります。

22.5.12 スタティックルーティングの設定

スタティックルーティングの詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 6 *ルーティングプロトコル “スタティックルーティング”* を参照してください。

コンフィグレーションプロファイル View での、スタティックルーティング設定の手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし

操作	コマンド	補足
3． スタティックルートを設定する	**ip route-static** *dest-address* { *mask-length* | *mask* } *next-hop-address*	デフォルト：設定なし

22.5.13 ACL の設定

ACL の詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 8 *ACL and QoS "ACL"* を参照してください。

コンフィグレーションプロファイル View での、ACL 設定の手順を以下に示します。

I. 標準 ACL の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． 標準 IPv4 ACL を作成し、その view に移行する	• **acl basic** { *acl-number* | **name** *acl-name* } • **acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	デフォルト：設定なし *acl-number*の設定範囲は2000～2999です。
4． （オプション設定項目） ルールの番号づけステップを設定する	**step** *step-value*	デフォルト：5
5． ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **source** { *source-address source-wildcard* | **any** } | **time-range** *time-range-name*] *	デフォルト：設定なし
6． （オプション設定項目） ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

II. 拡張 ACL の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	ー
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． 拡張 IPv4 ACL を作成し、その view に移行する	• **acl advanced** { *acl-number* | **name** *acl-name* } • **acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	デフォルト：設定なし *acl-number*の設定範囲は3000～3999です。

操作	コマンド	補足
4．（オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
5．ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } *protocol* [{ { **ack** *ack-value* | **fin** *fin-value* | **psh** *psh-value* | **rst** *rst-value* | **syn** *syn-value* | **urg** *urg-value* } * | **established** } | **destination** { *dest-address dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | { **dscp** *dscp* | { **precedence** *precedence* | **tos** *tos* } * } | **fragment** | **icmp-type** { *icmp-type* [*icmp-code*] | *icmp-message* } | **source** { *source-address source-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-range-name*] *	デフォルト：設定なし
6．（オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

III. L2 ACL の設定

操作	コマンド	補足
1．system view に移行する	**system-view**	ー
2．L2 ACL を作成し、その view に移行する	● **acl mac** { *acl-number* | **name** *acl-name* } ● **acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]	デフォルト：設定なし *acl-number*の設定範囲は4000～4999です。
3．（オプション設定項目）ルールの番号付けステップを設定する	**step** *step-value*	デフォルト：5
4．ルールを作成/修正する	**rule** [*rule-id*] { **deny** | **permit** } [**cos** *dot1p* | **dest-mac** *dest-address dest-mask* | { **lsap** *lsap-type lsap-type-mask* | **type** *protocol-type protocol-type-mask* } | **source-mac** *source-address source-mask* | **time-range** *time-range-name*] *	デフォルト：設定なし
5．（オプション設定項目）ルールの説明を設定する	**rule** *rule-id* **comment** *text*	デフォルト：設定なし

IV. インタフェースへの ACL 適用

🕮 メモ：

- Ethernet インタフェース、アグリゲートインタフェースに適用した ACL は、Layer2 通信パケットに対してのみ動作します。
- VLAN インタフェースに適用した ACL は、Layer3 通信パケットに対してのみ動作します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． インタフェースに ACL を適用する	**packet-filter [mac] { acl-number | name** *acl-name* **} { inbound | outbound }**	デフォルト：指定なし

22.5.14 QoS の設定

QoS の詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 8 *ACL and QoS “プライオリティマッピング”* を参照してください。

コンフィグレーションプロファイル View での、QoS 設定の手順を以下に示します。

I. プライオリティマッピングのパケットプライオリティを信用するインタフェースの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． パケットプライオリティタイプの信用を設定する	**qos trust** { **dot1p** | **dscp** }	デフォルト：ポートプライオリティを信用する

II. インタフェースのポートプライオリティの変更

操作	コマンド	補足
1． system view に移行する	**system-view**	―

操作	コマンド	補足
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． interface view に移行する	**interface** *interface-type interface-number*	―
4． ポートプライオリティを設定する	**qos priority** *priority-value*	デフォルト：0

22.5.15 ローカルユーザの設定

ローカルユーザの詳細は、QX-W1000/W1100 シリーズ アクセスポイント オペレーションマニュアルのセクション 9 *セキュリティ “AAA”* を参照してください。

コンフィグレーションプロファイル View での、ローカルユーザ設定の手順を以下に示します。

操作	コマンド	補足
1． system view に移行する	**system-view**	―
2． コンフィグレーションプロファイルを作成し、その View に移行する	**configuration profile** *profile-name* [**model** *model-name*]	設定なし
3． ローカルユーザ（装置管理ユーザ）を追加し、local user view に移行する	**local-user** *user-name* **class manage**	デフォルト：設定なし。 最大16の装置管理ユーザを作成できます。
4． （オプション設定項目） ローカルユーザのパスワードを設定する	**password** { **cipher** | **simple** } *string*	デフォルト：設定なし
5． ローカルユーザのサービスタイプを指定する	装置管理ユーザ： **service-type { ftp | { telnet | terminal } }**	デフォルト：設定なし
6． （オプション設定項目） ローカルユーザの許可属性を設定する	**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minutes* | **user-profile profile-name** | **user-role** *role-name* | **vlan** *vlan-id* | **work-directory** *directory-name* }	デフォルト：以下に示します。 ● FTPユーザはNASのルートディレクトリがありますが、アクセス許可がありません。 ● network-operatorユーザロールは、network-adminまたはレベル15ユーザによって作成されるローカルユーザに割り当てられます。

22.6 設定例

22.6.1 コンフィグレーションプロファイルの設定例

I. ネットワーク要件

図 22-1 に示すように、コンフィグレーションプロファイルを AP に適用し、FIT-AP のコンフィグを設定します。

FIT-AP に適用するコンフィグレーションプロファイルには、以下の設定を行います。

- VLAN 10、20 を作成します
- VLAN-Interface 1 を作成し、固定 IP アドレス(10.1.1.2/24)を割り当てます。
- デフォルトゲートウェイ 10.1.1.254 を割り当てます。
- GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN1，VLAN10,VLAN20 を割り当てます。

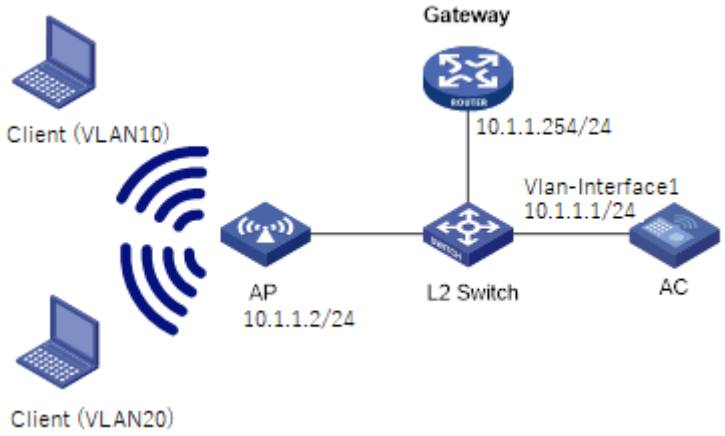


図22-1 ネットワーク図

II. 設定手順

1)　コンフィグレーションプロファイル CP1 を作成します。

```
<AC> system-view
[AC] configuration profile CP1 model QX-W1030
[AC-config-profile-CP1]
```

2)　コンフィグレーションプロファイルに、コンフィグを設定します。

VLAN 10、VLAN 20 を作成します。

```
[AC-config-profile-CP1] vlan 10
[AC-config-profile-CP1-vlan10] quit
[AC-config-profile-CP1] vlan 20
[AC-config-profile-CP1-vlan20] quit
```

#VLAN-Interface 1 を作成し、IP アドレスを割り当てます。

```
[AC-config-profile-CP1] interface vlan-interface 1
[AC-config-profile-CP1-Vlan-interface1] ip address 10.1.1.2 24
[AC-config-profile-CP1-Vlan-interface1] quit
```

#デフォルトルートを設定します。

```
[AC-config-profile-CP1] ip route-static 0.0.0.0 0.0.0.0 10.1.1.254
```

#GigabitEthernet 1/0/1 をトランクポートとして設定し、VLAN1 と VLAN10 と VLAN20 を割り当てます。

```
[AC-config-profile-CP1] interface GigabitEthernet 1/0/1
[AC-config-profile-CP1-GigabitEthernet1/0/1] port link-type trunk
[AC-config-profile-CP1-GigabitEthernet1/0/1] port trunk permit vlan 1 10 20
[AC-config-profile-CP1-GigabitEthernet1/0/1] quit
[AC-config-profile-CP1] quit
```

3) AP 名が ap1 の手動 AP を作成し、コンフィグレーションプロファイルを関連付けます。

#AP ap1 を AP モデル QX-W1030 を指定して作成し、シリアル ID を設定します

```
[AC] wlan ap ap1 model QX-W1030
[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
```

#AP ap1 にコンフィグレーションプロファイル CP1 を関連付けます。

```
[AC-wlan-ap-ap1] configuration-profile CP1
```

III. 設定の確認

#以下の情報を検証します。(詳細は省略します。)

- AP と AC が通信できること
- Client(VLAN10)が通信できること
- Client(VLAN20)が通信できること

目次

23 章 Web リダイレクトの設定 23-1
23.1.1 Web リダイレクトについて 23-1
23.1.2 Web リダイレクトの設定 23-1

23章 Web リダイレクトの設定

23.1.1 Web リダイレクトについて

Web リダイレクトは、簡略化されたポータル機能です。Web リダイレクトでは、ユーザはポータル認証を実行せず、ブラウザでの最初の Web アクセス試行時に、指定された URL に直接リダイレクトされます。指定されたリダイレクト間隔が経過すると、ユーザは訪問中の Web サイトから指定された URL に再度リダイレクトされます。

Web リダイレクトは、ISP に拡張サービスを提供できます。たとえば、ISP は、リダイレクトされた Web ページに広告を配置し、情報を公開できます。

23.1.2 Web リダイレクトの設定

🕮 **メモ：**

- Web リダイレクトの設定は、ソフトウェアバージョン 7.2.63 を含む以降のソフトウェアからサポートしています。
- Web リダイレクトの機能は、デフォルトのポート番号 80 を使用する HTTP パケットに対してのみ有効です。

以下に、Web リダイレクトの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. service template view に移行する	**wlan service-template** *service-template-name*	—
3. サービステンプレートで Web リダイレクトを設定する	**web-redirect url** *url-string* [**interval** *interval*]	デフォルト　　：無効 デフォルト間隔：86400秒

目次

24 章 IoT 機能の設定 24-1
24.1 概要 24-1
24.2 ワイヤレスロケーション 24-1
24.2.1 ワイヤレスロケーションの概要 24-1
24.2.2 ワイヤレスロケーションシステム 24-1
24.2.3 ワイヤレスロケーションのメカニズム 24-2
24.3 設定作業リスト 24-2
24.4 BLE 機能の設定 24-3
24.4.1 手動モジュールの設定 24-3
24.4.2 自動モジュールおよび自動モジュール変換の設定 24-3
24.4.3 モジュールの説明の設定 24-4
24.4.4 サポート対象モジュールタイプの指定 24-5
24.4.5 モジュールの有効化 24-5
24.4.6 モジュールの送信電力の設定 24-6
24.4.7 BLE デバイスのエージングタイムの設定 24-7
24.4.8 BLE モジュールの iBeacon 送信設定 24-8
24.4.9 モジュールの再起動 24-9
24.4.10 モジュールの自動ファームウェアアップグレードの設定 24-9
24.4.11 IoT AP の表示および管理 24-10
24.5 サーバへの IoT データのレポート設定 24-10
24.5.1 IoT トランスポートプロファイルの作成 24-10
24.5.2 IoT データレポート用のサーバアドレスの設定 24-11
24.5.3 Microsoft Azure IoT Hub DPS の設定 24-11
24.5.4 ロケーションパケットのフィルタリングの設定 24-12
24.5.5 サーバに送信するキープアライブパケットの送信間隔の設定 24-12
24.5.6 IoT データをサーバにレポートする間隔の設定 24-13
24.5.7 IoT トランスポートプロファイルの有効化 24-13
24.5.8 IoT トランスポートプロファイルのバインド 24-13
24.5.9 IoT トランスポートプロファイルの表示および管理 24-14
24.6 ワイヤレスロケーション共通パラメータの設定 24-15
24.6.1 パケットの間引きの設定 24-15
24.6.2 ビーコンフレームの無視の設定 24-16
24.6.3 AP フレームの無視の設定 24-17
24.6.4 RSSI ベースのパケットフィルタリングの設定 24-18
24.6.5 クライアントパケットレート制限の設定 24-19
24.6.6 ロケーションパケットレート制限の設定 24-20
24.6.7 ワイヤレスロケーションのキープアライブの設定 24-21
24.6.8 ワイヤレスロケーションの表示および管理 24-22
24.7 BLE 機能の設定例 24-23
24.7.1 iBeacon を送信する 24-23
24.7.2 AP が収集した周辺装置のレポートを Azure IoT Hub DPS へ送信する 24-24

24章 IoT 機能の設定

24.1 概要

QX-W シリーズは以下の IoT 機能をサポートしています。

- BLE 機能
  - iBeacon の送信
  - AP の周辺に存在する BLE デバイスのスキャン
- Microsoft Azure IoT Hub DPS への IoT データのレポート

24.2 ワイヤレスロケーション

24.2.1 ワイヤレスロケーションの概要

802.11 ワイヤレスロケーショントラックまたは Bluetooth Low Energy (BLE) デバイスにより、医療監視、資産管理、物流管理が可能です。

24.2.2 ワイヤレスロケーションシステム

図 24-1 に示すように、ワイヤレスロケーションシステムには、802.11 または BLE デバイス、情報レシーバ (802.11 または BLE AP) 、およびロケーションサーバが含まれています。802.11 のデバイスには、タグ (定期的に 802.11 パケットのみを送信できる小型のワイヤレスデバイス) と MU(タグを除くすべての 802.11 デバイス) が含まれます。

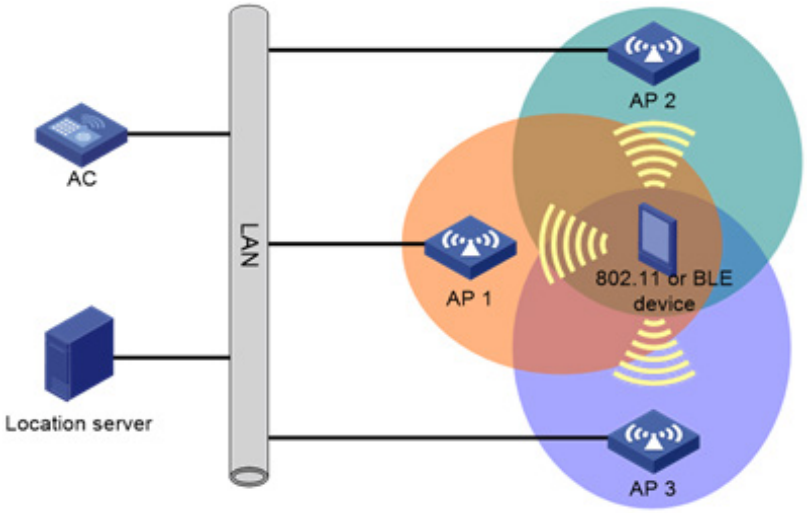


図24-1 ネットワーク図

24.2.3 ワイヤレスロケーションのメカニズム

ワイヤレスロケーションは次のように動作します。

1) 802.11 または BLE デバイスがワイヤレスパケットを送信します。
2) ワイヤレスパケットを受信すると、AP は収集したロケーション情報 (RSSI およびタイムスタンプを含む) をロケーションパケットにカプセル化し、そのパケットをロケーションサーバに送信します。
3) ロケーションサーバは、802.11 または BLE デバイスのロケーションを計算します。ロケーションサーバは、802.11 または BLE デバイスを見つけるために、少なくとも 3 つの AP からのロケーション情報を必要とします。

24.3 設定作業リスト

作業リスト
BLE 機能の設定
(必須設定項目) 以下のうちの1つを実行します。 • 手動モジュールの設定 • 自動モジュールおよび自動モジュール変換の設定
(オプション設定項目) モジュールの説明の設定
(必須設定項目) サポート対象モジュールタイプの指定
(必須設定項目) モジュールの有効化
(オプション設定項目) モジュールの送信電力の設定
(オプション設定項目) BLEデバイスのエージングタイムの設定
(オプション設定項目) BLEモジュールのiBeacon送信設定
(オプション設定項目) モジュールの再起動
(オプション設定項目) モジュールの自動ファームウェアアップグレードの設定
サーバへの IoT データのレポート設定
(オプション設定項目) IoTトランスポートプロファイルの作成
(オプション設定項目)IoTデータレポート用のサーバアドレスの設定
(オプション設定項目) Microsoft Azure IoT Hub DPSの設定
(オプション設定項目)ロケーションパケットのフィルタリングの設定
(オプション設定項目) サーバに送信するキープアライブパケットの送信間隔の設定
(オプション設定項目) IoTデータをサーバにレポートする間隔の設定
(オプション設定項目) IoTトランスポートプロファイルの有効化
(オプション設定項目) IoTトランスポートプロファイルのバインド
ワイヤレスロケーション共通パラメータの設定
(オプション設定項目) パケットの間引きの設定
(オプション設定項目) ビーコンフレームの無視の設定
(オプション設定項目) APフレームの無視の設定
(オプション設定項目) RSSIベースのパケットフィルタリングの設定
(オプション設定項目) クライアントパケットレート制限の設定
(オプション設定項目) ロケーションパケットレート制限の設定
(オプション設定項目) ワイヤレスロケーションキープアライブの設定
(オプション設定項目) ワイヤレスロケーションの表示および管理

24.4 BLE機能の設定

⚠ **注意：**

2.4GHz 無線インタフェースでのデータ通信は、BLE モジュールでの通信にパケットロス等の影響を与える為、同一 AP で 2.4GHz 無線インタフェースと BLE 機能は併用しないことを推奨します。

🕮 **メモ：**

- BLE 機能の設定は、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
- BLE 機能は、QX-W1110 の AP でのみサポートしています。
- BLE 機能は、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。

24.4.1 手動モジュールの設定

AP でモジュールを設定および管理するには、AP のモジュール view に移行する必要があります。

以下に、手動モジュールの設定を示します。

I. AP View での手動モジュールの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. 手動モジュールを設定する	**module** *module-id*	デフォルト：設定なし

II. AP group View での手動モジュールの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. 手動モジュールを設定する	**module** *module-id*	デフォルト：設定なし

24.4.2 自動モジュールおよび自動モジュール変換の設定

自動モジュールを設定するには、自動モジュールを手動モジュールに変換するか、AP グループを介して設定する必要があります。

自動モジュール変換機能を有効にすると、モジュールがオンラインになった後、自動的に自動モジュールを手動モジュールに変換します。手動モジュールに自動的に変換されるのは、自動モジュール変換機能を有効にした後でオンラインになったモジュールのみです。オンライン状態の自動モジュールを手動モジュールに変換する場合は、iot auto-module persistent all コマンドを使用します。

以下に、自動モジュールおよび自動モジュール変換の設定を示します。

I. AP View での自動モジュールおよび自動モジュール変換の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. 自動モジュールを有効にする	**iot auto-module { disable | enable }**	デフォルト：AP group viewの設定を使用します
4. (任意) 自動モジュール変換を有効にする	**iot auto-module persistent { disable | enable }**	デフォルト：AP group viewの設定を使用します
5. (任意) すべてのオンライン自動モジュールを手動モジュールに変換する	**iot auto-module persistent all**	—

II. AP group View での自動モジュールおよび自動モジュール変換の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. 自動モジュールを有効にする	**iot auto-module { disable | enable }**	デフォルト：無効
4. (任意) 自動モジュール変換を有効にする	**iot auto-module persistent { disable | enable }**	デフォルト：無効
5. (任意) すべてのオンライン自動モジュールを手動モジュールに変換する	**iot auto-module persistent all**	—

24.4.3 モジュールの説明の設定

IoT AP にインストールまたは接続されているモジュールを効率的に管理するには、モデル、場所、および機能に基づいたモジュールの説明を設定します。

以下に、モジュールの説明を設定する手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—

操作	コマンド	補足
4． モジュールの説明を設定する	**description** *text*	デフォルト：設定なし

24.4.4 サポート対象モジュールタイプの指定

AP 上のモジュールを正しく動作させるには、サポート対象モジュールタイプが物理モジュールタイプと一致している必要があります。

以下に、サポートされるモジュールタイプの指定の設定を示します。

I. AP View でのサポート対象モジュールタイプの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． モジュール view に移行する	**module** *module-id*	—
4． サポート対象モジュールタイプを設定する	**type BLE**	デフォルト：AP group viewの設定を使用します

II. AP group View でのサポート対象モジュールタイプの指定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． モジュール view に移行する	**module** *module-id*	—
5． サポート対象モジュールタイプを設定する	**type BLE**	デフォルト：設定なし

24.4.5 モジュールの有効化

以下に、モジュールの有効化の設定を示します。

I. AP View でのモジュールの有効化

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． モジュール view に移行する	**module** *module-id*	—

操作	コマンド	補足
4. モジュールを有効化する	**module enable**	デフォルト：AP group viewの設定を使用します

II. AP group View でのモジュールの有効化

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. モジュール view に移行する	**module** *module-id*	—
5. モジュールを有効化する	**module enable**	デフォルト：無効

24.4.6 モジュールの送信電力の設定

モジュールの送信電力は、送信電力レベルまたは送信電力値で指定することができます。

送信できる送信電力レベル、送信電力値を以下に示します。

- レベル 1 (4dBm)
- レベル 2 (-1dBm)
- レベル 3 (-5dBm)
- レベル 4 (-9dBm)

以下に、モジュールの送信電力の設定を示します。

I. AP View でのモジュールの送信電力の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—
4. モジュールの送信電力を設定する	**tx-power** { *power-level* | **value** *power-value* }	デフォルト：AP group viewの設定を使用します

II. AP group View でのモジュールの送信電力の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—

操作	コマンド	補足
4． モジュール view に移行する	**module** *module-id*	—
5． モジュールの送信電力を設定する	**tx-power {** *power-level* **| value** *power-value* **}**	デフォルト：レベル1

24.4.7 BLE デバイスのエージングタイムの設定

以下に、BLE デバイスのエージングタイムの設定を示します

I. AP view での BLE デバイスのエージングタイムの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． モジュール view に移行する	**module** *module-id*	—
4． BLE デバイスのエージングタイムを設定する	**rfid-tracking ble aging-time** *aging-time*	デフォルト：AP group viewの設定を使用します

II. AP group view での BLE デバイスのエージングタイムの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	—
3． AP model view に移行する	**ap-model** *ap-model*	—
4． モジュール view に移行する	**module** *module-id*	—
5． BLE デバイスのエージングタイムを設定する	**rfid-tracking ble aging-time** *aging-time*	デフォルト：global configuration viewの設定を使用します

III. global configuration view での BLE デバイスのエージングタイムの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． global configuration view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． BLE デバイスのエージングタイムを設定する	**rfid-tracking ble aging-time** *aging-time*	デフォルト：180秒

24.4.8 BLE モジュールの iBeacon 送信設定

この機能により、BLE モジュールは iBeacon アドバタイズメントを定期的にブロードキャストできます。iBeacon アドバタイズメントには、UUID、Major-ID、Minor-ID、および測定電力が含まれます。iBeacon アドバタイズメントを受信したアプリケーションソフトウェアは、アドバタイズメント情報に応じた具体的なアクションを行い、ソフトウェア機能を実現します。

BLE モジュールの iBeacon 送信設定の手順を以下に示します。

I. AP view での BLE モジュールの iBeacon 送信の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—
4. サポートされるモジュールタイプを設定する	**type BLE**	デフォルト：AP group viewの設定を使用します
5. BLE モジュールの iBeacon 送信を設定する	**rfid-tracking ble advertisement { disable | enable }**	デフォルト：AP group viewの設定を使用します
6. アドバタイズメント情報を設定する	**rfid-tracking ble advertisement [** *ad-number* **] { major-id** *major-id* **| measured-power** *measured-power* **| minor-id** *minor-id* **| uuid** *uuid* **}**	デフォルト：AP group viewの設定を使用します
7. iBeacon アドバタイズメントの送信間隔を設定する	**rfid-tracking ble advertisement [** *ad-number* **] interval** *interval*	デフォルト：AP group viewの設定を使用します
8. BLE アドバタイズメントモードを設定する	**rfid-tracking ble advertisement mode { continuous** *ad-number* **| periodic {** *ad-number period* *}&<2>* **}**	デフォルト：AP group viewの設定を使用します
9. iBeacon の送信パラメータを設定する	**rfid-tracking ble advertisement [** *ad-number* **] { major-id** *major-id* **| measured-power** *measured-power* **| minor-id** *minor-id* **| uuid** *uuid* **}**	デフォルト：AP group viewの設定を使用します

II. AP group view での BLE モジュールの iBeacon 送信の設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. モジュール view に移行する	**module** *module-id*	—
5. サポートされるモジュールタイプを設定する	**type BLE**	デフォルト：設定なし
6. BLE モジュールの iBeacon 送信を設定する	**rfid-tracking ble advertisement { disable | enable }**	デフォルト：ad1およびad2アドバタイズメントのiBeacon送信は無効

操作	コマンド	補足
7. アドバタイズメント情報を設定する	**rfid-tracking ble advertisement [** *ad-number* **] { major-id** *major-id* **| measured-power** *measured-power* **| minor-id** *minor-id* **| uuid** *uuid* **}**	デフォルト：UUIDは E1CC5B618C06428E8720FE619DB80193、major-IDは1、minor-IDは1、測定電力はad 1またはad 2 iBeaconアドバタイズメントで-58 dBmです
8. iBeacon アドバタイズメントをブロードキャストする間隔を設定する	**rfid-tracking ble advertisement [** *ad-number* **] interval** *interval*	デフォルト：100センチ秒
9. BLE アドバタイズメントモードを設定する	**rfid-tracking ble advertisement mode { continuous** *ad-number* **| periodic {** *ad-number period* **}&<2> }**	デフォルト：ad 1アドバタイズメントを連続モードで送信します
10. iBeacon のアドバタイズメント情報を設定する	**rfid-tracking ble advertisement [** *ad-number* **] { major-id** *major-id* **| measured-power** *measured-power* **| minor-id** *minor-id* **| uuid** *uuid* **}**	デフォルト：ad1とad2のアドバタイズメント情報は以下のとおりです。 Major-idは1 Minor-idは1 measured-powerは-58dBm uuidは E1CC5B618C06428E8720FE619DB80193です

24.4.9 モジュールの再起動

system view で以下の操作を実行します

操作	コマンド
1. system view に移行する	**system-view**
2. モジュールを再起動する	**wlan execute module reset ap** *ap-name* **module** *module-id*

24.4.10 モジュールの自動ファームウェアアップグレードの設定

この機能を有効にすると、モジュールのファームウェアバージョンが AP のイメージファイルに保存されているバージョンと異なる場合、モジュールはすぐにファームウェアをアップグレードします。この機能を有効にすると、モジュールがインストールされている IoT AP が再起動するたびにこの機能が有効になります。

以下に、モジュールの自動ファームウェアアップグレードの設定を示します。

I. AP view でのモジュールの自動ファームウェアアップグレードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. モジュール view に移行する	**module** *module-id*	—

操作	コマンド	補足
4. モジュールの自動ファームウェアアップグレードを設定する	**module firmware-upgrade { disable | enable }**	デフォルト：AP group viewの設定を使用します

II. AP group view でのモジュールの自動ファームウェアアップグレードの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	—
3. AP model view に移行する	**ap-model** *ap-model*	—
4. モジュール view に移行する	**module** *module-id*	—
5. モジュールの自動ファームウェアアップグレードを設定する	**module firmware-upgrade { disable | enable }**	デフォルト：有効

24.4.11 IoT AP の表示および管理

すべての view で display コマンドを実行できます。

操作	コマンド
APのモジュール情報を表示する	**display wlan module-information { all | ap** *ap-name* **module { all |** *module-id* **} } [online]**
APの検出した周辺装置情報を表示する	**display iot ble neighbor-information ap** *ap-name* **{ module all | module** *module-id* **| mac** *mac-addr* **}**

24.5 サーバへのIoTデータのレポート設定

🕮 **メモ：**

- サーバへの IoT データのレポート設定は、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
- サーバへの IoT データのレポート設定は、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。

24.5.1 IoT トランスポートプロファイルの作成

IoT トランスポートプロファイルには、IoT データレポート用のサーバアドレスやレポート間隔などを設定します。最大 8 つの IoT トランスポートプロファイルを作成できます。

IoT トランスポートプロファイルを削除する際は、事前に IoT トランスポートプロファイルのバインドを解除する必要があります。

以下に、IoT トランスポートプロファイルの作成手順を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし

24.5.2 IoT データレポート用のサーバアドレスの設定

IoT トランスポートプロファイルを有効にするには、IoT データレポート用のサーバアドレスを設定する必要があります。サーバアドレスを編集するには、最初に IoT トランスポートプロファイルを無効にします。

以下に、IoT データレポート用のサーバアドレスの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし
3. IoT データレポート用のサーバアドレスを設定する	**server-url** *server-url-string*	デフォルト：設定なし

24.5.3 Microsoft Azure IoT Hub DPS の設定

IoT データレポート用のサーバが Microsoft Azure IoT hub DPS の場合、IoT トランスポートプロファイルを有効にする前に、Microsoft Azure IoT Hub DPS の設定が必要です。Microsoft Azure IoT Hub DPS の設定を編集するには、IoT トランスポートプロファイルを無効にする必要があります。

以下に、Microsoft Azure IoT Hub DPS の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし
3. Microsoft Azure IoT Hub DPS のグループ対称キーを設定する	**azure-dps group-symmetric-key { cipher | simple }** *string*	デフォルト：設定なし
4. Microsoft Azure IoT Hub DPS の ID スコープを設定する	**azure-dps id-scope** *id-scope*	デフォルト：設定なし

24.5.4 ロケーションパケットのフィルタリングの設定

IoT ロケーションシナリオで無効なロケーションパケットを処理することによる IoT AP および IoT サーバの負荷を軽減するには、次のフィルタを使用してロケーションパケットをフィルタリングします。

- RSSI のしきい値。
- RSSI の変動しきい値。RSSI 変動は、同じ IoT エンドポイントによって送信されるロケーションパケットの RSSI が変動した場合に発生します。
- 各ロケーションパケットレポート間隔の最新のサブ間隔。
- レポート間隔中の RSSI 値。

以下に、ロケーションパケットのフィルタリングの設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transportprofile-name*	—
3. ロケーションパケットをフィルタリングするための RSSI しきい値を指定する	**filter rssi threshold** *rssi-threshold*	デフォルト：設定なし
4. ロケーションパケットをフィルタリングするための RSSI 変動しきい値を設定する	**filter rssi-fluctuation threshold** *rssi-threshold*	デフォルト：設定なし
5. IoT AP が、各レポート間隔の指定された最新のサブ間隔で受信したロケーションパケットのみをレポートできるよう設定する	filter recent-packet duration duration	デフォルト：設定なし
6. 各 IoT エンドポイントからの RSSI が最も高いロケーションパケットのみをレポート間隔で IoT サーバにレポートするように IoT AP を設定する	**filter highest-rssi**	デフォルト：レポート間隔中にすべてのロケーションパケットをIoTサーバにレポートします。

24.5.5 サーバに送信するキープアライブパケットの送信間隔の設定

以下に、サーバに送信するキープアライブパケットの送信間隔の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし

操作	コマンド	補足
3. サーバに送信するキープアライブパケットの送信間隔を設定する	**keepalive interval** *interval*	デフォルト：60秒

24.5.6 IoT データをサーバにレポートする間隔の設定

レポートする間隔が長すぎるとサービスに影響しますが、間隔を短くすると AC の負荷が増加するため、適切な値を設定する必要があります。

以下に、IoT データをサーバに報告する間隔の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし
3. IoT データをサーバにレポートする間隔を設定する	**report interval** *interval*	デフォルト：60秒

24.5.7 IoT トランスポートプロファイルの有効化

以下に、IoT トランスポートプロファイルの有効化の設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. IoT トランスポートプロファイルを作成し、その view に移行する	**iot transport-profile** *transport-profile-name*	デフォルト：設定なし
3. IoT トランスポートプロファイルを有効にする	**transport-profile enable**	デフォルト：無効

24.5.8 IoT トランスポートプロファイルのバインド

オンライン AP は、グローバルコンフィグレーション view で IoT トランスポートプロファイルをバインドした後にのみ、IoT データをサーバにレポートします。

既存の IoT トランスポートプロファイル名のみを指定できます。

このコマンドを複数回実行した場合は、最新の設定が有効になります。

以下に、IoT トランスポートプロファイルのバインド設定を示します。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． グローバルコンフィグレーション view に移行する	**wlan global-configuration**	—
3． IoT トランスポートプロファイルをバインドする	**iot-transport-profile** *transport-profile-name*	デフォルト：設定なし

24.5.9 IoT トランスポートプロファイルの表示および管理

すべての view で display コマンドを実行できます。

操作	コマンド
IoTトランスポートプロファイルに関する情報を表示する	**display iot transport-profile**
使用中のIoTトランスポートプロファイル情報を表示する	**display iot transport-profile in-use**

24.6 ワイヤレスロケーション共通パラメータの設定

🕮 **メモ：**

- ワイヤレスロケーション共通パラメータの設定は、ソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。
- ワイヤレスロケーション共通パラメータの設定は、Anchor-AC が QX-W1100 シリーズの場合のみサポートしています。

24.6.1 パケットの間引きの設定

この機能を使用すると、AP は特定の数のワイヤレスパケットを受信したとき、または特定の間隔でロケーションパケットを送信します。これにより、ロケーションサーバと AP の負荷を軽減することができます。

パケットの間引き係数を 10、タイムアウトタイマを 5 秒に設定した場合、パケットの間引きは次のように動作します。

- AeroScout ロケーションまたは RF フィンガープリントが有効の場合、AP は MU クライアントから、10 個のワイヤレスパケット(管理パケット、ブロードキャストパケットを除く)を受信するたびにロケーションパケットを送信します。タイムアウトのタイマ時間が経過する前に AP が MU クライアントから 10 個のワイヤレスパケットを受信できなかった場合、AP は最新のワイヤレスパケットをロケーションサーバに送信します。
- CUPID ロケーションが有効の場合、AP は関連付けられていないクライアントから 10 個のプローブ要求を受信するたびにロケーション測定を実行します。タイムアウトのタイマが経過する前に AP がアソシエートされていないクライアントから 10 個のプローブ要求を受信できなかった場合、タイマが時間切れになると AP はロケーション測定を実行します。

I. 制限及びガイドライン

この機能は、スタティック AeroScout ロケーションまたは RF フィンガープリントの MU クライアント、および CUPID ロケーションに関連付けられていないクライアントでのみ有効です。

II. 設定手順

1) AP View でのパケットの間引きの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. パケットの間引きを有効にする	**rfid-tracking dilution enable**	デフォルト：AP group Viewの設定を使用します。
4. パケットの間引き係数とタイムアウトタイマを設定する	**rfid-tracking dilution factor** *factor* **timeout** *timeout*	デフォルト：AP group Viewの設定を使用します。

2) AP group View でのパケットの間引きの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． パケットの間引きを有効にする	**rfid-tracking dilution enable**	デフォルト：Global configuration Viewの設定を使用します。
4． パケットの間引き係数とタイムアウトタイマを設定する	**rfid-tracking dilution factor** *factor* **timeout** *timeout*	デフォルト：Global configuration Viewの設定を使用します。

3)　Global configuration View でのパケットの間引きの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Global configuration view に移行する	**wlan global-configuration**	—
3． パケットの間引きを有効にする	**rfid-tracking dilution enable**	デフォルト：無効
4． パケットの間引き係数とタイムアウトタイマを設定する	**rfid-tracking dilution factor** *factor* **timeout** *timeout*	デフォルト：設定なし

24.6.2 ビーコンフレームの無視の設定

ビーコンフレームを無視することで、トラフィックフラッディングを防止します。

I. 制限及びガイドライン

この機能は、AeroScout ロケーションまたは RF フィンガープリントが設定されている場合にだけ有効です。

II. 設定手順

1)　AP View でのビーコンフレームの無視の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． ビーコンフレームの無視を有効にする	**rfid-tracking ignore beacon enable**	デフォルト：AP group Viewの設定を使用します。

2)　AP group View でのビーコンフレームの無視の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—

操作	コマンド	補足
2． AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． ビーコンフレームの無視を有効にする	**rfid-tracking ignore beacon enable**	デフォルト：Global configuration Viewの設定を使用します。

3) Global configuration View でのビーコンフレームの無視の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Global configuration view に移行する	**wlan global-configuration**	—
3． ビーコンフレームの無視を有効にする	**rfid-tracking ignore beacon enable**	デフォルト：無効

24.6.3 AP フレームの無視の設定

AP フレームは、AP が他の AP から受信したフレームです。この機能は、AP を検索または監視する必要がない場合に設定します。

I. 制限及びガイドライン

この機能は、AeroScout ロケーションまたは RF フィンガープリントが設定されている場合にだけ有効です。

II. 設定手順

1)　AP View での AP フレームの無視の設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3.　AP フレームの無視を有効にする	**rfid-tracking ignore ap-frame enable**	デフォルト：AP group Viewの設定を使用します。

2)　AP group View での AP フレームの無視の設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3.　AP フレームの無視を有効にする	**rfid-tracking ignore ap-frame enable**	デフォルト：Global configuration Viewの設定を使用します。

3)　Global configuration View での AP フレームの無視の設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　Global configuration view に移行する	**wlan global-configuration**	—
3.　AP フレームの無視を有効にする	**rfid-tracking ignore ap-frame enable**	デフォルト：無効

24.6.4 RSSI ベースのパケットフィルタリングの設定

RSSI ベースのパケットフィルタリングが有効の場合、AP は RSSI しきい値よりも低い RSSI を持つパケットのロケーション情報を報告しません。この機能により、AP は AP から遠く離れたクライアントを見つけることができなくなります。

I. 制限及びガイドライン

この機能は、AeroScout ロケーションまたは RF フィンガープリントが設定されている場合にだけ有効です。

II. 設定手順

1)　AP View での RSSI ベースのパケットフィルタリングの設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—

操作	コマンド	補足
3． RSSI ベースのパケットフィルタリングを有効にする	**rfid-tracking rssi enable**	デフォルト：AP group Viewの設定を使用します。
4． RSSI しきい値を設定する	**rfid-tracking rssi threshold** *rssi-threshold*	デフォルト：5 (-123dBm)

2)　AP group View での RSSI ベースのパケットフィルタリングの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． RSSI ベースのパケットフィルタリングを有効にする	**rfid-tracking rssi enable**	デフォルト：Global configuration Viewの設定を使用します。
4． RSSI しきい値を設定する	**rfid-tracking rssi threshold** *rssi-threshold*	デフォルト：5 (-123dBm)

3)　Global configuration View での RSSI ベースのパケットフィルタリングの設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Global configuration view に移行する	**wlan global-configuration**	—
3． RSSI ベースのパケットフィルタリングを有効にする	**rfid-tracking rssi enable**	デフォルト：無効
4． RSSI しきい値を設定する	**rfid-tracking rssi threshold** *rssi-threshold*	デフォルト：5 (-123dBm)

24.6.5 クライアントパケットレート制限の設定

この機能により、CIR と CBS の両方を超過した場合に、AP が過剰なクライアントパケットからのロケーション情報を報告しないようにすることができます。これにより、各クライアントのロケーション情報をロケーションサーバに送信できるようになり、クライアントパケットが AP にフラッディングするのを防ぐことができます。

I. 制限及びガイドライン

この機能は、AeroScout ロケーションまたは RF フィンガープリントが設定されている場合にだけ有効です。

パケットの間引きが有効の場合、この機能は間引きされたパケットのレートを制限します。

II. 設定手順

1)　AP View でのクライアントパケットレート制限の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3． クライアントパケットレート制限を有効にする	**rfid-tracking client rate-limit enable**	デフォルト：無効
4． クライアントパケットの CIR と CBS を設定する	**rfid-tracking client rate-limit cir** *cir* [**cbs** *cbs*]	デフォルト：設定なし

2)　AP group View でのクライアントパケットレート制限の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3． クライアントパケットレート制限を有効にする	**rfid-tracking client rate-limit enable**	デフォルト：無効
4． クライアントパケットの CIR と CBS を設定する	**rfid-tracking client rate-limit cir** *cir* [**cbs** *cbs*]	デフォルト：設定なし

3)　Global configuration View でのクライアントパケットレート制限の設定

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Global configuration view に移行する	**wlan global-configuration**	—
3． クライアントパケットレート制限を有効にする	**rfid-tracking client rate-limit enable**	デフォルト：無効
4． クライアントパケットの CIR と CBS を設定する	**rfid-tracking client rate-limit cir** *cir* [**cbs** *cbs*]	デフォルト：設定なし

24.6.6 ロケーションパケットレート制限の設定

この機能を使用すると、CIR と CBS の両方が超過した場合に、AP が過剰なロケーションパケットを破棄します。これにより、ロケーションパケットがロケーションサーバにフラッディングするのを防ぐことができます。

I. 制限及びガイドライン

この機能は、AeroScout ロケーションまたは RF フィンガープリントが設定されている場合にだけ有効です。

II. 設定手順

1)　AP View でのロケーションパケットレート制限の設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3.　ロケーションパケットレート制限を有効にする	**rfid-tracking rate-limit enable**	デフォルト：無効
4.　ロケーションパケットの CIR と CBS を設定する	**rfid-tracking rate-limit cir** *cir* [**cbs** *cbs*]	デフォルト：設定なし

2)　AP group View でのロケーションパケットレート制限の設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3.　ロケーションパケットレート制限を有効にする	**rfid-tracking rate-limit enable**	デフォルト：無効
4.　ロケーションパケットの CIR と CBS を設定する	**rfid-tracking rate-limit cir** *cir* [**cbs** *cbs*]	デフォルト：設定なし

3)　Global configuration View でのロケーションパケットレート制限の設定

操作	コマンド	補足
1.　system view に移行する	**system-view**	—
2.　Global configuration view に移行する	**wlan global-configuration**	—
3.　ロケーションパケットレート制限を有効にする	**rfid-tracking rate-limit enable**	デフォルト：無効
4.　ロケーションパケットの CIR と CBS を設定する	**rfid-tracking rate-limit cir** *cir* [**cbs** *cbs*]	デフォルト：設定なし

24.6.7 ワイヤレスロケーションのキープアライブの設定

この機能を有効にすると、AP は 15 秒間隔で Hello パケットをロケーションサーバに送信します。ロケーションサーバが 30 秒以内に AP からパケットを受信しない場合、ロケーションサーバは AP がオフラインであると判断します。

I. 制限及びガイドライン

この機能は、RF フィンガープリント、CUPID ロケーション、または BLE ロケーションが設定されている場合にのみ有効です。

ロケーションサーバが Hello パケットを処理できない場合は、この機能を無効にします。

II. 設定手順

1) AP View でのワイヤレスロケーションのキープアライブの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP view に移行する	**wlan ap** *ap-name* [**model** *model-name*]	—
3. ワイヤレスロケーションのキープアライブを有効にする	**rfid-tracking keepalive** { **disable** | **enable** }	デフォルト：無効

2) AP group View でのワイヤレスロケーションのキープアライブの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. AP group view に移行する	**wlan ap-group** *group-name*	デフォルト：デフォルトAPグループ（default-group）が存在し、デフォルトAPグループは削除することができません。
3. ワイヤレスロケーションのキープアライブを有効にする	**rfid-tracking keepalive** { **disable** | **enable** }	デフォルト：無効

3) Global configuration View でのワイヤレスロケーションのキープアライブの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Global configuration view に移行する	**wlan global-configuration**	—
3. ワイヤレスロケーションのキープアライブを有効にする	**rfid-tracking keepalive** { **disable** | **enable** }	デフォルト：無効

24.6.8 ワイヤレスロケーションの表示および管理

すべての view で display コマンドを実行できます。

操作	コマンド
ワイヤレスロケーションの無線情報を表示する	**display wlan rfid-tracking radio** [**ap** *apname*]

24.7 BLE機能の設定例

24.7.1 iBeacon を送信する

I. ネットワーク要件

図 24-2 に示すように、AP から iBeacon を送信するようにします。

iBeacon のアドバタイズメント情報は、major-id を 1234、minor-id を 5678、uuid を 11223344556677881122334455667788 で送信するものとします。

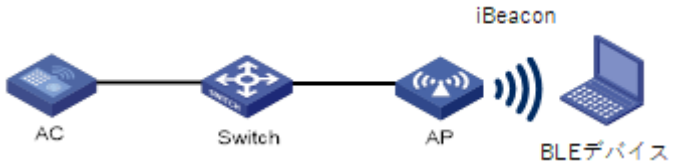


図24-2 ネットワーク図

II. 設定手順

1)　AP の BLE モジュールを設定します。

#AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A0CNC148165154
```

#モジュール 1 を作成し、モジュールタイプ BLE を設定します。

```
[AC-wlan-ap-ap1] module 1
[AC-wlan-ap-ap1-module-1] type BLE
[AC-wlan-ap-ap1-module-1] module enable
```

2)　iBeacon の送信設定をします。

#iBeacon の送信を有効化します。

```
[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement enable
```

#iBeacon のアドバタイズメント情報(major-id、minor-id、uuid)を設定します。

```
[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement major-id 1234
[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement minor-id 5678
[AC-wlan-ap-ap1-module-1] rfid-tracking ble advertisement uuid
11223344556677881122334455667788
```

III. 設定確認

BLE デバイスで、AP が送信した iBeacon を受信できるか確認します。

（詳細は省略します。）

24.7.2 AP が収集した周辺装置のレポートを Azure IoT Hub DPS へ送信する

I. ネットワーク要件

図 24-3 に示すように、AP が収集した周辺装置のレポートを、Microsoft Azure IoT Hub DPS へ送信するようにします。

- 事前に外部ネットワークへの接続設定が完了しているものとします。
- 事前に、Azure Cloud サービスにログインし、IoT Hub と DPS サービスの設定が完了しているものとします。
- IoT データレポート用のサーバアドレスは” global.azure-devices-provisioning.net”を設定するものとします。
- Microsoft Azure IoT Hub DPS の ID スコープは”12345678”を設定するものとします。
- Microsoft Azure IoT Hub DPS 登録グループのは”abcdefgh”を設定するものとします。

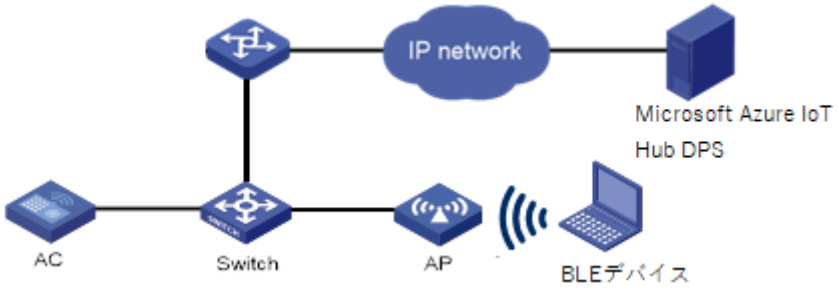


図24-3 ネットワーク図

II. 設定手順

1)　Microsoft Azure Hub DPS にレポートを送信する設定をします。

IoT トランスポートプロファイル “azure-profile”を作成します。

```
<AC> System-View
[AC] iot transport-profile azure-profile
```

#IoT データレポート用のサーバアドレスを設定します。

```
[AC-iot-transport-profile-azure-profile] server-url global.azure-devices-provisioning.net
```

Microsoft Azure IoT Hub DPS の ID スコープを設定します。

```
[AC-iot-transport-profile-azure-profile] azure-dps id-scope 12345678
```

Microsoft Azure IoT Hub DPS 登録グループの対称キーを設定します。

```
[AC-iot-transport-profile-azure-profile] azure-dps group-symmetric-key simple abcdefgh
```

#IoT トランスポートプロファイルを有効化します。

```
[AC-iot-transport-profile-azure-profile] transport-profile enable
[AC-iot-transport-profile-azure-profile] quit
```

#グローバルコンフィグレーション view で IoT トランスポートプロファイルをバインドします。

```
[AC] wlan global-configuration
[AC-wlan-global-configuration] iot-transport-profile azure-profile
[AC-wlan-global-configuration] quit
```

2)　AP の IoT モジュールを設定します。

#AP 名 ap1 の AP を作成し、モデル名、シリアル番号を指定します。

```
[AC] wlan ap ap1 model QX-W1110
[AC-wlan-ap-ap1] serial-id 219801A0CNC148165154
```

#モジュール 1 を作成し、モジュールタイプ BLE を設定します。

```
[AC-wlan-ap-ap1] module 1
[AC-wlan-ap-ap1-module-1] type BLE
[AC-wlan-ap-ap1-module-1] module enable
```

3)　設定の確認

Microsoft Azure IoT Hub DPS との接続を確認する為、**display iot transport-profile in-use** コマンドを使用します。

```
<AC> display iot transport-profile in-use
Connect status: connected
Connected for: 0d 0h 0m 12s
Profile name: azure-profile
Server URL: global.azure-devices-provisioning.net
Server type: azure iot
Azure DPS information
  ID scope: 12345678
  Key type: symmetric
  Group key(cipher): /5LdDRZLigriZAsBwv…….
  Register ID: sn-210235A3KXA8765408
Report interval: 60 seconds
Keepalive interval: 60 seconds
Total sent messages: 0
Sent BLE data messages: 0
Sent keepalive messages: 0
Total received messages: 0
```

#AP が収集した周辺の BLE デバイス情報を確認する為、**display iot ble neighbor-information ap ap1 module 1** コマンドを使用します。

```
<AC> display iot ble neighbor-information ap ap1 module 1
ModuleID  MAC address      Address type          RSSI   Last update time
 ------------------------------------------------------------------------
------
 1         c61b-fa2f-d008   Static                -82    Mon May 16
15:17:03 2022
 1         5d86-6f24-c949   Static                -83    Mon May 16
15:16:38 2022
 1         63b9-fead-f9c0   Static                -80    Mon May 16
15:17:12 2022
 1         ff8b-4380-0a5d   Static                -84    Mon May 16
15:17:07 2022
```

```
 1          47d5-895d-1553   Static                -77    Mon May 16
15:16:54 2022
 1          5714-552b-06cb   Static                -82    Mon May 16
15:16:17 2022
 1          7e89-b341-2d98   Static                -83    Mon May 16
15:17:14 2022
 1          4d37-de1a-b0ae   Static                -73    Mon May 16
15:17:12 2022
 1          d005-e316-7e99   Public                -81    Mon May 16
15:16:53 2022
 1          1c52-14c0-da52   Public                -83    Mon May 16
15:17:15 2022
 1          0758-9970-5e38   Static                -79    Mon May 16
15:17:11 2022
 1          2b6f-b895-029b   Static                -76    Mon May 16
15:17:15 2022
```

#Azure IoT Hub のページで、AP 周辺の BLE デバイス情報が登録されていることを確認します。

（詳細は省略します。）

目次

25 章 Hotspot 2.0 の設定 25-1
25.1 概要 25-1
25.1.1 Hotspot 2.0 の動作メカニズム 25-1
25.1.2 プロトコルと標準 25-4
25.2 Hotspot 2.0 のタスクの概要 (バージョン 1 の場合) 25-4
25.3 Hotspot 2.0 のタスクの概要 (バージョン 2 の場合) 25-5
25.4 Hotspot 2.0 ポリシーの設定 25-5
25.4.1 Hotspot 2.0 ポリシーを設定するための前提条件 25-5
25.4.2 Hotspot 2.0 ポリシーの作成 25-6
25.4.3 サービスプロバイダ情報の設定 25-6
25.4.4 Hotspot 2.0 ネットワークパラメータ設定 25-7
25.4.5 Hotspot 2.0 ネットワーク最適化の設定 25-8
25.4.6 サービステンプレートへの Hotspot 2.0 ポリシーのバインド 25-9
25.5 オンラインサインアップサービスの設定 25-9
25.5.1 OSU サーバの設定 25-9
25.5.2 オンラインサインアップサービスの SSID の設定 25-10
25.5.3 OSU サーバアイコンの管理 25-10
25.5.4 OSU サーバの Hotspot 2.0 ポリシーへのバインド 25-11
25.6 AP 場所情報の設定 25-11
25.6.1 場所 URL でのエスケープから特定の特殊文字を除外する 25-12
25.7 Hotspot 2.0 の表示および管理 25-12
25.8 Hotspot 2.0 設定の例 25-13
25.8.1 例:Hotspot 2.0 Samsung アプリケーションの設定 25-26
25.8.2 例:Hotspot 2.0 の設定 (バージョン 2 の場合) 25-35

25章 Hotspot 2.0 の設定

🕮 **メモ：**

Hotspot 2.0 の設定は、QX-W1000 シリーズではソフトウェアバージョン 7.2.74、QX-W1100 シリーズではソフトウェアバージョン 7.2.75 を含む以降のソフトウェアからサポートしています。

25.1 概要

Wi-Fi Alliance によって開発された Hotspot 2.0 は、ワイヤレスクライアントに自動ネットワーク検出、自動認証、およびシームレスなローミングを提供します。

Hotspot 2.0 には 2 つのバージョンがあります。バージョン 2 はバージョン 1 と完全に互換性があります。

25.1.1 Hotspot 2.0 の動作メカニズム

Hotspot 2.0 は次のように動作します。

1) クライアントは、Hotspot 2.0 ネットワークを検出するワイヤレススキャンを実行します。
2) クライアントは、AP と Generic Advertisment Service (GAS) フレームを交換して Hotspot 2.0 の情報を取得し、最適な BSS を選択します。
3) クライアントはオンラインのサインアップを実行します。このステップは Hotspot 2.0 のバージョン 2 でのみ要求されます。

I. スキャン

次のスキャンタイプを使用できます。

- **アクティブスキャン**

図 25-1 に示すように、ワイヤレスクライアントは、プローブ要求を送信して周囲のワイヤレスネットワークを定期的にスキャンし、受信したプローブ応答からネットワーク情報を取得します。

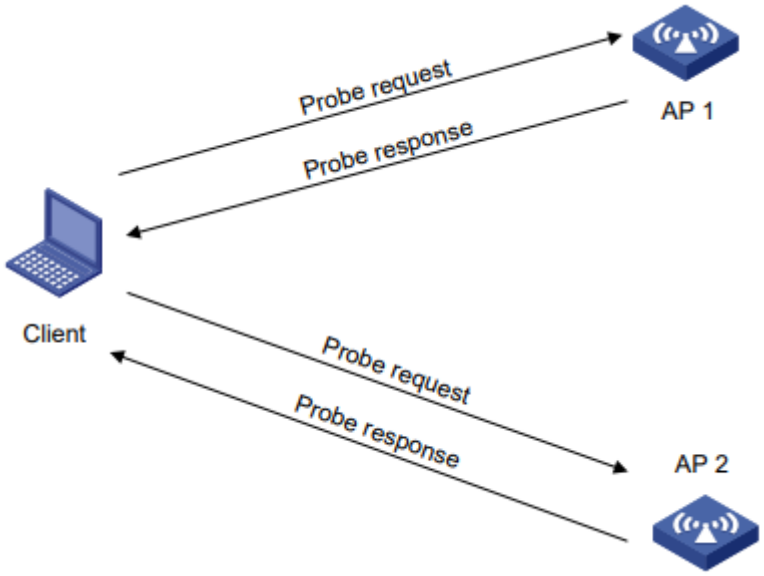


図 25-1 アクティブスキャン図

- **パッシブスキャン**

ワイヤレスクライアントは、サポートされているチャネルで AP から送信されたビーコンフレームを定期的にリッスンし、図 25-2 に示すように周辺のワイヤレスネットワークに関する情報を取得します。

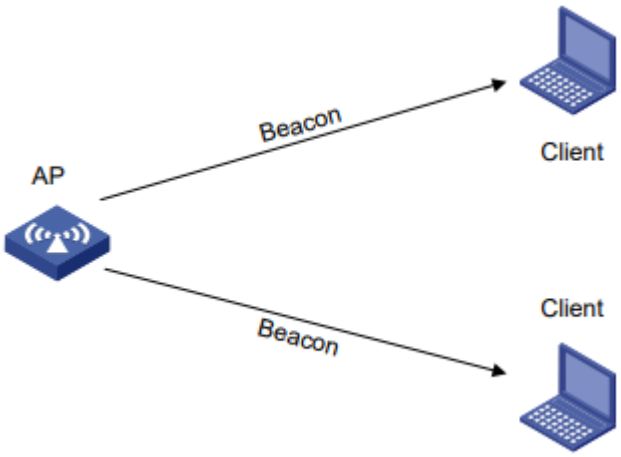


図 25-2 パッシブスキャン図

II. GAS フレーム交換

アクティブまたはパッシブスキャンによって Hotspot 2.0 ネットワークを検出した後、クライアントは、AP の Hotspot 2.0 情報を取得するために、AP と GAS フレームを交換します。取得した Hotspot 2.0 情報とローカル設定に基づいて、クライアントは最適な BSS を選択します。

図 24-3 に示すように、クライアントは、次のプロセスを使用して、AP と GAS フレームを交換します。

1) クライアントは、GAS 初期要求を送信します。
2) 要求を受信すると、AP は GAS 初期応答に Hotspot 2.0 情報をカプセル化し、応答の長さを調べます。
   - 長さが制限を超えない場合、AP は GAS 初期応答をクライアントに送信します。GAS フレーム交換が完了し、クライアントは認証要求を送信できます。
   - 長さが制限を超えると、AP は応答をフラグメント化し、GAS 初期応答の最初のフラグメントをクライアントに送信します。応答は、カムバック遅延後に Hotspot 2.0 情報を要求するようにクライアントに通知します。
3) クライアントは、カムバック遅延後に GAS カムバック要求を AP に送信します。
4) AP は、2 番目のフラグメントをクライアントに通信する GAS カムバック応答を送信します。
5) 応答の長さが制限を超える場合、クライアントと AP はステップ 3 と 4 を繰り返し、すべてのフラグメントがクライアントに送信されるまで処理を続けます。

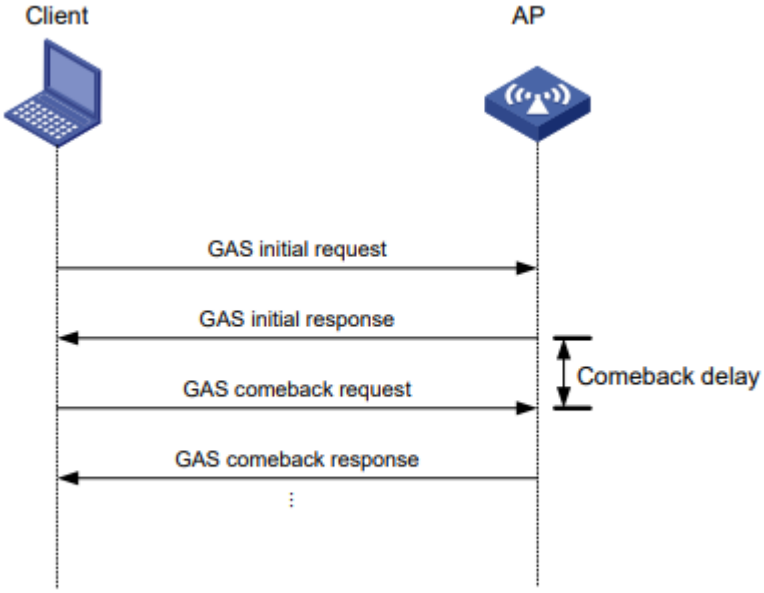


図 25-3 GAS フレーム交換図

III. オンラインサインアップ (バージョン 2 の場合)

GAS フレーム交換の後、クライアントは OSU AP を介して Online Sign Up (OSU) サーバに接続し、オンラインでサインアップします。サインアップしたクライアントはクレデンシャルを取得し、再認証されることなく自動的に Hotspot 2.0 ネットワークにアクセスできます。クライアントは、次の方法を使用して OSU AP に関連付けることができます。

- **Open OSU** – 認証なし
- **OSEN OSU** – Layer2 認証

図 24-4 に示すように、オンラインサインアップは次のように動作します。

1) クライアントは、AP と GAS フレームを交換することによって AP から OSU サーバリストを取得し、OSU サーバを選択します。
2) クライアントは、オープン OSU または OSEN OSU を介して OSU AP と関連付けられます。
3) OSU サーバは、資格情報と認証情報をクライアントに送信するか、クライアントの期限切れの資格情報を更新します。
4) 新しくプロビジョニングされた資格情報を使用して、クライアントは OSU AP との関連付けを解除し、Hotspot 2.0 サービスを提供する AP に関連付けます。

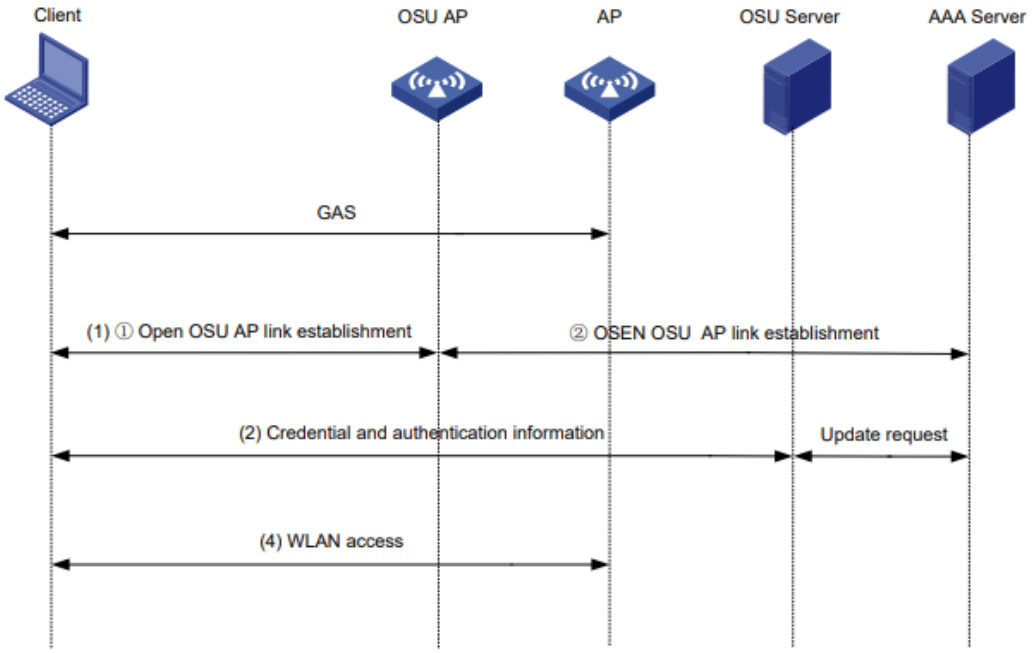


図 25-4 オンラインサインアップ図

25.1.2 プロトコルと標準

- IEEE Standard for Information technology—Telecommunications and information exchange between systems— Local and metropolitan area networks— Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 9: Interworking with External Networks
- Wi-Fi Alliance Technical Committee Hotspot 2.0 Technical Task Group Hotspot 2.0 (Release 2)Technical Specification Version 3.04

25.2 Hotspot 2.0のタスクの概要 (バージョン1の場合)

Hotspot 2.0 (バージョン 1) を設定するには、次のタスクを実行します。

I. Hotspot 2.0 ポリシーの設定

a) (必須項目)Hotspot 2.0ポリシーの作成

b) (必須項目)サービスプロバイダ情報の設定

c) (必須項目)Hotspot 2.0ネットワークパラメータの設定

d) (オプション設定項目) Hotspot 2.0ネットワーク最適化の設定

e) (必須項目)Hotspot 2.0ポリシーのサービステンプレートへのバインド

II. (オプション設定項目) オンラインサインアップサービスの設定

25.3 Hotspot 2.0のタスクの概要 (バージョン2の場合)

Hotspot 2.0 (バージョン 2) を設定するには、次のタスクを実行します。

I. Hotspot 2.0 ポリシーの設定

a) (必須項目)Hotspot 2.0ポリシーの作成

b) (必須項目)サービスプロバイダ情報の設定

c) (オプション設定項目) Hotspot 2.0ネットワークパラメータの設定

d) (オプション設定項目) Hotspot 2.0ネットワーク最適化の設定

e) (必須項目)Hotspot 2.0ポリシーをサービステンプレートにバインドする

II. オンラインサインアップサービスの設定

a) (必須項目)OSUサーバの設定

b) (必須項目)オンラインサインアップサービスのSSIDの設定

c) (必須項目)OSUサーバのアイコンの管理

d) (必須項目)OSUサーバのHotspot 2.0ポリシーへのバインド

III. (オプション設定項目) AP の場所情報の設定

25.4 Hotspot 2.0ポリシーの設定

25.4.1 Hotspot 2.0 ポリシーを設定するための前提条件

Hotspot 2.0 には、802.1X AKM モード、RSN IE、および AES-CCMP cipher スイートが必要です。

バージョン 1 のみをサポートしているクライアントが Hotspot 2.0 ネットワークにアクセスするには、まずクライアントで OI、NAI、ドメインなどのネットワーク情報を設定します。次に、これらの設定をクライアントの設定ファイルに保存します。

25.4.2 Hotspot 2.0 ポリシーの作成

I. このタスクについて

Hotspot 2.0 ポリシーは、Hotspot 2.0 パラメータのセットを定義します。

II. 設定手順

Hotspot 2.0 ポリシーの作成は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーを作成し、その view を開始する	**wlan hotspot-policy** *policy-number*	—
3. (オプション設定項目) Hotspot 2.0 ポリシーの名前を指定する	**policy-name** *name*	デフォルトでは、Hotspot 2.0 ポリシーに名前は指定されません。

25.4.3 サービスプロバイダ情報の設定

I. このタスクについて

- NAI realm and authentication type — アクセスネットワークの NAI レルムおよび NAI レルムの認証タイプ。
- [Organization identifier] (OI;組織 ID) — ローミングコンソーシアム ID。クライアントがローミングコンソーシアムに対する証明書を持っている場合、クライアントはローミングコンソーシアムが提供するすべての無線サービスにローミングできます。
- 3rd Generation Partnership Project] (3GPP) 情報 — 国コードとネットワークコードが含まれます。国コードは国を識別し、ネットワークコードは国内のサービスプロバイダを識別します。
- ISP domain — クライアントの ISP ドメイン。
- Service provider name — サービスプロバイダ名と言語コード。

II. 設定手順

サービスプロバイダ情報の設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーview に移行します。	**wlan hotspot-policy** *policy-number*	—
3. NAI レルムを作成し、NAI レルムの認証タイプを指定します。	**nai-realm name** *realm-name* **eap-method** *eap-method-id* **auth-method** *auth-method-id* **authentication** *authentication*	デフォルトでは、NAIレルムは存在しません。
4. 設定された順序で保存される NAI レルム設定	**nai-realm config-order**	デフォルトでは、NAIレルムは辞書順に保存されます。

操作	コマンド	補足
5. OI を指定します。	**roam-oi** *oi* [**in-beacon**]	デフォルトでは、OIは指定されません。 この手順は、Hotspot 2.0のバージョン2にのみ必須設定項目です。
6. (オプション設定項目) 3GPP 情報設定。	**3gpp-info country-code** *mobile-country-code* **network-code** *mobile-network-code*	デフォルトでは、国コードおよびネットワークコードは設定されていません。
7. ドメイン名を設定します。	**domain-name** *domain-name*	デフォルトでは、ドメイン名は設定されていません。 この手順は、Hotspot 2.0のバージョン1にのみ必須設定項目です。
8. (オプション設定項目) サービスプロバイダ名を指定します。	**operator-name** *operator-name* **lang-code** *lang-code*	デフォルトでは、サービスプロバイダ名は指定されません。

25.4.4 Hotspot 2.0 ネットワークパラメータ設定

I. 概要

Hotspot 2.0 ネットワークパラメータには、次のものがあります。

- アクセスネットワークタイプ — 詳細については、コマンドマニュアルのセクション 2 WLAN"*Hotspot 2.0 の設定*"を参照してください。
- 同種 ESS 識別子 (HESSID) — HESSID は同種 ESS を一意に識別します。
- ネットワーク認証タイプ — 詳細については、コマンドマニュアルのセクション 2 WLAN"*Hotspot 2.0 の設定*"を参照してください。
- IP アドレスの可用性 — 関連付けられたクライアントに割り当てられている IP アドレスのバージョンとタイプ。
- WAN リンクステータスパラメータ — 速度とリンクステータス情報が含まれます。Hotspot 2.0 がアップリンクとダウンリンクの速度とリンクステータス (WAN のクローズ、テスト中、有効など) を配信できるようにパラメータを設定できます。
- IP プロトコルのポートステータス — closed、open、および unknown が含まれます。

II. 設定手順

Hotspot 2.0 ネットワークパラメータ設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーview に移行する。	**wlan hotspot-policy** *policy-number*	—
3. アクセスネットワークの種別を設定する。	**network-type** *network-type* [**access-internet**]	デフォルトでは、アクセスネットワークの種別は設定されていない。
4. HESSID を設定する。	**hessid** *hessid*	デフォルトでは、HESSIDは設定されていません。 この手順は、Hotspot 2.0のバージョン1にのみ必要です。

操作	コマンド	補足
5. (オプション設定項目) ネットワーク認証の種類を指定します。	**authentication-type** { **0** [**redirect-url** *url*] | **1** | **2 redirect-url** *url* | **3** }	デフォルトでは、ネットワーク認証の種類は指定されていません。
6. IP アドレスの可用性設定。	**ip-type ipv4** *ipv4-type* **ipv6** *ipv6-type*	デフォルトでは、IPv4アドレスの可用性は1、IPv6アドレスの可用性は2です。
7. IP プロトコルのポートステータスを設定します。	**ip-protocol** { **esp** | **icmp** | **tcp** | **udp** } **port-number** *port-number* { **closed** | **open** | **unknown** }	デフォルトでは、IPプロトコルのポートステータスは設定されていません。
8. WAN リンクステータスパラメータを設定します。	**wan-metrics** { **link-down** | **link-test** | **link-up** } [**asymmetric downlink-speed** *downlink-speed* **uplink-speed** *uplink-speed* | **symmetric link-speed** *link-speed*]	デフォルトでは、WANリンクステータスパラメータは設定されていません。

25.4.5 Hotspot 2.0 ネットワーク最適化の設定

I. 概要

Hotspot 2.0 ネットワークでは、次のネットワーク最適化機能を使用できます。

- Downstream Group-Addressed Forwarding (DGAF) — AP がすべてのダウンストリームワイヤレスブロードキャスト ARP パケットおよびワイヤレスマルチキャストパケットを転送できるようにします。ダウンストリームマルチキャストを使用したスプーフィング攻撃を防止するには、AP の DGAF 機能をディセーブルにします。
- Comeback delay — クライアントが GAS カムバック要求を頻繁に送信しないようにします。
- GAS initial request limit — AC の負荷を軽減するために、クライアントが指定された間隔内に送信できる GAS 初期要求の最大数を制限します。

II. 設定手順

Hotspot 2.0 ネットワーク最適化の設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーを作成し、その view を開始する	**wlan hotspot-policy** *policy-number*	—
3. DGAF 機能を無効にします。	**undo dgaf enable**	デフォルトでは、DGAF機能は有効になっています。
4. カムバック遅延を設定します。	**comeback-delay** *value*	デフォルトでは、カムバック遅延は1 TU (1024ミリ秒) です。
5. 指定した間隔内にクライアントが送信できる GAS 初期要求の最大数を設定します。	**gas-limit number** *number* **interval** *interval*	デフォルトでは、クライアントが送信できるGAS初期要求の数は制限されません。

25.4.6 サービステンプレートへの Hotspot 2.0 ポリシーのバインド

I. 概要

Hotspot 2.0 ネットワークを構築するには、サービステンプレートを使用して、Hotspot 2.0 ポリシーを AP のサービステンプレートにバインドする必要があります。

II. 設定手順

サービステンプレートへの Hotspot 2.0 ポリシーのバインド設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. サービステンプレート view を入力します。	**wlan service-template** *service-template-name*	—
3. Hotspot 2.0 ポリシーをサービステンプレートにバインドします。	**hotspot-policy** *policy-number*	デフォルトでは、Hotspot 2.0 ポリシーはサービステンプレートにバインドされていません。

25.5 オンラインサインアップサービスの設定

25.5.1 OSU サーバの設定

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. OSU サーバを作成してその view に移行するか、既存の OSU サーバの view に移行する	**wlan osu-provider** *osu-provider-number*	—
3. OSU サーバの名前を設定する	**friendly-name** *friendly-name* **lang-code** *lang-code*	デフォルト：設定なし
4. OSU サーバの URI を指定する	**uri** *uri*	デフォルト：指定なし
5. クライアントが OSU サーバと通信するためのプロトコルを指定する	**method** *method-id*	デフォルト：指定なし
6. OSU サーバのアイコンを指定する	**icon-file** *filename* **lang-code** *lang-code* **icon-type** *icon-type*	デフォルト：指定なし OSUサーバのアイコンを指定する前に、バージョンファイルが保存されているルートディレクトリでmkdirコマンドを使用してディレクトリアイコンが作成されていることを確認してください。次に、FTPまたはTFTPを使用して、アイコンファイルをディレクトリにダウンロードしてください。

操作	コマンド	補足
7. (オプション設定項目) OSU サーバの説明を設定する	**description** *description* **lang-code** *lang-code*	デフォルト：設定なし
8. (オプション設定項目) OSU サーバのネットワークアクセス識別子（NAI）を設定する	**nai** *nai*	デフォルト：設定なし

25.5.2 オンラインサインアップサービスの SSID の設定

I. 設定の制限とガイドライン

オンラインサインアップサービス用に設定された SSID が、オンラインサインアップサービステンプレートの SSID と同じであることを確認します。

II. 設定手順

オンラインサインアップサービスの SSID の設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. Hotspot 2.0 ポリシーview に移行します。	**wlan hotspot-policy** *policy-number*	—
3. オンラインサインアップサービスの SSID を設定します。	**osu-ssid** *ssid-name*	デフォルトでは、オンラインサインアップサービスに SSIDは設定されていません。

25.5.3 OSU サーバアイコンの管理

I. 概要

このタスクでは、OSU サーバに指定されたすべてのアイコンファイルをロードして、アイコンファイルの変更が発生したときに変更を検証したり、アイコンファイルを無効にしたりできます。

II. 設定手順

OSU サーバアイコンの管理は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—

操作	コマンド	補足
2． OSU サーバのアイコンファイルを管理します。 OSU サーバのアイコンファイルを読み込みます。	**wlan hotspot osu-icon upload**	—
OSU サーバのアイコンファイルを管理します。 OSU サーバのアイコンファイルをアンロードします。	**wlan hotspot osu-icon unload**	—

25.5.4 OSU サーバの Hotspot 2.0 ポリシーへのバインド

I. 設定の制限とガイドライン

Hotspot 2.0 ポリシーは、最大 32 台の OSU サーバにバインドできます。

OSU サーバを Hotspot 2.0 ポリシーにバインドする前に、OSU サーバに必要なすべての設定が完了していることを確認してください。

II. 設定手順

OSU サーバの Hotspot 2.0 ポリシーへのバインド設定は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． Hotspot 2.0 ポリシーview に移行する。	**wlan hotspot-policy** *policy-number*	—
3． OSU サーバを Hotspot 2.0 ポリシーにバインドします。	**osu-provider** *osu-provider-number*	デフォルトでは、OSUサーバはHotspot 2.0ポリシーにバインドされていません。

25.6 AP場所情報の設定

I. 概要

AP 場所情報は AP の場所を示し、クライアントが最適な AP に接続するのに役立ちます。

II. 設定手順

AP 場所情報の設定は以下の通りです。

操作	コマンド	補足
1． system view に移行する	**system-view**	—
2． APview を入力します。	**wlan ap** *ap-name*	—

操作	コマンド	補足
3. AP の場所グループと場所タイプを指定します。	**venue group** *venue-group-number* **type** *venue-type-number*	デフォルトでは、APの場所グループと場所タイプは指定されていません。 この手順は、Hotspot 2.0のバージョン1の場合にのみ必要です。
4. AP の場所名を設定します。	**venue name** *venue-name* ***lang-code*** *lang-code* [**url** *url*]	デフォルトでは、APに場所名は設定されていません。 この手順は、Hotspot 2.0バージョン1の場合だけ必要です。

25.6.1 場所 URL でのエスケープから特定の特殊文字を除外する

I. 概要

クライアントが特殊文字を構文またはコマンドとして解釈し、意図した意味を変更しないようにするには、これらの文字を安全な形式 (エスケープ文字) に変換する必要があります。

実際には、サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、エラーが発生することがあります。このような場合は、このタスクを実行して、特定の特殊文字をエスケープから除外できます。

場所 URL では、大文字と小文字および数字以外の文字はエスケープする必要がなく、このコマンドを使用して残りの特殊文字を構成できます。

デフォルトでは、装置は composition1 の特殊文字をエスケープしません。

サーバによっては、URL 内の特定の特殊文字のエスケープ文字が認識されず、例外が発生する場合があります。これに対処するには、これらの特定の文字がエスケープされないように機能を構成します。

II. 設定手順

場所 URL でのエスケープから特定の特殊文字を除外する設定は以下の通りです。

操作	コマンド	補足
1. system view に移行する	**system-view**	—
2. 場所 URL のエスケープから特定の特殊文字を除外します。	**wlan venue url-unescape-chars** { **composition1** | **composition2** | **custom** *character-string* }	デフォルトでは、Venue URL はcomposition1方式を採用し、composition1に含まれる特殊文字はエスケープされません。

25.7 Hotspot 2.0の表示および管理

任意の view で表示コマンドを実行します。(バージョン 1 の場合)

操作	コマンド
サービステンプレートの情報を表示する。	**display wlan service-template** [*service-template-name*] [**verbose**]

任意の view で表示コマンドを実行する。(バージョン 2 の場合)

操作	コマンド
ロードされているすべての OSU サーバのアイコンファイルを表示します。	**display wlan hotspot uploaded-osu-icon**
サービステンプレートの情報を表示します。	**display wlan service-template** [*service-template-name*] [**verbose**]

25.8 Hotspot 2.0 設定の例

I. ネットワーク要件

図 24-5 に示すように、Hotspot 2.0 を構成して、携帯電話ネットワークからワイヤレスネットワークに電話を切り替えることができるようにします。

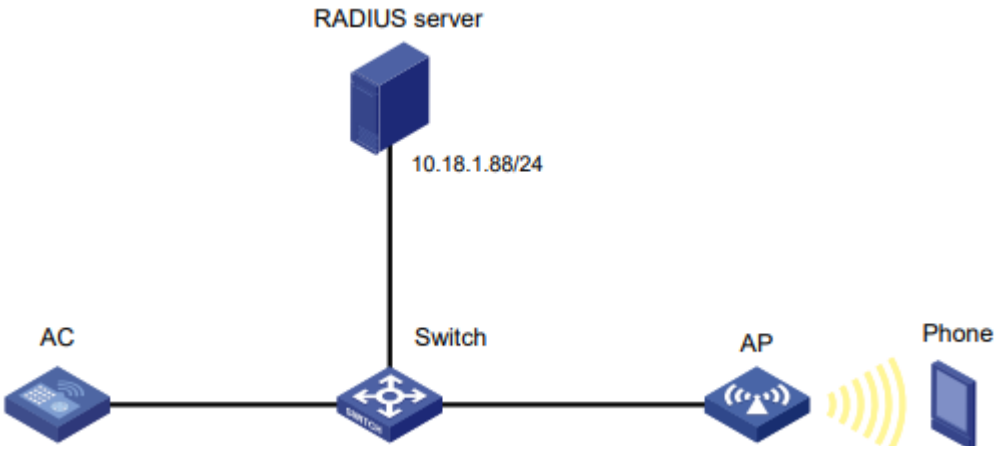


図 25-5 ネットワーク図

II. 前提条件

クライアント認証、許可、アカウンティングを正しく動作させるには、RADIUS サーバに証明書をインストールし、ユーザアカウントを作成する必要があります。AAA の詳細は、オペレーションマニュアルのセクション 9 セキュリティ"*AAA*"の"*一般的に使われる標準 RADIUS 属性*"を参照してください。

III. AC の設定

1)　Hotspot 2.0 ポリシー設定:

Hotspot 2.0 ポリシーを作成します。

```
<AC> system-view
[AC] wlan hotspot-policy 1
```

EAP-TLS 認証設定します。

```
[AC-wlan-hs-1] nai-realm name abc.com eap-method 6 auth-method 2 authentication 4
```

ドメイン名を abc.com に設定。

```
[AC-wlan-hs-1] domain-name abc.com
```

HESSID を 1232 ff23-0123 に設定します。

```
[AC-wlan-hs-1] hessid 1232-ff23-0123
[AC-wlan-hs-1] quit
```

2) 802.1X 認証および RADIUS スキーム設定:

802.1X 認証方式を EAP として設定します。

```
[AC] dot1x authentication-method eap
```

RADIUS スキーム imcc を作成します。

```
[AC] radius scheme imcc
```

プライマリー・認証・サーバの IP アドレスとポート番号をそれぞれ 10.18.1.88 と 1812 に設定します。

```
[AC-radius-imcc] primary authentication 10.18.1.88 1812
```

プライマリー・アカウンティング・サーバーの IP アドレスとポート番号をそれぞれ 10.18.1.88 と 1813 に設定します。

```
[AC-radius-imcc] primary accounting 10.18.1.88 1813
```

認証サーバおよびアカウンティングサーバとパケットを交換する AC の共有鍵を 12345678 に設定します。

AC を設定して、RADIUS サーバに送信されたユーザ名のドメイン名を削除します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

3) ドメイン imc を作成し、認証、許可、およびアカウンティングに RADIUS スキーム imcc を使用するようにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

IV. AP の設定

サービステンプレート service1 の作成。

```
<AC> system-view
[AC] wlan service-template service1
```

SSID を service に設定します。

```
[AC-wlan-st-service1] ssid service
```

Hotspot 2.0 ポリシー1 をサービステンプレートにバインドします。

```
[AC-wlan-st-service1] hotspot-policy 1
```

ビーコンおよびプローブ応答で RSN IE を有効にします。

```
[AC-wlan-st-service1] security-ie rsn
```

AES-CCMP cipher スイートをイネーブルにします。

```
[AC-wlan-st-service1] cipher-suite ccmp
```

認証および鍵管理モードを 802.1X に設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

WLAN クライアントの認証モードを 802.1X に設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

認証ドメインとしてドメイン imc を指定します。

```
[AC-wlan-st-service1] dot1x domain imc
```

サービステンプレートを有効にします。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

AP ap1 を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap ap1 model W1120
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#AP の無線 2 にサービステンプレートサービスをバインドします。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] service-template service1
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

V. RADIUS サーバの設定 (IMCv7)

この例は、IMC PLAT 7.1 および IMC UAM 7.1 で作成されました。

IMC サーバを設定するには、次の手順を実行します。

1) IMC プラットフォームにログインします。
2) [User] タブをクリックします。
3) アクセス装置を追加します。

a) ナビゲーションツリーから、[User Access Policy] > [Access Device Management] >

[Access Device] を選択します。

b)　アクセス装置の設定ページで、[Add] をクリックします。

c)　[Add Access Device] ページで、次のパラメータを設定します。

- 共有鍵を 12345678 に設定します。
- IP アドレス 10.18.1.1 (AC の IP アドレス) の装置を選択または手動で追加します。
- その他のパラメータはデフォルト設定を使用します。

d)　[OK]をクリックします。

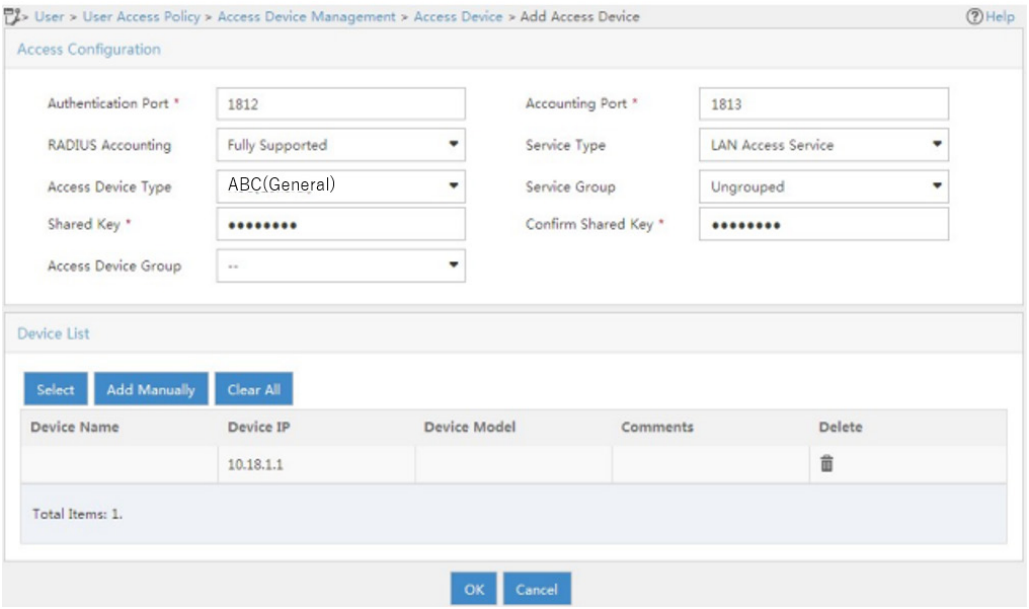


図 25-6 アクセス装置の追加図

4)　アクセスポリシーを追加します。

a)　ナビゲーションツリーから、[User Access Policy] > [Access Policy] を選択します。

b)　アクセス装置の設定ページで、[Add] をクリックします。

c)　[Add Access Policy] ページで、次のパラメータを設定します。

- アクセスポリシー名を 802.1X_policy に設定します。
- [Certificate Type] リストから [EAP-PEAP Authentication] を選択し、[Certificate Sub-Type] リストから、クライアントの認証方式と同じ証明書サブタイプを選択します。
- その他のパラメータにはデフォルト設定を使用します。

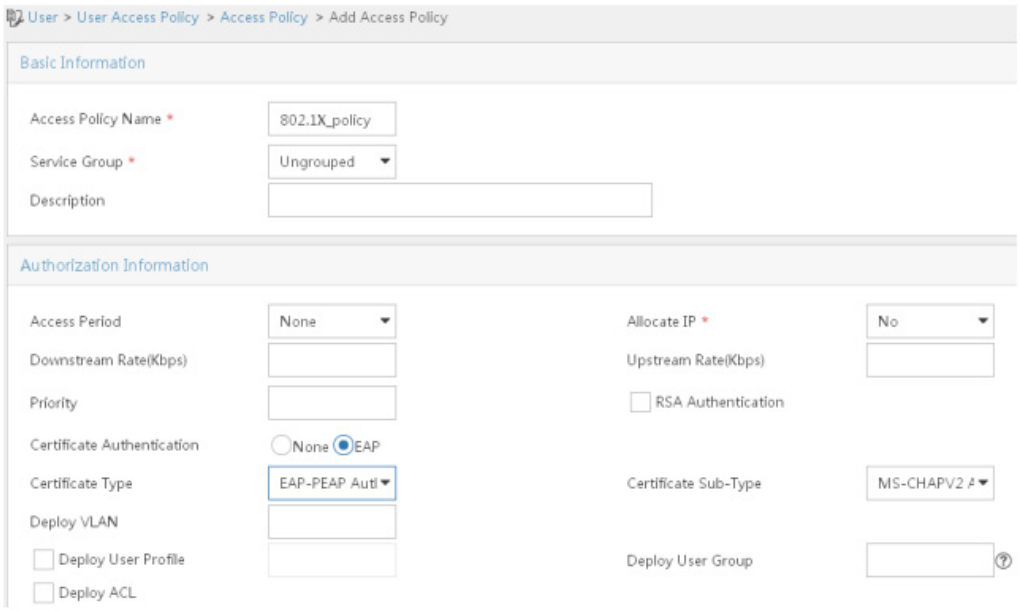


図 25-7 アクセスポリシーの追加図

5)　アクセスサービスを追加します。

a)　ナビゲーションツリーから、[User Access Policy] > [Access Service] を選択します。

b)　アクセスサービス設定ページで、[Add] をクリックします。

c)　[Add Access Service] ページで、サービス名を802.1X_serとして設定し、作成した802.1Xポリシーをデフォルトのアクセスポリシーとして使用します。

d)　その他のパラメータにはデフォルト設定を使用します。

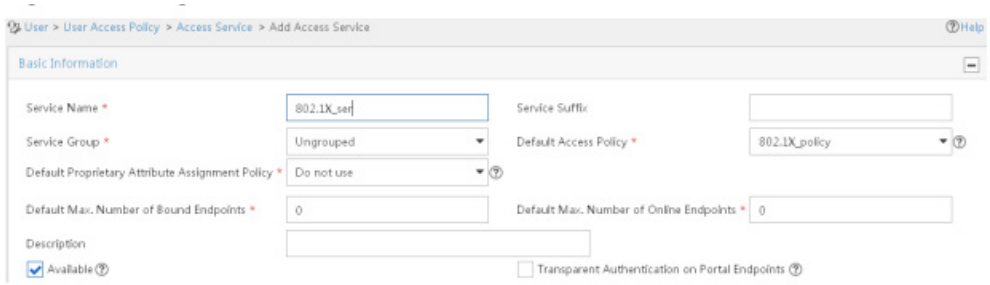


図 25-8 アクセスサービスの追加図

6)　アクセスユーザを追加します。

a)　ナビゲーションツリーから、[Access User] > [All Access Users] を選択します。

b)　アクセスユーザ 設定ページで、[Add] をクリックします。

c)　[Add Access User] ページで、[Add User] をクリックします。

d)　[Add User] ウィンドウで、次のパラメータを設定します。

- ユーザ名を admin に設定します。
- アカウント名を admin に設定します。
- [Access Service] 領域で設定した 802.1X ユーザを選択します。

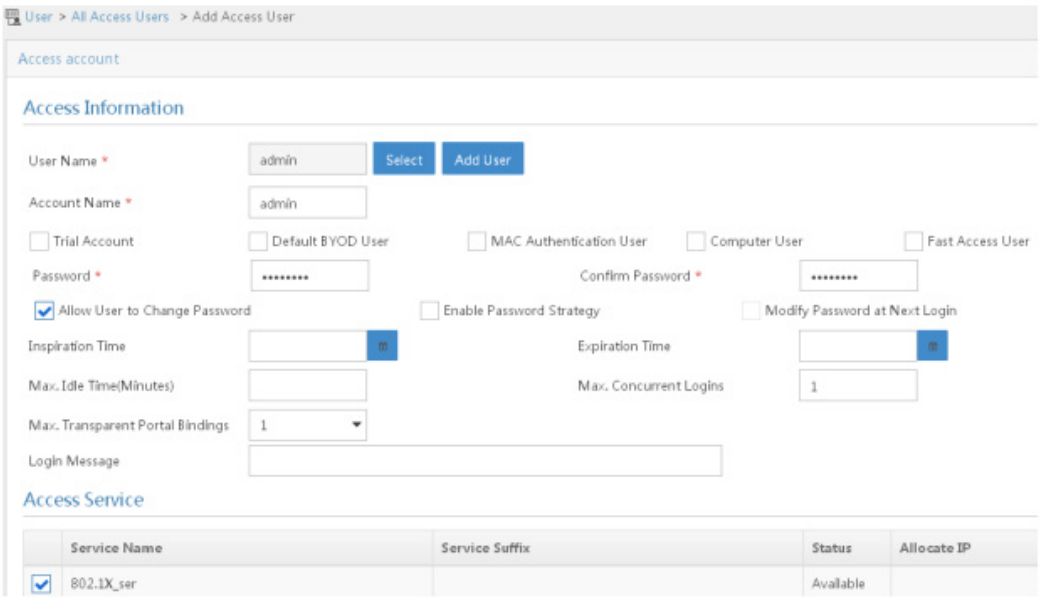


図 25-9 アクセスユーザの追加図

VI. 電話機の設定

この例は、iPhone 5S を使用して作成しました。

電話機を設定するには、次の手順を実行します。

1)　MacBook Air に Apple 設定 App をインストールし、iPhone 5S をラップトップに接続します。



図 25-10 設定アプリの適用図

2)　Apple Configurator アプリを開き、上部のメニューから [Supervise] を選択します。次に、リストの下にある [+] をクリックし、[Create New Profile] を選択します。

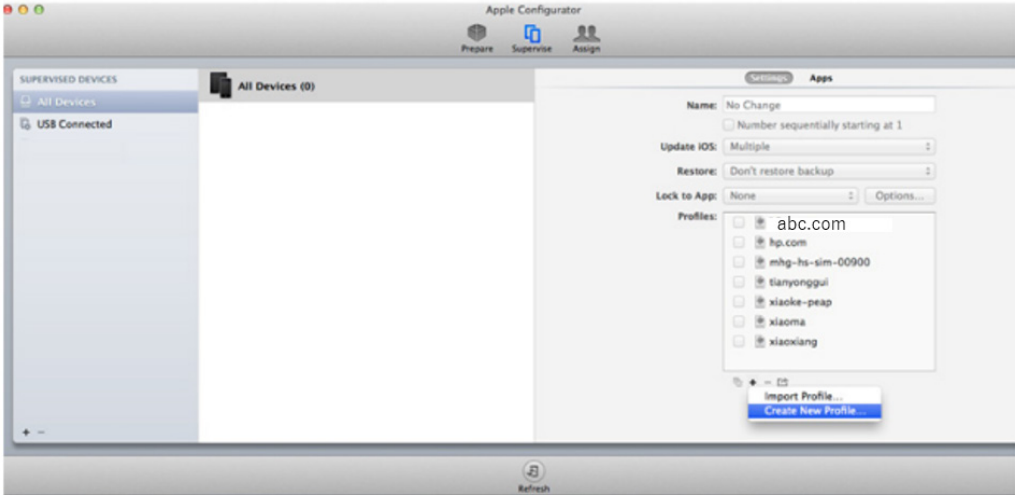


図 25-11 新しいプロファイルの作成図

3)　左側のナビゲーションツリーで [General] をクリックし、[Name] フィールドに「abc.com」と入力します。その他のパラメータは省略可能です。



図 25-12 General 設定図

4)　左側のナビゲーションツリーで [Wi-Fi] をクリックし、メニューから [Configure] をクリックします。次に、[Network Type] リストから [Passpoint] を選択します。



図 25-13 パスポイントの有効化図

5)　表示されるページで、次のタスクを実行します。

- [Accepted EAP Types] 領域で、[PEAP] を選択します。
- [Username] 領域と [Password] 領域にそれぞれ admin と 12345678 を入力します。
- [Identity Certificate] リストから [None] を選択します。
- [Outer Identity] 領域に admin と入力します。

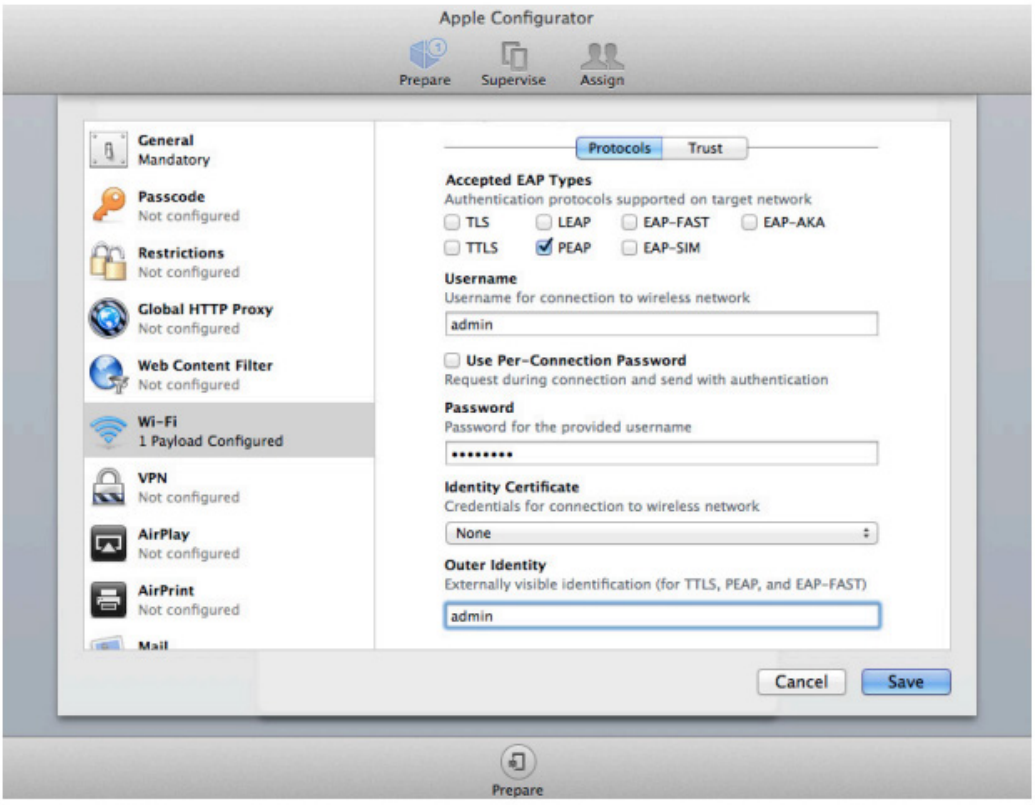


図 25-14 EAP-PEAP 認証の設定図

- [Provider Display Name] フィールドに「abc.com」と入力し、AC の Hotspot ポリシーで設定したドメイン名を入力します。

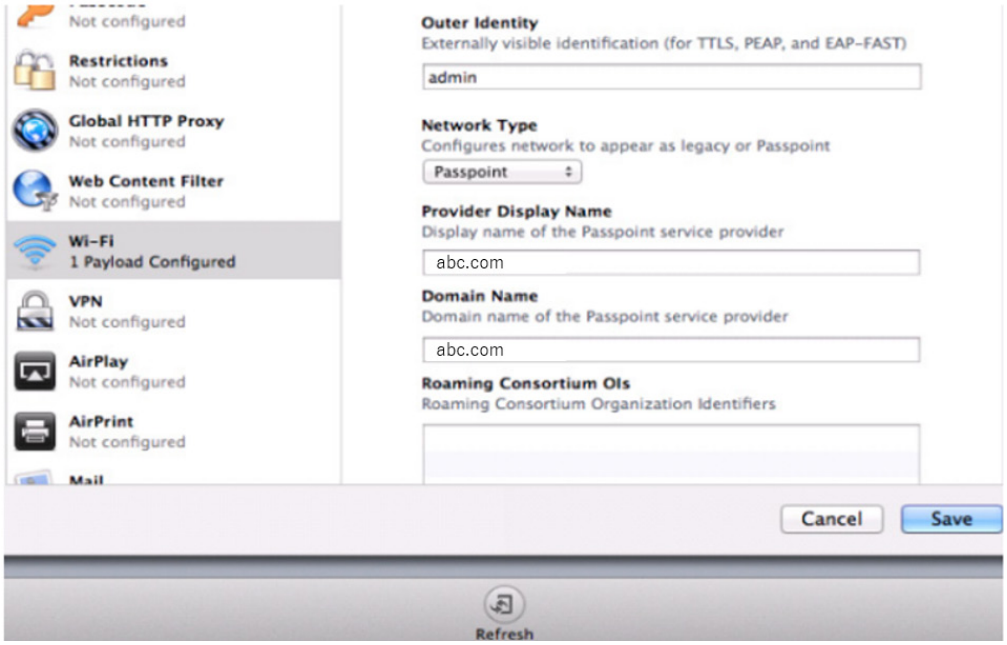


図 25-15 ドメイン名の設定図

- Roaming Consortium OIs (ローミングコンソーシアム)、NAI Real Names、および MCC/MNC を空白のままにするか、AC の Hotspot ポリシーで設定した値を入力します。次に、[Save] をクリックします。

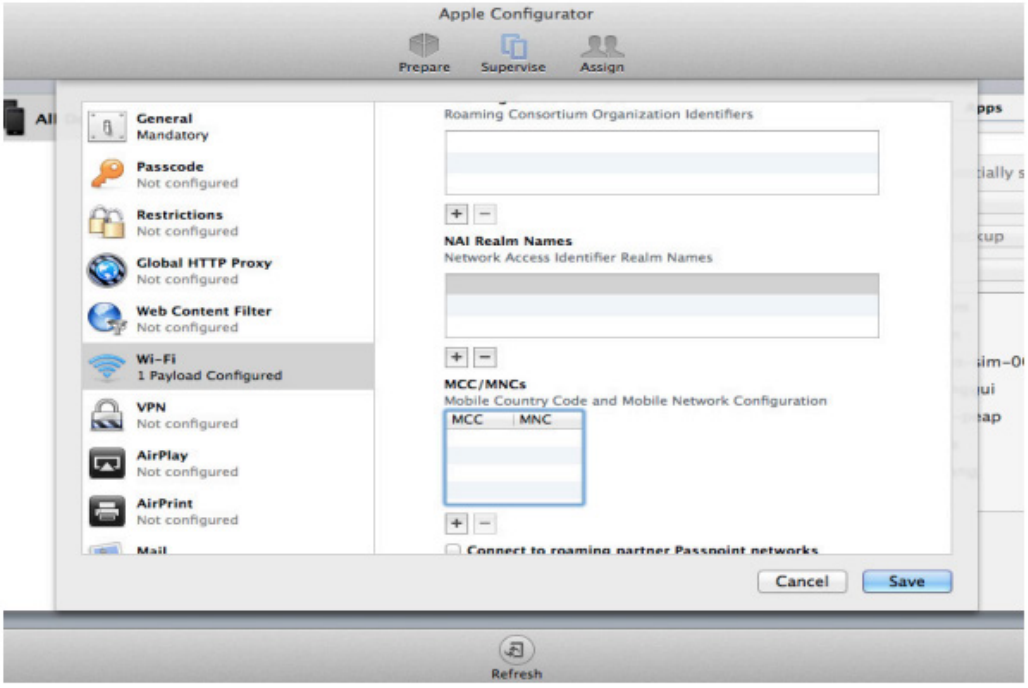


図 25-16 その他のオプションの設定図

6)　[Prepare] をクリックし、[Setting] タブの [Install Profiles…] をクリックします。

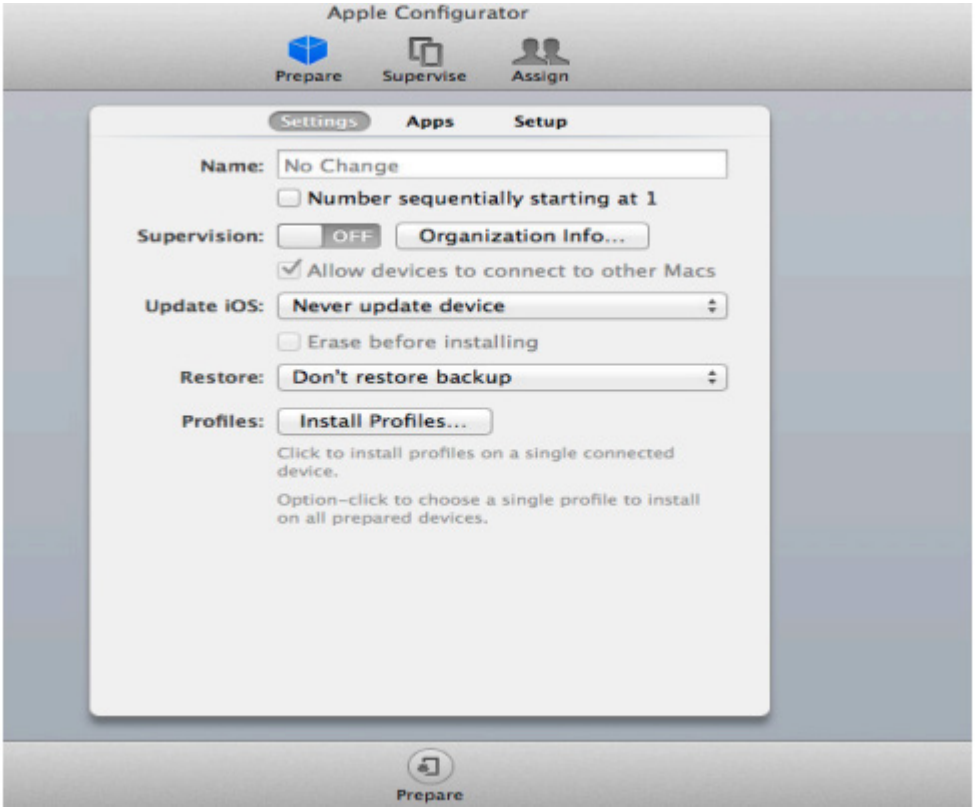


図 25-17 プロファイルのインストール図

7)　[Next] をクリックします。



図 25-18 プロファイルのインストール図

8)　プロファイル abc.com を選択し、[Next] をクリックします。

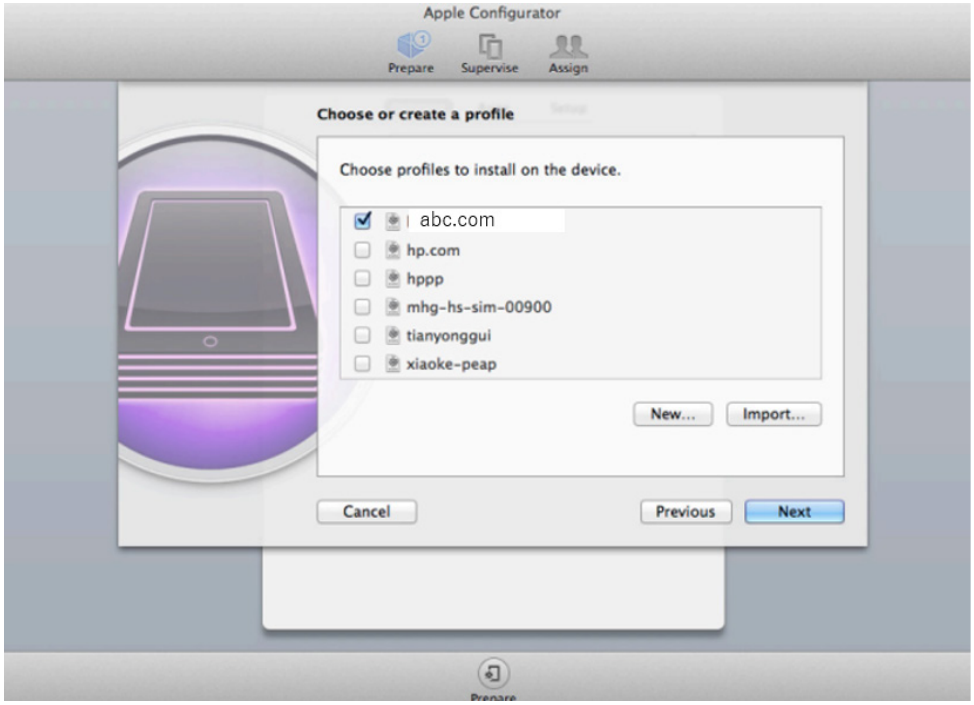


図 25-19 作成したプロファイルの選択

9)　[Install] をクリックします。



図 25-20 プロファイルのインストール図

インストールが完了すると、[Apple Configurator] ページに [Install Succeeded] と表示され、すべての設定が iPhone 5S に導入されます。電話機は必要なサービスを見つけると、自動的に WLAN に接続します。

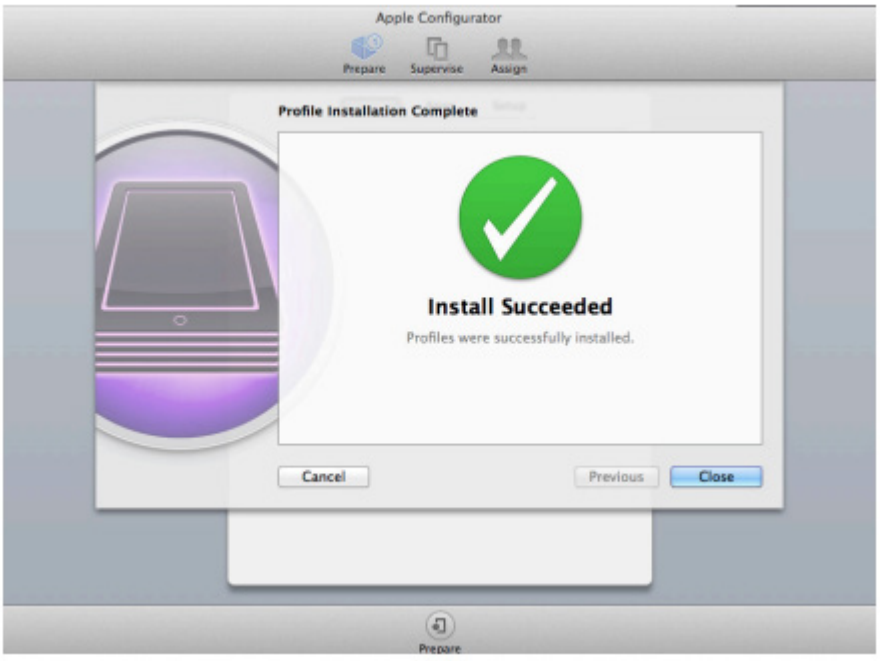


図 25-21 インストール完了図

VII. 設定の確認

#電話機が WLAN サービスに自動的に接続できることを確認します。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                    : 6021-c05d-19e0
IPv4 address                   :105.0.0.5
IPv6 address                   : N/A
Username                       : admin
AID                            : 1
AP ID                          : 2
AP name                        : ap1
Radio ID                       : 2
Channel                        : 36
SSID                                : service
BSSID                          : 70f9-6dd7-cfd0
VLAN ID                        : 1
Sleep count                    : 0
Wireless mode                  : 802.11gn
Channel bandwidth              : 20MHz
SM power save                  : Enabled
SM power save mode             : Static
Short GI for 20MHz             : Supported
Short GI for 40MHz             : Not supported
STBC RX capability             : Not supported
STBC TX capability             : Not supported
LDPC RX capability             : Not supported
Block Ack                      : TID 0 In
Support HT-MCS set             : 0, 1, 2, 3, 4, 5, 6, 7
Supported rates                : 1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps
QoS mode                       : WMM
Listen interval                : 10
RSSI                           : 49
Rx/Tx rate                     : 1/72.2 Mbps
Authentication method          : Open system
Security mode                  : RSN
AKM mode                       : 802.1X
Cipher suite                   : CCMP
```

User authentication mode	: 802.1X
WPA3 status	: N/A
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Authorization CAR	: N/A
Roam status	: N/A
Key derivation	: SHA1
PMF status	: N/A
Forwarding policy name	: N/A
Online time	: 0days 0hours 0minutes 36seconds
FT status	: Inactive

25.8.1 例:Hotspot 2.0 Samsung アプリケーションの設定

I. ネットワーク要件

図 24-22 に示すように、Hotspot 2.0 を設定して、電話機が携帯電話ネットワークからワイヤレスネットワークに切り替えられるようにします。

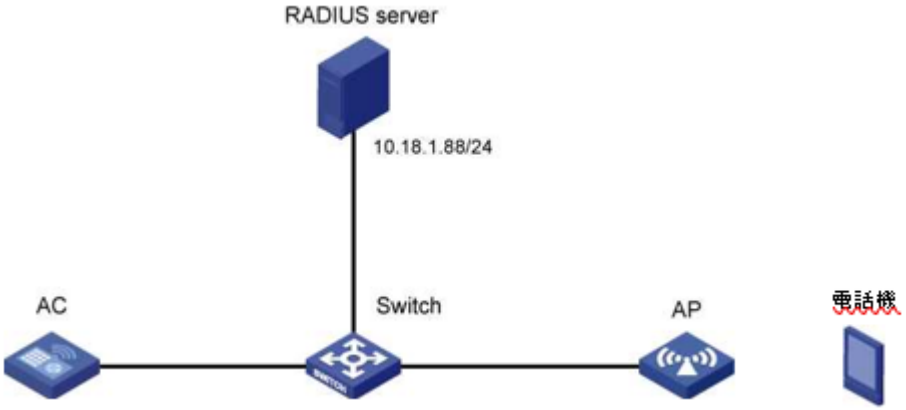


図 25-22 ネットワーク図

II. 前提条件

Hotspot 2.0 を設定する前に、次の作業を完了します。

- クライアントの認証、許可、アカウンティングを正しく動作させるには、RADIUS サーバに証明書をインストールし、ユーザアカウントを作成する必要があります。AAA の詳細は、オペレーションマニュアルのセクション 9 セキュリティ"*AAA*"の"*一般的に使われる標準 RADIUS 属性*"を参照してください。
- 802.1X にアクセスし、電話機に証明書をインストールします。

III. AC の設定

1)　Hotspot 2.0 ポリシーを設定します。

#Hotspot 2.0 ポリシーを作成します。

```
<AC>system-view
[AC] wlan hotspot-policy 1
```

#NAI レルム abc.com の認証タイプを設定する。

```
[AC-wlan-hs-1] nai-realm name abc.com eap-method 6 auth-method 2 authentication 4
```

ドメイン名を domain.abc.com に設定する。

```
[AC-wlan-hs-1] domain-name domain.abc.com
```

#HESSID を AP の MAC アドレスである 1232 ff23-0123 に設定します。

```
[AC-wlan-hs-1] hessid 1232-ff23-0123
[AC-wlan-hs-1] quit
```

2)　802.1X 認証および RADIUS スキーム:

#802.1X 認証方式を EAP として使用します。

```
[AC] dot1x authentication-method eap
```

#RADIUS スキーム imcc を作成します。

```
[AC] radius scheme imcc
```

プライマリー認証サーバの IP アドレスとポート番号それぞれを 10.18.1.88、1812 に設定します。

```
[AC-radius-imcc] primary authentication 10.18.1.88 1812
```

プライマリー・アカウンティング・サーバーの IP アドレスとポート番号をそれぞれ 10.18.1.88 と 1813 に設定します。

```
[AC-radius-imcc] primary accounting 10.18.1.88 1813
```

#認証サーバおよびアカウンティングサーバとパケットを交換する AC の共有鍵を 12345678 に設定します。

```
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
```

#AC を設定して、RADIUS サーバに送信されたユーザ名のドメイン名を削除します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

3)　ドメイン imc を作成し、認証、許可、およびアカウンティングに RADIUS スキーム imcc を使用するようにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

IV. AP の設定

#サービステンプレートサービスの作成。

```
<AC> system-view
[AC] wlan service-template service1
```

#SSID を service に設定する。

```
[AC-wlan-st-service1] ssid service
```

#Hotspot 2.0 ポリシー1 をサービステンプレートにバインドする。

```
[AC-wlan-st-service1] hotspot-policy 1
```

#ビーコンおよびプローブ応答で RSN IE を有効にする。

```
[AC-wlan-st-stname] security-ie rsn
```

#AES-CCMP cipher スイートをイネーブルにします。

```
[AC-wlan-st-service1] cipher-suite ccmp
```

#認証および鍵管理モードを 802.1X に設定します。

```
[AC-wlan-st-service1] akm mode dot1x
```

#WLAN クライアントの認証モードを 802.1X に設定します。

```
[AC-wlan-st-service1] client-security authentication-mode dot1x
```

#認証ドメインとしてドメイン imc を指定します。

```
[AC-wlan-st-service1] dot1x domain imc
```

#サービステンプレートを有効にする。

```
[AC-wlan-st-service1] service-template enable
[AC-wlan-st-service1] quit
```

#AP ap1 を作成し、AP モデルとシリアル ID を指定する。

```
[AC] wlan ap1 model W1120
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#サービステンプレート service1 を AR の無線 2 にバインドする。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap 1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] service-template service1
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

V. RADIUS サーバの設定 (IMCv7)

この例は、IMC PLAT 7.1 および IMC UAM 7.1 で作成されています。

IMC サーバを設定するには、次の手順を実行します。

1) IMC プラットフォームにログインします。
2) [User] タブをクリックします。
3) アクセス装置を追加します。

a) ナビゲーションツリーから、[User Access Policy] > [Access Device Management] > [Access Device] を選択します。

b) アクセス装置の設定ページで、[Add] をクリックします。

c) [Add Access Device] ページで、次のパラメータを設定します。

- 共有鍵を 12345678 に設定します。
- IP アドレス 10.18.1.1 (AC の IP アドレス) の装置を選択または手動で追加します。
- その他のパラメータにはデフォルト設定を使用します。

d) [OK] をクリックします。 [Accepted EAP Types] 領域で、[PEAP] を選択します。

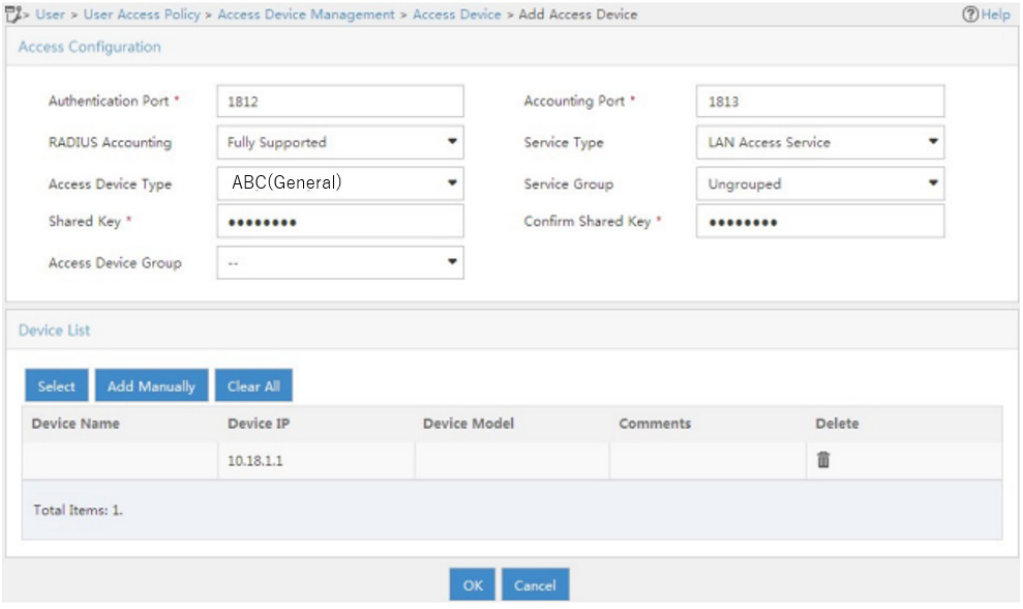


図 25-23 アクセス装置の追跡図

4) アクセスポリシーを追加します。

a) ナビゲーションツリーから、User Access Policy] > [Access Policy] を選択します。

b) アクセスポリシーの設定ページで、[Add] をクリックします。

c) [Add Access Policy] ページで、次のパラメータを設定します。

- アクセスポリシー名を 802.1X_policy に設定します。
- [Certificate Type] リストから [EAP-PEAP Authentication] を選択し、[Certificate Sub-Type] リストから、クライアントの認証方式と同じ証明書サブタイプを選択します。
- その他のパラメータにはデフォルト設定を使用します。

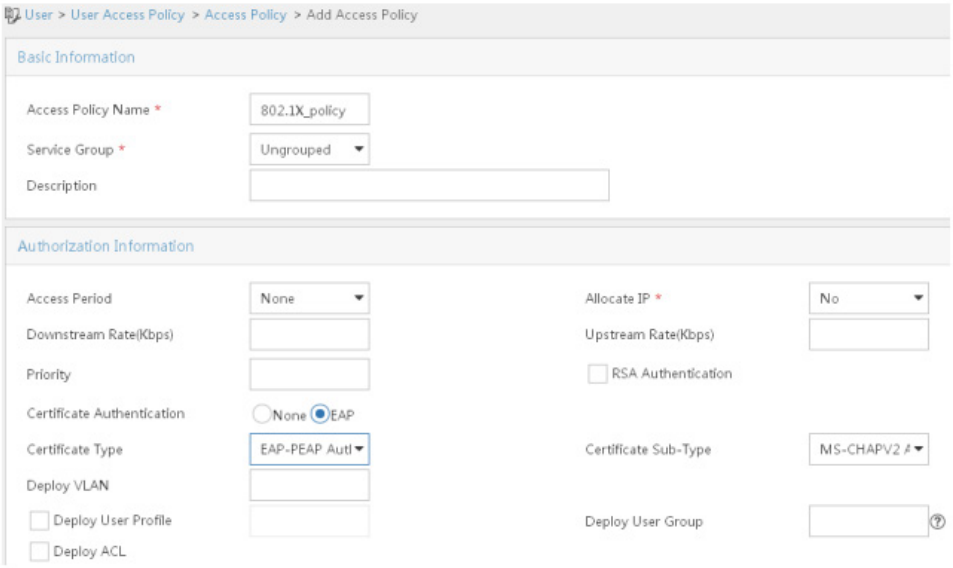


図 25-24 アクセスポリシーの追加図

5) アクセスサービスを追加します。

a) ナビゲーションツリーから、[User Access Policy] > [Access Service] を選択します。

b) アクセスサービス設定ページで、[Add] をクリックします。

c) [Add Access Service] ページで、サービス名を802.1X_serとして設定し、作成した802.1Xポリシーをデフォルトのアクセスポリシーとして使用します。

d) その他のパラメータにはデフォルト設定を使用します。

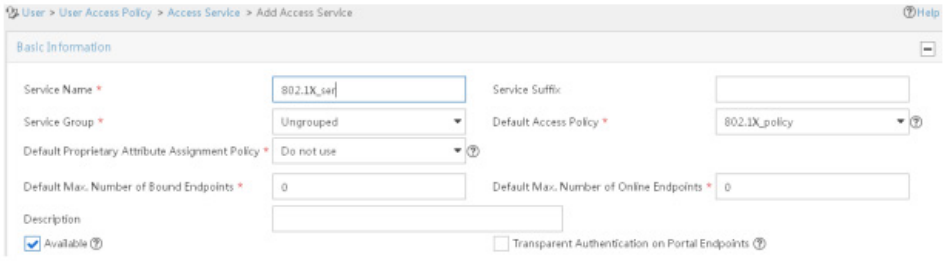


図 25-25 アクセスサービスの追加図

6)　アクセスユーザを追加します。

a)　ナビゲーションツリーから、[Access User] > [All Access Users] を選択します。

b)　アクセスユーザ 設定ページで、[Add] をクリックします。

c)　[Add Access User] ページで、[Add User] をクリックします。

d)　[ユーザの追加] 画面で、次のパラメータを設定します。

- ユーザ名を admin に設定します。
- アカウント名を admin に設定します。
- エリアで設定した 802.1X ユーザを選択します。

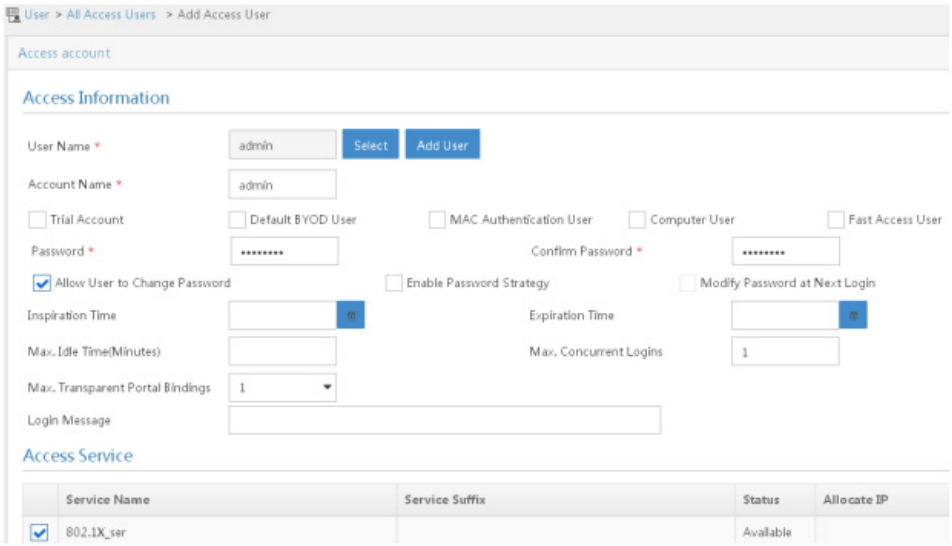


図 25-26 アクセスユーザの追加図

VI. 電話機の設定

重要：

- 電話機と AC の Hotspot 2.0 ポリシーの両方に同じレルム名とドメインを設定します。
- 設定電話機と RADIUS サーバの両方に同じユーザ名とパスワードを設定します。
- 設定では、電話機、AC の Hotspot 2.0 ポリシー、および RADIUS サーバに同じ認証タイプを使用します。

この例では、Samsung S4 電話機を使用します。

電話機を設定:

1)　テキストエディタを使用して Hotspot 2.0 設定ファイルを編集し、cred.conf という名前で PC または電話機に保存します。

```
cred={
realm="abc.com"
username="admin"
password="12345678"
```

domain="domain.abc.com"

eap=PEAP

phase2="auth=MSCHAPV2"}

2) 設定ファイルを電話機のルートディレクトリに保存します。

- PC で設定ファイルを編集する場合は、次のどちらかの方法で設定ファイルを電話機にインポートし、ルートディレクトリに保存します。
  - □ USB ケーブルを使用して電話機を PC に接続し、cred.conf を PC から電話機にコピーします。
  - □ cred.conf を添付した電子メールを電話機に送信し、ファイルを電話機に保存します。
- テキストエディタを使用して電話機でファイルを編集する場合は、電話機のルートディレクトリに保存します。

3) 電話機で WLAN をオンにします。



図 25-27 WLAN オン図

4) [Advanced] をクリックします。

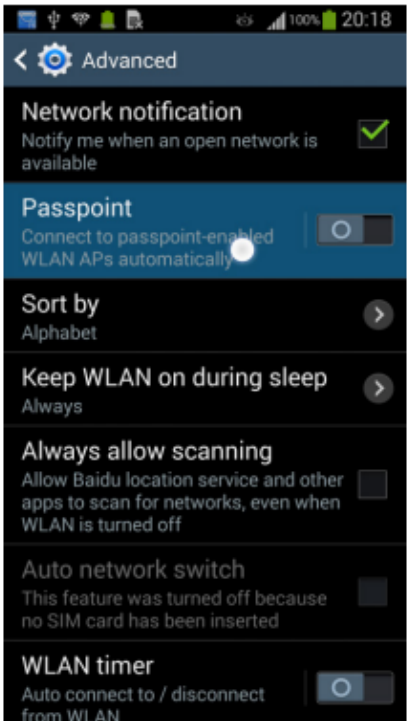


図 25-28 WLAN の詳細設定の構成図

5)　[Advanced] ページで、Passpoint を有効にします。



図 25-29 パスポイントの有効化図

VII. 設定の確認

#電話機が WLAN サービスに自動的に接続できることを確認します。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                    : 000f-e265-6400
IPv4 address                   : 10.1.1.114
IPv6 address                   : 2001::1234:5678:0102:0304
Username                       : admin
AID                            : 1
AP ID                          : 2
AP name                        : ap1
Radio ID                       : 2
Channel                        : 36
SSID                           : service
BSSID                          : 0026-3e08-1150
VLAN ID                        : 1
Sleep count                    : 0
Wireless mode                  : 802.11gn
Channel bandwidth              : 20MHz
SM power save                  : Enabled
SM power save mode             : Static
Short GI for 20MHz             : Supported
Short GI for 40MHz             : Not supported
STBC RX capability             : Not supported
STBC TX capability             : Not supported
LDPC RX capability             : Not supported
Block Ack                      : TID 0 In
Support HT-MCS set             : 0, 1, 2, 3, 4, 5, 6, 7
Supported rates                : 1, 2, 5.5, 6, 9, 11,
                                 12, 18, 24, 36, 48, 54 Mbps
QoS mode                       : WMM
Listen interval                : 10
RSSI                           : 49
Rx/Tx rate                     : 130/11 Mbps
Authentication method          : Open system
Security mode                  : RSN
AKM mode                       : 802.1X
```

Cipher suite	: CCMP
User authentication mode	: 802.1X
WPA3 status	: N/A
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Roam status	: N/A
Key derivation	: SHA1
PMF status	: N/A
Forwarding policy name	: N/A
Online time	: 0days 0hours 0minutes 36seconds
FT status	: Inactive

25.8.2 例:Hotspot 2.0 の設定 (バージョン 2 の場合)

I. ネットワーク要件

図 24-30 に示すように、Hotspot 2.0 を設定して、電話機がセルラーネットワークからワイヤレスネットワークに切り替えられるようにします。

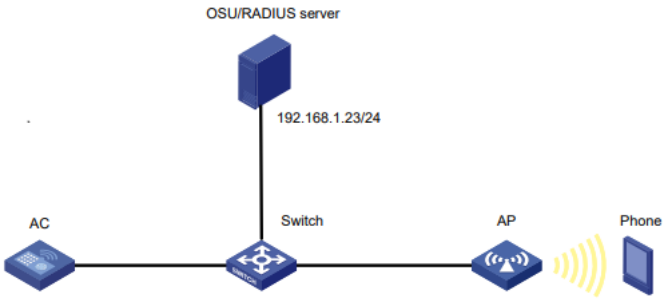


図 25-30 ネットワーク図

II. 設定の制限とガイドライン

Hotspot 2.0 を設定する場合は、次の設定の制限とガイドラインに従ってください。

1) AAA の詳細は、オペレーションマニュアルのセクション 9 セキュリティ"*AAA*"の"*一般的に使われる標準 RADIUS 属性*"を参照してください。
2) OSU サーバのアイコンをアップロードする前に、バージョンファイルが保存されているルートディレクトリにアイコンファイルがあることを確認します。FTP または TFTP を使用してアイコンファイルを送信できます。

III. 設定手順

1)　OSU サーバ設定:

#OSU サーバ 1 を作成します。

```
<AC>system-view
[AC] wlan osu-provider 1
```

#OSU サーバの名前を osu_test に設定します。

```
[AC-wlan-osu-1] friendly-name osu_test lang-code eng
```

#OSU サーバの URI を指定します。

```
[AC-wlan-osu-1] uri https://192.168.1.23:8088/service
```

#クライアントが OSU サーバと通信する際のプロトコルを SOAP-XML SPP に設定します。

```
[AC-wlan-osu-1] method 1
```

#OSU サーバのアイコンを指定します。

```
[AC-wlan-osu-1] icon-file test.png lang-code eng icon-type png
```

#設定 OSU サーバの説明。

```
[AC-wlan-osu-1] description "The OSU provider." lang-code eng
```

#NAI を設定します。

```
[AC-wlan-osu-1] nai example.com
[AC-wlan-osu-1] quit
```

2)　Hotspot 2.0 ポリシー設定:

#Hotspot の作成 2.0 ポリシー1。

```
[AC] wlan hotspot-policy 1
```

#NAI レルム example.com の認証タイプを指定します。

```
[AC-wlan-hs-1] nai-realm name example.com eap-method 5 auth-method 2 authentication 4
```

#アクセスネットワークタイプを「ワイルドカード」に設定します。

```
[AC-wlan-hs-1] network-type 15
```

#OI を 80F62E に設定し、ビーコンに OI を追加します。

```
[AC-wlan-hs-1] roam-oi 80F62E in-beacon
```

ドメイン名を domain.com に設定します。

```
[AC-wlan-hs-1] domain-name domain.com
```

#IPv4 アドレスおよび IPv6 アドレスの可用性を 1 に設定します。

```
[AC-wlan-hs-1] ip-type ipv4 1 ipv6 1
```

#オンラインサインアップサービスの SSID を osu-ssid に設定します。

```
[AC-wlan-hs-1] osu-ssid osu-ssid
```

#OSU サーバ 1 を Hotspot 2.0 ポリシー1 にバインドします。

```
[AC-wlan-hs-1] osu-provider 1
[AC-wlan-hs-1] quit
```

#指定したアイコンファイルが変更された場合、指定した OSU サーバのアイコンをアップロードする。

```
[AC] wlan hotspot osu-icon upload
```

3)　オンラインサインアップサービス用のサービステンプレート設定

#サービステンプレート osu を作成する。

```
[AC] wlan service-template osu
```

#SSID を osu-ssid に設定する。

```
[AC-wlan-st-osu] ssid osu-ssid
```

#サービステンプレートを有効にする。

```
[AC-wlan-st-osu] service-template enable
[AC-wlan-st-osu] quit
```

4)　802.1X 認証と RADIUS サーバ設定:

#設定 802.1X 認証方式を EAP として使用。

```
[AC] dot1x authentication-method eap
```

#RADIUS スキーム imcc を作成。

```
[AC] radius scheme imcc
```

プライマリー認証サーバの IP アドレスを「192.168.1.23」、ポート番号を「1813」に設定する。

```
[AC-radius-imcc] primary authentication 192.168.1.23 1812
```

プライマリーアカウンティングサーバの IP アドレスを「192.168.1.23」、ポート番号を「1813」に設定する。

```
[AC-radius-imcc] primary accounting 192.168.1.23 1813
```

#認証およびアカウンティングサーバとパケット交換する AC の共有鍵を「12345678」に設定する。

```
[AC-radius-imcc] key authentication simple 12345678
[AC-radius-imcc] key accounting simple 12345678
```

#AC を設定して、RADIUS サーバに送信されたユーザ名のドメイン名を削除します。

```
[AC-radius-imcc] user-name-format without-domain
[AC-radius-imcc] quit
```

5)　ISP ドメイン設定:

ドメイン imc を作成し、認証、許可、アカウンティングに RADIUS スキーム imcc を使用するようにドメインを設定します。

```
[AC] domain imc
[AC-isp-imc] authentication lan-access radius-scheme imcc
[AC-isp-imc] authorization lan-access radius-scheme imcc
[AC-isp-imc] accounting lan-access radius-scheme imcc
[AC-isp-imc] quit
```

6)　無線サービス用の設定サービステンプレート設定:

#サービステンプレート stname の作成。

```
[AC] wlan service-template stname
```

#SSID を service に設定する。

```
[AC-wlan-st-stname] ssid service
```

#Hotspot 2.0 ポリシー1 をサービステンプレートにバインドします。

```
[AC-wlan-st-stname] hotspot-policy 1
```

7)　AP 設定:

#AP ap1 を作成し、AP モデルとシリアル ID を指定します。

```
[AC] wlan ap1 model W1120
[AC-wlan-ap-ap1] serial-id 219801A28N819CE0002T
```

#AP の場所名を設定します。

```
[AC-wlan-ap-ap1] venue name "ABC lab" lang-code eng url
```

#サービステンプレート stname を AP の無線 2 にバインドする。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] radio enable
[AC-wlan-ap-ap1-radio-2] service-template stname
[AC-wlan-ap-ap1-radio-2] service-template osu
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

IV. 設定の確認

#OSU サーバアイコンがロードされていることを確認します。

```
[AC] display wlan hotspot uploaded-osu-icon
Total number of icons: 1
Icon name Icon type
test.png    png
```

#電話機が WLAN サービスに自動的に接続できることを確認します。

```
[AC] display wlan client verbose
Total number of clients: 1

MAC address                    : d022-bee8-a267
IPv4 address                   : 192.168.1.52
IPv6 address                   : N/A
Username                       : abcd
AID                            : 2
AP ID                          : 1
AP name                        : ap1
Radio ID                       : 2
Channel                        : 36
SSID                           : service
BSSID                          : 5866-ba74-e790
VLAN ID                        : 1
Sleep count                    : 37
Wireless mode                  : 802.11gn
Channel bandwidth              : 20MHz
SM power save                  : Disabled
Short GI for 20MHz             : Supported
Short GI for 40MHz             : Not supported
STBC RX capability             : Supported
STBC TX capability             : Not supported
LDPC RX capability             : Not supported
Block Ack                      : TID 0 Both
                                 TID 2 Out
Supported HT MCS set           : 0, 1, 2, 3, 4, 5, 6, 7
Supported rates                : 1, 2, 5.5, 6, 9, 11,
                                 12, 18, 24, 36, 48, 54 Mbps
QoS mode                       : WMM
Listen interval                : 10
RSSI                           : 45
Rx/Tx rate                     : 72.2/72.2 Mbps
Authentication method          : Open system
Security mode                  : RSN
AKM mode                       : 802.1X
```

Cipher suite	: CCMP
User authentication mode	: 802.1X
WPA3 status	: N/A
Authorization ACL ID	: N/A
Authorization user profile	: N/A
Authorization CAR	: N/A
Roam status	: N/A
Key derivation	: SHA1
PMF status	: N/A
Forwarding policy name	: N/A
Online time	: 0days 0hours 1minutes 29seconds
FT status	: Inactive