H3Cアクセスコントローラ
WLAN APの管理

New h3c Technologies Co.,Ltd.

http://www.h3c.com

Document version: 6W103-20200507 Product version: R5426P02

商標

注意

本書に記載されている情報は、予告なしに変更されることがあります。このドキュメントに記載されているすべての内容(記述、情報、推奨事項を含む)は、正確であると考えられますが、明示的であるか黙示的であるかを問わず、いかなる種類の保証もなく提供されています。H3Cは、本書に含まれている技術的または編集上の誤りまたは脱落に対して責任を負わないものとします。

内容

APの管理

概要

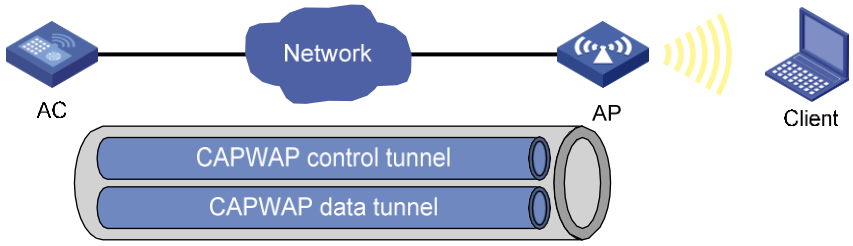
多数のAPの管理には時間とコストがかかります。適合するAP+ACネットワークアーキテクチャにより、ACは多数のAPを使用してControl And Provisioning of Wireless Access Points(CAPWAP)トンネルを確立し、APの管理とメンテナンスを一元化できます。

CAPWAPトンネル

CAPWAPは、APがACと通信する方法を定義します。APとAC間の一般的なカプセル化および転送メカニズムを提供します。CAPWAPはUDPを使用し、IPv4とIPv6の両方をサポートします。

図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のデータトンネルと、制御パケットを転送するための制御トンネルを確立します。

図1 CAPWAPトンネル



AC検出

0設定で起動した後、APは自動的にVLAN-interface1を作成し、インターフェイス上でDHCPクライアント、DHCPv6クライアント、およびDNS機能をイネーブルにします。次に、DHCPサーバーから自身のIPアドレスを取得し、次の方法を使用してACを検出します。

- 静的IPアドレス:

  APに対してAC IPアドレスが手動で設定されている場合、APは各AC IPアドレスにユニキャスト検出要求を送信してACを検出します。

- DHCPオプション:

  a. APは、DHCPサーバーから送信されたオプション138、オプション43からAC IPv4アドレスを取得し、オプション52からIPv6アドレスを取得します。これらのアドレスは降順で使用されます。

  b. APは、受信した各ACアドレスにユニキャストディスカバリ要求を送信して、ACを検出します。

  DHCPオプションの詳細については、『Layer3IP Services Configuration Guide』を参照してください。

- DNS:

  a. APは、DHCPサーバーからドメイン名のサフィックスを取得します。

  b. APによってホスト名にサフィックスが追加されます。

  c. DNSサーバーはドメイン名をIPアドレスに変換します。

  d. APは各IPアドレスにユニキャスト検出要求を送信して、ACを検出します。DNSの詳細については、『Layer3IP Services Configuration Guide』を参照してください。

- ブロードキャスト:

  APはディスカバリ要求をIPアドレス255.255.255.255にブロードキャストして、ACを検出します。

- IPv4マルチキャスト:

  APはIPv4アドレス224.0.1.140にマルチキャストディスカバリ要求を送信して、ACを検出します。

- IPv6マルチキャスト:

  APはIPv6アドレスFF0E::18Cにマルチキャストディスカバリ要求を送信して、ACを検出します。

静的IPアドレス、DHCPv4オプション、ブロードキャスト、IPv4マルチキャスト、IPv4DNS、IPv6マルチキャスト、DHCPv6オプション、およびIPv6DNSの各方式は、降順で使用されます。

APは、検出されたACのいずれかとのCAPWAPトンネルを確立するまで、AC検出を停止しません。

CAPWAPトンネルの確立

図2 CAPWAPトンネルの確立

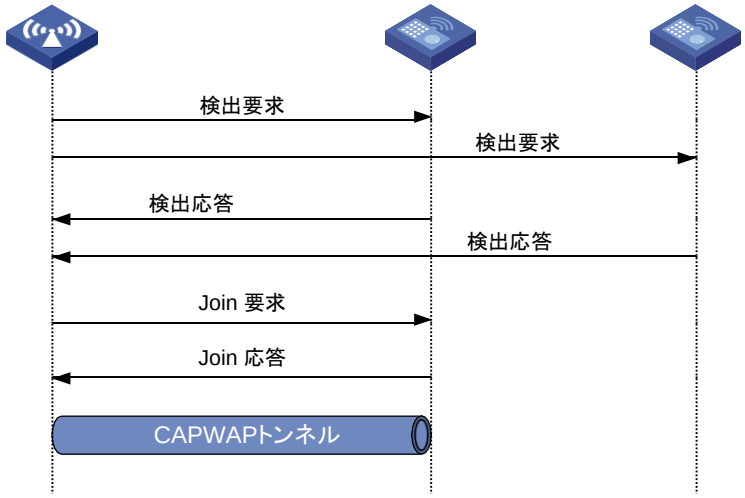


図2に示すように、APとACは、次の手順を使用してCAPWAPトンネルを確立します。

1. APは各ACにディスカバリ要求を送信して、ACを検出します。
2. ACは、ディスカバリ要求を受信すると、次の手順を実行して、ディスカバリ応答を送信するかどうかを決定します。

   a. ディスカバリ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。
- ブロードキャストパケットまたはマルチキャストパケット: ユニキャストディスカバリ要求だけに応答する機能によってディセーブルになっている場合、ACはステップbに進みます。この機能がイネーブルの場合、ACはディスカバリ応答を送信しません。

b. 検出要求で指定されたAPモデルの手動AP設定があるかどうかを識別します。

- 手動AP構成が存在する場合、ACはAPに対して検出応答を送信します。検出応答には、ACがAPの手動構成を持っているかどうか、AP接続優先度およびACの負荷ステータスに関する情報が含まれます。
- 手動AP構成が存在しない場合、ACはステップcに進む。

c. 自動APがイネーブルであるかどうかを示します。

- 自動APが有効な場合、ACはAPに対して検出応答を送信します。検出応答には、自動APの有効化ステータス、AP接続優先度およびACの負荷情報が含まれます。
- 自動APがディセーブルの場合、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は降順で最適なACを選択します。

- APに関する情報を保存するAC。
- 自動AP機能がイネーブルになっているAC。
- AP接続プライオリティの高いAC。
- 負荷の軽いACです。

4. APは、最適なACにJoin要求を送信します。

5. 加入要求を受信した後、ACは要求内の情報を調べて、アクセスサービスをAPに提供するかどうかを決定し、加入応答を送信します。

6. 加入応答を受信した後、APは応答の結果コードを調べます。

- 結果コードが障害を示す場合、APはACとの間にCAPWAPトンネルを確立しません。
- 結果コードが成功を示す場合、APはACとの間にCAPWAPトンネルを確立します。

AC再検出

AC再検出がイネーブルになっているACは、APに送信された検出応答にCAPWAP Control IP Addressメッセージ要素を追加します。このような検出応答を受信すると、APは次の手順に従ってCAPWAPトンネルを確立します。

1. CAPWAP Control IP Addressメッセージ要素で指定されたIPアドレスにディスカバリ要求が送信されたかどうかを調べます。

2. 次のいずれかの操作を実行します。

- ディスカバリ要求が送信された場合に、CAPWAPの確立に最適なACを表す指定のIPアドレスに加入要求を送信します。
- 検出要求が送信されていない場合は、指定された各IPアドレスに検出要求を送信して、新

しいAC検出プロセスを開始します。

AC再検出で無効化されたACは、APに送信される検出応答にCAPWAP Control IP Addressメッセージ要素を追加しません。検出応答を受信したAPは、ACとのCAPWAPトンネルを確立するために、検出応答の送信元IPアドレスにJoin要求を送信します。

APの設定方法

APを設定するには、次のいずれかの方法を使用します。

- APビューでAPを1つずつ設定します。
- APをAPグループに割り当て、APグループビューでAPグループを設定します。
- すべてのAPをグローバルコンフィギュレーションビューで設定します。

APの場合、APビュー、APグループビュー、およびグローバルコンフィギュレーションビューでの設定の優先順位は降順です。

APDB

ACのAccess Point Information Database(APDB)には、次のAP情報が格納されます。

- APモデル。
- ハードウェアバージョンとソフトウェアバージョンのマッピング。
- APモデルでサポートされる無線に関する情報。
  - 無線の数。
  - 無線タイプ。
  - 有効なリージョンコード。
  - 有効なアンテナのタイプ。
  - 最大伝送パワー。

ACがAPとのCAPWAPトンネルを確立できるのは、APDBに対応するAPモデル情報が含まれている場合だけです。

システムスクリプトおよびユーザースクリプトを使用して、APDB内のデータを管理できます。システムスクリプトはACソフトウェアバージョンとともにリリースされ、ACが起動するたびに自動的にロードされます。新しいAPモデルを追加する必要がある場合は、ACソフトウェアバージョンをアップグレードするか(『Fundamentals Configuration Guide』を参照)、ユーザースクリプトを作成してACにロードします(「APDBユーザースクリプトのロード」を参照)。

プロトコルおよび標準

- RFC5415『Control And Provisioning of Wireless Access Points(CAPWAP)Protocol Specification』
- RFC5416『Control and Provisioning of Wireless Access Points(CAPWAP)Protocol Binding for IEEE802.11』
- RFC5417『Control And Provisioning of Wireless Access Points(CAPWAP)Access Controller DHCP Option』

構成タスクリスト

タスクの概要
(必須)。CAPWAPトンネル確立の設定
(オプション)AC再検出の設定
(オプション)APのソフトウェアのアップグレード
(オプション)APのVLANの設定
(オプション)CAPWAPトンネルの設定
(オプション)AC要求再送信の設定
(オプション)統計情報レポート間隔の設定
(オプション)リモートAPの設定
(オプション)デフォルトの入力電力レベルの設定
(オプション)APのUSBインターフェイスのイネーブル化またはディセーブル化
(オプション)APのリセット
(オプション)手動APの名前の変更
(オプション)APのファイルシステムの管理
(オプション)APインターフェイスの管理
(オプション)APグループの設定
(オプション)APの事前プロビジョニング
(オプション)SNMP通知のイネーブル化
(オプション)APDBユーザースクリプトのロード

構成の前提条件

APを管理する前に、次の作業を完了してください。

- DHCPサーバー上にDHCPアドレスプールを作成して、IPアドレスをAPに割り当てます。
- DHCPオプションをAC検出に使用する場合は、DHCPサーバー上の指定されたDHCPアドレスプールでオプション138、オプション43、またはオプション52を構成します。
- DNSがAC検出に使用される場合は、DHCPサーバー上の指定されたDHCPアドレスプールにDNSサーバーのIPアドレスおよびACドメイン名接尾辞を構成します。次に、DNSサーバー上のドメイン名

とAC IPアドレス間のマッピングを構成します。

- APとACが相互に到達できることを確認します。

DHCPおよびDNSの詳細については、Layer3IP Services Configuration Guideを参照してください。

CAPWAPトンネルの確立の設定

手動APの作成

使用しているAPのAPモデル、シリアルID、およびMACアドレスに従って、AC上に手動APを作成できます。APは、手動AP設定を保存するACを使用してCAPWAPトンネルを確立することを希望します。

手動APを作成する手順は、次のとおりです。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.手動APを作成し、そのビューます。	**wlan ap** *ap-name* [**model** *model-name*]	デフォルトでは、手動APは存在しません。 APを作成する場合は、モデル名を指定する必要があります。
3.APのシリアルIDまたはMACアドレスを指定します。	• APのシリアルIDを指定します。 **serial-id** *serial-id* • APのMACアドレスを指定します。 **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)APの説明を設定します。	**description** *text*	デフォルトでは、APの説明は設定されていません。

自動APの管理

自動AP機能を使用すると、手動でAPを設定しなくてもAPをACに接続できます。ACはMACアドレスによって自動APに名前を付けます。この機能により、WLANに多数のAPを配置する場合の設定が簡素化されます。

自動AP機能のイネーブル化

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.自動AP機能を有効にします。	**wlan auto-ap enable**	デフォルトでは、自動AP機能はディセーブルです。

自動APから手動APへの変換

次の理由により、自動APをオンラインにした後で手動APに変換する必要があります。

- 自動AP設定を変更できるのは、手動APに変換された場合だけです。
- セキュリティ上の理由から、自動APは、手動APに変換された場合に限り、ACリブートまたはCAPWAPトンネルの終了時にACと再関連付けることができます。

自動APを手動APに変換する手順は、次のとおりです。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.自動APを手動APに変換します。	• オンライン自動APを手動APに変換します。 **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後、自動APを手動APに自動的に変換します。 **wlan auto-persistent enable**	いずれかのコマンドを使用します。 デフォルトでは、自動APは手動APに変換されません。 **wlan auto-persistent enable**コマンドは、すでにオンラインになっている自動APには適用されません。

AC電源のAP接続優先度を設定する

ACは、検出応答でAP接続の優先順位を設定します。次のいずれかの条件が存在する場合、APは、より高い接続優先順位を持つACとともにCAPWAPトンネルを確立することを選択します。

- 複数のACには、AP用の手動AP設定があります。
- ACにはAP用の手動AP設定はありませんが、自動AP機能によって複数のACがイネーブルになります。

APビューでのAP接続優先順位の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2. APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.ACのAP接続優先度を設定します。	**Priority** *prioroty*	デフォルトでは、APはAPグループビュー内の設定を使用します。 数値が大きいほど、優先度が高くなります。

APグループビューでのAP接続優先順位の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.ACのAP接続優先度を設定します。	**Priority** *prioroty*	デフォルト設定は4です。 数値が大きいほど、優先度が高くなります。

ACがユニキャスト検出要求にのみ応答できるようにする

APは、ユニキャスト、マルチキャスト、およびブロードキャストの検出要求を送信して、ACを検出できます。この機能により、ACはユニキャスト検出要求にのみ応答できます。

ACがユニキャスト検出要求だけに応答できるようにするには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.ACがユニキャスト検出要求にのみ応答できるようにします。	**wlan capwap discovery-policy unicast**	デフォルトでは、ACはユニキャスト、マルチキャスト、およびブロードキャストのディスカバリ要求に応答できます。

AC再検出の設定

APビューでのAC再検出の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** ap-name [**model** *model-name*]	該当なし
3.AC再検出を設定します。	**control-address { disable | enable }**	デフォルトでは、APはAPグループビューの設定を使用します。APグループビューに設定が存在しない場合、APはグローバルコンフィギュレーションビューの設定を使用します。
4.CAPWAP Control IP Addressメッセージで伝送されるIPアドレスを指定します。	**control-address** { **ip** *ipv4-address* | **ipv6** *ipv6-address* }	デフォルトでは、APはAPグループビューの設定を使用します。APグループビューに設定が存在しない場合、APはグローバルコンフィギュレーションビューの設定を使用します。 CAPWAP Control IP Addressメッセージ要素に追加するIPv4またはIPv6アドレスは、最大3つまで指定できます。

APグループビューでのAC再検出の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group group-name**	該当なし
3.AC再検出を設定します。	**control-address { disable | enable }**	デフォルトでは、APはグローバルコンフィギュレーションビューの設定を使用します。
4.CAPWAP Control IP Addressメッセージで伝送されるIPアドレスを指定します。	**control-address** { **ip** *ipv4-address* | **ipv6** *ipv6-address* }	デフォルトでは、APはグローバルコンフィギュレーションビューの設定を使用します。 CAPWAP Control IP Addressメッセージ要素に追加するIPv4またはIPv6アドレスは、最大3つまで指定できます。

グローバルコンフィギュレーションビューでのAC再検出の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.グローバルコンフィギュレーションビューを開始します。	**Wlan global-configuration**	該当なし
3.AC再検出を設定します。	**control-address { disable | enable }**	デフォルトでは、AC再検出はディセーブルです。
4.CAPWAP Control IP Addressメッセージで伝送されるIPアドレスを指定します。	**control-address** { **ip** *ipv4-address* | **ipv6** *ipv6-address*}	デフォルトでは、エレメント内のアドレスはACのIPアドレスです。 CAPWAP Control IP Addressメッセージ要素に追加するIPv4またはIPv6アドレスは、最大3つまで指定できます。

APのソフトウェアのアップグレード

概要

APのソフトウェアアップグレードは、次のように行われます。

1. APは、ソフトウェアバージョンおよびAPモデル情報をACに報告します。
2. ACは、受信したAPソフトウェアバージョンを検査します。
   - 一致が見つかった場合、ACはAPとの間にCAPWAPトンネルを確立します。
   - 一致が見つからない場合、ACは、APソフトウェアバージョンの不一致をAPに通知するメッセ

ージを送信します。

3. 不整合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. ACは要求を受信した後、ソフトウェアバージョンをAPに割り当てます。
5. APはソフトウェアバージョンをアップグレードし、を再起動してACとのCAPWAPトンネルを確立します。

ソフトウェアアップグレードの構成

ACは、ソフトウェアアップグレードがイネーブルの場合にのみ、CAPWAPトンネルの確立中にAPソフトウェアバージョンを検査します。この機能がディセーブルの場合、ACはAPのソフトウェアバージョンを検査せず、APと直接CAPWAPトンネルを確立します。

APビューでのソフトウェアアップグレードの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.ソフトウェアのアップグレードを構成します。	**firmware-upgrade { disable enable }**	デフォルトでは、APはAPグループビューの設定を使用します。APグループビューにソフトウェアアップグレード設定が存在しない場合、APはグローバルコンフィギュレーションビューの設定を使用します。

APグループビューでのソフトウェアアップグレードの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**Systtem-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.ソフトウェアのアップグレードを構成します。	**firmware-upgrade { disable enable }**	デフォルトでは、APはグローバルコンフィギュレーションビューの設定を使用します。

グローバルコンフィギュレーションビューでのソフトウェアアップグレードの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.グローバルコンフィギュレーションビューを開始します。	**Wlan global-configuration**	該当なし
3.ソフトウェアのアップグレードを構成します。	**firmware-upgrade { disable enable }**	デフォルトでは、ソフトウェアアップグレード機能はイネーブルになっています。

APモデルのソフトウェアバージョンとハードウェアバージョン間のマッピングの設定

△ 注意

CAPWAPトンネルの確立障害を回避するには、H3Cサポートのガイダンスに従ってこの機能を使用します。

ソフトウェアアップグレード用のAPモデルのソフトウェアバージョンとハードウェアバージョン間のマッピングを設定するには、次の作業を実行します。

この作業は、APDBに格納されているAPモデルのAPソフトウェアバージョンが、APモデルに対して予想されるソフトウェアバージョンと一致しない場合にのみ実行してください。APDB内の各APモデルのAPソフトウェアバージョンを表示するには、display wlan ap-modelコマンドを使用します。

たとえば、APDBにはAPモデルWA4320i-CAN用のハードウェアバージョンとソフトウェアバージョンのマッピングエントリ(ハードウェアバージョンVer.CおよびソフトウェアバージョンE2108)があります。このAPがオンラインになったときにソフトウェアバージョンE2105を使用すると予想される場合は、次の手順を実行します。

1. APモデルWA4320i-ACNのソフトウェアバージョンE2105とハードウェアバージョンVer.C間のマッピングを設定します。
2. ソフトウェアバージョンE2105のAPイメージファイルをACのローカルフォルダに保存します。
3. ローカルフォルダに格納されているAPイメージファイルを優先してソフトウェアバージョンを割り当てるように、ACを設定します。

APモデルのソフトウェアバージョンとハードウェアバージョン間のマッピングを設定するには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APモデルのソフトウェアバージョンとハードウェアバージョン間のマッピングを設定します。	**wlan apdb** *model-name hardware-version software-version*	デフォルトでは、APモデルのハードウェアバージョンのソフトウェアバージョンは、APDBユーザースクリプトに格納されるソフトウェアバージョンです。

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

CAPWAPトンネルの確立中にAPが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のRAMまたはローカルフォルダとして優先ロケーションを指定して、APイメージファイルを取得できます。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。

設定に関する制限事項とガイドライン

ACがAPイメージファイルを取得するための優先イメージロケーションを指定する場合は、次の制約事項およびガイドラインに従ってください。

- ACは、.ipe APイメージファイルだけを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 CFカードをデフォルトのファイルシステムとして使用し、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格納されていることを確認します。

設定手順

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には、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.ACがAPイメージファイルを取得する優先的な場所を指定します。	**wlan image-load filepath { local | ram }**	デフォルトでは、ACはソフトウェアバージョンをAPに割り当てるときに、RAMに格納されているAPイメージファイルを優先します。

オンラインAPへイメージファイルを適用する

オンラインApへイメージを適用するについて

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をリブートします。

設定手順

1. システムビューに入ります。
   <H3C> **System-view**
2. 全てのオンラインAPにイメージファイルを適用する。
   [H3C] **wlan ap-image-deploy**

APのVLANの設定

注:
この機能のサポートは、APモデルによって異なります。

ACがパケット転送および隔離のためにAPにVLAN設定を割り当てることができるようにするには、次の作業を実行します。たとえば、クライアントデータトラフィックを転送するようにAPをイネーブルにする場合、異なるVLANからのクライアント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の詳細については、『Layer2LAN Switching Configuration Guide』を参照してください。クライアントデータトラフィックフォワーダの設定については、「Configuring WLAN access」を参照してください。

基本VLAN設定の構成

APビューでの基本VLAN設定の構成

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.(オプション)VLANを作成してそのビューに入るか、VLANのリストを作成します。	**Vlan** { *vlan-id1* [**to** *vlan-id2*] **all** }	デフォルトでは、VLAN1(システムのデフォルトVLAN)だけが存在します。
4.VLANビューに入ります。	**vlan vlan-id**	VLANのリストを作成する場合は必須です。
5.VLANに名前を割り当てます。	**name** *text*	デフォルトでは、APはAPグループビュー内の設定を使用します。
6.VLANの説明を設定します。	**description** *text*	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループビューでの基本VLAN設定の指定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group group-name**	該当なし
3.(オプション)VLANを作成してVLANのリストを表示または作成します。	**Vlan** { *vlan-id1* [**to** *vlan-id2*] すべて}	デフォルトでは、VLAN1(システムのデフォルトVLAN)だけが存在します。
4.VLANビューに入ります。	**vlan vlan-id**	VLANのリストを作成する場合は必須です。

5.VLANに名前を割り当てます。	**name** *text*	デフォルトでは、VLANの名前はVLAN vlan-idです。vlan-id引数には、VLAN IDを4桁の形式で指定します。VLAN IDが4桁未満の場合は、先行ゼロが追加されます。たとえば、VLAN100の名前はVLAN0100です。
6.VLANの説明を設定します。	**description** *text*	デフォルトでは、VLANの説明はVLAN vlan-idです。vlan-id引数には、VLAN IDを4桁の形式で指定します。VLAN IDが4桁未満の場合は、先行ゼロが追加されます。たとえば、VLAN100のデフォルトの説明はVLAN0100です。

ポートベースVLANの設定

VLANへのアクセスポートの割り当て

APのレイヤ2イーサネットインターフェイスビューでアクセスポートをVLANに割り当てるには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [*model model-name*]	該当なし
3.レイヤ2イーサネットインターフェイスビューに入ります。	• GigabitEthernetインターフェイスビューに入ります。 **gigabitethernet** *interface-number* • Smarterateイーサネットインターフェイスビューに入ります。 **Smartrate-ethernet** *interface-number*	APモデルおよびネットワーク要件に従って、いずれかのコマンドを使用します。
4.リンクタイプをaccessに設定します。	**Port link-type access**	デフォルトでは、ポートはAPグループのレイヤ2イーサネットインターフェイスビューの設定を使用します。
5.アクセスポートをVLANに割り当てます。	**port access vlan** *vlan-id*	デフォルトでは、アクセスポートはAPグループのレイヤ2イーサネットインターフェイスビューの設定を使用します。

アクセスポートをAPグループのレイヤ2イーサネットインターフェイスビュー内のVLANに割り当てるには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group group-name**	該当なし
3.APモデルビューに入ります。	**ap-model ap-model**	該当なし
4.レイヤ2イーサネットインタフェースビューに入ります。	• GigabitEthernetインターフェイスビューに入ります: **gigabitethernet** interface-number • Smarterateイーサネットインターフェイスビューに入ります。 **smartrateイーサネット** • interface-number	APモデルおよびネットワーク要件に従っていずれかのコマンドを使用します。
5.リンクタイプをaccessに設定します。	**Port link-type access**	デフォルトでは、すべてのポートがアクセスポートです。
6.アクセスポートをVLANに割り当てます。	**Port access vlan** *vlan-id*	デフォルトでは、アクセスポートはVLAN1に属します。

トランクポートのVLANへの割り当て

APのレイヤ2イーサネットインターフェイスビューでトランクポートをVLANに割り当てるには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.レイヤ2イーサネットインターフェイスビューに入ります。	• GigabitEthernetインターフェイスビューに入ります。**gigabitethernet** *interface-number* • Smarterateイーサネットインターフェイスビューに入ります。**smartrate-ethernet** *interface-number*	APモデルおよびネットワーク要件に従って、いずれかのコマンドを使用します。
4.リンクタイプをtrunkに設定します。	**port link-type trunk**	デフォルトでは、ポートはAPグループのレイヤ2イーサネットインターフェイスビューの設定を使用します。
5.トランクポートを指定されたVLANに割り当てます。	**port trunk permit VLAN** { *vlan-id-list* | **all** }	デフォルトでは、トランクポートはAPグループのレイヤ2イーサネットインターフェイスビューの設定を使用します。
6.(オプション)トランクポートのPVIDを設定します。	**port trunk pvid vlan** *vlan-id*	デフォルトでは、トランクポートはAPグループのレイヤ2イーサネットインターフェイスビューの設定を使用します。

APグループのレイヤ2イーサネットインターフェイスビューでVLANにトランクポートを割り当てるには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group group-name**	該当なし
3.APモデルビューに入ります。	**ap-model ap-model**	該当なし
4.レイヤ2イーサネットインターフェイスビューに入ります。	• GigabitEthernetインターフェイスビューに入ります。**gigabitethernet** *interface-number* • Smarterateイーサネットインターフェイスビューに入ります。**smartrate-ethernet** *interface-number*	APモデルおよびネットワーク要件に従ってコマンドを使用します。
5.リンクタイプをtrunkに設定します。	**Port link-type trunk**	デフォルトでは、すべてのポートがアクセスポートです。
6.トランクポートを指定されたVLANに割り当てます。	**Port trunk permit VLAN** { *vlan-id-list* | **all** }	デフォルトでは、トランクポートはVLAN1だけを許可します。
7.(オプション)トランクポートのPVIDを設定します。	**Port trunk pvid vlan** *vlan-id*	デフォルト設定はVLAN1です。

ハイブリッドポートのVLANへの割り当て

APのレイヤ2イーサネットインターフェイスビューでハイブリッドポートをVLANに割り当てるには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.レイヤ2イーサネットインターフェイスビューに入ります。	• GigabitEthernetインターフェイスビューに入ります。 **gigabitethernet** *interface-number* • Smarterateイーサネットインターフェイスビューに入ります。 **smartrate-ethernet** *interface-number*	APモデルおよびネットワーク要件に従って、いずれかのコマンドを使用します。
4.リンクタイプをハイブリッドに設定します。	**Port link-type hybrid**	デフォルトでは、ポートはAPグループのレイヤ2イーサネットインターフェイスビューの設定を使用します。
5.指定されたVLANにハイブリッドポートを割り当てます。	**port hybrid vlan** *vlan-id-list* { **tagged | untagged** }	デフォルトでは、ハイブリッドポートはAPグループのレイヤ2イーサネットインターフェイスビュー内の設定を使用します。
6.(オプション)ハイブリッドポートのPVIDを設定します。	**Port hybrid pvid vlan** *vlan-id*	デフォルトでは、ハイブリッドポートはAPグループのレイヤ2イーサネットインターフェイスビュー内の設定を使用します。

APグループのレイヤ2イーサネットインターフェイスビューでハイブリッドポートをVLANに割り当てるには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group group-name**	該当なし
3.APモデルビューに入ります。	**ap-model ap-model**	該当なし
4.レイヤ2イーサネットインターフェイスビューに入りします。	• GigabitEthernetインターフェイスビューに入ります。 **gigabitethernet** *interface-number* • Smarterateイーサネットインターフェイスビューに入ります。 **Smartrate-ethernet** *interface-number*	APモデルおよびネットワーク要件に従って、いずれかのコマンドを使用します。
5.リンクタイプをハイブリッドに設定します。	**Port link-type hybrid**	デフォルトでは、すべてのポートがアクセスポートです。

ステップ	コマンド	備考
6.指定されたVLANにハイブリッドポートを割り当てます。	**port hybrid vlan vlan-id-list** {tagged untagged}	デフォルトでは、リンクタイプがaccessの場合、ハイブリッドポートはポートが属するVLANのタグ無メンバーです。
7.(オプション)ハイブリッドポートのPVIDを設定します。	**ポートハイブリッドpvid vlan vlan-id**	デフォルトでは、ハイブリッドポートのPVIDは、リンクタイプがaccessの場合、ポートが属するVLANのIDです。

リモート構成割り当ての構成

ACは、この機能がイネーブルまたはAPグループに割り当てられるのは、この機能がイネーブルの場合だけです。

APビューでのリモート設定割り当ての設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [model model-name]	該当なし
3.リモート構成の割り当てを構成します。	**remote-configuration** { **disable** | **enable**}	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループビューでのリモート設定割り当ての設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group group-name**	該当なし
3.リモート構成の割り当てを構成します。	**remote-configuration** { **disable** | **enable** }	デフォルトでは、リモートコンフィギュレーションの割り当てはディセーブルです。

CAPWAPトンネルの設定

CAPWAPトンネル遅延検出の設定

この機能を使用すると、ACは、APからACおよびその逆方向へのCAPWAP制御フレームまたはデータフレームの伝送遅延を検出できます。

この機能は、CAPWAPトンネルが確立された後にマスターACでだけ有効になります。

APがオフラインになると、CAPWAPトンネル遅延検出は自動的に停止します。APがオンラインになったときにCAPWAPトンネル遅延検出を再開するには、tunnel latency-detect startコマンドを再度実行します。

CAPWAPトンネル遅延情報を表示するには、**display wlan tunnel latency ap name**を使用します。で行ないます。

CAPWAPトンネル遅延検出を設定するには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.CAPWAPトンネル遅延検出を設定します。	**Tunnel latency-detect { start | stop }**	デフォルトでは、CAPWAPトンネル遅延検出は開始されません。

APのコントロールトンネルキープアライブ時間の設定

APは、指定されたエコー間隔でACにエコー要求を送信し、CAPWAP制御トンネルが正常に動作しているかどうかを確認します。ACは、エコー応答を送信して応答します。APがキープアライブ時間内にエコー応答を受信しない場合、APは接続を終了します。ACがキープアライブ時間内にエコー要求を受信しない場合、ACは接続を終了します。キープアライブ時間は、エコー間隔にエコー要求の最大送信試行回数を乗算した値です。

APビューでのAPのコントロールトンネルキープアライブ時間の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入りします。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.APがエコー要求を送信する間隔を設定します。	**echo-interval** *interval*	デフォルトでは、APはAPグループビュー内の設定を使用します。
4.エコー要求の最大送信試行回数を設定します。	**Echo-count** *count*	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループビューでのAPのコントロールトンネルキープアライブ時間の設定

ステップ	コマンド	備考
1.システムビューに入りします。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.APがエコー要求を送信する間隔を設定します。	**echo-interval** *interval*	デフォルト設定は10秒です。
4.エコー要求の最大送信試行回数を設定します。	**Echo-count** *count*	デフォルト設定は3です。

APのデータトンネルのキープアライブ時間の設定

APとACの間にCAPWAPトンネルが確立された後、APは指定されたキープアライブ時間にデータチャネ

ルキープアライブパケットをACに送信します。

APビューでのAPのデータトンネルキープアライブ時間の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.データトンネルのキープアライブ間隔を設定します。	**keepalive-interval**間隔	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループビューでのAPのデータトンネルキープアライブ時間の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.データトンネルのキープアライブ間隔を設定します。	**keepalive-interval** *interval*	デフォルト設定は10秒です。

CAPWAPパケットの最大フラグメントサイズの設定

APがインターネット経由でACに接続する場合に、中間デバイスがACとAPの間でパケットをドロップしないようにするには、次の作業を実行します。

最大フラグメントサイズの変更は、オンラインAPでただちに有効になります。

APビューでのCAPWAPパケットの最大フラグメントサイズの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.CAPWAP制御パケットまたはデータパケットの最大フラグメントサイズを設定します。	**fragment-size** { **control** *control-size* | **data** *data-size*}	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループビューでのCAPWAPパケットの最大フラグメントサイズの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.CAPWAP制御パケットまたはデータパケットの最大フラグメントサイズを設定します。	**fragment-size** { **control** *control-size* | **data** *data-size* }	デフォルトでは、CAPWAP制御パケットおよびデータパケットの最大フラグメントサイズは、それぞれ1450バイトと1500バイトです。

CAPWAPトンネルのTCP MSSの設定

TCP MSSの設定について

CAPWAPトンネルを介して送信されるSYNパケットのMaximum Segment Size(MSS)オプションの値を設定するには、次の作業を実行します。

MSSオプションは、送信者が受け入れることができる最大セグメントを受信者に通知します。各エンドは、TCP接続の確立中にMSSを通知します。TCPセグメントのサイズが受信者のMSS以下の場合、TCPはTCPセグメントをフラグメンテーションなしで送信します。それ以外の場合、TCPは受信者のMSSに基づいてセグメントをフラグメント化します。

手順

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.CAPWAPトンネルのTCP MSSを設定します。	**wlan tcp mss** *value*	デフォルト設定は1460バイトです。

AC要求再送信の設定

ACは、要求の再送信試行が最大数に達するか、応答が受信されるまで、再送信間隔でAPに送信された要求を送信します。

APビューでのAC要求再送信の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.要求再送信の最大試行回数を設定します。	**retransmit-count** *value*	デフォルトでは、APはAPグループビュー内の設定を使用します。
4.AC要求が再送信される間隔を設定します。	**retransmit-interval** *interval*	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループビューでのAC要求再送信の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.要求再送信の最大数を設定します。	**retransmit-count** *value*	デフォルト設定は3です。
4.AC要求が再送信される間隔を設定します。	**retransmit-interval** *interval*	デフォルト設定は5秒です。

統計レポートの間隔の設定

APが統計情報をレポートする間隔を変更するには、次の作業を実行します。これらの統計情報を使用して、AP上の無線の動作ステータスを監視できます。

APビューでの統計レポートの間隔の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.統計レポートの間隔を設定します。	**Statistics-interval** *interval*	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループビューでの統計情報レポート間隔の設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.統計レポートの間隔を設定します。	**Statistics-interval** *interval*	デフォルト設定は50秒です。

リモートAPの設定

APとACの間のトンネルが切断されると、APはクライアントに対するサービスの提供を停止します。この機能により、APとACの間のトンネルが切断されると、APは次のタスクを自動的に実行できます。

- クライアントトラフィックを転送します。
- ローカル認証がイネーブルで、APでアソシエーションがイネーブルの場合に、クライアントアクセスサ

ービスを提供します。

リモートAPは、ローカル転送モードで動作するAPだけで有効になります。

ACとAP間のトンネルが復旧すると、ACをオーセンティケータとするクライアントは再認証が必要になります。APをオーセンティケータとするクライアントはオンラインのままです。

リモートAPは、テレコミューティング、小規模ブランチ、およびSOHOソリューションに適用できます。

APビューでのリモートAPの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.リモートAPを設定します。	**hybrid-remote-ap** { **disable** | **enable** }	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループビューでのリモートAPの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group group-name**	該当なし
3.リモートAPを設定します。	**hybrid-remote-ap** { **disable** | **enable** }	デフォルトでは、リモートAPは無効になっています。

デフォルト入力電力レベルの設定

注:
この機能のサポートは、デバイスモデルによって異なります。

APが起動時に入力電力レベルを取得できない場合に備えて、APのデフォルト入力電力レベルを設定します。

入力電力レベルの概要

APは、起動時に入力電力レベルを取得するために電源モード検出を自動的に実行します。APが入力電力レベルを取得できない場合は、ACに関連付ける前に低電力レベルで動作します。関連付け後は、設定されたデフォルトの入力電力レベルで動作します。

APには、電源アダプタまたはそのPoEまたはPoE+ポートを介して電力を供給できます。次の表に、APの電源モードと入力電力レベルの関係を示します。

電源モード	入力電力レベル
• 電源アダプタ。 • 複数のPoE+ポート。 • PoEポートとPoE+ポートの組み合わせ。	高
• 単一のPoE+ポート	中
• 複数のPoEポート • 単一のPoEポート	低

MIMOモードおよびUSBインターフェイスに対するAPのサポートは、表1に示すように、入力電力レベルによって異なります。

表1APによるMIMOモードおよびUSBインターフェイスのサポート

入力電力レベル	サポートされるMIMOモード	USBインタフェースを有効にできるかどうか
高	1×1、2×2、3×3、4×4	はい
中	1×1、2×2、3×3、4×4	MIMOモードが1×1または2×2の場合できます
低	1×1	No.

設定に関する制限事項とガイドライン

APのデフォルトの入力電力レベルを設定する場合は、設定がその電源モードと一致していることを確認してください。入力電力レベルが過度に低いと、APが正常に動作しなくなります。入力電力レベルが過度に高いと、電力不足の場合にAPの過負荷が発生します。

APビューでのデフォルト入力電力レベルの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.デフォルトの入力電力レベルを設定します。	**Power-level default { high | low | middle }**	デフォルトでは、APはAPグループのAPモデルビュー内の設定を使用します。

APグループのAPモデルビューでのデフォルト入力電力レベルの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.APモデルビューに入ります。	**ap-model ap-model**	該当なし
4.デフォルト入力電力レベルを構成します。	**Power-level default** { **high | low | middle** }	既定の設定は中です。

APのUSBインターフェイスのイネーブル化またはディセーブル化

注:
この機能のサポートは、APモデルによって異なります。

APのUSBインターフェイスをイネーブルにした後は、次のいずれかの要件が満たされている場合に限り、USBインターフェイスがアクティブになります。

- APの入力電力レベルは高い。
- APの入力電力レベルは中間であり、MIMOモードは1×1または2×2である。

入力電力レベルについて詳しくは、「デフォルト入力電力レベルの設定」を参照してください。MIMOモードについて詳しくは、「無線管理の設定」を参照してください。

APビューでのUSBインターフェイスの有効化または無効化

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.USBインタフェースを有効または無効にします。	**usb { enable | disable }**	デフォルトでは、APはAPグループのAPモデルビュー内の設定を使用します。

APグループのAPモデルビューでのUSBインターフェイスの有効化または無効

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.APモデルビューに入ります。	**ap-model** *ap-model*	該当なし
4.USBインタフェースを有効または無効にします。	**usb { enable | disable }**	デフォルトでは、USBインターフェイスは無効になっています。

APのリセット

ユーザービューで次のタスクを実行します。

タスク	コマンド
すべてのAPまたは指定されたAPをリセットします。	**reset wlan ap** { **all** | **ap-group** *group-name* | **model** *model-name* | **name** *ap-name* }

手動APの名前の変更

ステップ	コマンド
1.システムビューに入ります。	**System-view**
2.手動APの名前を変更します。	**wlan rename-ap** *ap-name new-ap-name*

APのファイルシステムの管理

APがACとの間でCAPWAPトンネルを確立した後、ACで次のタスクを実行して、APのファイルを管理できます。

- APのファイル情報を表示します。
- 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。この機能は、マスターACでのみ有効です。

APのファイルシステムを管理するには、次の手順に従います。

ステップ	コマンド
1.AP上のファイルまたはファイルフォルダに関する情報を表示します。	**display wlan ap files name** *ap-name*
2.システムビューに入ります。	**System-view**
3.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]
4.APからファイルを削除します。	**delete file** *filename*
5.イメージファイルをAPにダウンロードします。	**download file** *file-name*

APインターフェイスの管理

注:
この機能のサポートは、APモデルによって異なります。

インターフェイスタイプのGigabitEthernetへの変更

インタフェースタイプの変更について

一部のAPモデルでは、必要に応じてインターフェイスタイプをIoTまたはWTUからGigabitEthernetに変更できます。GigabitEthernetインターフェイスはAPをPCなどの端末デバイスに接続し、WTUポートはAPをWTUsに接続し、IoTインターフェイスはAPをIoTモジュールに接続します。

注:
WTUポートおよびIoTインターフェイスのサポートは、APモデルによって異なります。

設定に関する制限事項とガイドライン

この機能は、GigabitEthernetとIoTまたはWTUとの間のインターフェイスタイプスイッチオーバーをサポートするインターフェイスだけで有効になります。

インターフェイスにGigabitEthernetインターフェイスタイプを指定すると、インターフェイスタイプスイッチオーバーをサポートする同じAP上の他のすべてのインターフェイスについて、デフォルトのインターフェイスタイプ設定が復元されます。たとえば、UAP300では、interface3およびinterface4はインターフェイスタイプスイッチオーバーをサポートします。両方のインターフェイスのインターフェイスタイプをGigabitEthernetに設定し、次にinterface4のインターフェイスタイプをGigabitEthernetに設定すると、インターフェイス3はIoTインターフェイスになります。

APビューでのAPインターフェイスのインターフェイスタイプのGigabitEthernetへの変更

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.APインターフェイスタイプをGigabitEthernetに変更します。	**port-type gigabitethernet number** *port-number*	デフォルトでは、APはAPグループのAPモデルビュー内の設定を使用します。

APグループのAPモデルビューで、APインターフェイスのインターフェイスタイプをGigabitEthernetに変更する

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.APモデルビューに入ります。	**ap-model** *ap-model*	該当なし
4.APインターフェイスタイプをGigabitEthernetに変更します。	**port-type gigabitethernet number** *port-number*	デフォルト設定はAPモデルによって異なります。インターフェイスタイプの切り替えをサポートするAPインターフェイスは、IoTインターフェイスまたはWTUポートになります。

PIに対するPoEのイネーブル化またはディセーブル化

APビューでのPIに対するPoEのイネーブル化またはディセーブル化

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.PIのPoEを有効または無効にします。	**poe port** *port-number1* [**to** *port-number2*] { **disable | enable** }	デフォルトでは、APはAPグループのAPモデルビュー内の設定を使用します。

APグループのAPモデルビューでのPIに対するPoEの有効化または無効化

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** group-name	該当なし
3.APモデルビューに入ります。	**ap-model** ap-model	該当なし
4.PIのPoEを有効または無効にします。	**poe port** *port-number1* [**to** *port-number2*] { **disable | enable** }	デフォルトでは、PoEはPIに対してディセーブルです。

APグループの設定

この機能を使用すると、複数のAPをバッチで設定して、設定作業負荷を軽減できます。

APグループ内のAPは、グループ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グループは作成または削除できません。

AP名、シリアルID、MACアドレスおよびIPアドレスでAPグループ化ルールを構成して、指定したAPグループにAPを追加できます。これらのグループ化ルールの優先度は降順です。APがグループ化ルールと一致しない場合は、デフォルトのAPグループに追加されます。

設定に関する制限事項とガイドライン

APグループを設定する場合は、次の制約事項およびガイドラインに従ってください。

- APを追加できるAPグループは1つだけです。
- APを含むAPグループは削除できません。
- デフォルトAPグループにはグループ化ルールを作成できません。
- 異なるAPグループに同じグループ化ルールを作成することはできません。これを行うと、最新の設定が有効になります。
- APビュー、APグループビュー、およびグローバルコンフィギュレーションビューでのAPの設定の優先順位は降順です。1つのビューで設定が構成されていない場合、優先順位の低いビューの設定が使用されます。3つのビューのいずれかで設定が構成されていない場合、APは優先順位が最も低いビューのデフォルト設定を使用します。
- APグループまたは異なるAPグループのIPv4またはIPv6アドレスによるAPグループ化ルールは、相互に重複できません。
- APグループは、IPv4またはIPv6アドレスごとに最大32個のAPグループ規則をサポートします。

APグループの作成

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループを作成し、そのビューに入ります。	**wlan ap-group** *group-name*	デフォルトでは、デフォルトのAPグループが存在します。
3.(オプション)APグループの説明を設定します。	**description** *text*	デフォルトでは、APグループの説明は設定されていません。
4.AP名によるAPグループ化ルールを作成します。	**ap** *ap-name-list*	該当なし
5.シリアルIDによるAPグループ化ルールを作成します。	**serial-id** *serial-id*	該当なし
6.MACアドレスによるAPグループ化ルールを作成します。	**mac-address** *mac-address*	該当なし
7.IPv4アドレスによるAPグループ化ルールを作成します。	**if-match ip** *ip-address* { *mask-length* | *mask* }	該当なし
8.IPv6アドレスによるAPグループ化ルールを作成します。	**if-match ipv6** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }	該当なし
9.(オプション)AP再グループ化ルールを作成します。	**wlan re-group** { **ap** *ap-name* **ap-group** *old-group-name* | **mac-address** *mac-address* **serial-id** *serial-id* } *group-name*	該当なし

APの事前プロビジョニング

AP事前プロビジョニングを使用すると、AC上のFIT APのネットワーク設定を構成できます。ACは、バッチ内のCAPWAPトンネルを介して、実行状態のFIT APにこれらの設定を自動的に割り当てます。これにより、大規模なWLANネットワークでの作業負荷が軽減されます。

これらの設定は、APのコンフィギュレーションファイルwlan_ap_prvs.xmlに保存する

必要があります。この機能は、マスターACでのみ有効です。

APプロビジョンビューまたはAPグループプロビジョンビューでネットワーク設定を構成できます。APプロビジョンビューの設定の方が優先度が高くなります。

APの事前プロビジョニングされた設定を変更する場合は、事前プロビジョニングされたコンフィギュレーションファイルに設定を再保存します。

save wlan ap-provisionコマンドは、reset wlan ap provisionコマンドと同じ効果があります。
コマンドを使用します。

プロビジョニングビューで事前にプロビジョニングされた設定は
save wlan ap provisionコマンド。

プロビジョニングビューで事前プロビジョニングされた設定をキャンセルしても
save wlan ap provisionコマンド。APでキャンセルを有効にするには、APを再起動します。reset wlan ap

provisionコマンドをAPで有効にするには、実行後にAPを再起動します。

APの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.APの事前プロビジョニングを有効にし、APプロビジョンビューに入ります。	**Provision**	デフォルトでは、APはAPグループビュー内の設定を使用します。
4.APにACを指定します。	**ac** { **host-name** *host-name* | **ip** *ipv4-address* | **ipv6** *ipv6-address* }	デフォルトでは、APはAPグループビュー内の設定を使用します。
5.管理VLANインターフェイスのIPv4アドレスを指定します。	**ip address** *ip-address* { *mask* | *mask-length* }	デフォルトでは、管理VLANインターフェイスにIPv4アドレスは指定されていません。
6.管理VLANインターフェイスのIPv6アドレスを指定します。	**ipv6 address** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* }	デフォルトでは、管理VLANインターフェイスにIPv6アドレスは指定されていません。
7.ゲートウェイのIPアドレスを設定します。	**gateway** { **ip** *ipv4-address* **ipv6** *ipv6-address* }	デフォルトでは、APにゲートウェイIPアドレスは指定されません。

8.DNSサーバーを指定します。	**dns server** { **ip** *ipv4-address* **ipv6** *ipv6-address* }	デフォルトでは、APはAPグループビュー内の設定を使用します。
9.DNSドメイン名のサフィックスを設定します。	**dns domain** *domain-name*	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループのネットワーク設定の構成

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group *group-name***	該当なし
3.APの事前プロビジョニングを有効にし、APグループのプロビジョニングビューに入ります。	**provision**	デフォルトでは、APの事前プロビジョニングはディセーブルです。
4.ACを指定します。	**ac** { **host-name** *host-name* | **ip** *ip-address* | **ipv6** *ipv6-address* }	デフォルトでは、APにスタティックACは指定されていません。
5.DNSサーバーを指定します。	**dns server** { **ip** *ip-address* | **ipv6** *ipv6-address* }	デフォルトでは、APにDNSサーバーは指定されていません。
6.DNSサーバーのドメイン名サフィックスを設定します。	**dns domain domain-name**	デフォルトでは、DNSサーバーにドメイン名のサフィックスは指定されません。

事前にプロビジョニングされた設定のAPへの割り当て

ACが事前プロビジョニングされた設定を、ACがCAPWAPトンネルを確立したAPに割り当てることができるようにするには、次の作業を実行します。事前プロビジョニングされた設定は、APのコンフィギュレーションファイルwlan_ap_prvs.xmlに保存され、コンフィギュレーションファイルに保存されたネットワーク設定が上書きされます。

事前にプロビジョニングされた設定をAPに割り当てるには、次のいずれかの方法を使用できます。

- 手動設定:事前にプロビジョニングされた設定を設定ファイルに保存します。
  wlan_ap_prvs.xmlは、APがオンラインになった後にAPで使用されます。

  APの構成ファイル内のACアドレス構成を変更すると、新しい最適AC選択プロセスがトリガーされます。その後、APは元のCAPWAPトンネルを終了し、新しいACとのCAPWAPトンネルを確立します。
- 事前プロビジョニング設定の自動割り当て:事前プロビジョニング設定は、APがオンラインになるときにAPに割り当てられます。APは、事前プロビジョニング設定で指定されたACを使用してCAPWAPトンネルを確立します。最適なAC選択の詳細は、「CAPWAPトンネルの確立」を参照してください。

AP上のコンフィギュレーションファイルへのネットワーク設定の保存

オプションのビューで次のタスクを実行します。

タスク	コマンド
指定したAPまたはすべてのAPで、事前にプロビジョニングされたコンフィギュレーションファイル **wlan_ap_prvs.xml**にネットワーク設定を保存します。	**save wlan ap provision** { **all** | **name** *ap-name* }

事前にプロビジョニングされた設定の自動割り当ての構成

APビューで事前プロビジョニングされた設定の自動割り当てを設定するには、次の手順を実行します。

ステップ	コマンド	備考
1.システビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.APのために事前プロビジョニングされた設定の自動割り当てを構成します。	**Provision auto-update** { **disable** | **enable** }	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループビューで事前プロビジョニング設定の自動割り当てを設定するには、次の手順を実行します。

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.APグループ内のAPに対して事前にプロビジョニングされた設定の自動割り当てを設定します。	**Provision auto-update** { **disable** | **enable**}	デフォルトでは、事前にプロビジョニングされた設定の自動割り当ては無効になっています。

事前にプロビジョニングされた設定の自動ロードの構成

事前にプロビジョニングされた設定を自動的にロードすることにより、APとAC間でCAPWAPトンネルが正常に確立されます。この機能をイネーブルにすると、APは次の手順を使用してACを検出します。

1. 事前にプロビジョニングされた設定を使用して、APの手動または自動AP構成を持つACを検出します。
2. AC検出に失敗した場合は、再起動して他の方法でACを検出します。
3. APがまだターゲットACの検出に失敗した場合は、再起動し、事前にプロビジョニングされた設定を再度使用してACを検出します。

このAC検出プロセスは、APがターゲットACを検出してCAPWAPトンネルを確立するまで繰り返されます。

AP用に事前プロビジョニングされた設定の自動ロードの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APビューに入ります。	**wlan ap** *ap-name* [**model** | *model-name*]	該当なし
3.事前にプロビジョニングされたAP設定の自動ロードを設定します。	**Provision auto-recovery** { **disable | enable** }	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループの事前プロビジョニングされた設定の自動ロードの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	該当なし
3.APグループ内のAPに対して事前にプロビジョニングされた設定の自動ロードを設定します。	**Provision auto-recovery { disable | enable }**	デフォルトでは、事前プロビジョニングされた設定の自動ロードは有効になっています。

SNMP通知のイネーブル化

重要なWLANイベントをNMSにレポートするには、SNMP通知をイネーブルにします。WLANイベント通知が正しく送信されるようにするには、『Network Management and Monitoring Configuration Guide』の説明に従ってSNMPも設定する必要があります。

SNMP通知をイネーブルにするには、次の手順を実行

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.SNMP通知を有効にします。	• AP管理のためのSNMP通知のイネーブル化: **snmp-agent trap enable wlan ap** • CAPWAPのSNMP通知をイネーブルにします。 **snmp-agent trap enable wlan capwap**	デフォルトでは、AP管理およびCAPWAPのSNMP通知はディセーブルです。

APDBユーザースクリプトのロード

ACソフトウェアをアップグレードせずに新しいAPモデルをAPDBに追加するには、次の作業を実行します。

設定に関する制限事項とガイドライン

APDBユーザースクリプトをロードする場合は、次の制約事項およびガイドラインに従ってください。

- ユーザー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ドに失敗する可能性があります。
- ユーザースクリプト内の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に複数のユーザースクリプトをロードすると、最後にロードされたユーザースクリプトによって古いユーザースクリプトが上書きされます。
- ファイルシステムでユーザースクリプトの名前を変更した場合は、ユーザースクリプトをリロードして、ACリブート後にユーザースクリプト内のAPモデル設定が失われないようにします。
- ファイルシステム内でユーザースクリプトを新しいユーザースクリプトに置き換えた場合は、新しいユーザースクリプトをリロードします。新しいユーザースクリプトに、置き換えたユーザースクリプトに保存されているAPモデル情報が含まれていない場合、ACの再起動後にAPモデル情報が失われます。
- ファイルシステム内のユーザースクリプトを削除すると、ACリブート後にユーザースクリプト内のAPモデル構成が失われます。

古いユーザースクリプトがすでに存在する場合は、APDBユーザースクリプトをロードする際に次の制限事

項およびガイドラインに従ってください。

- 古いユーザースクリプトにモデルがリストされている手動APまたはオンライン自動APが存在する場合は、AC上の対応するAPモデル情報を削除した場合にのみ、新しいユーザースクリプトをロードできます。
- 古いユーザースクリプトにリストされているAPモデルのAPがAPグループに追加されている場合は、APグループからAPを削除したときにだけ新しいユーザースクリプトをロードできます。
- 古いユーザースクリプトに、ソフトウェアバージョンがすでに設定されているAPモデルが含まれている場合は、wlan apdbコマンドを使用して元のソフトウェアバージョンを復元する場合に限り、新しいユーザースクリプトをロードできます。

設定手順

APDBユーザースクリプトをロードする手順は、次のとおりです。

ステップ	コマンド	備考
1.システムビューに入ります。	**system-view**	該当なし
2.APDBユーザースクリプトをロードします。	**wlan apdb file** *user.apdb*	デフォルトでは、ユーザースクリプトはACにロードされません。

AP管理の表示と保守

LED照明モードを設定する

APのLEDは、次のモードで点滅するように設定できます。

- **quiet**: すべてのLEDが消灯します。
- **awake**: すべてのLEDが1分ごとに点滅します。このモードのサポートは、APモデルによって異なります。
- **always-on**: すべてのLEDが点灯します。このモードのサポートは、APモデルによって異なります。
- **normal**: このモードでのLEDの点滅方法はAPのモデルによって異なります。このモードでは、APの実行ステータスを識別できます。

APグループビューでLED照明モードを[awake]または[always-on]に設定した場合、この設定は、指定されたLED照明モードをサポートするメンバーAPに対してのみ有効になります。

APビューでのLED照明モードの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし

2.APビューに入ります。	**wlan ap** *ap-name* [**model** *model-name*]	該当なし
3.LEDの点灯モードを設定します。	**led-mode { always-on | awake | normal | quiet }**	デフォルトでは、APはAPグループビュー内の設定を使用します。

APグループ表示でのLED点灯モードの設定

ステップ	コマンド	備考
1.システムビューに入ります。	**System-view**	該当なし
2.APグループビューに入ります。	**wlan ap-group** *group-name*	デフォルトでは、デフォルトのAPグループ**default-group**が存在し、削除できません。
3.LEDの点灯モードを設定します。	**led-mode { always-on | awake | normal | quiet }**	デフォルトでは、LED照明モードは通常です。

AP管理情報の表示

オプションのビューで表示コマンドを実行します。

タスク	コマンド
すべてのAPまたは指定されたAPに関する情報を表示します。	**display wlan ap** { **all | name** *ap-name* } [**verbose**]
すべてのAPまたは指定されたAPのアドレス情報を表示します。	**display wlan ap** { **all | name** *ap-name* } **address**
APアソシエーション障害レコードを表示します。	**display wlan ap association-failure-record**
ACのAP接続レコードを表示します。	**display wlan ap connection record { all | name** *ap-name* }
すべてのAPまたは指定されたAPのGPS情報を表示します。	**display wlan ap { all | name** *ap-name* } **gps**
APのオンライン期間を表示します。	**display wlan ap online-time { all | name** *ap-name* }
指定したAPの再起動ログを表示します。	**display wlan ap reboot-log name** *ap-name*
すべてのAPまたは指定されたAPの実行コンフィギュレーションを表示します。	**display wlan ap running-configuration { all | ap-name** *ap-name* } [**verbose**]
CAPWAPトンネルダウンレコードを表示します。	**wlan ap tunnel-down-record**
すべてのAPグループまたは指定したAPグループに関する情報を表示します。	**display wlan ap-group [brief | name** *group-name*]
APモデル情報を表示します。	**display wlan ap-model { all | name** *model-name* }
指定されたCAPWAPトンネルのトンネル遅延情報を表示します。	**display wlan tunnel latency ap name** *ap-name*
ACの接続APの配信に関する情報を表示します。	**display wlan ap-distribution { all | slot** *slot-number* }
APの接続場所を表示します。	**display wlan ap-distribution ap-name** *ap-name*

AP管理情報の消去

ユーザービューでリセットコマンドを実行します。

タスク	コマンド
すべてのAPまたは指定されたAPのリブートログをクリアします。	**reset wlan ap reboot-log { all | name** *ap-name* }
すべてのCAPWAPトンネルまたは指定されたCAPWAPトンネルのトンネル遅延情報をクリアします。	**reset wlan tunnel latency ap { all | name** *ap-name* }
すべてのAPまたは指定されたAPからコンフィギュレーションファイル**wlan_ap_prvs.xml**を削除します。	**reset wlan ap provision { all | name** *ap-name* }

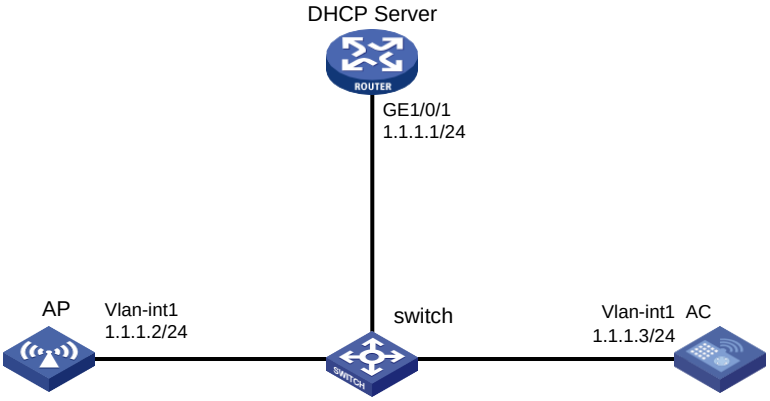
AP管理の設定例

DHCPによるCAPWAPトンネルの確立の設定例

ネットワーク要件

図3に示すように、DHCPオプション43を使用してDHCPサーバーからIPアドレスとAC IPアドレスを取得するようにAPを設定します。APはACのIPアドレスを使用して、ACとのCAPWAPトンネルを確立します。

図3 ネットワーク図



構成手順

3. DHCPサーバーを設定します。
   #DHCPサービスを有効にします。
   <DHCP server> System-view
   [DHCP server] dhcp enable
   #DHCPアドレスプール1を設定します。
   [DHCP server] dhcp servre ip-pool 1
   [DHCP server-dhcp-pool-1] network 1.1.1.0 mask 255.255.255.0
   #オプション43を構成して、アドレスプール0内のACのIPアドレスを指定します。一番右のバイト01010103(1.1.1.3)は、ACのIPアドレスを表します。
   [DHCP Server-dhcp-pool-1] option 43 hex 800700000101010103
   [DHCP Server-dhcp-pool-1] quit
   [DHCP server] quit
4. ACを次のように設定します。
   #AC上のVLANインターフェイス1のIPアドレスを1.1.1.3/24に設定します。
   <AC>System-view
   [AC] interface vlan-interface 1
   [AC-Vlan-interface1] ip address 1.1.1.3 24
   [AC-Vlan-interface1] quit
   #モデルWA4320i-ACNでAP ap1を作成し、そのシリアルIDを210235A1BSC123000050に設定します。
   [AC] wlan ap ap1 model WA6638-JP
   [AC-wlan-ap-ap1] serial-id 210235A1BSC123000050
   [AC-wlan-ap-ap1] quit
   #APを起動します。APは次の操作を実行します。

- DHCPサーバーからIPアドレス1.1.1.2を取得します。
- オプション43を使用してACのIPアドレスを取得します。
- ACとの間にCAPWAPトンネルを確立します。

設定の確認

#次の情報を確認します。

- APはDHCPを介してACのIPアドレスを取得します。
- APとACは、CAPWAPトンネルを確立しています。
- APはRun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                         : WA6638-JP
Region code                   : CN
Region code lock              : Disable
Serial ID                     : 219801A0CNC138011454
MAC address                   : 0AFB-423B-893C
IP address                    : 192.168.1.50
UDP control port number       : 18313
UDP data port number          : N/A
H/W version                   : Ver.C
S/W version                   : R2206P02
Boot version                  : 1.01
USB state                     : N/A
Power Level                   : N/A
PowerInfo                     : N/A
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                : 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
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
    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
    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
    Smart antenna           : Enabled
    Smart antenna policy    : Auto
    Protection mode         : rts-cts
    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
    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,
```

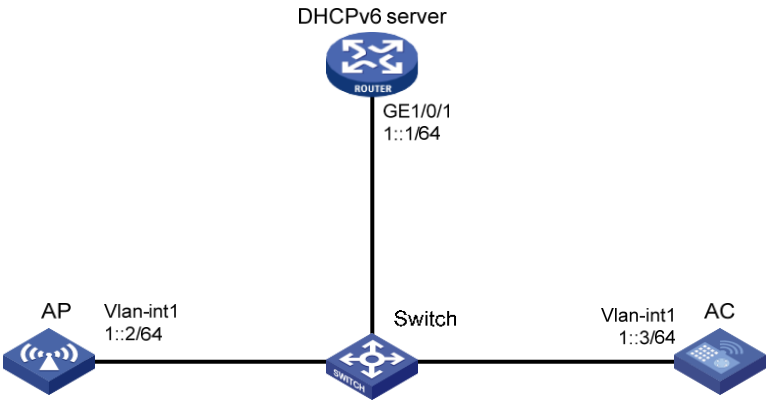
```
10, 11, 12, 13, 14, 15
Multicast               : Not configured
Channel                 : 5(auto)
Channel usage(%)        : 0
Max power               : 20 dBm
Preamble type           : Short
Operational rate:
Mandatory               : 1, 2, 5.5, 11 Mbps
Multicast               : Auto
Supported               : 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
Smart antenna           : Enabled
Smart antenna policy    : Auto
Protection mode         : rts-cts
Continuous mode         : N/A
HT protection mode      : No protection
```

DHCPv6によるCAPWAPトンネルの確立の設定例

ネットワーク要件

図4に示すように、DHCPオプション52を使用してDHCPv6サーバーからAPのIPアドレスとACのIPアドレスを取得するようにAPを構成します。APはACのIPアドレスを使用して、ACとのCAPWAPトンネルを確立します。

図4:ネットワーク図



構成手順

1. DHCPv6サーバーを設定します。

   #IPv6アドレスをGigabitEthernet1/0/1に割り当てます。

   <DHCPv6 Server> System-view

   [DHCPv6Server] interface gigabitethernet 1/0/1

   [DHCPv6Server-GigabitEthernet1/0/1] ipv6 address 1::1/64

   #RAメッセージアドバタイズの抑制をディセーブルにします。

   [DHCPv6Server-GigabitEthernet1/0/1] undo ipv6 nd ra halt

   #送信されるRAアドバタイズメントのmanaged address configuration flag(M)を1に設定します。

   [DHCPv6Server-GigabitEthernet1/0/1] ipv6 nd autoconfig managed-address-flag

   #送信されるRAアドバタイズメントのother stateful configuration flag(O)を1に設定します。
   [DHCPv6Server-GigabitEthernet1/0/1] ipv6 nd autoconfig other-flag

   #GigabitEthernet1/0/1上でDHCPv6サービスをイネーブルにします。

   [DHCPv6Server-GigabitEthernet1/0/1] ipv6 dhcp select server

   [DHCPv6Server-GigabitEthernet1/0/1] quit

   #DHCPv6アドレスプールを作成し、DHCPv6アドレスプールで動的に割り当てるIPv6サブネットを指定します。

   [DHCPv6Server] ipv6 dhcp pool 1

   [DHCPv6Server-dhcp6-pool-1] network 1::0/64

[DHCPv6Server-dhcp6-pool-1] quit

#DHCPv6アドレスプール1のACアドレス1::3を指定するオプション52を構成します。
[DHCPv6Server-dhcp-pool-1] option 52 hex 000100000000000000000000000000003

[DHCPv6Server-dhcp-pool-1] quit

[DHCPv6Server] quit

2. ACを次のように設定します。

#VLANインターフェイス1のIPv6アドレスを1::3/64に設定します。

<AC> System-view

[AC] interface vlan-interface 1

[AC-Vlan-interface1] ipv6 address 1::3 64

#ap1という名前のAPを作成し、そのモデルとシリアルIDを指定します。

[AC] wlan ap ap1 model WA6638-JP

[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050

[AC-wlan-ap-ap1] quit

#APを起動します。APは次の操作を実行します。

- DHCPサーバーからIPv6アドレス1::2を取得します。
- オプション52を介してACのIPv6アドレスを取得します。
- ACとの間にCAPWAPトンネルを確立します。

設定の確認

#次の情報を確認します。

- APはDHCPを介してACのIPアドレスを取得します。
- APとACは、CAPWAPトンネルを確立しています。
- APはRun状態です。

[AC]display wlan ap name ap1verbose

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	: WA4320i-ACN
Region code	: CN
Region code lock	: Disable
Serial ID	: 219801A0CNC138011454
MAC address	: 0AFB-423B-893C
IP address	: 1::2
UDP control port number	: 18313

UDP data port number : N/A
H/W version : Ver.C
S/W version : R2206P02
Boot version : 1.01
USB state : N/A
Power Level : N/A
PowerInfo : N/A
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 : 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
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
    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
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
Smart antenna : Enabled
Smart antenna policy : Auto
Protection mode : rts-cts
Continuous mode : N/A
HT protection mode : No protection

Radio 2:

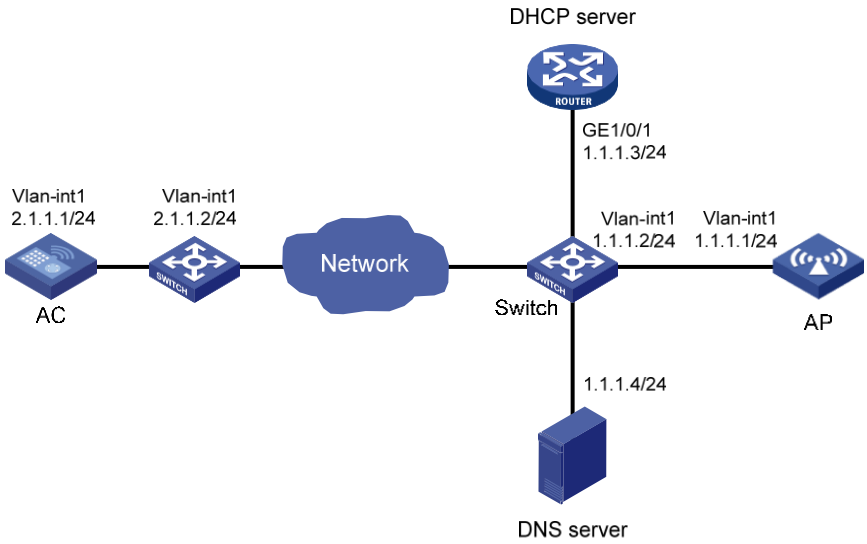
Basic BSSID : 7848-59f6-3950
Admin state : Down
Radio type : 802.11b
Antenna type : internal
Client dot11n-only : Disabled
Channel band-width : 20MHz
Active band-width : 20MHz
Secondary channel offset : SCN
Short GI for 20MHz : Supported
Short GI for 40MHz : Supported
A-MSDU : Enabled
A-MPDU : Enabled
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 : 5(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
Smart antenna : Enabled
Smart antenna policy : Auto
Protection mode : rts-cts
Continuous mode : N/A
HT protection mode : No protection

DNSによるCAPWAPトンネルの確立の設定例

ネットワーク要件

図5に示すように、APを設定してDNS経由でACのIPアドレスを取得し、ACとの間にCAPWAPトンネルを確立します。

図5:ネットワーク図



構成手順

1. DHCPサーバーを設定します。

   #DHCPサービスを有効にして、DHCPアドレスプール1を設定し、ACのドメイン名サフィックスをabcに設定します。

   <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

   [DHCP server-dhcp-pool-1] dns-list 1.1.1.4

   [DHCP server-dhcp-pool-1] gateway-list 1.1.1.2

   [DHCP server-dhcp-pool-1]quit

   [DHCP server] quit

2. ドメイン名h3c.abcとIPアドレス2.1.1.1/24間のマッピングを設定します。詳細については、『Layer3IP Services Configuration Guide』を参照してください(詳細は省略)。

3. ACを次のように設定します。

   #VLANインターフェイス1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

#ネクストホップアドレスが2.1.1.2のデフォルトルートを設定します。

[AC] ip route-static 0.0.0.0 0 2.1.1.2

#AP ap1を作成し、そのモデルとシリアルIDを指定します。

[AC]wlan ap ap1 model WA6638-JP

[AC-wlan-ap-ap1] serial-id 210235A1BSC123000050

#APを起動します。

[AC-wlan-ap-ap1] quit

APは、次の操作を実行します。

- DHCPサーバーからIPアドレス1.1.1.1、ACのドメイン名 サフィックス、およびDNSサーバーのIPアドレスを取得します。
- ドメイン名の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クライアントに通知します。
- ACのIPアドレスを使用して、ACとのCAPWAPトンネルを確立します。

設定の確認

#次の情報を確認します。

- APとACは、CAPWAPトンネルを確立しています。
- APはRun状態です。
- APは、DNSを介して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                           : WA4320i-ACN
Region code                      : CN
Region code lock                : Disable
Serial ID                        : 210235A1BSC123000050
MAC address                     : 0AFB-423B-893C
IP address                      : 1.1.1.1
UDP control port number         : 18313
UDP data port number            : N/A
H/W version                     : Ver.C
S/W version                      : R2206P02
Boot version                    : 1.01
USB state                       : N/A
```

Power Level : N/A
PowerInfo : N/A
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 : 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
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
    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
    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
Smart antenna : Enabled
Smart antenna policy : Auto
Protection mode : rts-cts
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
A-MSDU : Enabled
A-MPDU : Enabled
LDPC : Not Supported

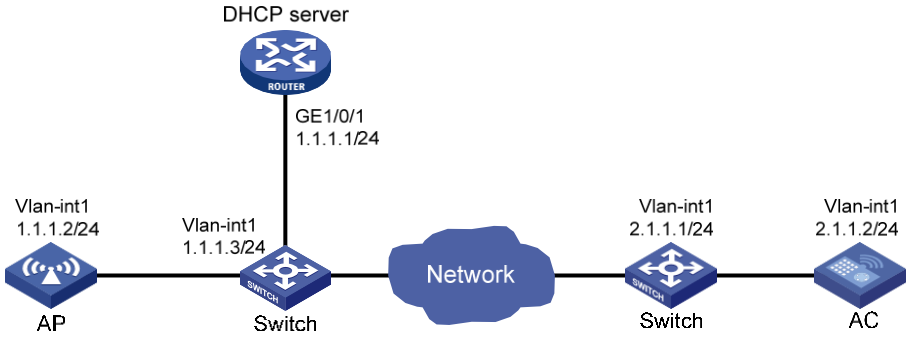
STBC : Supported
Operational HT MCS Set:
Mandatory : Not configured
Supported : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9,
10, 11, 12, 13, 14, 15
Multicast : Not configured
Channel : 5(auto)
Channel usage(%) : 0
Max power : 20 dBm
Preamble type : Short
Operational rate:
Mandatory : 1, 2, 5.5, 11 Mbps
Multicast : 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
Smart antenna : Enabled
Smart antenna policy : Auto
Protection mode : rts-cts
Continuous mode : N/A
HT protection mode : No protection

自動APの設定例

ネットワーク要件

図6に示すように、ACで自動AP機能を有効にします。APはDHCPオプション43を使用してAC IPアドレスを取得し、ACとのCAPWAPトンネルを確立します。

図6ネットワーク図



構成手順

1. DHCPサーバーを設定します。

   #DHCPサービスを有効にします。

   <DHCP server> System-view

   [DHCP server] dhcp enable

   #DHCPアドレスプール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

   #オプション43を構成して、アドレスプール0内のACのIPアドレスを指定します。一番右のバイト02010102(2.1.1.2)は、ACのIPアドレスを表します。

   [DHCP Server-dhcp-pool-1] option 43 ip-address hex800700000102010102

   [DHCP Server-dhcp-pool-1] gateway-list 1.1.1.3

   [DHCP Server-dhcp-pool-1] quit

   [DHCP Server] quit

2. ACを次のように設定します。

   #AC上のVLANインターフェイス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

   #ネクストホップが2.1.1.1のデフォルトルートを設定します。

   [AC] ip route-static 0.0.0.0 0 2.1.1.1

#自動APを有効にします。

[AC] wlan auto-ap enable

設定の確認

#APがACとの間にCAPWAPトンネルを確立していることを確認します。

[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	: WA6638-JP
Region code	: CN
Region code lock	: Disable
Serial ID	: 219801A0CNC138011454
MAC address	: 0011-2200-0101
IP address	: 1.1.1.2
UDP control port number	: 18313
UDP data port number	: N/A
H/W version	: Ver.C
S/W version	: R2206P02
Boot version	: 1.01
USB state	: N/A
Power Level	: N/A
PowerInfo	: N/A
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	: 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
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
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
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
Smart antenna : Enabled
Smart antenna policy : Auto
Protection mode : rts-cts
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
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 : 5(auto)
Channel usage(%) : 0

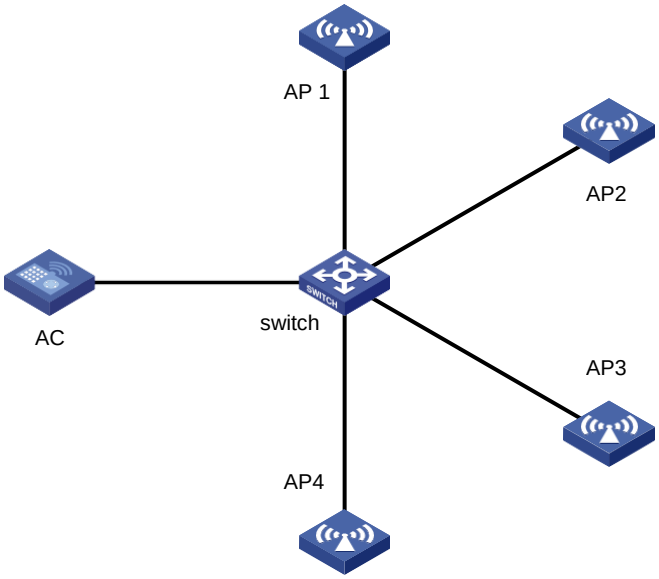
Max power : 20 dBm
Preamble type : Short
Operational rate:
Mandatory : 1, 2, 5.5, 11 Mbps
Multicast : Auto
Supported : 6, 9, 12, 18, 24, 36, 48, 54 Mbps
Disabled : Not configured
Distance : 1 km
ANI : Enabled
Fragmentation threshold : 2346 bytes
Beacon interval : 100 TU
Protection threshold : 2346 bytes
Long retry threshold : 4
Short retry threshold : 7
Maximum rx duration : 2000 ms
Noise Floor : 0 dBm
Smart antenna : Enabled
Smart antenna policy : Auto
Protection mode : rts-cts
Continuous mode : N/A
HT protection mode : No protection

APグループの設定例

ネットワーク要件

図7に示すように、APグループを構成して、APグループgroup1にAP1を追加し、APグループgroup2にAP2、AP3、およびAP4を追加します。

図7:ネットワーク図



設定手順

1. DHCPサーバーからIPアドレスとAC IPアドレスを取得するようにAPを設定します(詳細は表示されません)。
2. 手動APを設定します(詳細は表示されません)。
3. APグループを設定します。

   #APグループgroup1を作成します。

   <AC>System-view

   [AC]wlan ap-group group 1

   #APグループgroup1にap1を追加します。

   [AC-wlan-ap-group-group1] ap ap1

   [AC-wlan-ap-group-group1] quit

   #APグループgroup2を作成します。

   [AC] wlan ap-group group 2

   #APグループgroup2にap2、ap3、およびap4を追加します。

   [AC-wlan-ap-group-group2] ap ap2 ap3 ap4

   [AC-wlan-ap-group-group2] quit

   [AC] quit

設定の確認

#AP1がAPグループgroup1に属し、AP2、AP3、およびAP4がAPグループgroup2に属していることを確認します。

```
[AC-wlan-ap-group-group2] display wlan ap-group AP
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                        : WA6638-JP
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                        : WA6638-JP
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)
```