H3Cアクセスコントローラ

WLANアクセス設定ガイド

New h3c Technologies
Co.,Ltd.http://www.h3c.com

Document version: 6W103-20200507
Product version: R5426P02

はじめに

アクセスコントローラのマニュアルセットには、アクセスコントローラのソフトウェア機能とソフトウェア設定手順が記載されています。これらのマニュアルには、さまざまなネットワークシナリオにソフトウェア機能を適用するための設定例も記載されています。

『WLAN Access Configuration Guide』では、WLANアクセス設定について説明します。ここでは、マニュアルに関する次のトピックについて説明します。

- 対象者
- 表記規則
- ドキュメントのフィードバック

対象者

このマニュアルの対象読者:

- ネットワークプランナー
- フィールドテクニカルサポートおよびサービスエンジニア
- H3Cアクセスコントローラを操作するネットワーク管理者

表記規則

ここでは、マニュアルで使用されている表記規則について説明します。

コマンドの規則

表記規則	説明
太字	太字のテキストは、表示されているとおりに入力したコマンドとキーワードを表します。
Italic	斜体テキストは、実際の値に置き換える引数を表します。
[ ]	角カッコは、オプションの構文選択(キーワードまたは引数)を囲みます。
{ x | y | ... }	中カッコは、必要な構文のセットを縦棒で区切って囲み、その中から1つを選択します。
[x | y | ...]	角かっこは、オプションの構文オプションのセットを縦棒で区切って囲み、その中から1つまたは何も選択しないようにします。
{ x | y | ... } *	アスタリスクでマークされた中カッコは、必要な構文の選択肢を縦棒で区切ったもので、その中から1つ以上を選択します。
[x | y | ...] *	アスタリスクの付いた角カッコは、オプションの構文の選択肢を縦棒で区切って囲みます。縦棒では、1つの選択肢、複数の選択肢、またはなしを選択できます。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1～n回入力できます。
#	#記号で始まる行がコメントです。

GUIの規則

表記規則	説明
太字	ウィンドウ名、ボタン名、フィールド名およびメニューアイテムは太字で表示されます。 たとえば、**新規ユーザー**ウィンドウが開き、**OK**をクリックします。

表記規則	説明
>	マルチレベルメニューは山括弧で区切られます。たとえば、File > Create > Folder

記号

表記規則	説明
⚠	重要な情報への注意を喚起するアラートで、理解またはフォローしないと人身事故につながる可能性があります。
△	重要な情報への注意を喚起するアラート。理解またはフォローしていないと、データの消失、データの破損、ハードウェアまたはソフトウェアの損傷につながる可能性があります。
ⓘ	重要な情報への注意を促すアラート。
注:	追加情報または補足情報を含むアラート。
	有用な情報を提供するアラート。

ネットワークトポロジアイコン

表記規則	説明
	ルータ、スイッチ、ファイアウォールなどの汎用ネットワークデバイスを表します。
	ルータやレイヤ3スイッチなどのルーティング対応デバイスを表します。
	レイヤ2またはレイヤ3スイッチなどの一般的なスイッチ、またはレイヤ2その他のレイヤ2機能をサポートするルータを表します。
	統合有線WLANスイッチ上のアクセスコントローラ、統合有線WLANモジュール、またはアクセスコントローラエンジンを表します。
	アクセスポイントを表します。
	ワイヤレスターミネータユニットを表します。
	ワイヤレスターミネータを表します。
	メッシュアクセスポイントを表します。
	全方向信号を表します。
	方向信号を表します。
	ファイアウォール、UTM、マルチサービスセキュリティゲートウェイ、ロードバランシングデバイスなどのセキュリティ製品を表します。
	ファイアウォール、ロードバランシング、NetStream、SSL VPN、IPS、ACGモジュールなどのセキュリティモジュールを表します。

本書に記載されている例

このドキュメントの例では、使用しているデバイスとハードウェアモデル、構成、またはソフトウェアバージョンが異なるデバイスを使用している場合があります。通常、ポート番号、サンプル出力、スクリーンショット、およびその他の情報は、使用しているデバイスとは異なります。

ドキュメントに関するフィードバック

製品ドキュメントに関するご意見は、info@h3c.comまで電子メールでお寄せください。

ご意見をいただければ幸いです。

内容

WLANアクセスの設定 8
WLANアクセスについて 8
WLANアクセスプロセス 8
スキャン中 8
関連付け 10
クライアントアクセス制御 10
APグループベースのアクセス制御 10
SSIDベースのアクセス制御 11
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制御 12
ACLベースのアクセス制御 13
ゲスト トンネル 13
ゲスト トンネルについて 13
ゲスト トンネルの確立 13
制約事項およびガイドライン:WLANアクセス設定 13
WLANアクセスタスクの概要 14
リージョンコードの設定 16
リージョンコードを指定する 16
ビーコンフレームおよびプローブ応答における領域コードの包含または除外 17
ワイヤレスサービスの設定 17
サービステンプレートの設定 17
サービステンプレートの説明の設定 18
SSIDの設定 18
サービステンプレートに関連付けられたクライアントの最大数の設定 18
サービステンプレートの有効化 19
サービステンプレートのワイヤレスへのバインド 19
APグループから指定されたサービステンプレートを継承しないようにAPを設定する 20
クライアントデータ転送の構成 20
クライアント トラフィックフォワーダの指定 20
クライアント トラフィック転送のイネーブル化 21
クライアントデータフレームのカプセル化形式の設定 23
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指定 23
クライアント管理の構成 24
ACまたはAPでのクライアントアソシエーションのイネーブル化 24
クイックアソシエーションの有効化 24
クライアント情報が報告されるWebサーバーの指定 24
指定した形式でのクライアントログの生成の有効化 25
クライアントのVLAN割り当て方法の設定 25
ローミング後に認可VLANを優先するようにクライアントを設定する 26
ローカル認証が成功した場合の即時クライアントアソシエーションのイネーブル化 27
クライアントのキャッシュのエージングタイマーの設定 27
クライアント再認証前のアイドル期間の設定 27
クライアントトラフィックのディファレンシエーテッド アカウンティングの設定 28
ローミング拡張の有効化 29
クライアント メンテナンスの設定 30
クライアント アイドルタイムアウトの設定 30
クライアント キープアライブの設定 31
ワイヤレスリンク品質テストの実行 31
クライアント統計レポートの設定 31
NAS IDの設定 32
NASポートタイプの設定 33
クライアントアソシエーション比率の最適化の設定 34
iMCサーバーの指定 34
VIPクライアントの設定 34
VIPクライアントグループの設定 34
非VIPクライアントレート制限の設定 35
ポリシーベース転送の設定 35
ハードウェアとポリシーベース転送の互換性 35
ポリシーベース転送の制約事項およびガイドライン 37

ポリシーベース転送の前提条件 37
転送ポリシーの設定 37
ローカル転送モードでの外部ネットワークへのトラフィック転送のイネーブル化 37
サービステンプレートへの転送ポリシーの適用 38
ユーザープロファイルへの転送ポリシーの適用 38
ゲスト トンネルの設定 39
ゲスト トンネルとのハードウェア互換性 39
エッジACのための集約ACの指定 40
集約ACのエッジACの指定 41
ゲスト トンネルフロー配信のイネーブル化 42
クライアントアクセス制御の構成 42
クライアントアソシエーションの許可APグループの指定 42
クライアントアソシエーションの許可SSIDの指定 42
ホワイトリストへのクライアントの追加 43
スタティック ブラックリストへのクライアントの追加 43
ダイナミック ブラックリストの設定 43
ACLベースのアクセス制御の設定 44
ブロードキャストプローブ要求に対するAPの応答のディセーブル化 45
WLANアクセスに対するSNMP通知の有効化 45
スマートクライアントアクセスの有効化 46
WLANアクセス用の表示およびメンテナンスコマンド 46
WLANアクセスの設定例 48
例:WLANアクセスの設定 48
例:ホワイトリストベースのアクセスコントロールの設定 50
例:スタティックブラックリストベースのアクセスコントロールの設定 50
例:ACLベースのアクセスコントロールの設定 51
例:ゲストトンネルの設定 52
例:IPSecゲストトンネルの設定 53
例:NATを介したIPSecゲストトンネルの設定 57

WLANアクセスの設定

WLANアクセスについて

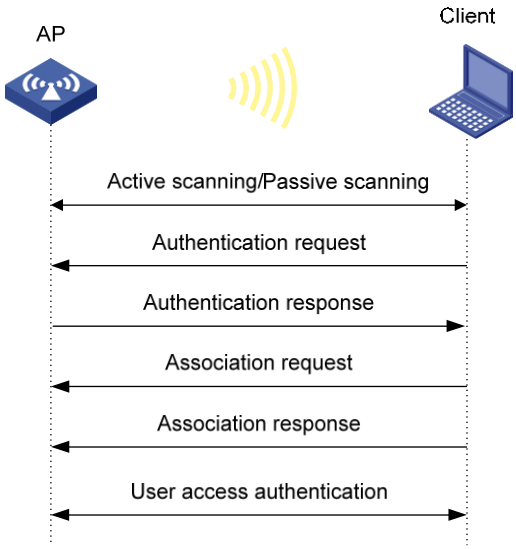
ワイヤレスアクセスは、有線ネットワークのエッジに配置されたAPによって提供されます。APは、有線接続を介してアップリンクに接続し、ダウンリンククライアントにワイヤレスアクセスサービスを提供します。

WLANアクセスプロセス

ワイヤレスクライアントがWLANにアクセスできるのは、スキャン、リンクレイヤ認証、アソシエーション、およびWLAN認証プロセスが完了した場合だけです。

データリンク層認証の詳細については、『WLAN Security Configuration Guide』を参照してください。WLAN認証の詳細については、『User Access and Authentication Configuration Guide』を参照してください。

図1 WLANアクセスプロセス



スキャン中

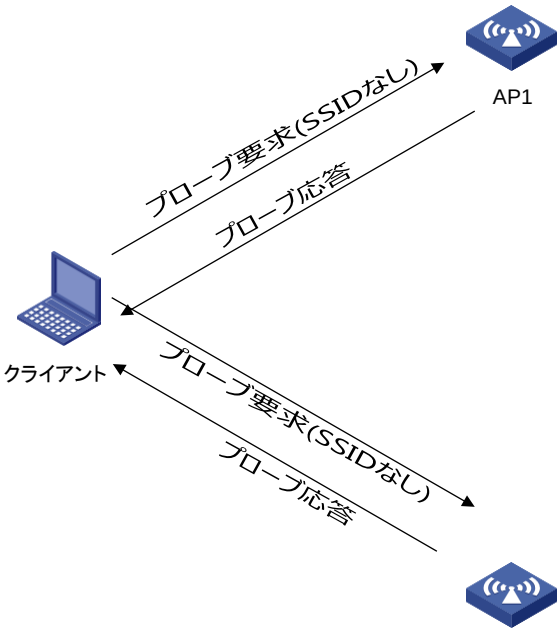
アクティブスキャン

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ます。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。プローブ要求にSSIDが含まれているかどうかに基づいて、アクティブスキャンは次のタイプに分類できます。

- すべてのワイヤレスネットワークのアクティブスキャン。

  図2に示すように、クライアントは、ワイヤレスネットワークをスキャンするために、サポートされている各チャネルにプローブ要求を定期的に送信します。プローブ要求を受信したAPは、使用可能なワイヤレスネットワーク情報を伝送するプローブ応答を送信します。クライアントは、最適なAPに関連付けされます。

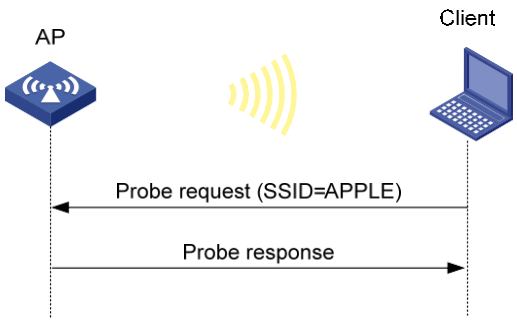
図2 すべてのワイヤレスネットワークのスキャン



- 特定のワイヤレスネットワークのアクティブスキャン。

  図3に示すように、クライアントは、指定されたSSIDまたはクライアントが関連付けられているワイヤレスネットワークのSSIDを含むプローブ要求を定期的に送信します。指定されたSSIDでワイヤレスサービスを提供できるAPがプローブ要求を受信すると、プローブ応答を送信します。

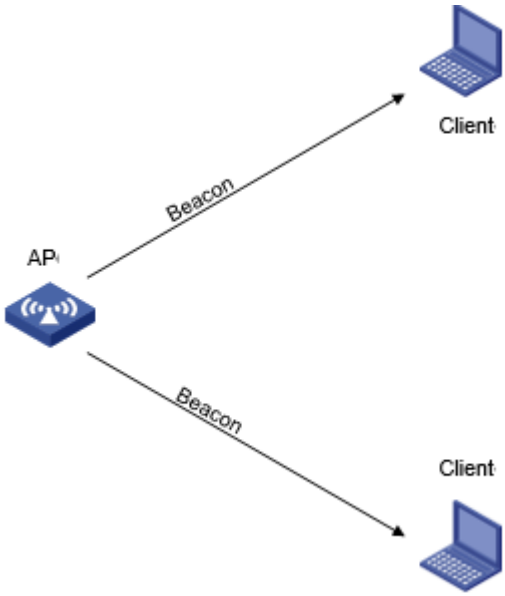
  図3 特定のワイヤレスネットワークのスキャン



パッシブスキャン

図4に示すように、クライアントは、サポートされているチャネル上のAPから送信されるビーコンフレームを定期的にリッスンして、周囲のワイヤレスネットワークに関する情報を取得します。次に、クライアントはアソシエーション用のAPを選択します。パッシブスキャンは、クライアントが電力を節約したい場合に使用します。

図4 パッシブスキャン



関連付け

クライアントは、データリンク層認証を通過した後、関連付けられたAPにアソシエーション要求を送信します。要求を受信すると、APはワイヤレスクライアントがサポートする機能を決定し、クライアントにアソシエーション応答を送信します。クライアントはAPに関連付けられます。

クライアントアクセス制御

次のクライアントアクセス制御方式を使用できます。

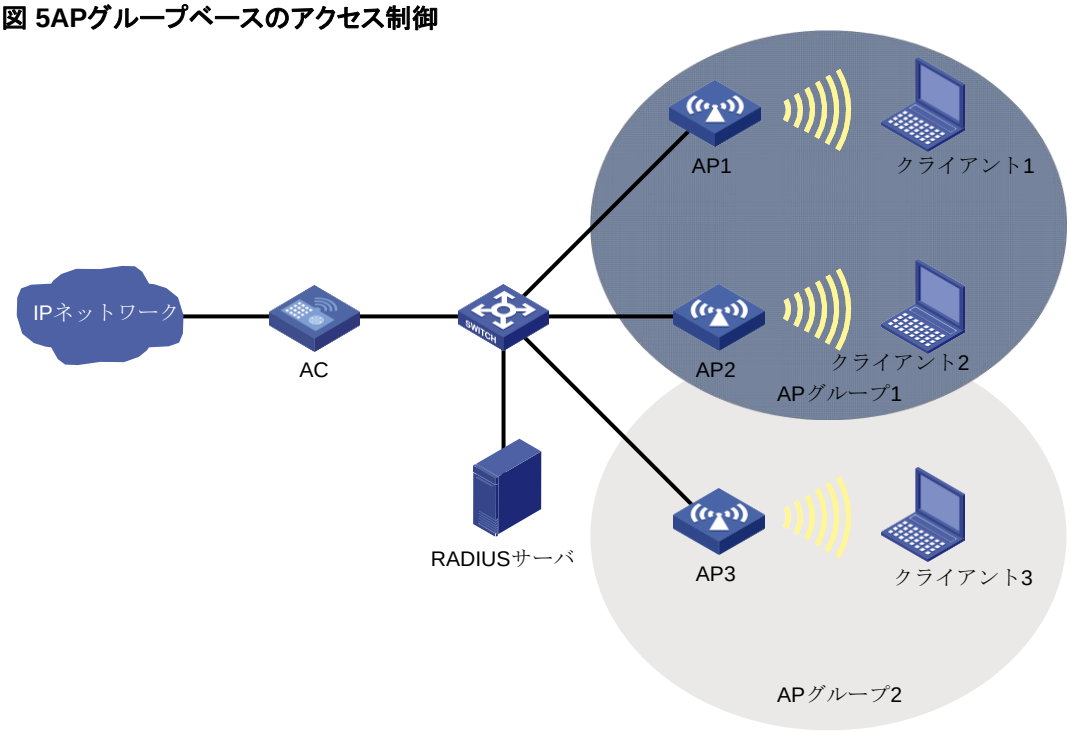
- APグループベースのアクセスコントロール： 指定したAPグループ内のAPに関連付けられたクライアントがWLANにアクセスできるようにします。
- SSIDベースのアクセスコントロール： 指定したSSIDに関連付けられたクライアントがWLANにアクセスできるようにします。
- ホワイトリストおよびブラックリストベースのアクセスコントロール： ホワイトリストおよびブラックリストを使用して、クライアントアクセスを制御します。
- ACLベースのアクセスコントロール： APまたはサービステンプレートにバインドされたACLルールを使用して、クライアントアクセスを制御します。

APグループベースのアクセス制御

図5に示すように、APグループベースのアクセスコントロールの場合、APグループ1をクライアント1およびクライアント2の許可APグループとして設定し、APグループ2をクライアント3の許可APグループとして設定します。

クライアントが認証に合格すると、サーバーは関連するユーザープロファイルをACに送信します。ACは、クライアントが関連付けられているAPが許可されたAPグループに含まれているかどうかを調べます。含まれている場合、クライアントはWLANにアクセスできます。含まれていない場合、ACはクライアントからログオフします。

図 5APグループベースのアクセス制御

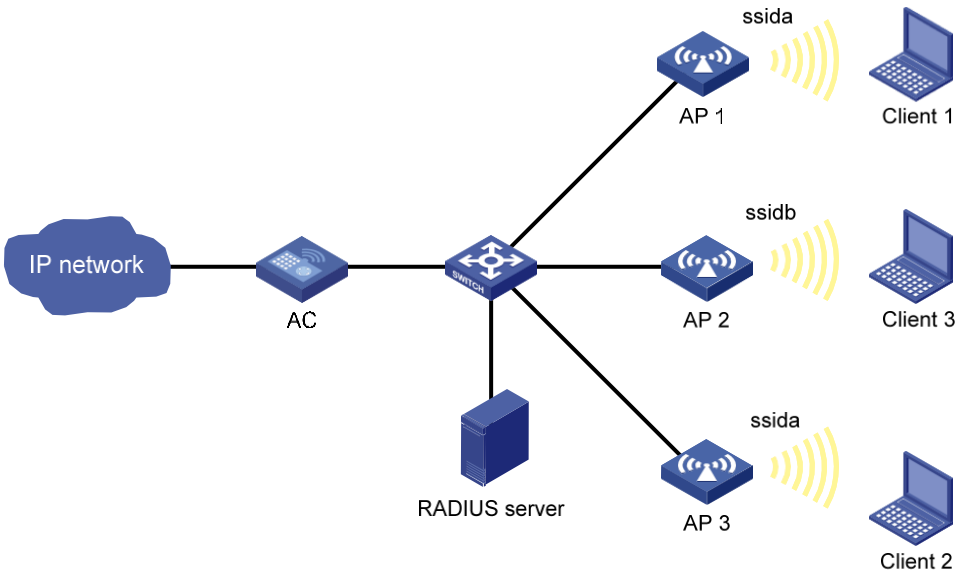


SSIDベースのアクセス制御

図6に示すように、SSIDベースのアクセス制御では、ssidaをクライアント1とクライアント2の許可されたSSIDとして設定し、ssdbをクライアント3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、サーバーは関連するユーザープロファイルを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。SSIDである場合、クライアントはWLANにアクセスできます。SSIDでない場合、ACはクライアントからログオフします。

図6 SSIDベースのアクセス制御



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制御

クライアントアクセスコントロール用にクライアントからフレームをフィルタリングするようにホワイトリストまたはブラックリストを設定できます。

ホワイトリストベースのアクセス制御

ホワイトリストには、WLANへのアクセスが許可されているすべてのクライアントのMACアドレスが含まれています。ホワイトリストに含まれていないクライアントからのフレームは廃棄されます。このリストは手動で設定されます。

ブラックリストベースのアクセス制御

アクセス制御には、次のブラックリストを使用できます。

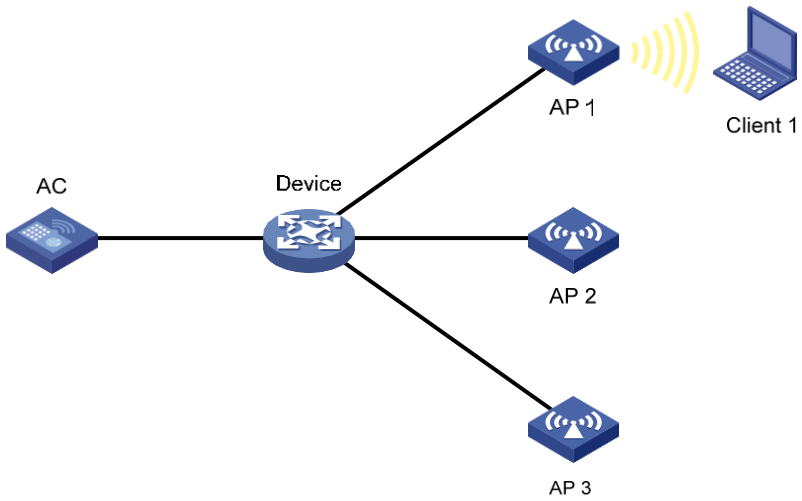
- スタティックブラックリスト： WLANへのアクセスが禁止されているクライアントのMACアドレスが含まれます。このリストは手動で設定します。
- ダイナミックブラックリスト： WLANへのアクセスが禁止されているクライアントのMACアドレスが含まれます。APは、WLANへのアクセスが禁止されているクライアントのMACアドレスを、WIPSが設定されている場合、またはWLAN MAC認証クライアントに対してURLリダイレクションが有効になっている場合に、リストに追加します。エージングタイムが経過すると、リスト内のエントリは削除されます。ダイナミックブラックリストは、設定に応じてACまたはAPに対して有効にできます。WIPSの詳細については、『WLAN Security Configuration Guide』を参照してください。WLAN MAC認証の詳細については、『User Access and Authentication Configuration Guide』を参照してください。

動作メカニズム

APがアソシエーション要求を受信し、Add Mobileメッセージを ACに送信すると、ACは次の操作を実行して、クライアントを許可するかどうかを決定します。

1. ホワイトリストを検索します。
   - クライアントMACアドレスがホワイトリストのど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。
   - 一致が見つかった場合、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に、スタティックおよびダイナミックブラックリストを検索します。
   - 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。
   - 一致が見つからない場合、また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7 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制御



ACLベースのアクセス制御

この機能は、APまたはサービステンプレートにバインドされたACLルールを使用してクライアントアクセスを制御します。クライアントからアソシエーション要求を受信すると、デバイスは次のアクションを実行します。

- 一致が検出され、ルールアクションが許可されている場合に、クライアントがWLANにアクセスできるようにします。
- 一致が見つからない場合、または一致したルールにdeny文が含まれる場合、クライアントのWLANへのアクセスを拒否します。

ゲストトンネル

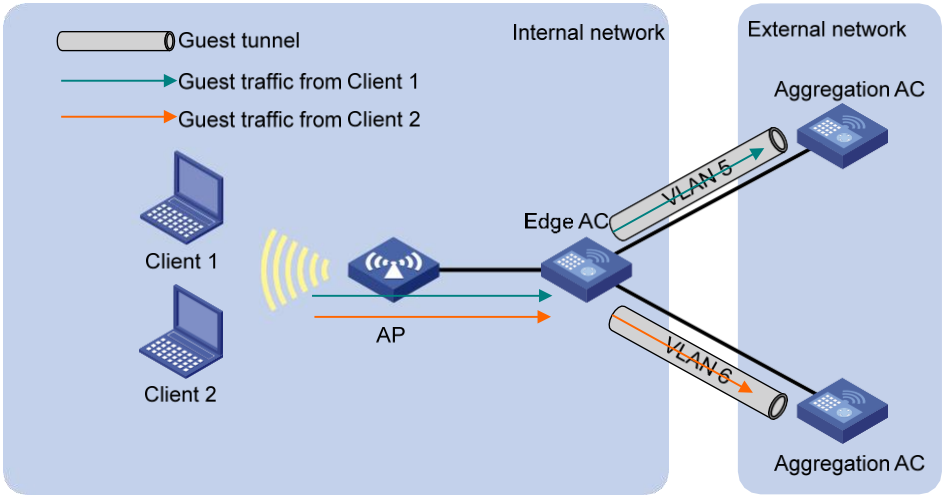
ゲストトンネルについて

ゲスト トンネル機能を使用すると、ACは外部ネットワーク宛てのゲス トトラフィックを、隔離されたトンネルを介して外部ネットワーク内のACに転送し、内部ネットワークを保護できます。

図8に示すように、ゲスト トンネルは、ユーザーアクセスおよび認証用の内部ネットワーク内のエッジACと、データ処理用の外部ネットワーク内の集約ACとの間に確立されます。ゲストは特定のゲストVLANからのみ内部ネットワークにアクセスでき、ゲスト トラフィックはゲストと同じVLAN内の集約ACに転送されます。

ゲス トトンネルは、トンネル暗号化のためのIPSec、およびNATを介したトンネル確立のためのNATトラバーサルもサポートしています。

図8 ゲストトンネルの動作メカニズム



ゲストトンネルの確立

ゲスト トンネル設定がエッジACと集約ACで設定された後、エッジACはキープアライブ要求を集約ACに送信します。要求を受信すると、集約ACはキープアライブ応答を送信します。ゲストトンネルは、エッジACが応答を受信すると確立されます。

制約事項およびガイドライン:WLANアクセス

設定

次の方法を使用してAPを設定できます。

- 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、同じパラメータに対してこれらのビューで行った設定は、APビュー、APグループビュー、グローバルコンフィギュレーションビューの順に有効になります。

WLANアクセスタスクの概要

WLANアクセスを設定するには、次の作業を実行します。

1. (オプション)リージョンコードの設定
    - リージョンコードの指定
    - ビーコンフレームおよびプローブ応答におけるリージョンコードの包含または除外
2. ワイヤレスサービスの設定
    - サービステンプレートの設定
    - (オプション)サービステンプレートの説明の設定
    - SSIDの設定
    - (オプション)サービステンプレートに関連付けられているクライアントの最大数の設定
    - サービステンプレートの有効化
    - サービステンプレートのワイヤレスへのバインド
    - (オプション)指定したサービステンプレートをAPグループから継承しないようにAPを設定する
3. (オプション)クライアントデータ転送の構成
    - クライアントトラフィックフォワーダの指定
    - クライアントトラフィック転送の有効化
    - クライアントデータフレームのカプセル化形式の設定
    - 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指定
4. (オプション)クライアント管理の構成
    - ACまたはAPでのクライアントアソシエーションのイネーブル化
    - クイックアソシエーションの有効化

- クライアント情報が報告されるWebサーバーの指定
- 指定された形式でのクライアントログの生成の有効化
- クライアントのVLAN割り当て方法の設定
- ローミング後に許可VLANを優先するようにクライアントを設定する
- ローカル認証が成功した場合の即時クライアントアソシエーションの有効化
- クライアントのキャッシュのエージングタイマーの設定
- クライアント再認証前のアイドル期間の設定
- クライアントトラフィックのディファレンシエーテッドアカウンティングの設定
- ローミング拡張の有効化

5. (オプション)クライアントメンテナンスの設定
   - クライアントアイドルタイムアウトの設定
   - クライアントキープアライブの設定
   - ワイヤレスリンク品質テストの実行
   - クライアント統計レポートの設定
   - NAS IDの設定
   - NASポートタイプの設定
   - クライアントのアソシエーション比率の最適化の構成
   - iMCサーバーの指定
6. (オプション)VIPクライアントの設定
   - VIPクライアントグループの設定
   - 非VIPクライアントレート制限の設定
7. (オプション)ポリシーベース転送の設定
8. (オプション)ゲストトンネルの設定
9. (オプション)クライアントアクセス制御の設定
   - クライアントアソシエーションの許可APグループの指定
   - クライアントアソシエーションの許可SSIDの指定
   - ホワイトリストへのクライアントの追加
   - 静的ブラックリストへのクライアントの追加

- ダイナミックブラックリストの設定
- ACLベースのアクセス制御の設定

10. (オプション)ブロードキャストプローブ要求へのAPの応答のディセーブル化
11. (オプション)WLANアクセスに対するSNMP通知のイネーブル化

リージョンコードの設定

リージョンコードを指定する

このタスクについて

リージョンコードは、使用可能な周波数、使用可能なチャネル、送信電力レベルなどの特性を決定します。APを設定する前に、有効なリージョンコードを設定してください。

リージョンコードの変更による規定違反を防ぐには、リージョンコードをロックします。

手順

1. システムビューに入ります。

   system-view
2. APビュー、APグループビュー、グローバルコンフィギュレーションビュー、APプロビジョニングビュー、またはAPグループプロビジョニングビューを入力します。
   - APビューに入ります。

     wlan ap *ap-name*
   - APグループビューに入ります。

     wlan ap-group *group-name*
   - 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
   - 次のコマンドを順番に実行して、APプロビジョニングビューを開始します。

     wlan ap *ap-name*

     provision
   - 次のコマンドを順番に実行して、APグループプロビジョニングビューを開始します。

     wlan ap-group *group-name*

     provision
3. リージョンコードを指定します。

   region-code *code*

   デフォルトは:
   - APビューでは、APはAPグループビューの設定を使用します。APグループビューにリージョンコードが存在しない場合、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は、リージョンコードは指定されません。
   - APプロビジョニングビューでは、APはAPグループプロビジョニングビューの設定を使用します。
   - APグループプロビジョニングビューでは、リージョンコードが指定されていません。
4. (オプション)リージョンコードをロックします。

region-code-lock *enable*

デフォルトは:

- APビューでは、APはAPグループビューの設定を使用します。APグループビューにリージョンコードが存在しない場合、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は、リージョンコードはロックされません。

ビーコンフレームおよびプローブ応答における領域コードの包含または除外

制約事項とガイドライン

ビーコンフレームおよびプローブ応答にリージョンコードを含めるようにAPをイネーブルにする場合は、APインストール環境も指定する必要があります。異なるサービステンプレートをAPのワイヤレスにバインドする場合は、サービステンプレートが同じインストール環境タイプで指定されていることを確認してください。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*
3. ビーコンフレームおよびプローブ応答にリージョンコードを含めるか除外し、インストール環境タイプを指定します。

   region-code-ie { **disable** | **enable** { **any** | **indoor** | **outdoor** } }

   デフォルトでは、ビーコンフレームおよびプローブ応答にはリージョンコードが含まれますが、インストール環境タイプは含まれません。

ワイヤレスサービスの設定

サービステンプレートの設定

このタスクについて

サービステンプレートは、SSIDや認証方式などの一連のワイヤレスサービス属性を定義します。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートを作成します。

   wlan service-template *service-template-name*

   デフォルトでは、サービステンプレートは存在しません。
3. (任意)サービステンプレートを介してオンラインになるクライアントを、指定したVLANに割り当てます。

   vlan *vlan-id*

   デフォルトでは、クライアントはサービステンプレートを介してオンラインになった後にVLAN1に割り当てられます。

サービステンプレートの説明の設定

1. システムビューに入ります。
   system-view
2. サービステンプレートビューに入ります。
   wlan service-template *service-template-name*
3. サービステンプレートの説明を設定します。
   description *text*
   デフォルトでは、サービステンプレートの説明は設定されていません。

SSIDの設定

このタスクについて

APはビーコンフレーム内のSSIDをアドバタイズします。BSS内のクライアント数が制限を超えている場合、またはBSSが利用できない場合は、SSID-hiddenを有効にして、クライアントがBSSを検出できないようにすることができます。SSID-hiddenを有効にすると、BSSはビーコンフレーム内のSSIDを隠し、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を持つプローブ要求を送信する必要があります。この機能により、WLANが攻撃されないように保護できます。

手順

1. システムビューに入ります。
   system-view
2. サービステンプレートビューに入ります。
   wlan service-template *service-template-name*
3. サービステンプレートのSSIDを設定します。
   ssid *ssid-name*
   デフォルトでは、サービステンプレートにSSIDは設定されていません。
4. (任意)SSIDをイネーブルにします(ビーコンフレームで非表示)。
   beacon ssid-hide
   デフォルトでは、ビーコンフレームはSSIDを伝送します。

サービステンプレートに関連付けられたクライアントの最大数の設定

このタスクについて

過負荷を回避するために、関連付けられたクライアント数を制限するには、次の作業を実行します。この機能を設定すると、新しいクライアントはWLANにアクセスできなくなり、最大数に達するとSSIDが非表示になります。

手順

1. システムビューに入ります。
   system-view
2. サービステンプレートビューに入ります。
   wlan service-template *service-template-name*

3. サービステンプレートに関連付けられているクライアントの最大数を設定します。

   client max-count *max-number*

   デフォルトでは、サービステンプレートに関連付けられているクライアントの数に制限はありません。

サービステンプレートの有効化

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*
3. サービステンプレートを有効にします。

   service-template enable

   デフォルトでは、サービステンプレートはディセーブルです。

サービステンプレートのワイヤレスへのバインド

このタスクについて

サービステンプレートをワイヤレスにバインドすると、APはサービステンプレートで定義されたワイヤレスサービスを提供できるBSSを作成します。

サービステンプレートをワイヤレスにバインドする場合は、次のタスクを実行できます。

- BSSに関連付けられたクライアントがVLANグループ内のすべてのVLANに均等に割り当てられるように、VLANグループをワイヤレスにバインドします。
- NASポートIDまたはNAS IDをワイヤレスにバインドして、ネットワークアクセスサーバーを識別します。
- APをイネーブルにして、ビーコンフレーム内のSSIDを非表示にします。

制約事項とガイドライン

最大16個のサービステンプレートをワイヤレスにバインドできます。

手順

1. システムビューに入ります。

   system-view
2. APビューまたはAPグループのAPモデルビューに入ります。
   - APビューを入力します。

     wlan ap *ap-name*
   - APグループのAPモデルビューを入力するには、次のコマンドを順番に実行します。

     wlan ap-group *group-name*

     ap-model *ap-model*
3. ワイヤレスビューに入ります。

   radio *radio-id*
4. サービステンプレートをワイヤレスにバインドします。

   service-template *service-template-name* [**vlan** *vlan-id1* [*vlan-id2*] | **vlan-group** *vlan-group-name*] [**ssid-hide**] [**nas-port-id** *nas-port-id*] [**nas-id** *nas-id*]

   デフォルトは:
   - ワイヤレスビューでは、APグループのワイヤレスビューの設定が使用されます。

- APグループのワイヤレスビューでは、ワイヤレスにバインドされているサービステンプレートはありません。

vlan-id2引数とのハードウェア互換性については、デバイスのコマンドリファレンスを参照してください。

APグループから指定されたサービステンプレートを継承しないようにAPを設定する

このタスクについて

デフォルトでは、APグループ内のAPは、APグループにバインドされたサービステンプレートを継承し、BSSを作成します。この作業を実行して、APが属しているAPグループから指定されたサービステンプレートを継承しないようにAPを設定できます。

手順

1. システムビューに入ります。

   system-view
2. APビューに入ります。

   wlan ap *ap-name*
3. ワイヤレスビューに入ります。

   radio *radio-id*
4. 指定したサービステンプレートをAPグループから継承しないようにAPを設定します。

   inherit exclude service-template *service-template-name*

   デフォルトでは、APは所属するAPグループにバインドされたサービステンプレートを継承します。

クライアントデータ転送の構成

クライアント トラフィックフォワーダの指定

このタスクについて

AC(集中型転送)またはAP(ローカル転送)は、クライアント トラフィックを転送できます。APを使用してクライアント トラフィックを転送すると、ACの転送負荷が解放されます。

APがクライアント トラフィックを転送する場合、指定したVLANからトラフィックを転送するVLANまたはVLAN範囲をAPに指定できます。ACは他のVLANからデータトラフィックを転送します。

制約事項とガイドライン

ACを使用してクライアント トラフィックを転送する設定を有効にするには、クライアント トラフィック転送がイネーブルになっていることを確認します。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*
3. クライアントトラフィックフォワーダを指定します。

   client forwarding-location { **ac** | **ap** [**vlan** { start-vlan [**to** end-vlan] }] }

デフォルト設定の詳細については、デバイスのコマンドリファレンスを参照してください。

ACキーワードとのハードウェア互換性については、デバイスのコマンドリファレンスを参照してください。

クライアント トラフィック転送のイネーブル化

このタスクについて

AC階層型ネットワークでは、クライアント トラフィックフォワーダがACの場合、中央ACでこの機能を無効にし、ローカルACでこの機能を有効にします。これにより、ローカルACがダウンした場合の中央ACの管理パフォーマンスが保証されます。

AC階層の詳細については、『WLAN Advanced Features Configuration Guide』を参照してください。

ハードウェアと機能の互換性

ハードウェアシリーズ	モデル	製品コード	機能の互換性
WX1800Hシリーズ	WX1804H	EWP-WX1804H-PWR-CN	Yes
WX2500Hシリーズ	WX2508H-PWR-LTE WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	Yes
WX3000Hシリーズ	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	Yes: • WX3010H • WX3010H-X • WX3024H • WX3024H- No: • WX3010H-L • WX3024H-L
WX3500Hシリーズ	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H	Yes
WX5500Eシリーズ	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	Yes
WX5500Hシリーズ	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	Yes
アクセスコントローラモジュール	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F	Yes

	EWPXM1MAC0F	EWPXM1MAC0F	

ハードウェアシリーズ	モデル	製品コード	機能の互換性
WX1800Hシリーズ	WX1804H WX1810H WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	Yes
WX3800Hシリーズ	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	Yes
WX5800Hシリーズ	WX5860H	EWP-WX5860H-GL	Yes

制約事項とガイドライン

ACをクライアント トラフィックフォワーダとして設定する場合は、この機能をイネーブルにする必要があります。

手順

1. システムビューに入ります。

   system-view
2. クライアントトラフィック転送をイネーブルにします。

   wlan client forwarding enable

   デフォルトでは、クライアント トラフィック転送はイネーブルになっています。

クライアントデータフレームのカプセル化形式の設定

このタスクについて

集中型転送インフラストラクチャでは、APはCAPWAPトンネルを介してクライアントからACにデータフレームを送信します。クライアントデータフレームのカプセル化形式は802.3または802.11に設定できます。ACがフレーム形式変換を実行する必要がないように、形式を802.3に設定することをお勧めします。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*
3. クライアントデータフレームのカプセル化形式を設定します。

   client frame-format { **dot3** | **dot11** }

   デフォルトでは、クライアントデータフレームは802.3形式でカプセル化されます。

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指定

このタスクについて

指定したサービステンプレートを使用してAPを設定し、不明なクライアントからデータパケットをドロップしてこれらのクライアントの認証を解除するか、パケットだけをドロップするには、次の作業を実行します。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*
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指定します。

   unknown-client [**deauthenticate** | **drop**]

   デフォルトでは、APは不明なクライアントからのパケットを廃棄し、これらのクライアントの認証を解除します。

クライアント管理の構成

ACまたはAPでのクライアントアソシエーションのイネーブル化

このタスクについて

ACでクライアントアソシエーションをイネーブルにすると、管理フレームがCAPWAPトンネル経由でACに送信されます。これにより、セキュリティが確保され、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場合は、APでクライアントアソシエーションをイネーブルにすることをお勧めします。

手順

1. システムビューに入ります。
   system-view
2. サービステンプレートビューに入ります。
   wlan service-template *service-template-name*
3. ACまたはAPでクライアントアソシエーションをイネーブルにします。
   client association-location { **ac | ap** }
   デフォルトでは、クライアントアソシエーションはACで実行されます。

クイックアソシエーションの有効化

このタスクについて

ロードバランシングまたはバンドナビゲーションを有効にすると、クライアントのアソシエーション効率に影響する場合があります。遅延の影響を受けやすいサービスの場合、またはロードバランシングとバンドナビゲーションが不要な環境では、サービステンプレートのクイックアソシエーションを有効にできます。

クイックアソシエーションでは、サービステンプレートに関連付けられたクライアントでロードバランシングまたはバンドナビゲーションがディセーブルになります。デバイスは、これらの2つの機能がWLANでイネーブルになっていても、トラフィックのバランスをとったり、バンドナビゲーションを実行したりしません。

手順

1. システムビューに入ります。
   system-view
2. サービステンプレートビューに入ります。
   wlan service-template *service-template-name*
3. クイックアソシエーションを有効にします。
   quick-association enable
   デフォルトでは、クイックアソシエーションは無効になっています。

クライアント情報が報告されるWebサーバーの指定

このタスクについて

クライアントMACアドレス、関連付けられたAP、関連付け時間などのクライアント情報を、HTTPを介して指定されたWebサーバーにデバイスがレポートできるようにするには、次のタスクを実行します。Webサーバーは、サーバーのホスト名、ポート番号およびパスが指定されている場合にのみ、クライアント情報を受け入れます。

手順

1. システムビューに入ります。
   system-view
2. Webサーバーのホスト名とポート番号を指定します。
   wlan web-server host *host-name* **port** *port-number*
   デフォルトでは、Webサーバーのホスト名とポート番号は指定されていません。
3. Webサーバーのパスを指定します。
   wlan web-server api-path *path*
   デフォルトでは、Webサーバーのパスは指定されていません。
4. (任意)一度にレポートできるクライアントエントリの最大数を設定します。
   wlan web-server max-client-entry *number*
   デフォルトでは、一度に最大10個のクライアントエントリをレポートできます。

指定した形式でのクライアントログの生成の有効化

このタスクについて

デバイスは、次の形式のクライアントログをサポートしています。

- H3C： AP名、ワイヤレスID、クライアントMACアドレス、SSID、BSSID、およびクライアントのオンラインステータスをログに記録します。デフォルトでは、デバイスはH3C形式のクライアントログのみを生成します。
- Normal： AP MACアドレス、AP名、クライアントIPアドレス、クライアントMACアドレス、SSID、およびBSSIDをログに記録します。
- Sangfor： AP MACアドレス、クライアントIPアドレス、およびクライアントMACアドレスをログに記録します。

この機能を使用すると、デバイスは標準またはsangfor形式のクライアントログを生成し、そのログをインフォメーションセンターに送信できます。ログの送信先は、インフォメーションセンターの設定によって決まります。インフォメーションセンターの詳細は、「システム管理構成ガイド」を参照してください。

この機能は、H3C形式のクライアントログの生成には影響しません。

手順

1. システムビューに入ります。
   system-view
2. デバイスが指定された形式でクライアントログを生成できるようにします。
   customlog format wlan { **normal** | **sangfor** }
   デフォルトでは、デバイスはH3C形式のクライアントログのみを生成します。

クライアントのVLAN割り当て方法の設定

このタスクについて

クライアントが初めてオンラインになると、関連付けられたAPによってランダムVLANが割り当てられます。クライアントが再びオンラインになると、クライアントに割り当てられるVLANは割り当て方法によって異なります。

- スタティック割り当て： クライアントは、割り当てられているVLANを継承します。IPアドレスリースの期限が切れていない場合、クライアントは同じIPアドレスを使用します。この方法は、IPアドレスの保

存に役立ちます。

- ダイナミック割り当て： APはVLANをクライアントに再割り当てします。この方法では、すべてのVLANでクライアントのバランスを取ります。
- 互換性のあるスタティック割り当て： クライアントは、Comware5およびComware7 AC間のローミング時に割り当てられたVLANを継承します。

制約事項とガイドライン

クライアントがオフラインになり、再びオンラインになると、次の状況でVLANが変更される場合があります。

- スタティックまたは互換性のあるスタティック割り当てモードでは、元のVLANがVLANグループから削除されている場合、APはクライアントに新しいVLANを割り当てます。
- VLAN割り当て方法をダイナミックからスタティックまたはcompatible staticに変更すると、クライアントがオンラインに戻った後に、APがクライアントに異なるVLANを割り当てることがあります。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*
3. クライアントのVLAN割り当て方法を設定します。

   client vlan-alloc { **dynamic** | **static** | **static-compatible** }

   デフォルトでは、クライアントのVLAN割り当て方式はdynamicです。

   static-compatibleキーワードによるハードウェア互換性については、デバイスのコマンドリファレンスを参照してください。

ローミング後に認可VLANを優先するようにクライアントを設定する

このタスクについて

通常、クライアントのVLANはクライアントのローミング後も変更されません。ただし、クライアントが別のAPにローミングした後、IMCで設定されたセキュリティアラートをトリガーした場合、ユーザー分離のために発行された認可VLANが有効になります。

制約事項とガイドライン

この機能は、モビリティグループ内のすべてのACに設定することをお勧めし

ます。この機能は、802.1XおよびMAC認証クライアントでのみ有効です。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*
3. ローミング後に認可VLANを優先するようにクライアントを設定します。

   client preferred-vlan authorized

   デフォルトでは、クライアントはローミング後に認可VLANを優先します。

ローカル認証が成功した場合の即時クライアントアソシエーションのイネーブル化

このタスクについて

デフォルトでは、APは認証をACに渡すローカル認証クライアントに関する情報を報告します。ACはクライアントエントリを作成し、クライアントをオンラインにするようAPに通知します。ACとAP間のCAPWAPトンネルが正しく動作しない場合、クライアントはオンラインにならず、繰り返し再認証される可能性があります。

この問題を回避するには、ローカル認証が成功した直後にクライアントをオンラインにして、ACに到達できないときにAPがクライアントトラフィックを転送できるようにします。APは、トンネルが回復したときにクライアント情報をACに同期化します。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*
3. ローカル認証が成功した場合に、クライアントがただちにオンラインになるようにします。

   undo client report-mandatory

   デフォルトでは、ローカルで認証されたクライアントは、クライアント情報が正常に報告されるとオンラインになります。

クライアントのキャッシュのエージングタイマーの設定

このタスクについて

クライアントのキャッシュには、クライアントのPMKリスト、アクセスVLAN、およびその他の認可された情報が保存されます。エージングタイマーの期限が切れる前にオフラインクライアントが再びオンラインになると、高速ローミングのためにキャッシュ内のすべての情報を継承できます。エージングタイマーの期限が切れる前にクライアントがオンラインにならない場合、デバイスはクライアントキャッシュをクリアします。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*
3. クライアントのキャッシュのエージングタイマーを設定します。

   client cache aging-time *aging-time*

   デフォルトでは、クライアントのキャッシュのエージングタイマーは180秒です。

クライアント再認証前のアイドル期間の設定

このタスクについて

WLAN MAC認証のURLリダイレクションがイネーブルの場合、APは、RADIUSサーバーに情報が記録されていないクライアントを、Web認証用に指定されたURLにリダイレクトします。

Web認証を通過するクライアントはログオフされ、オンラインになるためにMAC再認証を実行する必要があります。ただし、クライアントに割り当てられたIPアドレスが期限切れになっていない場合、MAC再認証

は失敗します。

これらのクライアントがWeb認証に合格した後、指定されたアイドル期間にわたってダイナミックブラックリストに追加し、再認証の失敗を減らすには、次の作業を実行します。

手順

1. システムビューに入ります。

   system-view
2. クライアントの再認証前にアイドル時間を設定します。

   wlan client reauthentication-period [*period-value*]

   デフォルトでは、アイドル期間は10秒です。

クライアントトラフィックのディファレンシエーテッド アカウンティングの設定

このタスクについて

この機能により、APは、各ユーザープロファイルに適用されたアカウンティングポリシーに基づいて、クライアントトラフィックの差別化されたアカウンティングを実行できます。

クライアントアソシエーションでは、認証サーバーはクライアントアカウントにバインドされたユーザープロファイルをクライアントオーセンティケータ(ACまたはAP)に展開します。ACがオーセンティケータの場合は、ユーザープロファイルをAPに展開します。

ユーザープロファイルにアカウンティングポリシーが適用されていない場合、システムはAAAアカウンティングを実行します。

制約事項とガイドライン

ユーザープロファイルの削除を含むアカウンティングポリシーの変更は、オンラインクライアントに影響しません。

前提条件

認証サーバーで、ユーザープロファイルをクライアントにバインドします。

手順

1. システムビューに入ります。

   system-view
2. アカウンティングポリシーを作成し、そのビューに入るか、または既存のアカウンティングポリシーのビューに入ります。

   wlan accounting-policy *policy-name*
3. ACLベースアカウンティングのトラフィックレベルを指定します。

   accounting-level *level* **acl** { *acl-number* | **ipv6** *ipv6-acl-number* }

   デフォルトでは、ACLベースのアカウンティングにトラフィックレベルは指定されていません。
4. システムビューに戻ります。

   quit
5. ユーザープロファイルビューに入ります。

   user-profile *profile-name*
6. ユーザープロファイルにアカウンティングポリシーを適用します。

   wlan apply accounting-policy *policy-name*

デフォルトでは、アカウンティングポリシーは適用されません。

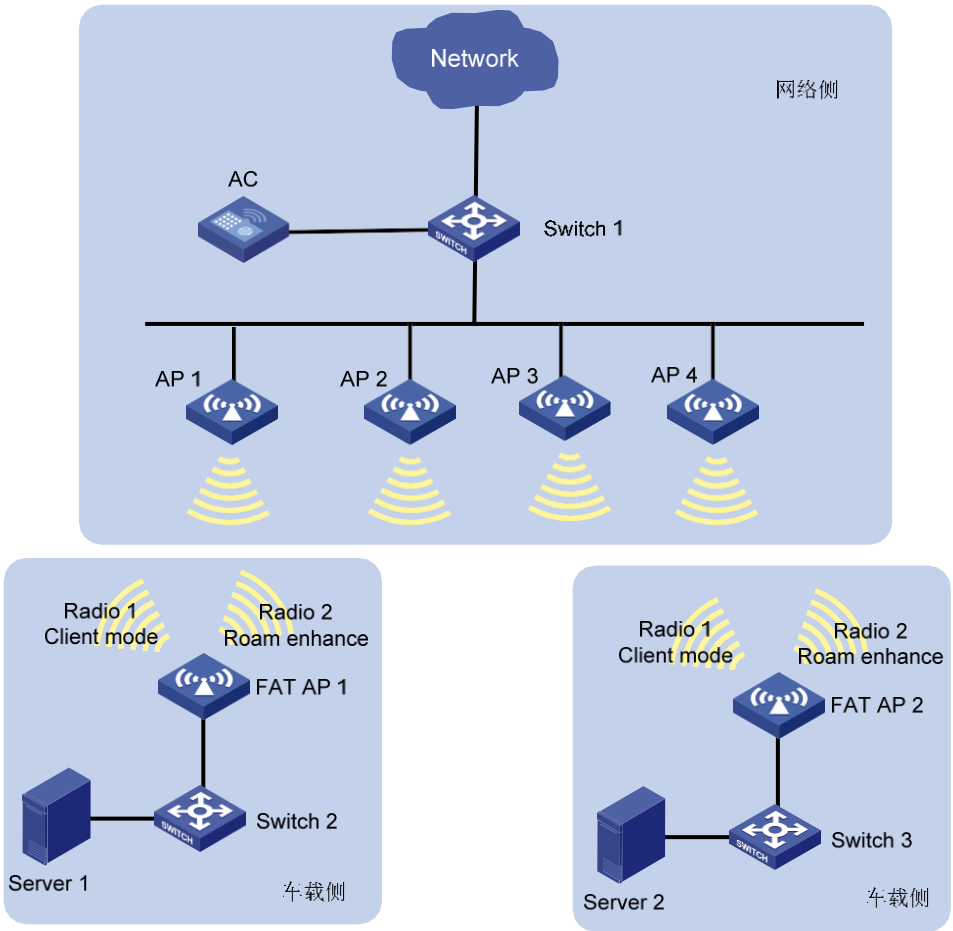
ローミング拡張の有効化

このタスクについて

図9に示すように、automated guided Vehicle(AGV)システムでは、車両に配置されたクライアントモードのFat APによって、ワイヤレスNICが搭載されていないオンボードデバイスへのワイヤレスアクセスが提供されます。このネットワーキングモードでは、各Fat APをスキャンして、より良いリンクを検索し、同時にデータを送信する必要があります。これにより、パケット損失が発生する可能性があります。

この問題を解決するには、Fit APのローミング拡張機能を設定して、チャネル、SSID、およびBSSID情報をビーコンフレームおよびプローブ応答に追加し、Fat APが高速にローミングできるようにします。

図9 AGVシステムのネットワーク図



制約事項とガイドライン

Fit APの場合、この機能は2.4Gワイヤレスに対してだけイネーブルにできます。この作業を複数回実行すると、最新の設定が有効になります。

この機能を有効にするには、車両に配置されているFat APのローミング拡張もイネーブルにする必要があります。

各フィットAPの5Gワイヤレスを次のように設定します。

- 5Gワイヤレスを、2.4Gワイヤレスのローミング拡張用に指定されたSSIDを使用する少なくと

も1つのサービステンプレートにバインドします。

- 指定したSSIDを使用する最大5つのサービステンプレートを5Gワイヤレスにバインドできます。
- パケット損失を避けるために、5Gワイヤレスをスキャンワイヤレスとして設定しないでください。
- 5Gワイヤレスはレーダーチャネルで動作できません。ベストプラクティスとして非レーダーチャネル、自動チャネル選択の[enable auto channel selection]、または[configure channel scanning whitelist or blacklist for the5G radio]を設定します。

手順

1. システムビューに入ります。

   system-view
2. APビューまたはAPグループのAPモデルビューに入ります。
   - APビューに入ります。

     wlan ap *ap-name*
   - APグループのAPモデルビューに入るには、次のコマンドを順番に実行します。

     wlan ap-group *group-name*

     ap-model *ap-model*
3. ワイヤレスビューに入ります。

   radio *radio-id*
4. Enable roaming enhancement.

   roam-enhance ssid *ssid*

   デフォルトでは:
   - ワイヤレスビューでは、APグループのワイヤレスビューの設定が使用されます。
   - APグループのワイヤレスビューでは、ローミング拡張はディセーブルです。

クライアント メンテナンスの設定

クライアント アイドルタイムアウトの設定

このタスクについて

クライアントアイドルタイムアウトタイマーの期限が切れる前に、オンラインクライアントが関連付けられたAPに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。

手順

1. システムビューに入ります。

   system-view
2. APビューまたはAPグループビューに入ります。
   - APビューに入ります。

     wlan ap *ap-name*
   - APグループビューに入ります。

     wlan ap-group *group-name*
3. クライアントのアイドルタイムアウトを設定します。

   client idle-timeout *timeout*

   デフォルト:

- APビューでは、APはAPグループビューの設定を使用します。
- APグループビューでは、クライアントのアイドルタイムアウトは3600秒です。

クライアント キープアライブの設定

このタスクについて

この機能を使用すると、APは指定された間隔でクライアントにキープアライブパケットを送信して、クライアントがオンラインかどうかを判断できます。APは、3つのキープアライブ間隔内にクライアントからの応答を受信しない場合、クライアントからログオフします。

手順

1. システムビューに入ります。

   system-view
2. APビューまたはAPグループビューを入力します。
   - APビューに入ります。

     wlan ap *ap-name*
   - APグループビューに入ります。

     wlan ap-group *group-name*
3. クライアントキープアライブをイネーブルにします。

   client keep-alive enable

   デフォルト:
   - APビューでは、APはAPグループビューの設定を使用します。
   - APグループビューでは、クライアントキープアライブはディセーブルです。
4. (任意)クライアントキープアライブインターバルを設定します。

   client keep-alive interval *interval*

   デフォルト:
   - APビューでは、APはAPグループビューの設定を使用します。
   - APグループビューでは、クライアントキープアライブインターバルは300秒です。

ワイヤレスリンク品質テストの実行

このタスクについて

この機能を使用すると、APはワイヤレスクライアントへのリンクの品質をテストできます。APはサポートされている各レートでクライアントに空のデータフレームを送信し、クライアントからの応答に基づいてRSSI、パケット再送信、RTTなどのリンク品質情報を計算します。

ワイヤレスリンク品質テストのタイムアウトは10秒です。タイムアウトまでにワイヤレスリンクテストが完了しないと、テスト結果を取得できません。

手順

ワイヤレスリンク品質テストを実行するには、ユーザービューで**wlan link-test** *mac-address*コマンドを実行します。

クライアント統計レポートの設定

このタスクについて

この機能を使用すると、APはクライアントエントリを更新するために指定された間隔でクライアント統計情報をACに報告できます。ACは、保存されたエントリにクライアントの情報が存在しない場合にクライアントをログオフするようAPに通知します。

頻繁なクライアントの再アソシエーションを回避するには、ネットワークの状態が悪いときにこの機能を無効にします。

手順

1. システムビューに入ります。

   system-view
2. APビューまたはAPグループビューに入ります。
   - APビューに入ります。

     wlan ap *ap-name*
   - APグループビューを入力します。

     wlan ap-group *group-name*
3. クライアント統計レポートを設定します。

   client-statistics-report { **disable** | **enable** [**interval** *interval*] }

   デフォルト:
   - APビューでは、APはAPグループビューの設定を使用します。
   - APグループビューでは、クライアント統計レポートがイネーブルになっています。

NAS IDの設定

このタスクについて

ネットワークアクセスサーバー識別子(NAS ID)、ネットワークアクセスサーバーポート識別子(NASポートID)、またはネットワークアクセスサーバーVLAN ID(NAS VLAN ID)は、クライアントのネットワークアクセスサーバーを識別し、クライアントトラフィックの送信元を区別します。

制約事項とガイドライン

サービステンプレートをワイヤレスにバインドするときにNAS IDまたはNASポートIDを指定した場合、ワイヤレスはサービステンプレートに指定されたNAS IDまたはNASポートIDを使用します。

nas-port-idコマンドを使用してNASポートIDが指定されている場合、クライアントは指定されたNASポートIDを使用します。NASポートIDが指定されていない場合、クライアントは指定されたNASポートID形式でNASポートIDを生成します。

手順

1. システムビューに入ります。

   system-view
2. クライアントのNASポートIDの形式を設定します。

   wlan nas-port-id format { **2** | **4** }

   デフォルトでは、クライアントは形式2を使用してNASポートIDを生成します。
3. APビュー、APグループビュー、またはグローバルコンフィギュレーションビューを入力します。
   - APビューに入ります。

     wlan ap *ap-name*
   - APグループビューに入ります。

wlan ap-group *group-name*

- 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

4. NAS IDを設定します。

   nas-id *nas-id*

   デフォルトは:

   - APビューでは、APはAPグループビューの設定を使用します。APグループビューでNAS IDが設定されていない場合、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は、NAS IDは設定されません。

5. NASポートIDを設定します。

   nas-port-id *nas-port-id*

   デフォルト:

   - APビューでは、APはAPグループビューの設定を使用します。APグループビューでNASポートIDが設定されていない場合、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は、NASポートIDは設定されません。

6. NAS VLAN IDを設定し、RADIUS要求でVLAN IDをカプセル化するようにACをイネーブルにします。

   nas-vlan *vlan-id*

   デフォルトでは、NAS VLAN IDは設定されません。RADIUSサーバーに送信される認証要求には、NAS VLAN IDフィールドは含まれません。

   この機能は、APビューでのみサポートされています。

   サードパーティ製Security Accounting Management(SAM)サーバーをRADIUSサーバーとして使用する場合は、NAS VLAN IDを設定します。

NASポートタイプの設定

このタスクについて

RADIUS要求は、802.1XおよびMAC認証クライアントのアクセスポートのタイプを示すNASポートタイプアトリビュートを伝送します。

制約事項とガイドライン

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。

手順

1. システムビューに入ります。

   system-view

2. サービステンプレートビューを入力します。

   wlan service-template *service-template*

3. NASポートタイプを設定します。

   nas-port-type *value*

   デフォルトでは、NASポートタイプはWLAN-IEEE802.11で、コード値は19です。

クライアントアソシエーション比率の最適化の設定

このタスクについて

この機能を使用すると、指定されたインデックスを使用してクライアントアソシエーション成功率、アソシエーション輻輳率、および異常なアソシエーション解除率を再計算し、より小さい比率値を取得できます。

クライアントアソシエーション成功率は、成功したクライアントアソシエーションの数をクライアントアソシエーション試行の合計数で割った値です。クライアントアソシエーション輻輳率は、APオーバーロードによって発生した失敗したクライアントアソシエーションの数をクライアントアソシエーション試行の合計数で割った値です。クライアントの異常なアソシエーション解除率は、異常なアソシエーション解除の数を成功したアソシエーションおよびオンラインクライアントの合計で割った値です。

手順

1. システムビューに入ります。

   system-view
2. グローバルコンフィギュレーションビューに入ります。

   wlan association optimization *value*

   デフォルトでは、インデックスは0です。デバイスはクライアントアソシエーション比を最適化しません。

iMCサーバーの指定

このタスクについて

この機能を使用すると、AP、クライアント、およびポータルユーザーのアソシエーションイベントとアソシエーション解除イベントをiMCサーバーに報告し、iMCプラットフォームから統計情報を表示できます。

手順

1. システムビューに入ります。

   system-view
2. IPアドレスとポート番号でiMCサーバーを指定します。

   wlan imc ip *ip-address* **port** *port-number*

   デフォルトでは、IMCサーバーは指定されていません。

VIPクライアントの設定

VIPクライアントグループの設定

このタスクについて

VIPクライアントグループには、同じワイヤレスに関連付けられたVIPクライアントのグループが含まれています。Oasisプラットフォームから、VIPクライアントグループ内のオンラインVIPクライアントに関する情報を表示できます。

制約事項とガイドライン

VIPクライアントグループにはVIPクライアントグループに追加できます。

手順

1. システムビューに入ります。

system-view

2. VIPクライアントグループを作成し、そのビューに入ります。

   wlan vip-client-group

3. VIPクライアントグループにクライアントを追加します。

   client-mac *mac-address*

   デフォルトでは、VIPクライアントグループにクライアントは存在しません。

4. (任意)APがVIPクライアント統計情報をACに報告する間隔を設定します。

   report-interval *interval*

   デフォルトでは、APは50秒間隔でVIPクライアント統計情報をACに報告します。

非VIPクライアントレート制限の設定

このタスクについて

非VIPクライアントレート制限が設定されている場合、ワイヤレスに関連付けられたすべての非VIPクライアントは、ワイヤレスがVIPクライアントに関連付けられているときに特定の値にレート制限されます。ワイヤレスがオフラインになり、非VIPクライアントはレート制限されません。ワイヤレスにVIPクライアントが関連付けられていない場合、非VIPクライアントはレート制限されません。

制約事項とガイドライン

着信トラフィックと発信トラフィックの両方をレート制限できます。

ワイヤレスベースのクライアントレート制限と非VIPクライアントレート制限の両方を設定した場合、非VIPクライアントのレートは小さい値になり、VIPクライアントはレート制限されません。

手順

1. システムビューに入ります。

   system-view

2. VIPクライアントグループを作成し、そのビューを入力します。

   wlan vip-client-group

3. 非VIPクライアントレート制限を設定します。

   non-vip limit rate { **inbound** | **outbound** } **cir** *cir*

   デフォルトでは、非VIPクライアントレート制限が設定されています。

ポリシーベース転送の設定

ハードウェアとポリシーベース転送の互換性

ハードウェアシリーズ	モデルモデル	製品コード	機能の互換性
WX1800Hシリーズ	WX1804H	EWP-WX1804H-PWR-CN	有り

WX2500Hシリーズ	WX2508H-PWR-LTE WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	有り
WX3000Hシリーズ	WX3010H WX3010H-X WX3010H-L WX3024H WX3024H-L WX3024H-F	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	はい: • WX3010H • WX3010H-X • WX3024H • WX3024H-F 番号: • WX3010H-L • WX3024H-L
WX3500Hシリーズ	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H	有り
WX5500Eシリーズ	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	有り
WX5500Hシリーズ	WX5540H WX5560H	EWP-WX5540H EWP-WX5560H	有り

ハードウェアシリーズ	モデルモデル	製品コード	機能の互換性
	WX5580H	EWP-WX5580H	
アクセスコントローラモジュール	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	有り

ハードウェアシリーズ	モデルモデル	製品コード	機能の互換性
WX1800Hシリーズ	WX1804H WX1810H WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	有り
WX3800Hシリーズ	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	有り
WX5800Hシリーズ	WX5860H	EWP-WX5860H-GL	有り

ポリシーベース転送の制約事項およびガイドライン

ACおよび関連付けられたAPが異なるネットワークセグメントにあることを確認します。

転送ポリシーは、サービステンプレートまたはユーザープロファイルに適用できます。ACは、クライアントトラフィックの転送を指示するために、ユーザープロファイルに適用された転送ポリシーを優先的に使用します。クライアントのユーザープロファイルに転送ポリシーがない場合、ACはサービステンプレートに適用された転送ポリシーを使用します。

ポリシーベース転送の前提条件

ポリシーベース転送を構成する前に、クライアントの認証を実行するACを指定する必要があります。認証ロケーションの指定の詳細は、『User Access and Authentication Configuration Guide』を参照してください。

転送ポリシーの設定

このタスクについて

転送ポリシーには、1つまたは複数の転送ルールが含まれています。各転送ルールでは、トラフィック一致基準および一致するトラフィックの転送モードを指定します。トラフィック一致基準には、基本ACL、拡張ACL、またはレイヤ2 ACLを指定できます。転送モードには、ローカル転送または集中転送を指定できます。

ACLルールで定義されたアクションは、ワイヤレスパケット転送では有効になりません。一致したすべてのパケットは、転送モードに基づいて転送されます。

ACLの詳細については、Security Configuration Guideを参照してください。

手順

1. システムビューに入ります。

   system-view
2. 転送ポリシーを作成し、そのビューに入ります。

   wlan forwarding-policy *policy-name*
3. 転送ルールを設定します。

   classifier acl { *acl-number* | **ipv6** *ipv6-acl-number* } **behavior** { **local** | **remote** }

   さらに転送ルールを設定するには、このコマンドを繰り返します。

ローカル転送モードでの外部ネットワークへのトラフィック転送のイネーブル化

このタスクについて

ローカル転送が有効な場合、APは外部ネットワークを宛先とするクライアントパケットをドロップします。この機能により、APは外部ネットワークを宛先とするクライアントパケットの宛先MACアドレスをAPのMACアドレスで置き換えることができます。NATにより、パケットの送信元IPアドレスはAPと同じネットワークセグメント内のIPアドレスに変換されます。これにより、APはクライアントトラフィックを外部ネットワークに正しく転送できます。

制約事項とガイドライン

この機能は、NATをサポートするAPでのみサポートされます。

手順

1. システムビューに入ります。

   system-view
2. WLAN転送ポリシービューを入力します。

   wlan forwarding-policy *policy-name*
3. ローカル転送が有効な場合、外部ネットワークへのトラフィック転送を有効にします。

   client behavior-local network-flow-forwarding enable

   デフォルトでは、ローカル転送がイネーブルの場合、APは外部ネットワーク宛てのクライアントパケットをドロップします。

サービステンプレートへの転送ポリシーの適用

1. システムビューに入ります。

   system-view
2. サービステンプレートビューに入ります。

   wlan service-template service-template-name
3. 転送ポリシーをサービステンプレートに適用します。

   client forwarding-policy-name *policy-name*

   デフォルトでは、転送ポリシーはサービステンプレートに適用されません。

   転送ポリシーを有効にするには、サービステンプレートのポリシーベース転送をイネーブルにする必要があります。
4. ポリシーベース転送をイネーブルにします。

   client forwarding-policy enable

   デフォルトでは、ポリシーベース転送はサービステンプレートに対してディセーブルです。

ユーザープロファイルへの転送ポリシーの適用

このタスクについて

ACがユーザープロファイルを使用するクライアントに対してポリシーベースの転送を実行するには、転送ポリシーをユーザープロファイルに適用します。クライアントが認証に合格すると、認証サーバーはクライアントに指定されたユーザープロファイル名をACに送信します。ACはユーザープロファイルに適用された転送ポリシーに基づいてクライアントのトラフィックを転送します。

制約事項とガイドライン

適用された転送ポリシーを変更または削除すると、クライアントが再びオンラインになったときに変更が有効になります。

手順

1. システムビューに入ります。

   system-view
2. ユーザープロファイルビューに入ります。

user-profile *profile-name*

3. 転送ポリシーをユーザープロファイルに適用します。

   wlan client forwarding-policy-name *policy-name*

   デフォルトでは、転送ポリシーはユーザープロファイルに適用されません。

   ユーザープロファイルに適用された転送ポリシーを有効にするには、ユーザープロファイルが使用するサービステンプレートのポリシーベース転送をイネーブルにする必要があります。

4. システムビューに戻ります。

   quit

5. サービステンプレートビューに入ります。

   wlan service-template *service-template-name*

6. ポリシーベース転送をイネーブルにします。

   client forwarding-policy enable

   デフォルトでは、ポリシーベース転送はサービステンプレートに対してディセーブルです。

ゲストトンネルの設定

ゲストトンネルとのハードウェア互換性

ハードウェアシリーズ	モデルモデル	製品コード	機能の互換性
WX1800Hシリーズ	WX1804H	EWP-WX1804H-PWR-CN	無し
WX2500Hシリーズ	WX2508H-PWR-LTE WX2510H WX2510H-F WX2540H WX2540H-F WX2560H	EWP-WX2508H-PWR-LTE EWP-WX2510H-PWR EWP-WX2510H-F-PWR EWP-WX2540H EWP-WX2540H-F EWP-WX2560H	有り
WX3000Hシリーズ	WX3010H WX3010H-X WX3010H-L	EWP-WX3010H EWP-WX3010H-X-PWR EWP-WX3010H-L-PWR	無し

ハードウェアシリーズ	モデルモデル	製品コード	機能の互換性
	WX3024H WX3024H-L WX3024H-F	EWP-WX3024H EWP-WX3024H-L-PWR EWP-WX3024H-F	
WX3500Hシリーズ	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H	有り
WX5500Eシリーズ	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	有り
WX5500Hシリーズ	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	有り
アクセスコントローラモジュール	LSUM1WCME0EW PXM1WCME0LSQ M1WCMX20LSUM 1WCMX20RT LSQM1WCMX40LS UM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	LSUM1WCME0EW PXM1WCME0LSQ M1WCMX20LSUM 1WCMX20RT LSQM1WCMX40LS UM1WCMX40RT EWPXM2WCMD0F EWPXM1MAC0F	無し

ハードウェアシリーズ	モデルモデル	製品コード	機能の互換性
WX1800Hシリーズ	WX1804H WX1810H WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	有り
WX3800Hシリーズ	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	無し
WX5800Hシリーズ	WX5860H	EWP-WX5860H-GL	無し

エッジACのための集約ACの指定

このタスクについて

エッジACに集約ACを指定すると、エッジACは指定された間隔で集約ACへのキープアライブ要求の送信を開始します。ゲストトンネルは、エッジACが集約ACからキープアライブ応答を受信すると確立されます。

エッジACは、指定された間隔でキープアライブ要求を送信し続け、トンネルの確立後にトンネル接続を検査します。エッジACが3つのキープアライブ間隔内にキープアライブ応答を受信できない場合、エッジACはトンネルを終了します。集約ACが3つのキープアライブ間隔内にキープアライブ要求を受信できない場合、集約ACはトンネルを終了します。

制約事項とガイドライン

エッジACのロールを集約に変更するには、最初にデフォルトのACロールを復元する必要があります。デ

フォルトのACロールを復元すると、AC上のすべてのゲストトンネル設定が削除されます。

エッジACは複数の集約ACでゲストトンネルを確立できますが、これらのトンネルは異なるVLANに属している必要があります。

エッジACは、集約ACとともに複数のゲストトンネルを確立できますが、異なる集約ACインターフェイスとともにトンネルを確立するには、異なる送信元IPアドレスを使用する必要があります。同じエッジAC IPアドレスに対して集約ACの複数のIPアドレスを指定した場合、集約ACは、トンネル確立のために最初に受信したキープアライブ要求のIPアドレスだけを使用します。

手順

1. システムビューに入ります。

   system-view
2. ACをエッジACとして指定し、そのビューに入ります。

   wlan guest-tunnel edge-ac

   デフォルトでは、ACはエッジACでも集約ACでもありません。
3. エッジACに集約ACを指定します。

   aggregation-ac ip *ipv4-address* **tunnel-source ip** *ipv4-address* **vlan** *vlan-id-list*

   デフォルトでは、エッジACに集約ACは指定されていません。
4. (任意)ゲストトンネルキープアライブインターバルを設定します。

   keep-alive interval *interval*

   デフォルトでは、キープアライブインターバルは10秒です。

集約ACのエッジACの指定

このタスクについて

キープアライブ要求を受信すると、集約ACは、要求が集約ACに指定されたエッジACからのものかどうかを調べます。要求が指定されたエッジACからのものである場合、集約ACはキープアライブ応答を送信します。要求が指定されたエッジACからのものでない場合、集約ACは要求を廃棄します。

制約事項とガイドライン

集約ACの役割をエッジに変更するには、最初にデフォルトのAC役割を復元する必要があります。デフォ

ルトのAC役割を復元すると、AC上のすべてのゲストトンネル設定が削除されます。

エッジACは複数の集約ACでゲストトンネルを確立できますが、これらのトンネルは異なるVLANに属している必要があります。

エッジACは、集約ACで複数のゲストトンネルを確立できますが、異なる集約ACインターフェイスでトンネルを確立するには、異なる送信元IPアドレスを使用する必要があります。

手順

1. システムビューに入ります。

   system-view
2. ACを集約ACとして指定し、そのビューを入力します。

   wlan guest-tunnel aggregation-ac

   デフォルトでは、ACはエッジACでも集約ACでもありません。
3. 集約ACのエッジACを指定します。

   edge-ac ip ipv4-address vlan *vlan-id-list*

デフォルトでは、集約ACにエッジACは指定されていません。

ゲストトンネルフロー配信のイネーブル化

このタスクについて

この機能を使用すると、IPSecによって暗号化される前に、デバイスがゲストトンネルフローを異なるCPUに分散して、転送効率を向上させることができます。

制約事項とガイドライン

この機能は、IPSecがゲストトンネル用に設定されている場合にだけイネーブルにしてください。

この機能は、ゲストトンネルのエッジACと集約ACで同時にイネーブルまたはディセーブルにする必要があります。

手順

1. システムビューに入ります。
   system-view
2. エッジACビューまたは集約ACビューに入ります。
   wlan guest-tunnel { **aggregation-ac** | **edge-ac** }
3. ゲストトンネルフロー配信をイネーブルにします。
   wlan guest-tunnel flow-distribute enable
   デフォルトでは、ゲストトンネルフロー配信はディセーブルです。

クライアントアクセス制御の構成

クライアントアソシエーションの許可APグループの指定

このタスクについて

クライアントが指定されたAPグループ内のAPとアソシエートできるようにするには、次の作業を実行します。

手順

1. システムビューに入ります。
   system-view
2. ユーザープロファイルビューを入力します。
   user-profile *profile-name*
3. クライアントアソシエーションに許可されるAPグループを指定します。
   wlan permit-ap-group *ap-group-name*
   デフォルトでは、クライアントアソシエーションに許可APグループは指定されていません。

クライアントアソシエーションの許可SSIDの指定

このタスクについて

クライアントが指定されたSSIDを介してWLANにアソシエートできるようにするには、次の作業を実行します。

手順

1. システムビューに入ります。

system-view

2. ユーザープロファイルビューに入ります。

   user-profile *profile-name*

3. クライアントアソシエーションに許可されるSSIDを指定します。

   wlan permit-ssid *ssid-name*

   デフォルトでは、クライアントアソシエーションに許可SSIDは指定されていません。

ホワイトリストへのクライアントの追加

制約事項とガイドライン

最初のクライアントをホワイトリストに追加すると、すべてのオンラインクライアントを切断するかどうかを確認するメッセージが表示されます。プロンプトでYと入力して、ホワイトリストを設定します。

手順

1. システムビューに入ります。

   system-view

2. ホワイトリストにクライアントを追加します。

   wlan whitelist mac-address *mac-address*

スタティック ブラックリストへのクライアントの追加

制約事項とガイドライン

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。

ホワイトリストおよびブラックリストが設定されている場合、ホワイトリストだけが有効になります。

手順

1. システムビューに入ります。

   system-view

2. クライアントをスタティックブラックリストに追加します。

   wlan static-blacklist mac-address *mac-address*

ダイナミック ブラックリストの設定

このタスクについて

ダイナミックブラックリストを設定して、ACまたはAPで有効にできます。

ダイナミックブラックリストをACに対して有効に設定すると、ACに接続されているすべてのAPはダイナミックブラックリスト内のクライアントを拒否します。ダイナミックブラックリストをAPに対して有効に設定すると、ダイナミックブラックリスト内のクライアントに関連付けられているAPはクライアントを拒否しますが、クライアントはACに接続されている他のAPと関連付けることができます。

ダイナミックブラックリストのエントリは、エージングタイマーの期限が切れると削除されます。

制約事項とガイドライン

ベストプラクティスとして、ダイナミックブラックリストを設定して、高密度環境のACで有効にします。

設定されたエージングタイマーは、ダイナミックブラックリストに新しく追加されたエントリに対してだ

け有効です。ホワイトリストおよびブラックリストが設定されている場合、ホワイトリストだけが有効です。

手順

1. システムビューに入ります。

   system-view
2. 必要に応じて、次のいずれかのオプションを選択します。
   - ダイナミックブラックリストをAPで有効にするように設定します。

     wlan dynamic-blacklist active-on-ap
   - ダイナミックブラックリストを設定して、ACで有効にします。

     undo wlan dynamic-blacklist active-on-ap

   デフォルトでは、ダイナミックブラックリストはAPで有効になります。
3. (任意)ダイナミックブラックリストエントリのエージングタイマーを設定します。

   wlan dynamic-blacklist lifetime *lifetime*

   デフォルトでは、エージングタイマーは300秒です。

   ダイナミックブラックリストエントリのエージングタイマーは、不正なクライアントエントリに対してだけ有効です。

ACLベースのアクセス制御の設定

制約事項とガイドライン

ACLベースのアクセスコントロール設定は、ホワイトリストおよびブラックリスト設定よりも優先されます。ベストプラクティスとして、ACLベースの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デバイスに設定しないでください。

指定したACLにdeny文が含まれている場合は、すべてのクライアントを許可するACLのpermit文を設定します。これを行わないと、どのクライアントもオンラインになりません。

APビューの設定は、サービステンプレートビューの設定よりも優先されます。

この機能はレイヤ2ACL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。別のタイプのACLを指定した場合、設定は有効になりません。

手順

1. システムビューに入ります。

   system-view
2. サービステンプレートビューまたはAPビューに入ります。
   - サービステンプレートビューを入力します。

     wlan service-template *service-template-name*
   - APビューに入ります。

     wlan ap *ap-name*
3. ACLを指定します。

   access-control acl *acl-number*

   デフォルトでは、ACLは指定されていません。

ブロードキャストプローブ要求に対するAPの応答のディセーブル化

このタスクについて

ブロードキャストプローブ要求では、SSIDは伝送されません。ブロードキャストプローブ要求を受信すると、APは、APのサービス情報を伝送するプローブ応答で応答します。

この機能により、APにユニキャストプローブ要求を送信するクライアントは、APとより簡単に関連付けることができます。

手順

1. システムビューに入ります。

   system-view
2. APビューまたはAPグループビューに入ります。
   - APビューに入ります。

     wlan ap *ap-name*
   - APグループビューに入ります。

     wlan ap-group *group-name*
3. ブロードキャストプローブ要求に対するAPの応答をディセーブルにします。

   broadcast-probe reply disable

   デフォルトは:
   - APビューでは、APはAPグループビューの設定を使用します。
   - APグループビューでは、APはブロードキャストプローブ要求に応答します。

WLANアクセスに対するSNMP通知の有効化

このタスクについて

重要なWLANアクセスイベントをNMSにレポートするには、WLANアクセスのSNMP通知を有効にします。WLANアクセスイベント通知を正しく送信するには、『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。

手順

1. システムビューに入ります。

   system-view
2. 必要に応じて設定するオプションを選択します。
   - クライアントアクセスのSNMP通知をイネーブルにします。

     snmp-agent trap enable wlan client
   - クライアント監査のSNMP通知をイネーブルにします。

     snmp-agent trap enable wlan client-audit

   デフォルトでは、SNMP通知はディセーブルです。

スマートクライアントアクセスの有効化

このタスクについて

この機能により、AKMモードがPSKに設定されている場合、またはワイヤレスが空のサービステンプレートにバインドされている場合に、H3CワイヤレスクライアントがWLANに自動的にアクセスできるようになります。

手順

1. システムビューに入ります。
   system-view
2. サービステンプレートビューを入力します。
   wlan service-template *service-template-name*
3. スマートクライアントアクセスを有効にします。
   client smart-access enable
   デフォルトでは、スマートクライアントアクセスは無効になっています。

WLANアクセス用の表示およびメンテナンスコマンド

重要

- WX1800Hシリーズ、WX2500Hシリーズ、およびWX3000Hシリーズのアクセスコントローラは、IRFモードでのみ使用可能なパラメータやコマンドをサポートしていません。
- **display wlan forwarding-policy**、**display wlan guest-tunnel**、および**reset wlan guest-tunnel**コマンドのサポートは、デバイスモデルによって異なります。詳細はコマンドリファレンスを参照してください。

任意のビューでdisplayコマンドを実行し、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
2.4GHz帯域と5GHz帯域の両方のオンラインクライアント数を表示します。	**display wlan ap all client-number**
各ワイヤレスのオンラインクライアント数とチャネル情報を表示します。	**display wlan ap all radio client-number**
APのリージョンコード情報を表示します。	**display wlan ap** { **all** | **name** *ap-name* } **region-code**
各APグループのオンラインクライアント数を表示します。	**display wlan ap-group all client-number**
ブラックリストエントリを表示します。	**display wlan blacklist** { **dynamic** | **static** }
基本サービスセット(BSS)情報を表示します。	**display wlan bss** { **all** | **ap** *ap-name* | **bssid** *bssid* } [**verbose**] IRFモードの場合: **display wlan bss** { **all** | **ap** *ap-name* | **bssid** bssid } [**slot** *slot-number*] [**verbose**]

クライアント情報を表示します。	**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IPv6アドレスに関する情報を表示します。	**display wlan client ipv6**
クライアントのオンライン時間を表示します。	display wlan client online-duration [ap ap-name] [verbose]
クライアントステータス情報を表示します。	**display wlan client status [mac-address** *mac-address*] [**verbose**]
WLAN転送ポリシー情報を表示します。	**display wlan forwarding-policy**
ACのゲストトンネル情報を表示します。	**display wlan guest-tunnel** { **all** | **ip** *ipv4-address* }
サービステンプレート情報を表示します。	**display wlan service-template** [*service-template-name*] [**verbose**]

タスク	コマンド
クライアント統計情報を表示します。	**display wlan statistics client** [**mac-address** *mac-address*]
クライアント接続履歴を表示します。	**display wlan statistics connect-history** { **ap** { **all** | **name** *ap-name* } | **service-template** *service-template-name* }
サービステンプレート統計情報の表示	**display wlan statistics service-template** *service-template-name*
APがACに報告するVIPクライアント統計情報を表示します。	**display wlan statistics vip-client**
ホワイトリストエントリを表示します。	**display wlan whitelist**
指定したクライアントまたはすべてのクライアントからログオフします。	**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削除します。	**reset wlan dynamic-blacklist** [**mac-address** *mac-address*]
指定したゲストトンネルまたはすべてのゲストトンネルを削除します。	**reset wlan guest-tunnel** { **all** | **ip** *ipv4-address* }
クライアント統計情報をクリアします。	**reset wlan statistics client** { **all** | **mac-address** *mac-address* }
サービステンプレート統計情報をクリアします。	**reset wlan statistics service-template** *service-template-name*

WLANアクセスの設定例

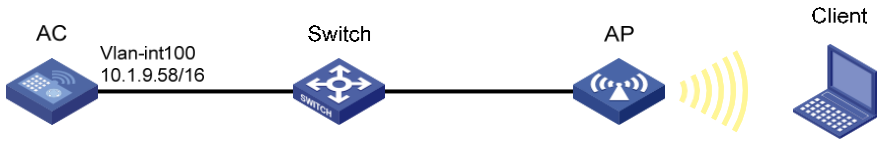
この文書のAPモデルとシリアル番号は、例としてのみ使用されています。APモデルとシリアル番号のサポートは、ACモデルによって異なります。

例:WLANアクセスの設定

ネットワーク構成

図10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サーバーとして機能します。APはSSIDのトレードオフでワイヤレスサービスを提供します。

図10 ネットワーク図



手順

1. VLAN100を作成し、VLAN-interface100にIPアドレスを割り当てます。

   <AC> system-view

   [AC] vlan 100

   [AC-vlan100]quit

   [AC] interface vlan-interface 100

   [AC-Vlan-interface100] ip address 10.1.9.58 16

2. 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 WA4320i-ACN

   [AC-wlan-ap-ap1] serial-id 219801A0CNC138011454

3. サービステンプレートを設定し、APワイヤレスにバインドします。

   #サービステンプレートservice1を作成し、SSIDをトレードオフに設定し、サービステンプレートを介してオンラインになるクライアントをVLAN100に割り当て、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のワイヤレス1の動作チャネルをチャネル157に設定します。

   [AC] wlan ap ap1

   [AC-wlan-ap-ap1] radio 1

   [AC-wlan-ap-ap1-radio-1] channel 157

   #サービステンプレートservice1をradio1にバインドします。

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

   [AC-wlan-ap-ap1-radio-1] service-template service1

設定の確認

#SSIDがトレードオフの関係にあり、サービステンプレートが有効になっていることを確認します。

[AC] display wlan service-template verbose Service
template name: service1

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 WPA3 status: 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に関連付けます(詳細は表示されていません)。

#クライアントがWLANにアクセスできることを確認します。

[AC] display wlan client service-template service1

Total number of clients: 1

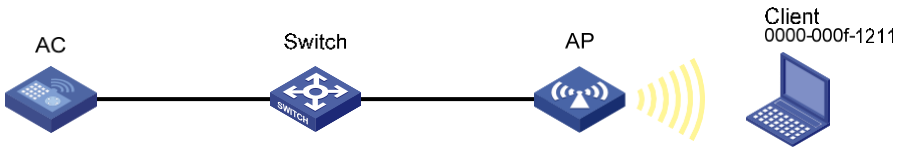
MAC address	Username	AP name	RID	IP address	VLAN
0023-8933-223b	N/A	ap1	1	3.0.0.3	100

例:ホワイトリストベースのアクセスコントロールの設定

ネットワーク構成

図11に示すように、ホワイトリストを設定して、MACアドレスが0000-000f-1211のクライアントだけがWLANにアクセスできるようにします。

図11 ネットワーク図



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

設定の確認

#MACアドレス0000-000f-1211がホワイトリストにあることを確認します。

[AC] display wlan whitelist Total

number of clients: 1

MAC addresses:

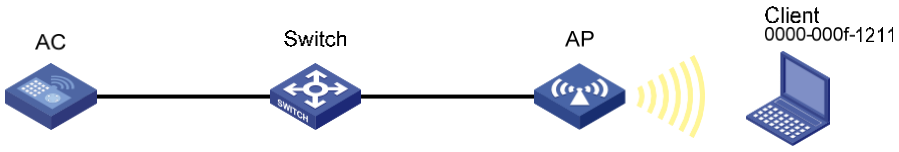
0000-000f-1211

例:スタティックブラックリストベースのアクセスコントロールの設定

ネットワーク構成

図12に示すように、スタティックブラックリストを設定して、MACアドレスが0000-000f-1211のクライアントがWLANにアクセスできないようにします。

図12 ネットワーク図



手順

#MACアドレス0000-000f-1211をスタティックブラックリストに追加します。

<AC> system-view

[AC] wlan static-blacklist mac-address 0000-000f-1211

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ことを確認します。

[AC] display wlan blacklist static Total number

of clients: 1

MAC addresses:

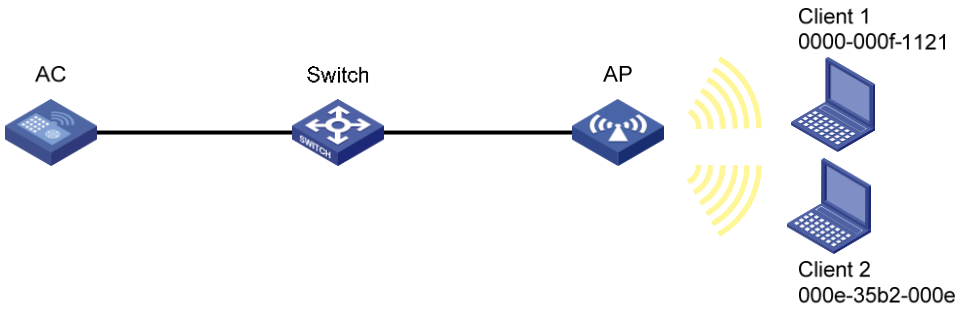
0000-000f-1211

例:ACLベースのアクセスコントロールの設定

ネットワーク構成

図13に示すように、クライアント1およびクライアント2と同じOUIを持つクライアントがWLANにアクセスできるように、ACLベースのアクセス制御を設定します。

図13 ネットワーク図



手順

#レイヤ2ACL4000を作成し、クライアント1およびクライアント2と同じOUIを持つクライアントを許可するACLルールを作成します。

<Sysname>system-view

[Sysname] acl mac 4000

[Sysname-acl-mac-4000] rule 0 permit source-mac 0000-000f-1121 ffff-ffff-ffff

[Sysname-acl-mac-4000] rule 1 permit source-mac 000e-35b2-000e ffff-ff00-0000

[Sysname-acl-mac-4000] quit

#ACL4000をサービステンプレートservice1にバインドします。

[Sysname] wlan service service1

[Sysname-wlan-st-service1] access-control acl 4000

設定の確認

#display wlan clientコマンドを実行して、クライアント1とクライアント2(クライアント2を含む)と同じOUIを持つクライアントだけがWLANにアクセスできることを確認します。

[AC] display wlan client Total number of clients: 2

MAC address	Username	AP name	RID	IPv4 address	VLAN
0000-000f-1121	N/A	ap	1	192.168.100.12	1
000e-35b2-000e	N/A	ap	1	192.168.100.13	1

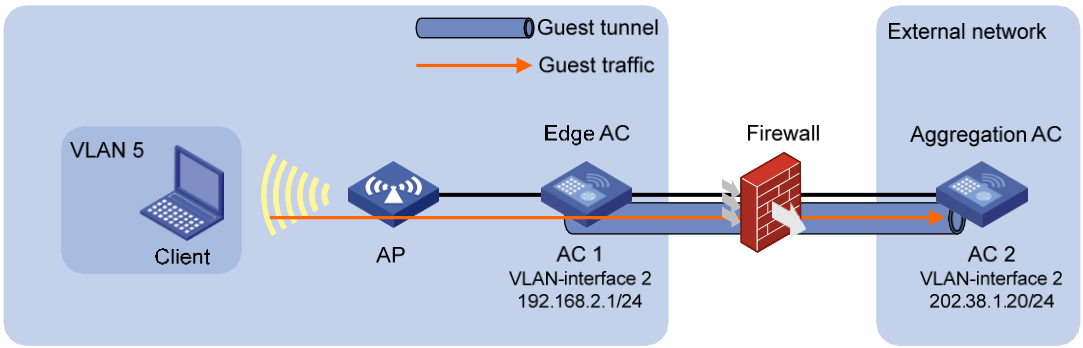
例:ゲストトンネルの設定

ネットワーク構成

図14に示すように、AC1はエッジACとして内部ネットワークに配置され、AC2は集約ACとして外部ネットワークに配置されます。WLANにアクセスするゲスト(この図のクライアント)はVLAN5に割り当てられます。

エッジACがゲストトラフィックを独立ゲストトンネル内の集約ACに転送できるように、ゲストトンネルを設定します。

図14 ネットワーク図



手順

1. AC1の設定:

#ACインターフェイスのIPアドレスを設定します(詳細は表示されません)。#ACをエッジACとして指定します。

<AC1> system-view

[AC1] wlan guest-tunnel edge-ac

#エッジACの集約ACとしてAC2を指定し、ゲストVLANとしてVLAN5を指定します。

[AC1-wlan-edge-ac]aggregation-ac ip202.38.1.20tunnel-source ip192.168.2.1vlan5

[AC1-wlan-edge-ac] quit

#service template1を作成し、SSIDをguestに設定し、サービステンプレートを有効にします。

[AC1] wlan service-template 1

[AC1-wlan-st-1] ssid guest

[AC1-wlan-st-1] service-template enable

[AC1-wlan-st-1] quit

#AP ap1を作成し、シリアルIDを設定します。

[AC1] wlan ap ap1 model WA4320i-ACN

[AC1-wlan-ap-ap1] serial-id 210235A35U007B000010

#サービステンプレート1をAP ap1のワイヤレス2にバインドし、サービステンプレートを介してオンラインになるクライアントをVLAN5に割り当てます。

[AC1-wlan-ap-ap1] radio 2

[AC1-wlan-ap-ap1-radio-2] service-template 1 vlan-id 5

#radio2を有効にします。

[AC1-wlan-ap-ap1-radio-2]radio enable

[AC1-wlan-ap-ap1-radio-2]quit

[AC1-wlan-ap-ap1] quit

2. AC2の設定:

#ACインターフェイスのIPアドレスを設定します(詳細は表示されません)。#ACを集約ACとして指定します。

<AC2> system-view

[AC2] wlan guest-tunnel aggregation-ac

#AC1をエッジACとして指定し、ゲストVLANをVLAN5に設定します。

[AC2-wlan-aggregation-ac]edge-ac ip192.168.2.1vlan5

[AC2-wlan-aggregation-ac]quit

設定の確認

#AC1でゲストトンネルがアップ状態であることを確認します。

[AC1]display wlan guest-tunnel all

Guest access tunnel information

Local Mode: Edge ACTunnel Count: 1

Peer IP AddressLocal IP AddressVLANsStateInterface 202.38.1.20192.168.2.15UpWLAN-Tunnel1

#AC2でゲストトンネルがアップ状態であることを確認します。

<AC2> display wlan guest-tunnel all

Guest access tunnel information

Local Mode: Aggregation ACTunnel Count: 1

Peer IP AddressVLANsStateInterface 192.168.2.15UpWLAN-Tunnel1

#クライアントがVLAN5経由でオンラインになっていることを確認します。

<AC1> display wlan client

MAC addressUser名	AP name	RID IP address	VLAN
508f-4c40-f3a6 N/A	ap1	1192.168.1.2	5

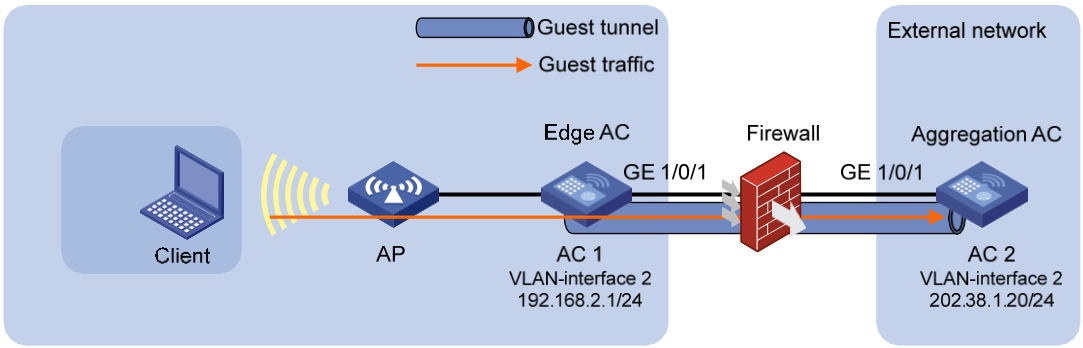
例:IPSecゲストトンネルの設定

ネットワーク構成

図15に示すように、AC1はエッジACとして内部ネットワークに配置され、AC2は集約ACとして外部ネットワークに配置されます。WLANにアクセスするゲスト(この図のクライアント)はVLAN5に割り当てられます。

エッジACがゲストトラフィックを暗号化し、独立したゲストトンネル内のファイアウォールを介してトラフィックを集約ACに転送できるように、IPSecゲストトンネルを設定します。

図15 ネットワーク図



手順

1. AC1の設定:

   #ACインターフェイスのIPアドレスを設定します(詳細は表示されません)。#ACをエッジACとして指定します。

   <AC1> system-view

   [AC1] wlan guest-tunnel edge-ac

   #エッジACの集約ACとしてAC2を指定し、ゲストVLANとしてVLAN5を指定します。

   [AC1-wlan-edge-ac] aggregation-ac ip 202.38.1.20 tunnel-source ip 192.168.2.1 vlan 5

   #ゲストトンネルフロー配信をイネーブルにします。

   [AC1-wlan-edge-ac] wlan guest-tunnel flow-distribute enable

   [AC1-wlan-edge-ac] quit

   #service template1を作成し、SSIDをguestに設定し、サービステンプレートを有効にします。

   [AC1] wlan service-template 1

   [AC1-wlan-st-1] ssid guest

   [AC1-wlan-st-1] service-template enable

   [AC1-wlan-st-1] quit

   #AP ap1を作成し、シリアルIDを設定します。

   [AC1] wlan ap ap1 model WA4320i-ACN

   [AC1-wlan-ap-ap1] serial-id 210235A35U007B000010

   #サービステンプレート1をAP ap1のワイヤレス2にバインドし、サービステンプレートを介してオンラインになるクライアントをVLAN5に割り当てます。

   [AC1-wlan-ap-ap1] radio 2

   [AC1-wlan-ap-ap1-radio-2] service-template 1 vlan-id 5

   #radio2を有効にします。

   [AC1-wlan-ap-ap1-radio-2] radio enable

   [AC1-wlan-ap-ap1-radio-2] quit

   [AC1-wlan-ap-ap1] quit

2. AC2の設定:

   #ACインターフェイスのIPアドレスを設定します(詳細は表示されません)。#ACを集約ACとして指定します。

   <AC2> system-view

[AC2] wlan guest-tunnel aggregation-ac

#AC1をエッジACとして指定し、ゲストVLANをVLAN5に設定します。

[AC2-wlan-aggregation-ac] edge-ac ip 192.168.2.1 vlan 5

#ゲストトンネルフロー配信をイネーブルにします。

[AC2-wlan-aggregation-ac] wlan guest-tunnel flow-distribute enable

[AC2-wlan-aggregation-ac] quit

3. IP Secを設定:

#IPv4拡張ACL3111を作成します。

[AC1] acl advanced 3111

#ポート18002からポート18002へのUDPトラフィックを許可するACLルールを作成します。

[AC1-acl-ipv4-adv-3111] rule permit udp source-port eq 18002 destination-port eq 18002

#ポート60016～60031からポート60016～60031へのUDPトラフィックを許可するACLルールを作成します。

[AC1-acl-ipv4-adv-3111] rule permit udp source-port range 60016 60031 destination-port range 60016 60031

[AC1-acl-ipv4-adv-3111] quit

#IPSecトランスフォームセットtran1を作成します。

[AC1] ipsec transform-set tran1

#IPパケットのカプセル化にトンネルモードを使用するようにIPSecトランスフォームセットを設定します。

[AC1-ipsec-transform-set-tran1] encapsulation-mode tunnel

#IPSecトランスフォームセットのESPプロトコルを指定します。

[AC1-ipsec-transform-set-tran1] protocol esp

#ESP暗号化アルゴリズムとしてAES-CBC-128アルゴリズムを使用し、ESP認証アルゴリズムとしてHMAC-SHA1アルゴリズムを使用するようにIPSecトランスフォームセットを設定します。

[AC1-ipsec-transform-set-tran1] esp encryption-algorithm aes-cbc-128

[AC1-ipsec-transform-set-tran1] esp authentication-algorithm sha1

[AC1-ipsec-transform-set-tran1] quit

#IKEキーチェーンkeychain1を作成します。

[AC1] ike keychain keychain1

#ピア202.38.1.20とのIKEネゴシエーションに使用する事前共有キーを次のように設定します。**123456TESTplat&!.**

[AC1-ike-keychain-keychain1] pre-shared-key address 202.38.1.20 255.255.255.0 key simple 123456TESTplat&!

[AC1-ike-keychain-keychain1] quit

#IKEプロファイルprofile1を作成します。

[AC1] ike profile profile1

#事前共有キー認証用のキーチェーンkeychain1を指定します。

[AC1-ike-profile-profile1] keychain keychain1

#IPアドレスのIDタイプと値202.38.1.20でピアIDを設定します。

[AC1-ike-profile-profile1] match remote identity address 202.38.1.20 255.255.255.0

[AC1-ike-profile-profile1] quit

#map1という名前とシーケンス番号10を持つIPSecポリシーを作成しIKEネゴシエーションでSAを設定します。

[AC1] ipsec policy map1 10 isakmp

#IPSecポリシーにIPv4拡張ACL3111を指定します。

[AC1-ipsec-policy-isakmp-map1-10]security acl3111

#IPSecポリシーにIPSecトランスフォームセットtran1を指定します。

[AC1-ipsec-policy-isakmp-map1-10]transform-set tran1

#IPSecトンネルのローカルアドレス192.168.2.1とリモートIPアドレス202.38.1.20を設定します。

[AC1-ipsec-policy-isakmp-map1-10] local-address 192.168.2.1

[AC1-ipsec-policy-isakmp-map1-10] remote-address 202.38.1.20

#IPSecポリシーにIKEプロファイルprofile1を指定します。

[AC1-ipsec-policy-isakmp-map1-10]ike-profile profile1

[AC1-ipsec-policy-isakmp-map1-10]quit

#IPアドレス192.168.2.1を割り当て、IPSecポリシーマップ1をVLAN-interface2に適用します。

[AC1] interface Vlan-interface 2

[AC1-Vlan-interface2] ip address 192.168.2.1 255.255.255.0

[AC1-Vlan-interface2] ipsec apply policy map1

[AC1-Vlan-interface2] quit

#GigabitEthernet1/0/1をトランクポートとして設定し、そのPVIDをVLAN2に設定し、ポートをVLAN2に割り当てます。

[AC1] interface GigabitEthernet 1/0/1

[AC1-GigabitEthernet 1/0/1] port link-type trunk

[AC1-GigabitEthernet 1/0/1] port trunk pvid vlan 2

[AC1-GigabitEthernet 1/0/1] port trunk permit vlan 2

[AC1-GigabitEthernet 1/0/1] quit

#AC1にIPSecを設定するのと同じ方法でAC2にIPSecを設定します(詳細は表示されません)。

設定の確認

設定が完了すると、AC1とAC2の間にIPSecトンネルが確立されます。送信元ポート18002と宛先ポート18002の間のトラフィック、および送信元ポート60016～60031と宛先ポート60016～60031の間のトラフィックはIPSecで保護されます。

#AC1上のIPSec SAを表示するには、display ipsec saコマンドを使用します。

```
[AC1] display ipsec sa
-------------------------------
Interface: Vlan-interface5
-------------------------------
-----------------------------
IPsec policy: map1
Sequence number: 10
Mode: ISAKMP
-----------------------------
Tunnel id: 0
Encapsulation mode: tunnel
Perfect Forward Secrecy:
Inside VPN:
Extended Sequence Numbers enable: N
Traffic Flow Confidentiality enable: N
Path MTU: 1428
Tunnel:
```

local address: 192.168.2.1
remote address: 202.38.1.20
Flow:
sour addr: 0.0.0.0/0.0.0.0 port: 18002 protocol: udp
dest addr: 0.0.0.0/0.0.0.0 port: 18002 protocol: udp

[Inbound ESP SAs]
SPI: 2485516269 (0x9425f7ed)
Connection ID: 38654705664
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843187/986
Max received sequence-number: 264
Anti-replay check enable: Y
Anti-replay window size: 64
UDP encapsulation used for NAT traversal: N
Status: Active

[Outbound ESP SAs]
SPI: 3088244842 (0xb812e06a)
Connection ID: 38654705665
Transform set: ESP-ENCRYPT-AES-CBC-128 ESP-AUTH-SHA1
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843187/986
Max sent sequence-number: 264
47
UDP encapsulation used for NAT traversal: N
Status: Active

#AC1でゲストトンネルがアップ状態であることを確認します。

[AC1] display wlan guest-tunnel all

Guest access tunnel information

Local Mode: Edge AC Tunnel Count: 1

Peer IP Address Local IP Address VLANs State Interface

202.38.1.20 192.168.2.1 5 Up WLAN-Tunnel1

#AC2でゲストトンネルがアップ状態であることを確認します。
[AC2] display wlan guest-tunnel all
Guest access tunnel information
Local Mode: Aggregation AC Tunnel Count: 1
Peer IP Address Local IP Address VLANs State Interface
192.168.2.1 202.38.1.20 5 Up WLAN-Tunnel1

例:NATを介したIPSecゲストトンネルの設定

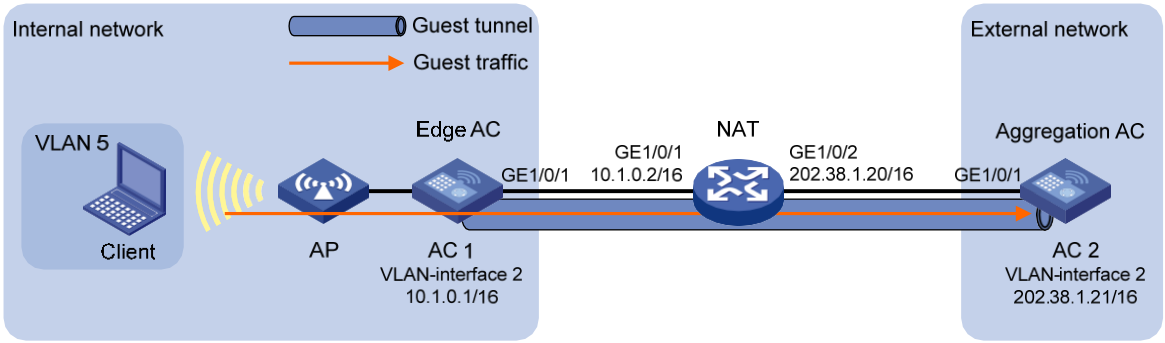
ネットワーク要件

図16に示すように、AC1はエッジACとして内部ネットワークに配置され、AC2は集約ACとして外部ネットワークに配置されます。WLANにアクセスするゲスト(この図のクライアント)はVLAN5に割り当てられます。

エッジACがゲストトラフィックを暗号化し、トラフィックをNATデバイスに転送できるように、IPSecゲストトンネルを設定します。エッジACから受信したトラフィックを集約ACに転送するようにNATデバイスを設定しま

す。

図16 ネットワーク図



手順

1. AC1の設定:

   #ACインターフェイスのIPアドレスを設定します(詳細は表示されません)。#ACをエッジACとして指定します。

   <AC1>system-view

   [AC1]wlan guest-tunnel edge-ac

   #エッジACの集約ACとしてAC2を指定し、ゲストVLANとしてVLAN5を指定します。

   [AC1-wlan-edge-ac]aggregation-ac ip202.38.1.21tunnel-source ip10.1.0.1vlan5

   #ゲストトンネルフロー分散を有効にします。

   [AC1-wlan-edge-ac]wlan guest-tunnel flow-distribute enable

   [AC1-wlan-edge-ac]quit

   #service template1を作成し、SSIDをguestに設定し、サービステンプレートを有効にします。

   [AC1]wlan service-template1

   [AC1-wlan-st-1]ssid guest

   [AC1-wlan-st-1]service-template enable

   [AC1-wlan-st-1]quit

   #AP ap1を作成し、シリアルIDを設定します。

   [AC1]wlan ap ap1モデルWA4320i-ACN

   [AC1-wlan-ap-ap1]シリアルID210235A35U007B000010

   #サービステンプレート1をAP ap1のワイヤレス2にバインドし、サービステンプレートを介してオンラインになるクライアントをVLAN5に割り当てます。

   [AC1-wlan-ap-ap1]radio 2

   [AC1-wlan-ap-ap1-radio-2]service-template1vlan-id5

   #radio2を有効にします。

   [AC1-wlan-ap-ap1-radio-2]radio enable

   [AC1-wlan-ap-ap1-radio-2]quit

   [AC1-wlan-ap-ap1]quit

2. AC2の設定:

   #ACインターフェイスのIPアドレスを設定します(詳細は表示されません)。

#ACを集約ACとして指定します。

<AC2>system-view

[AC2]wlan guest-tunnel aggregation-ac

#AC1をエッジACとして指定し、ゲストVLANをVLAN5に設定します。

[AC2-wlan-aggregation-ac]edge-ac ip10.1.0.1vlan5

#ゲストトンネルフロー配信をイネーブルにします。

[AC2-wlan-aggregation-ac]wlan guest-tunnel flow-distribute enable

[AC2-wlan-aggregation-ac]quit

3. NATの設定:

#GigabitEthernet1/0/1にIPアドレス10.1.0.2を割り当てます。

<NAT>system-view

[NAT]interface GigabitEthernet1/0/1

[NAT-GigabitEthernet1/0/1]ip address10.1.0.2 255.255.0.0

[NAT-GigabitEthernet1/0/1]quit

#NATアドレスグループ0を作成し、グループにアドレス202.38.1.23を追加します。

[NAT]nat address-group 0

[NAT-address-group-0]address202.38.1.23 202.38.1.23

[NAT-address-group-0]quit

#IPv4基本ACL2000を作成し、サブネット10.1.0.3/16からパススルー

[NAT] acl basic 2000

[NAT-acl-ipv4-basic-2000] rule permit source 10.1.0.3 0.0.0.255

[NAT-acl-ipv4-basic-2000] quit

#GigabitEthernet1/0/2にIPアドレス10.1.0.2を割り当てます。

[NAT] interface GigabitEthernet 1/0/2

[NAT-GigabitEthernet 1/0/2] ip address 202.38.1.20 255.255.0.0

#GigabitEthernet1/0/2で発信ダイナミックPATをイネーブルにします。ACLルールで許可されたパケットの送信元IPアドレスは、アドレスグループ0のアドレスに変換されます。

[NAT-GigabitEthernet 1/0/2] nat outbound 2000 address-group 0

[NAT-GigabitEthernet 1/0/2] quit

4. Configure IPsec on AC 1:

#IPv4拡張ACL3000を作成します。

[AC1] acl advanced 3000

#ポート18002からポート18002へのUDPトラフィックを許可するACLルールを作成します。

[AC1-acl-ipv4-adv-3000] rule permit udp source-port eq 18002 destination-port eq 18002

#ポート60016～60031からポート60016～60031へのUDPトラフィックを許可するACLルールを作成します。

[AC1-acl-ipv4-adv-3000] rule permit udp source-port range 60016 60031 destination-port range 60016 60031

[AC1-acl-ipv4-adv-3000] quit

#IPSecトランスフォームセットtran1を作成します。

[AC1] ipsec transform-set tran1

#IPパケットのカプセル化にトンネルモードを使用するようにIPSecトランスフォームセットを設定します。

[AC1-ipsec-transform-set-tran1] encapsulation-mode tunnel

#IPSecトランスフォームセットのESPプロトコルを指定します。

[AC1-ipsec-transform-set-tran1] protocol esp

#ESP暗号化アルゴリズムとして3DESアルゴリズムを使用し、ESP認証アルゴリズムとしてHMAC-MD5アルゴリズムを使用するようにIPSecトランスフォームセットを設定します。

[AC1-ipsec-transform-set-tran1] esp encryption-algorithm 3des-cbc

[AC1-ipsec-transform-set-tran1] esp authentication-algorithm md5

[AC1-ipsec-transform-set-tran1] quit

#IKEキーチェーンkeychain1を作成します。

[AC1] ike keychain keychain1

#ピア202.38.1.21とのIKEネゴシエーションに使用する事前共有キーを次のように設定します。**123456TESTplat&!.**

[AC1-ike-keychain-keychain1] pre-shared-key address 202.38.1.21 255.255.0.0 key simple 123456TESTplat&!

[AC1-ike-keychain-keychain1] quit

#IKEプロファイルprofile1を作成します。

[AC1] ike profile profile1

#事前共有キー認証用のキーチェーンkeychain1を指定します。

[AC1-ike-profile-profile1] keychain keychain1

#IKEネゴシエーションがアグレッシブモードで動作することを指定します。

[AC1-ike-profile-profile1]exchange-mode aggressive

#ローカルIDをFQDN名h3c.comに設定します。

[AC1-ike-profile-profile1] local-identity fqdn h3c.com

#IPアドレスのIDタイプと値202.38.1.21でピアIDを設定します。

[AC1-ike-profile-profile1] match remote identity address 202.38.1.21 255.255.0.0

[AC1-ike-profile-profile1] quit

#policy1という名前とシーケンス番号1を持つIPSecポリシーを作成し、IKEネゴシエーションを介してSAを設定するポリシーを指定します。

[AC1] ipsec policy policy1 1 isakmp

#IPSecポリシーにACL3000を指定します。

[AC1-ipsec-policy-isakmp-policy1-1] security acl 3000

#IPSecポリシーのIPSecトランスフォームセットtran1を指定します。

[AC1-ipsec-policy-isakmp-policy1-1] transform-set tran1

#IPSecトンネルのリモートIPアドレス202.38.1.21を設定します。

[AC1-ipsec-policy-isakmp-policy1-1] remote-address 202.38.1.21

#IPSecポリシーにIKEプロファイルprofile1を指定します。

[AC1-ipsec-policy-isakmp-policy1-1] ike-profile profile1

[AC1-ipsec-policy-isakmp-policy1-1] quit

#IPアドレス10.1.0.1を割り当て、IPSecポリシーマップ1をVLAN-interface5に適用します。

[AC1] interface Vlan-interface 5

[AC1-Vlan-interface5] ip address 10.1.0.1 255.255.0.0

[AC1-Vlan-interface5] ipsec apply policy policy1

[AC1-Vlan-interface5] quit

#GigabitEthernet1/0/1をトランクポートとして設定し、そのPVIDをVLAN2に設定し、ポートをVLAN2に割り当てます。

[AC1] interface GigabitEthernet 1/0/1

[AC1-GigabitEthernet1/0/1]port link-type trunk

[AC1-GigabitEthernet1/0/1]port trunk pvid vlan2

[AC1-GigabitEthernet1/0/1]port trunk permit vlan2

[AC1-GigabitEthernet1/0/1]quit

#ピアが応答しない場合、DPDが10秒ごとにトリガーされ、リトライ間で5秒ごとにトリガーされるように設定します。

[AC1] ike dpd interval 10 retry 5 on-demand

#スタティックルートを設定します。

[AC1] ip route-static 0.0.0.0 0 10.1.0.2

#(任意)AC1がIRFファブリックの場合、IPSec冗長性をイネーブルにします。

[AC1] ipsec redundancy enable

5. Configure IPsec on AC 2:

#IPSecトランスフォームセットtran1を作成します。

[AC2] ipsec transform-set tran1

#IPパケットのカプセル化にトンネルモードを使用するようにIPSecトランスフォームセットを設定します。

[AC2-ipsec-transform-set-tran1] encapsulation-mode tunnel

#IPSecトランスフォームセットのESPプロトコルを指定します。

[AC2-ipsec-transform-set-tran1] protocol esp

#ESP暗号化アルゴリズムとして3DESアルゴリズムを使用し、ESP認証アルゴリズムとしてHMAC-MD5アルゴリズムを使用するようにIPSecトランスフォームセットを設定します。

[AC2-ipsec-transform-set-tran1] esp encryption-algorithm 3des-cbc

[AC2-ipsec-transform-set-tran1] esp authentication-algorithm md5

[AC2-ipsec-transform-set-tran1] quit

#IKEキーチェーンkeychain1を作成します。

[AC2] ike keychain keychain1

#ピア202.38.1.23とのIKEネゴシエーションに使用する事前共有キーを次のように設定します。**123456TESTplat&!.**

[AC2-ike-keychain-keychain1] pre-shared-key address 202.38.1.23 255.255.0.0 key simple 123456TESTplat&!

[AC2-ike-keychain-keychain1] quit

#IKEプロファイルprofile1を作成します。

[AC2] ike profile profile1

#事前共有キー認証用のキーチェーンkeychain1を指定します。

[AC2-ike-profile-profile1] keychain keychain1

#IKEネゴシエーションがアグレッシブモードで動作することを指定します。

[AC2-ike-profile-profile1] exchange-mode aggressive

#FQDNの識別タイプとh3c.comの値でピアIDを設定します。

[AC2-ike-profile-profile1] match remote identity fqdn h3c.com

[AC2-ike-profile-profile1] quit

#template1という名前でシーケンス番号1のIPSecポリシーテンプレートを作成します。

[AC2] ipsec policy-template template1 1

#IPSecポリシーテンプレートにIPSecトランスフォームセットtran1を指定します。

[AC2-ipsec-policy-template-template1-1]transform-set tran1

#IPSecトンネルにローカルアドレス202.38.1.21を設定します。

[AC2-ipsec-policy-template-template1-1] local-address 202.38.1.21

#IPSecポリシーテンプレートにIKEプロファイルprofile1を指定します。

[AC2-ipsec-policy-template-template1-1] ike-profile profile1

[AC2-ipsec-policy-template-template1-1] quit

#IPSecポリシーテンプレートtemplate1を使用してIPSecポリシーエントリを作成しポリシー名をpolicy1とし、sequence number を1にします。

[AC2] ipsec policy policy1 1 isakmp template template1

#IPアドレス202.38.1.21を割り当て、IPSecポリシーpolicy1をVLAN-interface2に適用します。

[AC2] interface Vlan-interface 2

[AC2-Vlan-interface2] ip address 202.38.1.21 255.255.0.0

[AC2-Vlan-interface2] ipsec apply policy policy1

[AC2-Vlan-interface2] quit

#GigabitEthernet1/0/1をトランクポートとして設定し、そのPVIDをVLAN2に設定し、ポートをVLAN2に割り当てます。

[AC2] interface GigabitEthernet 1/0/1

[AC2-GigabitEthernet 1/0/1] port link-type trunk [AC2-GigabitEthernet

1/0/1] port trunk pvid vlan 2

[AC2-GigabitEthernet 1/0/1] port trunk permit vlan 2

[AC2-GigabitEthernet 1/0/1] quit

#ピアが応答しない場合、DPDが10秒ごとにトリガーされ、リトライ間で5秒ごとにトリガーされるように設定します。

[AC2] ike dpd interval 10 retry 5 on-demand

#スタティックルートを設定します。

[AC2] ip route-static 0.0.0.0 0 10.2.0.3

#(任意)AC2がIRFファブリックの場合、IPSec冗長性をイネーブルにします。

[AC2] ipsec redundancy enable

設定の確認

設定が完了すると、AC1とAC2の間にIPSecトンネルが確立されます。送信元ポート18002と宛先ポート18002の間のトラフィック、および送信元ポート60016～60031と宛先ポート60016～60031の間のトラフィックはIPSecで保護されます。

#AC1上のIPSec SAを表示するには、display ipsec saコマンドを使用します。

[AC1] display ipsec sa

Interface: Vlan-interface5

Tunnel id: 0 Encapsulation mode:

---

tunnel Perfect Forward Secrecy:

Inside VPN:

Extended Sequence Numbers enable: N Traffic Flow

Confidentiality enable: N Path MTU: 1436

Tunnel:

local address: 10.1.0.1

remote address: 202.38.1.21 Flow:

sour addr: 0.0.0.0/0.0.0.0 port: 18002 protocol: udp dest addr:
0.0.0.0/0.0.0.0 port: 18002 protocol: udp

[inbound ESP SA]
SPI: 3885901857 (0xe79e2821)
Connection ID: 55834574848
Transform set: ESP-ENCRYPT-3DES-CBC ESP-AUTH-MD5
SA duration (kilobytes/sec): 1843200/3600
SA remaining duration (kilobytes/sec): 1843199/3160 Max received
sequence-number: 5
Anti-replay check enable: Y Anti-
replay window size: 64
UDP encapsulation used for NAT traversal: Y Status:
Active

#AC1でゲストトンネルがアップ状態であることを確認します。

[AC1] display wlan guest-tunnel all
Guest access tunnel information
Local Mode: Edge ACTunnel Count:

Peer IP Address	Local IP Address	VLANs	State	Interface
202.38.1.21	10.1.0.1	5	Up	WLAN-Tunnel1

#AC2でゲストトンネルがアップ状態であることを確認します。

[AC2] display wlan guest-tunnel all
Guest access tunnel information
Local Mode: Aggregation ACTunnel Count: 1

Peer IP Address	VLANs	State	Interface
10.1.0.1	5	Up	WLAN-Tunnel1