H3Cアクセスコントローラ

ユーザーアクセスおよびWLAN認証ガイド

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

ドキュメントバージョン:6W103-20200507製品バージョン:R5426P02

内容

WLAN認証の設定

WLAN認証について

この章では、デバイスでのWLAN認証の実装について説明します。WLAN認証は、アクセスセキュリティを確保するために、WLANクライアントに対してMACベースのネットワークアクセスコントロールを実行します。

WLAN認証には、次の認証方式があります。

- **802.1X認証**: Extensible Authentication Protocol(EAP)を使用して、クライアント、オーセンティケータ、および認証サーバーの認証情報を転送します。
- **MAC認証**: 送信元MACアドレスを認証することによって、ネットワークアクセスを制御します。この機能にはクライアントソフトウェアは必要ありません。クライアントは、ネットワークアクセスのためにユーザー名やパスワードを入力する必要はありません。オーセンティケータは、不明な送信元MACアドレスを検出すると、MAC認証プロセスを開始します。MACアドレスが認証に合格すると、クライアントは許可されたネットワークリソースにアクセスできます。認証に失敗すると、オーセンティケータはMACアドレスをサイレントMACアドレスとしてマークし、クライアントのアクセスを拒否します。
- **OUI認証**: クライアントのMACアドレス内のOUIを調べます。クライアントのOUIが、オーセンティケータ用に構成されたOUIの1つと一致する場合、クライアントはOUI認証に合格します。

注:

OUIは、ベンダー、製造業者または組織を一意に識別する24ビットの数値です。MACアドレスでは、最初の3つのオクテットがOUIです。

認証モード

認証モード	作動機構	侵入防御を起動できるかどうか
bypass(デフォルト)	認証は実行しません。 クライアントは認証されることなくネットワークにアクセスできます。	いいえ
dot1x	802.1X認証だけを実行します。 クライアントは、ネットワークにアクセスする前に802.1X認証に合格する必要があります。	はい
mac	MAC認証だけを実行します。 クライアントは、ネットワークにアクセスする前にMAC認証に合格する必要があります。	はい

dot1x-then-mac	最初に802.1X認証を実行し、802.1X認証が失敗した場合はMAC認証を実行します。 クライアントは、802.1X認証またはMAC認証を通過した場合にネットワークにアクセスできます。	はい
oui-then-dot1x	OUI認証を最初に実行し、OUI認証が失敗した場合は802.1X認証を実行します。 クライアントは、OUI認証または802.1X認証のいずれかに合格すると、ネットワークにアクセスできます。	はい
mac-and-dot1x	最初にMAC認証を実行し、次に802.1X認証を実行します。 クライアントがネットワークにアクセスできるのは、MAC認証と802.1X認証の両方に合格した場合だけです。	はい
mac-then-dot1x	最初にMAC認証を実行し、MAC認証が失敗した場合は802.1X認証を実行します。 クライアントは、MAC認証または802.1X認証のいずれかに合格すると、ネットワークにアクセスできます。	はい

802.1X認証

802.1Xアーキテクチャ、EAPリレー、EAP終端、およびEAPパケットカプセル化の詳細については、「802.1Xの概要」および「802.1Xの設定」を参照してください。

認証方式

オーセンティケータで802.1X認証(ローカル認証)を実行することも、RADIUSサーバーを介して実行することもできます。RADIUS認証およびローカル認証の詳細については、「AAAの設定」を参照してください。

オーセンティケータ

オーセンティケータはクライアントを認証して、WLANへのアクセスを制御します。

AC+fit APネットワークでは、ACまたはAPのいずれかをオーセンティケータとして指定できます。
client-security authentication-locationコマンド。

EAPパケットカプセル化

802.1Xは、EAP over LAN(EAPOL)を定義して、WLANを介してクライアントとオーセンティケータの間でEAPパケットを渡します。802.1Xは、オーセンティケータと認証サーバーの間で、次のいずれかの方法を使用して認証情報を配信します。

- 「EAPリレー」で説明されているように、EAP over RADIUS(EAPOR)を使用してEAPパケットをRADIUSにカプセル化します。
- 「EAP終端」で説明されているように、EAPパケットから認証情報を抽出し、標準RADIUSパケットにカプセル化します。

EAPパケットカプセル化については、「802.1Xの概要」を参照してください。

EAPリレー

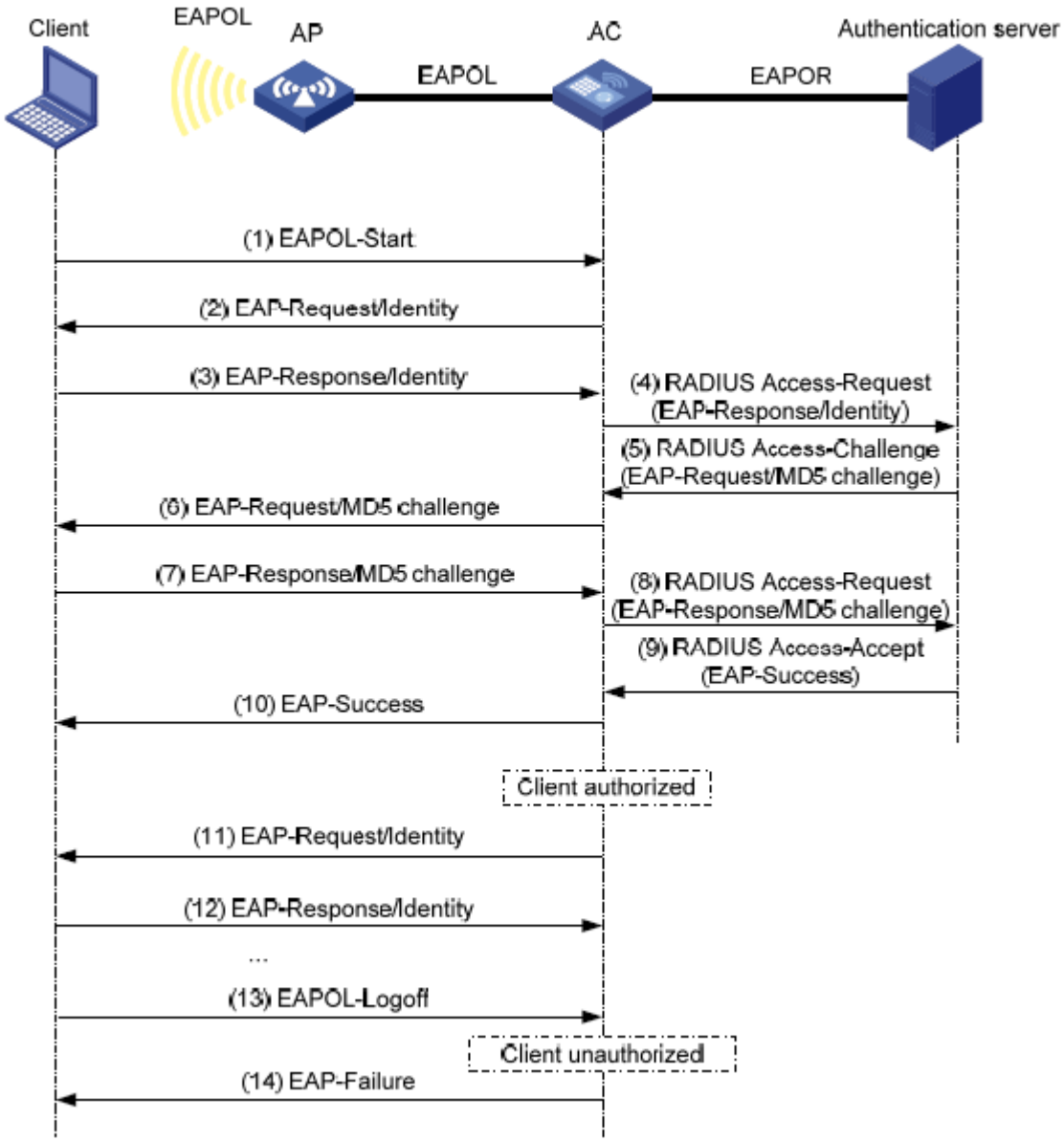
このモードでは、オーセンティケータはEAPORパケットを使用して認証情報をRADIUSサーバーに送信します。RADIUSサーバーは、EAP-MessageおよびMessage-Authenticatorアトリビュートをサポートする必要があります。

図1に、EAPリレーモードでの基本的な802.1X認証プロセスを示します。この例では、EAP-MD5が使用されています。

注:

APがオーセンティケータとして指定されている場合は、APがEAPおよびRADIUSパケットを処理することを除き、図1と同じ認証プロセスを使用します。

図1 EAPリレーモードでの802.1X認証プロセス(AC+fit APネットワーク)



次に、802.1X認証プロセスの手順を示します。

1. ユーザーが802.1Xクライアントを起動し、登録されたユーザー名とパスワードを入力すると、802.1Xクライアントは EAPOL-Startパケットをオーセンティケータに送信します。

クライアントとAPの関連付けについては、『WLAN Security Configuration Guide』の「WLAN Security」を参照してください。

2. オーセンティケータは、ユーザー名を要求するEAP-Request/Identityパケットで応答します。
3. クライアントは、EAP-Response/Identityパケットでユーザー名をオーセンティケータに送信します。
4. オーセンティケータは、RADIUS Access-Requestパケット内のEAP-Response/Identityパケットを認証サーバーにリレーします。
5. 認証サーバーは、RADIUS Access-Request内のユーザー名を使用してユーザーデータベースを検索します。一致するエントリが見つかった場合、サーバーはランダムに生成されたチャレンジ(EAP-Request/MD 5-チャレンジ)を使用してエントリ内のパスワードを暗号化します。次に、サーバーはRADIUS Access-Challengeパケット内のチャレンジをオーセンティケータに送信します。
6. オーセンティケータは、EAP-Request/MD5-Challengeパケットをクライアントに送信します。
7. クライアントは受信したチャレンジを使用してパスワードを暗号化し、暗号化されたパスワードをEAP-Response/MD5-Challengeパケットでオーセンティケータに送信します。
8. オーセンティケータは、RADIUS Access-Requestパケット内のEAP-Response/MD5-Challengeパケットを認証サーバーにリレーします。
9. 認証サーバーは、受信した暗号化パスワードとステップ5で生成した暗号化パスワードを比較します。2つのパスワードが同一である場合、サーバーはクライアントを有効と見なし、RADIUS Access-Acceptパケットをオーセンティケータに送信します。
10. RADIUS Access-Acceptパケットを受信すると、オーセンティケータはクライアントがネットワークにアクセスできるようにします。
11. クライアントがオンラインになった後、オーセンティケータは定期的にハンドシェイク要求を送信して、クライアントがまだオンラインであるかどうかを調べます。
12. ハンドシェイク要求を受信すると、クライアントは応答を返します。クライアントが連続した数回のハンドシェイク試行(デフォルトでは2回)の後に応答を返さない場合、オーセンティケータはクライアントをログオフします。このハンドシェイクメカニズムにより、異常にオフラインになった802.1Xクライアントが使用するネットワークリソースをタイムリーに解放できます。
13. クライアントはEAPOL-Logoffパケットを送信して、オーセンティケータからのログオフを要求します。
14. EAPOL-Logoffパケットに応答して、オーセンティケータはEAP-Failureパケットをクライアントに送信します。

EAPの終了

このモードでは、オーセンティケータは次の動作を実行します。

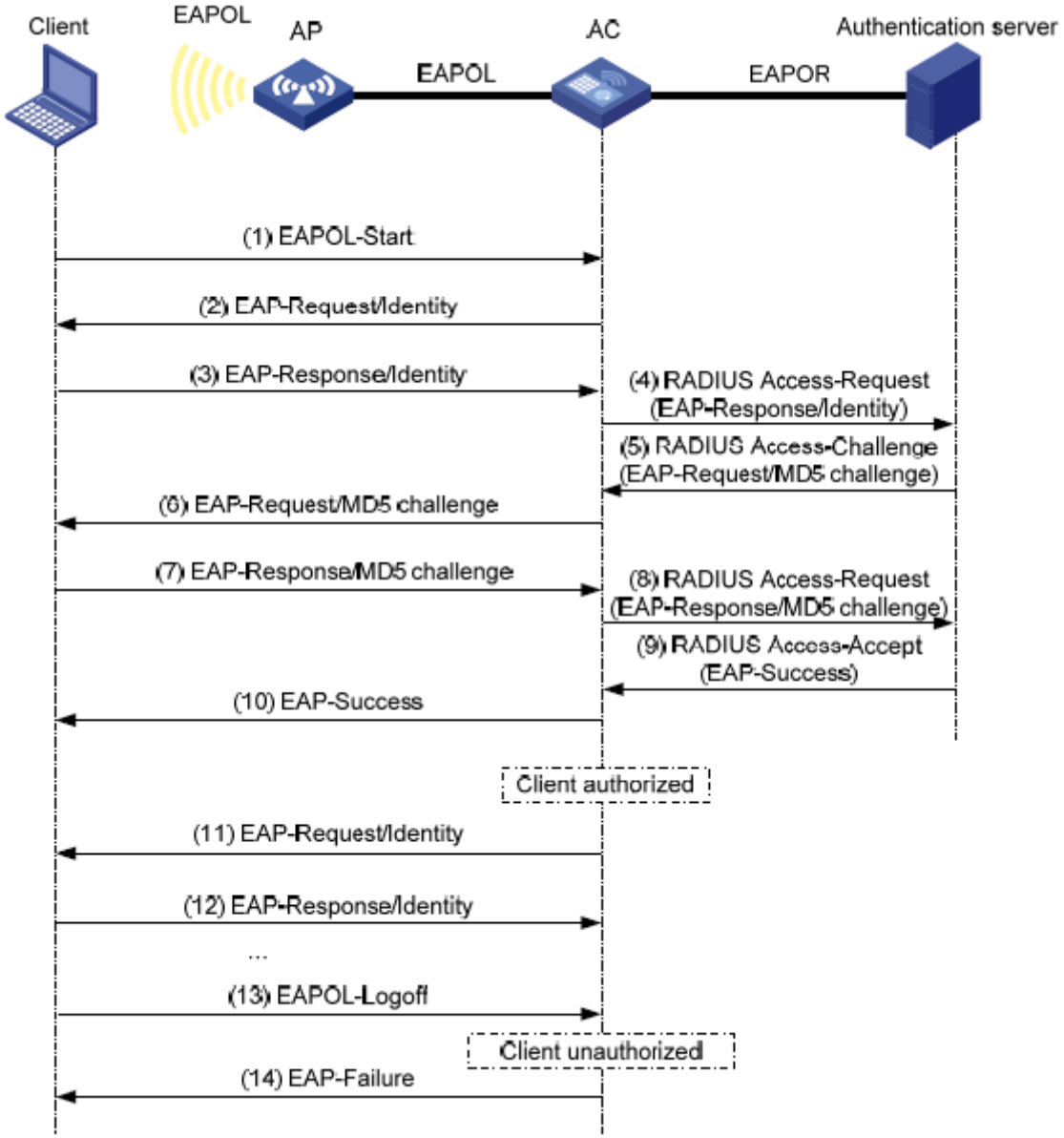
1. クライアントから受信したEAPパケットを終了します。
2. クライアント認証情報を標準RADIUSパケットにカプセル化します。
3. PAPまたはCHAPを使用してRADIUSサーバーと通信します。

図2は、EAP終了モードでの基本的な802.1X認証プロセスを示しています。この例では、CHAP認証が使用されています。

注:

APがオーセンティケータとして指定されている場合は、APがEAPおよびRADIUSパケットを処理することを除き、図2と同じ認証プロセスを使用します。

図2 EAP終端モードの802.1X認証プロセス(AC+fit APネットワーク)



EAP終了モードでは、認証サーバーではなく認証デバイスがパスワード暗号化用のMD5チャレンジを生成します。認証デバイスは次に、標準RADIUSパケット内のユーザー名および暗号化されたパスワードとともにMD5チャレンジをRADIUSサーバーに送信します。

802.1X認証の開始

クライアントとオーセンティケータの両方が802.1X認証を開始できます。

- **Client initiation**: クライアントがオーセンティケータに関連付けられた後、EAPOL-Startパケットをオーセンティケータに送信して802.1X認証を開始します。
- **Authenticator initiation**: クライアントがオーセンティケータに関連付けられた後、オーセンティケータはEAP-Request/Identityパケットを送信して認証を開始します。クライアントのタイムアウトタイマー内に応答が受信されなかった場合、オーセンティケータはパケットを再送信します。

MAC認証

認証方式

オーセンティケータでMAC認証(ローカル認証)を実行することも、RADIUSサーバーを介して実行することもできます。RADIUS認証およびローカル認証の詳細については、「AAAの設定」を参照してください。

オーセンティケータ

オーセンティケータはクライアントを認証して、WLANへのアクセスを制御します。

AC+fit APネットワークでは、ACまたはAPのいずれかをオーセンティケータとして指定できます。
client-security authentication-locationコマンド。

ユーザーアカウントポリシー

クライアントを識別するには、ユーザーカウントが必要です。MAC認証では、次のユーザーアカウントポリシーがサポートされます。

- クライアントごとに1つのMACベースのユーザーアカウント。オーセンティケータは、パケット内の未知の送信元MACアドレスを、MAC認証用のクライアントのユーザー名およびパスワードとして使用します。
- すべてのクライアントに対して1つの共有ユーザーアカウント。オーセンティケータ上のすべてのMAC認証クライアントに対して、1つのユーザー名とパスワード(必ずしもMACアドレスではない)を指定します。ユーザー名は、大文字と小文字が区別される1～55文字の文字列で、@記号(@)を含めることはできません。パスワードは、1～63文字のプレーンテキスト文字列または1～117文字の暗号文文字列です。

MAC認証手順

RADIUS認証:

- **MACベースのアカウント**: オーセンティケータは、認証のためにパケットの送信元MACアドレスをユーザー名およびパスワードとしてRADIUSサーバーに送信します。
- **共有アカウント**: オーセンティケータは、認証のために共有アカウントのユーザー名とパスワードをRADIUSサーバーに送信します。

ローカル認証:

- **MACベースのアカウント**: オーセンティケータはパケットの送信元MACアドレスをユーザー名およびパスワードとして使用して、一致するものをローカルアカウントデータベースで検索します。
- **共有アカウント**: オーセンティケータは、共有アカウントのユーザー名とパスワードを使用して、一致するローカルアカウントデータベースを検索します。

侵入防御

オーセンティケータが認証に失敗したクライアントからのアソシエーション要求を検出すると、侵入保護がトリガーされます。この機能は、要求を受信したBSSで次の定義済みアクションのいずれかを実行します。

- **temporary-block**(デフォルト) :要求の送信元MACアドレスをブロックされたMACアドレスリストに追加し、要求パケットをドロップします。ブロックされたMACアドレスのクライアントは、期間内にAPとの接続を確立できません。期間を設定するには
client-security intrusion-protection timer temporary-blockコマンド。
- **service-stop**: BSSが無線インターフェイス上で手動でイネーブルになるまで、要求を受信したBSSを停止します。
- **temporary-service-stop**: 要求を受信したBSSを一定期間停止します。期間を設定するには、クライアントセキュリティ侵入保護タイマーを使用します。
temporary-service-stopコマンド。

注:

侵入防御アクションは、バイパスモードではサポートされません。

WLAN VLANの操作

VLAN認証

WLANクライアントに許可VLANを指定して、ネットワークリソースへのクライアントのアクセスを制御できます。クライアントが802.1XまたはMAC認証を通過すると、認証サーバーは許可VLAN情報をオーセンティケータに割り当てます。デバイスがオーセンティケータとして動作する場合、次の形式のサーバー割り当てVLANを解決できます。

- VLAN ID
- VLAN名

  VLAN名は、アクセスデバイス上のVLANの説明を表します。
- VLANグループ名

  VLANグループの詳細については、『Network Connectivity Configuration Guide』の「VLAN configuration」を参照してください。
- VLAN IDとVLAN名の組み合わせ

  文字列では、一部のVLANはIDで表され、一部のVLANは名前で表されます。

サーバーがVLANグループを割り当てる場合、アクセスデバイスはVLAN IDフォーマットに従ってVLANを選択し、割り当てます。表1に、認可VLANグループのVLAN選択および割り当て規則を示します。

表1 認可VLANグループのVLAN選択および割り当て

許可されたVLANのタイプ	VLANの選択および割り当てルール
• ID別のVLAN • 名前別VLAN • VLAN IDとVLAN名の組み合わせ	デバイスは、VLANのグループから最も小さいIDを持つVLANを選択します。
VLANグループ名	1. デバイスは、オンラインユーザー数が最も少ないVLANを選択します。 2. 複数のVLANに同じ数のオンライン802.1Xユーザーが存在する場合、デバイスは最も小さいIDを持つVLANを選択します。

注:

デバイスは、クライアントにVLANを割り当てる前に、VLAN名とVLANグループ名をVLAN IDに変換します。

デバイスは、次の状況でクライアントのVLAN認可に失敗します。

- デバイスは許可VLAN情報の解決に失敗します。
- サーバーはVLAN名をデバイスに割り当てますが、デバイスにはその名前を使用するVLANがありません。
- サーバーはVLANグループ名をデバイスに割り当てますが、VLANグループが存在しないか、VLANグループにVLANが割り当てられていません。

許可VLAN情報はデータの転送を制御するために使用されるため、データトラフィックを転送するデバイスによって割り当てられる必要があります。VLAN割り当ては、オーセンティケータと転送デバイスが同じデバイスであるかどうかに応じて、ローカルVLAN割り当てまたはリモートVLAN割り当てになります。

- ローカルVLAN割り当て: オーセンティケータと転送デバイスは同じデバイスです。オーセンティケータは認可VLAN情報を取得した後、その情報を解決してVLANを割り当てます。
- リモートVLAN割り当て: オーセンティケータと転送デバイスは異なるデバイスです。オーセンティケータは認可VLAN情報を取得した後、その情報をリモート転送デバイスに送信します。転送デバイスはその情報を解決し、VLANを割り当てます。

認証失敗VLAN

WLAN Auth-fail VLAN(認証失敗VLAN)は、組織のセキュリティ戦略に準拠していないためにWLAN認証に失敗したクライアントに対応します。たとえば、VLANは、間違ったパスワードまたはユーザー名を入力したクライアントに対応します。Auth-fail VLAN(認証失敗VLAN)は、認証タイムアウトまたはネットワーク接続の問題で認証に失敗したWLANクライアントに対応しません。

Auth-fail VLAN(認証失敗VLAN)内のクライアントは、限られたネットワークリソースセットにアクセスできます。

RSNAを使用するクライアントは、802.1X認証に失敗した後はAuth-fail VLAN(認証失敗VLAN)に割り当てることができません。オーセンティケータはクライアントを直接ログオフします。

認証失敗VLAN機能は、侵入保護よりも優先されます。クライアントが認証に失敗した場合、認証失敗VLAN設定が最初に適用されます。認証失敗VLANが設定されていない場合、侵入保護機能が有効になります。どちらの機能も設定されていない場合、オーセンティケータはクライアントから直接ログオフします。

クリティカルVLAN

WLANクリティカルVLANは、ISPドメイン内のすべてのRADIUSサーバーが到達不能であるためにWLAN認証に失敗したクライアントに対応します。クリティカルVLANのクライアントは、設定に応じて、限られたネットワークリソースセットにアクセスできます。

オーセンティケータは、30秒間隔でクリティカルVLAN内のクライアントを再認証します。

- クライアントが再認証に合格すると、オーセンティケータはクライアントを認可VLANに割り当てます。認可VLANが設定されていない場合、クライアントは最初のVLANに割り当てられます。
- すべてのRADIUSサーバーが到達不能であるためにクライアントが再認証に失敗した場合、クライアントは引き続きクリティカルVLAN内に存在します。
- クライアントが到達不能なサーバー以外の理由で再認証に失敗した場合、デバイスはクライアントをAuth-fail VLAN(認証失敗VLAN)に割り当てます。Auth-fail VLAN(認証失敗VLAN)が設定されていない場合、デバイスは侵入保護の設定に応じてクライアントを処理します。侵入保護機能が設定されていない場合、デバイスはクライアントをログオフします。

クリティカルVLAN機能は、RSNAを使用するクライアントには適用されません。すべてのRADIUSサーバーが到達不能であるためにこれらのクライアントが認証に失敗した場合、オーセンティケータはクライアントから直接ログオフします。

ACLの割り当て

802.1XクライアントのACLを指定して、クライアントのネットワークリソースへのアクセスを制御できます。クライアントが認証を通過した後、認証サーバーは、このクライアントのトラフィックをフィルタリングするためにACLをクライアントに割り当てます。認証サーバーは、オーセンティケータとして動作するローカルデバイス上またはRADIUSサーバー上に存在できます。どちらの場合も、オーセンティケータ上でACLのルールを設定する必要があります。APがオーセンティケータとして動作する場合は、AC上でACLルールを設定する必要があります。

クライアントのアクセス制御基準を変更するには、次のいずれかの方法を使用できます。

- オーセンティケータのACLルールを変更します。
- 認証サーバー上のクライアントに別のACLを指定します。

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

ユーザープロファイルの割り当て

WLANクライアントのユーザープロファイルを指定して、ネットワークリソースへのクライアントのアクセスを制御できます。クライアントが802.1X認証を通過した後、認証サーバーはトラフィックをフィルタリングするためにユーザープロファイルをクライアントに割り当てます。認証サーバーは、オーセンティケータとして動作するローカルデバイス上またはRADIUSサーバー上に配置できます。どちらの場合も、オーセンティケータ上でユーザープロファイルを設定する必要があります。APがオーセンティケータとして動作する場合は、AC上でユーザープロファイルを設定する必要があります。

クライアントのアクセス許可を変更するには、次のいずれかの方法を使用できます。

- オーセンティケータのユーザープロファイル設定を変更します。
- 認証サーバー上のクライアントに別のユーザープロファイルを指定します。

ユーザープロファイルの詳細は、セキュリティ構成ガイドを参照してください。

CAR属性の割り当て

デバイスは、RADIUS拡張アトリビュートによって割り当てられたCARアトリビュートを使用して、認証されたオンライン802.1XまたはMAC認証サーバーのアクセスレートを制御できます。拡張RADIUSアトリビュートの詳細については、『Configuring AAA』を参照してください。

次のCARアトリビュートを使用できます。

- **Input-Average-Rate**: 着信トラフィックの平均レート(bps)。
- **Output-Average-Rate**: 発信トラフィックの平均レート(bps)。

BYODアクセス制御

この機能により、RADIUSサーバーは異なる登録ページをプッシュし、異なるエンドポイントデバイス上のクライアントに異なる認可アトリビュートを割り当てることができます。

注:

この機能は、現在のバージョンでRADIUSサーバーとして動作するIMCサーバーだけをサポートしています。

次のプロセスは、802.1XまたはMAC認証を通過するWLANクライアントのBYODアクセスコントロールを示しています。

1. オーセンティケータは次の動作を実行します。
   a. DHCPパケットからOption 55アトリビュートを取得します。
   b. Option 55アトリビュートをRADIUSサーバーに配信します。

   IMCサーバーでは、Option 55アトリビュートがUAMに配信されます。
2. BYOD対応RADIUSサーバーは、次の動作を実行します。
   a. Option 55アトリビュートを使用して、エンドポイントタイプ、オペレーティングシステム、ベンダーなどのエンドポイントデバイス情報を識別します。
   b. 登録ページを送信し、デバイス情報に従ってクライアントに認可アトリビュートを割り当てます。

制約事項:コマンドとハードウェアの互換性

WX1800Hシリーズ、WX2500Hシリーズ、およびWX3000Hシリーズアクセスコントローラは、IRFモードだけで使用可能なパラメータやコマンドをサポートしません。

WLAN認証タスクの概要

WLAN認証を設定するには、次の作業を実行します。

- グローバルWLAN認証パラメータの設定
- サービス固有のWLAN認証パラメータの設定
- BYOD許可トリガーの使用可能化
- 失敗許可機能の設定
  - 認証失敗許可の設定
  - 5G無線サイレンス失敗許可の設定
- サービステンプレートでの802.1X EAP終了のイネーブル化

WLAN認証の前提条件

802.1Xの前提条件

802.1X認証を設定する前に、次の作業を実行します。

- 802.1XサーバーのISPドメインおよびAAAスキーム(ローカルまたはRADIUS認証)を設定します。詳細については、「AAAの設定」を参照してください。
- RADIUS認証を使用する場合は、RADIUSサーバー上にユーザーアカウントを作成します。
- ローカル認証を使用する場合は、アクセスデバイス上にローカルユーザーアカウントを作成し、サービスタイプをlan-accessに設定します。

MAC認証の前提条件

MAC認証を設定する前に、ISPドメインを設定し、AAA方式を指定します。詳細については、『Security Configuration Guide』の「AAA」を参照してください。

- ローカル認証の場合は、ローカルユーザーアカウント(ユーザー名とパスワードを含む)を作成し、ローカルユーザーのLANアクセスサービスを指定する必要もあります。
- RADIUS認証では、デバイスとRADIUSサーバーが互いに到達できることを確認し、RADIUSサーバー上にユーザーアカウントを作成します。MACベースのアカウントを使用している場合は、各アカウントのユーザー名とパスワードが、各MAC認証サーバーのMACアドレスと同じであることを確認します。

グローバルWLAN認証パラメータの設定

OUI認証用のOUIの設定

このタスクについて

この作業は、oui-then-dot1x認証モードに対してだけ実行します。

制限事項とガイドライン

デバイスは最大16個のOUIをサポートします。

手順

1. システムビューに入ります。

   system-view
2. OUI認証のOUI値を設定します。

   port-security oui index *index-value* **mac-address** *oui-value*

   デフォルトでは、OUI認証にOUI値は設定されていません。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の「port security」を参照してください。

802.1X認証のEAPリレーまたはEAPターミネーションのイネーブル化

制限事項とガイドライン

EAPリレーモードを使用する場合は、次の制約事項および注意事項が適用されます。

- RADIUSスキームビューのuser-name-formatコマンドは有効になりません。デバイスは、クライアントからサーバーに認証データを変更なしで送信します。user-name-formatコマンドの詳細については、『User Access and Authentication Command Reference』の「AAA」を参照してください。
- RADIUSサーバーがクライアントと同じ認証方式を使用していることを確認します。オーセンティケータの場合は、dot1x authentication-method eapコマンドを使用するだけでEAPリレーをイネーブルにできます。

手順

1. システムビューに入ります。

   system-view
2. EAPリレーまたはEAPターミネーションをイネーブルにします。

   dot1x authentication-method { chap | eap | pap }

   デフォルトでは、デバイスはEAP終端を実行し、CHAPを使用してRADIUSサーバーと通信します。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の802.1Xを参照してください。

802.1 Xでサポートされるドメイン名区切り文字の指定

1. システムビューに入ります。

   system-view
2. 802.1Xクライアント用の一連のドメイン名デリミタを指定します。

   dot1x domain-delimiter *string*

   デフォルトでは、802.1Xユーザーのドメインデリミタはアットマーク(@)です。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の802.1Xを参照してください。

802.1X認証要求の最大試行回数の設定

1. システムビューに入ります。

   system-view

2. 802.1X認証要求を送信する最大試行回数を設定します。

   dot1x retry *retries*

   デフォルト設定は2です。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の802.1Xを参照してください。

802.1X認証タイマーの設定

このタスクについて

802.1Xは次のタイマーを使用して、クライアントおよびRADIUSサーバーとの相互作用を制御します。

- **クライアントタイムアウトタイマー**: デバイスがEAP-Request/MD5-Challengeパケットをクライアントに送信したときに開始されます。このタイマーが期限切れになってもデバイスが応答を受信しない場合、デバイスは要求をクライアントに再送信します。デバイスが応答を受信せずに最大送信試行を行った場合、クライアントは認証に失敗します。最大試行回数を設定するには、dot1x retryコマンドを使用します。
- **サーバータイムアウトタイマー**: デバイスがRADIUS Access-Requestパケットを認証サーバーに送信したときに開始されます。このタイマーが期限切れになってもデバイスが応答を受信しない場合、デバイスは要求をサーバーに再送信します。
- **ハンドシェイクタイマー**: オンラインユーザーハンドシェイクがイネーブルになっているときに、クライアントが認証に合格した後に開始されます。デバイスは、ハンドシェイク間隔ごとにクライアントにハンドシェイクメッセージを送信します。最大ハンドシェイク試行後にクライアントから応答を受信しなかった場合、デバイスはクライアントからログオフします。最大試行回数を設定するには、dot1x retryコマンドを使用します。
- **定期的な再認証タイマー**: 定期的なオンラインユーザー再認証がイネーブルになっているときに、クライアントが認証に合格した後に開始されます。デバイスは、設定された間隔でクライアントを再認証します。タイマーの変更は、変更後にオンラインになったクライアントに対してのみ有効です。

制限事項とガイドライン

ほとんどの場合、デフォルト設定で十分です。ネットワークの状態に応じて、タイマーを編集できます。次に2つの例を示します。

- 低速ネットワークでは、クライアントタイムアウトタイマーを増やします。
- パフォーマンスの異なる認証サーバーを使用するネットワークでは、サーバータイムアウトタイマーを調整します。

手順

1. システムビューに入ります。

   system-view

2. クライアントのタイムアウトタイマーを設定します。

   dot1x timer supp-timeout *supp-timeout-value*

   デフォルト設定は30秒です。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の802.1Xを参照してください。

3. サーバーのタイムアウトタイマーを設定します。

   dot1x timer server-timeout *server-timeout-value*

   デフォルト設定は100秒です。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の

802.1Xを参照してください。

4. ハンドシェイクタイマーを設定します。

   dot1x timer handshake-period *handshake-period-value*

   デフォルト設定は15秒です。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の802.1Xを参照してください。

5. 定期的な再認証タイマーを設定します。

   dot1x timer reauth-period *reauth-period-value*

   デフォルト設定は3600秒です。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の802.1Xを参照してください。

MAC認証ユーザーアカウントフォーマットの設定

1. システムビューに入ります。

   system-view

2. MAC認証ユーザーアカウントフォーマットを設定します。必

   要に応じて、次のいずれかのオプションを選択します。

   - クライアントごとに1つのMACベースのユーザーアカウントを使用します。

     mac-authentication user-name-format mac-address [{ with-hyphen [six-section | three-section] | without-hyphen } [lowercase | uppercase]]

   - すべてのクライアントに対して1つの共有ユーザーアカウントを使用します。

     mac-authentication user-name-format fixed [account *name* **]**
     [password { cipher | simple } *password* **]**

   デフォルトでは、デバイスはユーザーのMACアドレスをMAC認証のユーザー名およびパスワードとして使用します。MACアドレスはハイフンを含まない16進表記で、文字は小文字です。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の「MAC authentication」を参照してください。

グローバルMAC認証ドメインの指定

このタスクについて

MAC認証では、WLANクライアントのISPドメインが次の順序で選択されます。

1. サービステンプレートで指定されたドメイン。
2. システムビューで指定されたグローバルMAC認証ドメイン。
3. デフォルトのドメイン。

手順

1. システムビューに入ります。

   system-view

2. MAC認証クライアントのISPドメインを指定します。

   mac-authentication domain *domain-name*

   デフォルトでは、システムビューのMAC認証クライアントにISPドメインは指定されていません。

MAC認証タイマーの設定

このタスクについて

MAC認証では、次のタイマーが使用されます。

- **オフライン検出タイマー**: ユーザーがアイドル状態であると判断する前に、デバイスがユーザーからのトラフィックを待機する間隔を設定します。タイマーが期限切れになる前にデバイスがユーザーからトラフィックを受信しなかった場合、デバイスはそのユーザーをログオフし、アカウンティングサーバーにユーザーのアカウンティングを停止するよう要求します。
- **Quiet et timer**: MAC認証に失敗したユーザーに対してデバイスがMAC認証を実行できるようになるまで、デバイスが待機する必要がある間隔を設定します。MACアドレスからのすべてのパケットは、待機時間中にドロップされます。この待機メカニズムにより、認証の繰り返しがシステムのパフォーマンスに影響を与えることがなくなります。
- **サーバータイムアウトタイマー**: RADIUSサーバーが使用できないとデバイスが判断する前に、デバイスがRADIUSサーバーからの応答を待機する間隔を設定します。MAC認証中にタイマーが期限切れになると、ユーザーはネットワークにアクセスできなくなります。

手順

1. システムビューに入ります。

   system-view

2. MAC認証タイマーを設定します。

   mac-authentication timer { offline-detect *offline-detect-value* **| quiet** *quiet-value* **| server-timeout** *server-timeout-value* **}**

   デフォルトでは、オフライン検出タイマーは300秒、待機タイマーは60秒、サーバータイムアウトタイマーは100秒です。

   このコマンドの詳細については、『User Access and Authentication Command Reference』の「MAC authentication」を参照してください。

clear-previous-connection機能のイネーブル化

このタスクについて

一部のRADIUSサーバーは、クライアントのオンラインユーザーエントリがある場合、そのクライアントの認証を拒否します。不正にオフラインになったクライアントのオンラインユーザーエントリを削除できない場合、そのクライアントは認証されず、再びオンラインになります。

この問題を解決するには、clear-previous-connection機能を使用します。

この機能を使用すると、デバイスは、802.1XまたはMAC認証クライアントの認証要求をRADIUSサーバーに送信する前に、ローカルオンラインユーザーエントリをチェックします。エントリが見つかった場合、デバイスはエントリを削除し、RADIUSサーバーにstop-accounting要求を送信します。stop-accounting要求を受信すると、RADIUSサーバーはオンラインユーザーエントリを削除します。これにより、クライアントを正しく認証できます。

制限事項とガイドライン

この機能をイネーブルにすると、802.1X再認証、WLAN Auth-fail VLAN(認証失敗VLAN)、およびWLANクリティカルVLAN機能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. clear-previous-connection機能をイネーブルにします。
   wlan client-security authentication clear-previous-connection
   デフォルトでは、この機能はディセーブルになっています。

サービス固有のWLAN認証パラメータの設定

タスクの一覧

サービス固有のWLAN認証パラメータを設定するには、次の作業を実行します。

1. 認証モードの設定
2. (任意)WLANクライアントのオーセンティケータの指定
3. (任意)802.1X認証パラメータを設定します。
   - 802.1X認証のEAPモードの指定
   - 802.1X EAP終端のEAPプロファイルの指定
   - オンラインユーザーハンドシェイク機能の設定
   - オンラインユーザーハンドシェイクセキュリティ機能の設定
   - 802.1X認証ドメインの指定
   - 同時802.1Xクライアントの最大数の設定
   - 定期的なオンラインユーザー再認証機能のイネーブル化
4. (任意)MAC認証パラメータを設定します。
   - 同時MAC認証クライアントの最大数の設定
   - サービス固有のMAC認証ドメインの指定
5. (任意)WLAN認証の高度な機能の設定
   - 802.1XまたはMAC認証の失敗を無視する
   - WLAN MAC認証クライアントのURLリダイレクションのイネーブル化
   - WLAN Auth-fail VLAN(認証失敗VLAN)の設定
   - WLANクリティカルVLANの設定
   - サーバーからの許可情報を無視する
   - 許可失敗オフライン機能のイネーブル化
   - 侵入防御の設定
   - accounting-startトリガー機能の設定
   - accounting-update trigger機能の設定
   - accounting-restartトリガー機能の設定
   - IPプロトコルバージョンによる802.1Xデュアルスタッククライアントのトラフィックアカウンティングのイネーブル化
   - RADIUSパケットへのクライアントIPスヌーピング方式の組み込み
   - MAC認証済みACローミングクライアントの高速接続のイネーブル化
   - WLAN認証統計情報を最適化するための修飾子の設定

認証モードの設定

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を入力します。

   wlan service-template *service-template-name*
3. WLANクライアントの認証モードを設定します。

   client-security authentication-mode { dot1x | dot1x-then-mac | mac | mac-and-dot1x | mac-then-dot1x | oui-then-dot1x }

   デフォルトでは、バイパスモードが適用されます。デバイスは認証を実行しません。クライアントはデバイスに直接アクセスできます。

WLANクライアントのオーセンティケータの指定

このタスクについて

オーセンティケータとして動作するACまたはAPを指定して、WLANクライアントに対してローカルまたはRADIUSベースの認証を実行できます。

制限事項とガイドライン

ACがクライアントデータトラフィックを転送するように設定されている場合、認証に成功するためにオーセンティケータをAPにすることはできません。クライアントデータトラフィックを転送するためのデバイスの指定については、『WLAN Access 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. 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. WLANクライアントのオーセンティケータを指定します。

   client-security authentication-location { ac | ap }

   デフォルトでは、ACはWLANクライアントを認証するオーセンティケータとして認証します。

802.1X認証のEAPモードの指定

このタスクについて

EAPモードは、デバイスがクライアントと対話するために使用するEAPプロトコルの規定とパケット形式を決定します。

802.1Xは、次のEAPモードをサポートします。

- **extended**: H3C独自のEAPプロトコルで定義された規定およびパケット形式に従って、デバイスがクライアントと対話することを要求します。
- **standard**: 標準EAPプロトコルで定義された規定およびパケット形式に従って、デバイスがクライアントと対話することを要求します。

制限事項とガイドライン

このタスクは、IMCサーバーがRADIUSサーバーとして使用されている場合にだけ実行します。拡張モードを指定し、他のクライアントには標準モードを指定します。

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を入力します。

   wlan service-template *service-template-name*

3. 802.1X認証のEAPモードを指定します。

   dot1x eap { extended | standard }

   デフォルトでは、EAPモードは802.1X認証の標準です

802.1X EAP終端のEAPプロファイルの指定

このタスクについて

RADIUSサーバーがクライアントが使用する認証方式をサポートしていない場合、クライアントはEAPリレーモードでの認証に失敗します。認証の失敗を回避するには、この機能を使用して、デバイスがクライアントから受信したEAPパケットを終端し、クライアント認証情報を標準RADIUSパケットにカプセル化できるようにします。

制限事項とガイドライン

ベストプラクティスとして、サービステンプレートのすべてのクライアントがPEAP-GTC認証方式を使用している場合にだけ、この機能をサービステンプレートで使用してください。サービステンプレートで他の認証方式を使用しているクライアントは、認証に失敗します。

前提条件

EAPプロファイルを作成し、EAP認証方式をEAPプロファイルでPEAP-GTCに設定します。EAPプロファイル設定の詳細については、『Security Configuration Guide』の「AAA configuration」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. 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. 802.1X EAP終了用に作成されたEAPプロファイルを指定します。

   dot1x eap-termination eap-profile *eap-profile-name*

   デフォルトでは、802.1X EAP終端にEAPプロファイルは指定されていません。

オンラインユーザーハンドシェイク機能の設定

このタスクについて

オンラインユーザーハンドシェイク機能は、オンライン802.1Xクライアントの接続ステータスを調べます。デバイスは、dot1x timer handshake-periodコマンドで指定された間隔で、オンラインクライアントにハンドシェイクメッセージを送信します。デバイスが最大ハンドシェイク試行を行った後にオンラインクライアントから応答を受信しない場合、デバイスはクライアントをオフライン状態に設定します。

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. オンラインユーザーハンドシェイク機能をイネーブルにします。

dot1x handshake enable

デフォルトでは、この機能はディセーブルになっています。

オンラインユーザーハンドシェイクセキュリティ機能の設定

このタスクについて

オンラインユーザーハンドシェイクセキュリティ機能は、ハンドシェイクメッセージに認証情報を追加します。この機能を使用すると、不正なクライアントが合法的な802.1Xクライアントを偽造して交換できないようにすることができます。

ハンドシェイクメッセージをデバイスに送信します。この機能では、デバイスは、クライアントからのハンドシェイク応答メッセージ内の認証情報と、認証サーバーによって割り当てられた認証情報を比較します。一致する情報が見つからない場合、デバイスはクライアントからログオフします。

制限事項とガイドライン

オンラインユーザーハンドシェイクセキュリティ機能を使用するには、オンラインユーザーハンドシェイク機能がイネーブルになっていることを確認します。

オンラインユーザーハンドシェイクセキュリティ機能は、オンラインで認証された802.1Xクライアントだけを保護します。

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. オンラインユーザーハンドシェイク機能をイネーブルにします。

   dot1x handshake enable

   デフォルトでは、この機能はディセーブルになっています。
4. オンラインユーザーハンドシェイクセキュリティ機能をイネーブルにします。

   dot1x handshake secure enable

   デフォルトでは、この機能はディセーブルになっています。

802.1X認証ドメインの指定

このタスクについて

802.1X認証では、WLANクライアントのISPドメインが次の順序で選択されます。

- サービステンプレートで指定されたドメイン。
- usernameで指定されたドメイン。
- デフォルトのドメイン。

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802.1X認証ドメインを指定します。

dot1x domain *domain-name*

デフォルトでは、サービステンプレートに802.1X認証ドメインは指定されていません。

同時802.1Xクライアントの最大数の設定

このタスクについて

サービステンプレートの同時802.1Xクライアントの最大数に達すると、新しい802.1Xクライアントは拒否されます。

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に入ります。

   wlan service-template *service-template-name*
3. サービステンプレートの同時802.1Xクライアントの最大数を設定します。

   dot1x max-user *count*

   デフォルト設定は4096です。

定期的なオンラインユーザー再認証機能のイネーブル化

このタスクについて

定期的なオンラインユーザー再認証は、オンラインクライアントの接続ステータスを追跡し、サーバーによって割り当てられた認可アトリビュートを更新します。アトリビュートには、ACL、VLAN、およびユーザープロファイルベースのQoSが含まれます。再認証間隔はユーザーが設定できます。

ユーザーに割り当てられたセッションタイムアウトタイマー(Session-Timeoutアトリビュート)および終了アクション(Termination-Actionアトリビュート)は、定期的なオンラインユーザー再認証機能に影響を与える可能性がありますユーザーに割り当てられたセッションタイムアウトアトリビュートおよび終了アクションアトリビュートを表示するには、display dot1x connectionコマンドを使用します(『Security Command Reference』を参照)。

- 終了アクションが**Default(ログオフ)**の場合、デバイスでの定期的なオンラインユーザー再認証は、定期的な再認証タイマーがセッションタイムアウトタイマーより短い場合にだけ有効になります。
- 終了アクションが**Radius-request**の場合、デバイス上の定期的なオンラインユーザー再認証設定は有効になりません。デバイスは、セッションタイムアウトタイマーの期限が切れた後にオンライン802.1Xクライアントを再認証します。

Session-TimeoutおよびTermination-Actionアトリビュートの割り当てのサポートは、サーバーモデルによって異なります。

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. 定期的なオンラインユーザー再認証をイネーブルにします。

   dot1x re-authenticate enable

   デフォルトでは、この機能はディセーブルになっています。

同時MAC認証クライアントの最大数の設定

このタスクについて

サービステンプレートで同時MAC認証クライアントの最大数に達すると、新しいMAC認証クライアントは拒否されます。

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同時MAC認証クライアントの最大数を設定します。

   mac-authentication max-user *count*

   デフォルト設定は4096です。

サービス固有のMAC認証ドメインの指定

このタスクについて

MAC認証では、WLANクライアントのISPドメインが次の順序で選択されます。

- サービステンプレートで指定されたドメイン。
- システムビューで指定されたグローバルMAC認証ドメイン。
- デフォルトのドメイン。

手順

1. システムビューに入りに入ります。

   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. MAC認証クライアントのISPドメインを指定します。

   mac-authentication domain *domain-name*

   デフォルトでは、MAC認証クライアントにISPドメインは指定されていません。

802.1XまたはMAC認証の失敗を無視する

このタスクについて

この機能は、次のクライアントに適用されます。

- 802.1X認証を使用するクライアント。

  この機能により、デバイスは802.1X認証の失敗を無視し、802.1X認証に失敗したクライアントがオンラインになることを許可できます。
- RADIUSベースのMAC認証とポータル認証の両方を使用するクライアント。

  通常、WLANクライアントは、ネットワークリソースにアクセスするために、MAC認証とポータル認証を順に通過する必要があります。クライアントは、ポータル認証が実行されるたびにユーザー名とパスワードを提供します。

この機能により、クライアントの認証プロセスが次のように簡素化されます。

- RADIUSサーバーがクライアントのMAC認証情報をすでに記録している場合、クライアントはMAC認証に合格します。このデバイスを使用すると、クライアントはポータル認証を実行せずにネットワークリソースにアクセスできます。
- RADIUSサーバーがクライアントのMAC認証情報を記録しない場合、クライアントはMAC認証に失敗します。デバイスはMAC認証失敗を無視し、クライアントに対してポータル認証を実行します。クライアントがポータル認証に合格すると、ネットワークリソースにアクセスできます。ポータル認証されたクライアントのMACアドレスは、RADIUSサーバー上にMAC認証情報として記録されます。

制限事項とガイドライン

RSNを使用して新しいAPにローミングする802.1Xクライアントの場合は、この機能を設定しないでください。

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. 802.1XまたはMAC認証の失敗を無視するようにデバイスを設定します。

   client-security ignore-authentication

   デフォルトでは、デバイスは802.1X認証またはRADIUSベースのMAC認証を実行する無線クライアントの認証失敗を無視しません。

WLAN MAC認証クライアントのURLリダイレクションのイネーブル化

このタスクについて

RADIUSベースのMAC認証では、クライアントが認証を通過できるのは、RADIUSサーバーにクレデンシャル情報(ユーザー名とパスワード)とMACアドレスがある場合だけです。

URLリダイレクションは、MAC認証に失敗した後、クライアントがRADIUSサーバーに認証できるようにします。これは、サーバーにクレデンシャル情報とMACアドレスがないためです。この機能は、RADIUSサーバーがクライアントに関する認証情報を取得できるように、ポータル認証用に指定された認証WebページURLにクライアントをリダイレクトします。次に一般的なプロセスを示します。

1. クライアントがネットワークに接続すると、MAC認証は失敗します。
2. RADIUSサーバーは、許可ACLおよびリダイレクトURLを割り当てます。ACLはクライアントの外部ネットワークへのアクセスを拒否します。
3. デバイスは、クライアントのHTTPまたはHTTPSによるインターネットへのアクセス要求を受信すると、クライアントをリダイレクトURLの認証ページにリダイレクトします。
4. 認証ページで、クライアントはサービスプロバイダから提供されたユーザー名とパスワードを入力して、Webポータル認証を完了します。Web認証サーバーはクライアントの資格証明情報とMACアドレスを記録します。
5. クライアントがWebポータル認証に合格すると、Web認証サーバーはクライアント情報をRADIUSサーバーに送信し、DM要求を送信してクライアントからログオフします。

   DMの詳細については、『AAAの設定』を参照してください。
6. 次のネットワークアクセス試行では、クライアントはMAC認証を通過できます。

通常、リダイレクトの決定はRADIUSサーバーで行われます。RADIUSサーバーにクライアントに関するMAC認証情報が含まれている場合、クライアントはリダイレクトURLにリダイレクトされることなく認証を通過できます。すべてのクライアントがアドバタイズなどの目的でリダイレクトURLにアクセスするようにするには、URLリダイレクションモードをネイティブモードに設定します。このモードでは、デバイスはクライアントのリダイレクトURLアクセスレコードを維持し、次のようにレコードに基づいてURLリダイレクションの決定を行います。

- クライアントのURLアクセスレコードが見つからない場合に、クライアントをリダイレクトします。
- クライアントのURLアクセスレコードが存在する場合、HTTPクライアントのリダイレクトを停止します。
- リダイレクト停止タイマーが期限切れになる前に、リダイレクトURLのIPアドレスへの訪問回数が指定された制限に達した場合、HTTPSクライアントのリダイレクトを停止します。

制限事項とガイドライン

この機能は、RADIUSベースのMAC認証だけが使用されるシナリオに適用できます。

この機能を使用するには、次の制約事項およびガイドラインに従って、クライアントの認可ACLおよびリダイレクトURLを設定する必要があります。

- ACLは、クライアントとWeb認証サーバーがパケットを交換できるようにする必要があります。許可ACLの詳細は、「MAC認証の構成」を参照してください。
- クライアントがDHCPを使用してダイナミックIPアドレスを取得する場合、ACLはクライアントとDHCPサーバーがパケットを交換することを許可する必要があります。
- パケットをフィルタリングするために、必要に応じて他のACLルールを設定できます。
- リダイレクトURLは、クライアントがWeb認証に使用するWebアドレスです。
- 許可ACLが複数の機能で使用されている場合は、ルールの競合が発生する可能性があります。望ましくないリダイレクションの結果を回避するには、URLリダイレクションをトリガーするトラフィックと一致する専用ACLを指定します。

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. WLAN認証クライアントのURLリダイレクションをイネーブルにします。

   client url-redirect enable [mode native [https [redirect-stop-timer *seconds*] [**count** *number*]]]

   デフォルトでは、WLAN MAC認証クライアントのURLリダイレクションはディセーブルになっています。
4. (任意)URLリダイレクションをトリガーするトラフィックを照合するACLを指定します。

   client url-redirect acl *acl-number*

   デフォルトでは、URLリダイレクションをトリガーするトラフィックに一致するACLは指定されていません。

WLAN Auth-fail VLAN(認証失敗VLAN)の設定

このタスクについて

オーセンティケータは、Auth-fail VLAN内のクライアントを30秒間隔で再認証します。

- クライアントが再認証に合格すると、オーセンティケータはクライアントを認可VLANに割り当てます。認可VLANが設定されていない場合、クライアントは最初のVLANに割り当てられます。
- クライアントが再認証に失敗した場合、クライアントは引き続きAuth-fail VLAN内に存在します。

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. WLAN Auth-fail VLANを設定します。
   client-security authentication fail-vlan *vlan-id*
   デフォルトでは、WLAN Auth-fail VLANは存在しません。
   サービステンプレートに設定できるAuth-fail VLANは1つだけです。

WLANクリティカルVLAN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. WLANクリティカルVLANを設定します。
   client-security authentication critical-vlan *vlan-id*
   デフォルトでは、WLANクリティカルVLANは存在しません。
   サービステンプレートに設定できるクリティカルVLANは1つだけです。

サーバーからの許可情報を無視する

このタスクについて

クライアントが802.1XまたはMAC認証に合格した後に、サーバー(ローカルまたはリモート)から受信した認可情報を無視するようにデバイスを設定できます。認可情報には、VLAN、ACL、およびユーザープロファイル情報が含まれます。

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. 認証サーバーから受信した許可情報を無視します。
   client-security ignore-authorization
   デフォルトでは、認証サーバーから受信した認可情報が使用されます。

authorization-fail-offline機能のイネーブル化

このタスクについて

authorization-fail-offline 機能は、ACLまたはユーザープロファイルの認可に失敗したWLANクライアントをログオフします。

クライアントは、次の状況でACLまたはユーザープロファイルの認可に失敗します。

- デバイスまたはサーバーが、指定されたACLまたはユーザープロファイルをクライアントに認可できない。
- 許可されたACLまたはユーザープロファイルが存在しません。

制限事項とガイドライン

この機能は、VLAN認証に失敗したクライアントには適用されません。デバイスは常にこれらの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. 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. 許可失敗オフライン機能をイネーブルにします。

   client-security authorization-fail offline

   デフォルトでは、この機能はディセーブルになっています。デバイスは、失敗したACLまたはユーザープロファイル認可を持つクライアントからログオフせず、システムログを出力します。

侵入防御の設定

このタスクについて

この機能を使用すると、認証に失敗したクライアントからアソシエーション要求を受信するBSSで、デバイスは事前定義されたアクションを実行できます。詳細については、「侵入保護」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. 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. 侵入防御機能をイネーブルにします。

   クライアントセキュリティ侵入保護イネーブル

   デフォルトでは、侵入保護は無効になっています。
4. (任意)侵入防御アクションを設定します。

   client-security intrusion-protection action { service-stop | temporary-block | temporary-service-stop }

   デフォルトでは、**temporary-block**が使用されます。
5. (任意)不正なクライアントのブロック期間を設定します。

   client-security intrusion-protection timer temporary-block *time*

   デフォルト設定は180秒です。
6. (任意)BSSがディセーブルのままである無音期間を設定します。

   Client-security intrudion-proection timer temporary-service-stop *time*

   デフォルト設定は20秒です。

accounting-startトリガー機能の設定

このタスクについて

accounting-startトリガーは、クライアントが802.1XまたはMAC認証に合格した後に、デバイスがstart-accounting要求を送信するための条件を指定します。

accounting-startトリガーは、IPベースまたは非IPベースにできます。

- IPベースのアカウンティング開始トリガーを指定すると、802.1XまたはMAC認証済みクライアントが指定されたタイプのIPアドレスを使用している場合、デバイスは開始アカウンティング要求を送信します。
- 非IPベースのアカウンティング開始トリガーを指定した場合、クライアントがそのIPアドレスタイプを検査せずに認証に合格すると、デバイスは開始アカウンティング要求を送信します。

IPベースのアカウンティング開始トリガーとともに、アカウンティング遅延タイマーを設定できます。アカウンティング遅延タイマーは、指定されたアクションを実行する前に、デバイスが802.1XまたはMAC認証済みクライアントのIPアドレスを学習する最大間隔を指定します。

遅延タイマーは、クライアントが802.1XまたはMAC認証に合格したときに開始されます。アカウンティング遅延タイマーが期限切れになる前に、デバイスがIPベースのアカウンティング開始トリガーに一致するIPアドレスを学習できなかった場合、デバイスは次のいずれかのアクションを実行します。

- no-ip-logoffアクションが指定されていない場合は、ただちに開始アカウンティング要求を送信します。
- no-ip-logoffアクションが指定されている場合は、クライアントをログオフします。

遅延タイマーが設定されていない場合、デバイスはクライアントのIPアドレスを学習したときにだけ、そのクライアントに対する開始アカウンティング要求を送信します。アカウンティングの詳細については、「AAAの設定」を参照してください。

制限事項とガイドライン

トリガーがIPアドレスタイプベースの場合は、そのタイプの学習IPアドレスをイネーブルにする必要があります。無線クライアントIPアドレス学習の詳細については、『Configuring WLAN IP snooping』を参照してください。

トリガーは、トリガーの設定後にオンラインになったクライアントに対してだけ有効になります。

デバイスがクライアントのIPアドレスを学習する標準的な時間に応じて、アカウンティング遅延タイマーを設定します。パフォーマンスの低いネットワークでは、遅延タイマーを増やす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. クライアントのアカウンティング開始トリガーを設定します。

   client-security accounting-start trigger { ipv4 | ipv4-ipv6 | ipv6 | none }

   デフォルトでは、accounting-startトリガーはIPv4アドレスタイプに基づいています。
4. (任意)アカウンティング遅延タイマーを設定します。

   client-security accounting-delay time *time* **[no-ip-logoff]**

   デフォルトでは、デバイスはクライアントのIPアドレスを学習した場合にだけ、クライアントの開始アカウンティング要求を送信します。

accounting-update trigger機能の設定

このタスクについて

この機能を使用して、イベントベースのアカウンティング更新トリガーを指定します。この機能を使用すると、オンライン802.1XまたはMAC認証クライアントのIPアドレスが変更されたときに、デバイスは更新アカウンティング要求を送信できます。

制限事項とガイドライン

accounting-update triggerをaccounting-start triggerとともに使用します。accounting-update triggerは、**client-security accounting-start trigger**コマンドを使用してaccounting-start triggerを設定した場合にだけ有効になります。

イベントベースのアカウンティング更新トリガーに加えて、**timer realtime-accounting**コマンドを使用して、通常のアカウンティング更新間隔を設定できます。

accounting-updateトリガーは、トリガーが設定された後にオンラインになったクライアントに対してだけ有効です。

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を入力します。

   wlan service-template *service-template-name*
3. イベントベースのアカウンティング更新トリガーを指定します。

   client-security accounting-update trigger { ipv4 | ipv4-ipv6 | ipv6 }

   デフォルトでは、イベントベースのアカウンティング更新トリガーは設定されていません。デバイスは、アカウンティングサーバーに対して、サーバーが割り当てたか、またはサーバー定義のリアルタイムアカウンティングインターバル。RADIUSリアルタイムアカウンティングインターバルの詳細については、「AAAの設定」を参照してください。

accounting-restartトリガー機能の設定

このタスクについて

IPv4アドレスベースのアカウンティング再起動トリガーは、802.1XおよびMAC認証クライアントに適用されます。

このトリガーは、クライアントのIPv4アドレスが変更されたときに、アカウンティング停止要求とアカウンティング開始要求をアカウンティングサーバーに送信することによって、クライアントのアカウンティングを再開します。

stop-accounting要求とstart-accounting要求の間の遅延は設定可能です。

制限事項とガイドライン

IPv4アドレスベースのアカウンティング再開トリガーは、client-security accounting-update triggerコマンドを使用してIPv4用に設定されたアカウンティング更新トリガーよりも高いプライオリティを持ちます。

前提条件

サービステンプレートでこの機能を設定する前に、そのサービステンプレートを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. 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. IPv4アドレスベースアカウンティング再起動トリガーをイネーブルにします。

   client-security accounting-restart trigger ipv4 [delay *interval* **]**

   デフォルトでは、IPv4アドレスベースのアカウンティング再起動トリガーはディセーブルです。

IPプロトコルバージョンによる802.1Xデュアルスタッククライアントのトラフィックアカウンティングのイネーブル化

このタスクについて

802.1XデュアルスタッククライアントのIPv4およびIPv6トラフィックを個別に測定するには、この機能を使用します。この機能を使用すると、AAAアカウンティングサーバーに送信される約802.1Xデュアルスタッククライアントのトラフィックデータは、IPプロトコルバージョンによって分離されます。

この機能は、次のデュアルスタッククライアントに適用されます。

- 802.1X認証だけを使用するクライアント。
- dot1x-then-mac、mac-then-dot1x、またはoui-then-dot1x認証モードを使用するクライアント。この機能は、これらのクライアントがMAC認証だけを通過する場合でも、これらのクライアントに対して有効です。

制限事項とガイドライン

この機能は、ワイヤレスターミネータソリューションには適用されません。

前提条件

サービステンプレートでこの機能を設定する前に、そのサービステンプレートを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. 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. IPプロトコルバージョンごとに802.1Xデュアルスタッククライアントのトラフィックアカウンティングをイネーブルにします。

   client-security accounting dual-stack separate enable

   デフォルトでは、デバイスは802.1Xデュアルスタッククライアントのアカウンティング用にIPv4データとIPv6データをマージします。

RADIUSパケットへのクライアントIPスヌーピング方式の組み込み

このタスクについて

デバイスは、DHCPパケットやARPパケットなどのパケットをスヌーピングすることによって、クライアントのIPアドレスを取得できます。RADIUSサーバーが802.1X認証クライアントまたはMAC認証クライアントのIPアドレスがDHCPサーバーによって割り当てられているかどうかを判断できるようにするには、RADIUSパケット内のIPスヌーピング方式をサーバーに送信します。

IPスヌーピング方式は、H3c-Ip-Source-Modアトリビュート(ID 221の拡張RADIUSアトリビュート)でカプセル化されます。

IPスヌーピング方式を識別するには、RADIUSサーバーがベンダーID 25506の拡張RADIUSアトリビュートをサポートしている必要があります。詳細については、『Security Configuration Guide』の「AAA configuration」を参照してください。

前提条件

サービステンプレートでこの機能を設定する前に、そのサービステンプレートを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. 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. RADIUSパケットにクライアントIPスヌーピング方式を含めます。

   client-security aaa attribute ip-snooping-method

   デフォルトでは、RADIUSパケットにはクライアントIPスヌーピング方式は含まれません。

MAC認証済みACローミングクライアントの高速接続のイネーブル化

このタスクについて

この機能を使用すると、ACで一度認証されたMAC認証ローミングクライアントが、再認証なしにACに接続されている任意のAPからオンラインになることができます。

制限事項とガイドライン

この機能は、認証ロケーションとアソシエーションロケーションの両方がAC上にあるMAC認証無線クライアントだけに適用されます。

この機能は、MAC認証を使用し、特別な設定を必要とするAC間ローミングクライアントの表示ローミング状態に影響します。

- クライアントがAC間でローミングした場合、そのローミング状態は、**display wlan client verbose** コマンドの出力では**N/A**になります。
- AC間ローミングクライアントが異なるVLANに属している場合は、同じローミンググループ内のすべてのACのアップストリームポートで、これらのVLANからのトラフィックの通過が許可されていることを確認する必要があります。

前提条件

サービステンプレートでこの機能を設定する前に、そのサービステンプレートを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. 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. MAC認証済みAC内ローミングクライアントの高速接続をイネーブルにします。

   mac-authentication fast-connect enable

   デフォルトでは、MAC認証されたAC内ローミングクライアントの高速接続はディセーブルになっています。

WLAN認証統計情報を最適化するための修飾子の設定

WLAN認証統計情報の最適化について

認証成功率は、認証成功回数の合計認証回数に対する比率です。異常オフライン率は、次の式を使用して計算されます。異常オフライン率=クライアントが異常にオフラインになった回数÷(認証成功回数+現在のオンラインユーザー数)。

WLAN認証統計情報の最適化では、修飾子を使用して、802.1X認証、MAC認証、およびレイヤ2ポータル認証の認証成功率および異常オフライン率を調整します。

制限事項とガイドライン

この修飾子は、RADIUSベースの802.1X認証、MAC認証、およびレイヤ2ポータル認証に対してだけ有効です。

手順

1. システムビューに入ります。

   system-view

2. 修飾子を設定して、802.1X認証、MAC認証、およびレイヤ2ポータル認証の認証成功率と異常オフライン率を調整します。

   wlan authentication optimization *value*

   デフォルトでは、モディファイアは0です。デバイスは、802.1X認証、MAC認証、およびレイヤ2ポータル認証の認証成功率および異常オフライン率を調整しません。

BYOD許可トリガーの使用可能化

このタスクについて

この機能により、アクセスデバイスは、IPアドレスを含むクライアントのBYOD情報を取得した後に、認証されたクライアントに対するBYOD認可をトリガーできます。BYOD認可がトリガーされると、クライアントに割り当てられたセッションタイムアウトタイマーが再起動され、再認証が必要になる前にクライアントがオンライン状態を維持できる時間が延長されます。低パフォーマンスのネットワークでは、デバイスがクライアントのIPアドレスを取得するのに時間がかかるため、クライアントのオンライン時間の延長が望ましくないものになります。

この望ましくない問題を回避するためのベストプラクティスとして、この機能はBYOD許可が必要な場合にだけ使用し、ネットワークパフォーマンスが良好であることを確認します。BYOD許可の詳細については、「AAAの設定」を参照してください。

前提条件

サービステンプレートでこの機能を設定する前に、そのサービステンプレートを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. 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. BYOD許可トリガーをイネーブルにします。

   client-security authorization trigger byod

   デフォルトでは、BYOD許可トリガーはディセーブルになっています。

認証fail-permit の設定

認証fail-permit について

認証fail-permit (失敗オープンとも呼ばれます)を使用すると、802.1X、MAC認証、およびバイパスクライアントは、ACがRADIUSサーバーまたはAPから切断された後にネットワークにアクセスできます。いずれかのイベントが発生した場合、APは引き続きこれらのクライアントにアクセスサービスを提供し、トラフィックを転送します。

認証fail-permit イベントがクライアントに与える影響は、クライアントの認証方式によって異なります。

- **バイパスクライアント**は、既存のサービステンプレートを使用して、中断することなくネットワークに引き続きアクセスできます。
- **MAC認証クライアント**は、一時的な中断後も既存のサービステンプレートを使用して引き続きネットワークにアクセスできます。この場合、クライアントはログオフされ、自動的にネットワークに接続されます。
- **802.1Xクライアント**はログオフされます。ネットワークへのアクセスを続行するには、802.1Xクライアントが事前設定されたfail-permit サービステンプレートのSSIDに手動で再接続する必要があります。

認証fail-permit タスクの概要

認証fail-permit を設定するには、次の作業を実行します。

1. 認証クライアントのfail-permit のイネーブル化
2. 認証fail-permit サービステンプレートの指定の作業は、802.1Xクライアントに対して実行します。

認証クライアントの fail-permitのイネーブル化

このタスクについて

認証クライアントのサービステンプレートでfail-permit をイネーブルにするには、次の作業を実行します。

制限事項とガイドライン

この機能は、サービステンプレートがディセーブルの場合に設定可能であり、サービステンプレートがイネーブルになった後に有効になります。

前提条件

認証fail-permit を有効にするには、次の手順を実行します。

1. **radius-server test-profile**コマンドを実行して、RADIUSテストプロファイルを設定し、RADIUSサーバーの到達可能性をテストします。

   プロファイルでは、必要に応じて検出パケットを送信する間隔を設定します。間隔が短いほど、変更に対する応答が速くなります。

2. 認証ISPドメインのRADIUSスキームでプロファイルを使用します。

   fail-permit は、RADIUSサーバーが到達不能であると判断された場合に発生します。

RADIUSテストプロファイルの設定の詳細については、『AAAの設定』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. 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. fail-permitをイネーブルにします。

   fail-permit enable

   デフォルトでは、fail-permit はディセーブルになっています。

例

#ACに障害が発生したり、ACがRADIUSにアクセスできなかった場合、APにMAC認証で接続するクライアントが既存のサービステンプレートを使用して引き続き認証なしでネットワークにアクセスすることができます。

```
<Sysname> system-view
[Sysname] wlan service-template service 1
[Sysname-wlan-st-service1] ssid macauth
[Sysname-wlan-st-service1] client forwarding-location ap
[Sysname-wlan-st-service1] fail-permit enable
[Sysname-wlan-st-service1] client-security authentication-mode mac
[Sysname-wlan-st-service1] mac-authentication domain rem-domain
[Sysname-wlan-st-service1] service-template enable
[Sysname-wlan-st-service1] quit
[Sysname]quit
```

認証fail-permit サービステンプレートの指定

このタスクについて

802.1Xクライアントを含む1つのサービステンプレートでfail-permit をイネーブルにする場合は、802.1Xクライアント用のfail-permit サービステンプレートとして別のサービステンプレートを指定する必要があります。このテンプレートにより、ACがRADIUSサーバーまたはAPから切断された後に、802.1Xクライアントがネットワークに再接続できるようになります。

認証fail-permit 機能の詳細については、「認証fail-permit について」を参照してください。

制限事項とガイドライン

fail-permit template コマンドは、**fail-permit enable** コマンドと相互に排他的です。
コマンドは同じサービステンプレートを使用します。

fail-permit template コマンドは、サービステンプレートがディセーブルの場合に設定可能であり、サービステンプレートがイネーブルになった後に有効になります。

802.1Xクライアントのfail-permit を成功させるには、次の手順を実行します。

- AKMモードをPSKに設定するか、fail-permitサービステンプレートでAKMモードを指定しません。
- 802.1Xクライアントのfail-permit サービステンプレートと通常のサービステンプレートが、次のコマンドの設定で一貫していることを確認します。
  - **client-security authentication-location.**

- **client forwarding-location.**
- **client association-location.**

ベストプラクティスとして、AP上の802.1Xクライアントには、fail-permit サービステンプレートを1つだけ指定します。複数のfail-permit サービステンプレートを設定する場合は、AP上の無線に最初にバインドされたもの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. 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fail-permit テンプレートとして指定します。

   fail-permit template

   デフォルトでは、失敗許可サービステンプレートとして指定されているサービステンプレートはありません。

例

#ACに障害が発生したり、ACがRADIUSにアクセスできなかった場合、APにdot1x認証で接続するクライアントが認証に失敗します。この場合、再度同じSSID(障害時にはfail-permit templateのあるサービステンプレートがアクティブになります)に接続して引き続き認証なしでネットワークにアクセスすることができます。

```
<Sysname> system-view
[Sysname] wlan service-template service 1
[Sysname-wlan-st-service1] ssid h3cdot1x
[Sysname-wlan-st-service1] client forwarding-location ap
[Sysname-wlan-st-service1] akm mode dot1x
[Sysname-wlan-st-service1] cipher-suite ccmp
[Sysname-wlan-st-service1] security-ie rsn
[Sysname-wlan-st-service1] client-security authentication-mode dot1x
[Sysname-wlan-st-service1] dot1x domain rem-domain
[Sysname-wlan-st-service1] service-template enable
[Sysname-wlan-st-service1] quit
[Sysname] wlan service-template service 2
[Sysname-wlan-st-service2] ssid h3cdot1x
[Sysname-wlan-st-service2] client forwarding-location ap
[Sysname-wlan-st-service2] fail-permit template
[Sysname-wlan-st-service2] client-security authentication-mode dot1x
[Sysname-wlan-st-service2] dot1x domain rem-domain
[Sysname-wlan-st-service2] service-template enable
[Sysname-wlan-st-service2] quit
[Sysname] quit
```

5G無線サイレンスfail-permit の設定

5G無線サイレンスfail-permit について

5G無線サイレンスfail-permit を使用すると、5G無線に無線サイレンスが設定されている場合、APは、5G無線上のサービステンプレートのクライアントをネットワークアクセスのために別の無線に移動できます。

5G無線サイレンスfail-permit タスクの概要

5G無線サイレンスfail-permit を設定するには、次の作業を実行します。

1. 5Gクライアントのfail-permit のイネーブル化
2. 5G サイレンスfail-permit サービステンプレートの指定

5Gクライアントのfail-permit のイネーブル化

このタスクについて

5G無線上のサービステンプレートの5Gクライアントが、その5G無線に無線サイレンスが適用された後もネットワークにアクセスできるようにするには、サービステンプレートでfail-permit をイネーブルにします。

制限事項とガイドライン

この機能は、サービステンプレートがディセーブルの場合に設定可能であり、サービステンプレートがイネーブルになった後に有効になります。

手順

1. システムビューに入ります。

   system-view
2. 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. fail-permitをイネーブルにします。

   fail-permit enable

   デフォルトでは、fail-permit はディセーブルになっています。

5Gサイレンスfail-permit サービステンプレートの指定

このタスクについて

ある5G無線の5Gクライアントに対して、あるサービステンプレートでフェール許可をイネーブルにする場合は、別の5G無線の別のサービステンプレートをフェール許可サービステンプレートとして指定する必要があります。

5G無線サイレンスfail-permit の詳細については、「5G無線サイレンスfail-permit について」を参照してください。

制限事項とガイドライン

- 5G無線の5Gサービステンプレートごとに1つの5G silence fail-permit サービステンプレートを指定します。これらの5G サイレンスfail-permit サービステンプレートには、fail-permit enable コマンドを含めることができないことを除き、保護された5Gサービステンプレートと同じ設定を含める必要があります。
- 5G サイレンスfail-permit サービステンプレートを、保護された5Gサービステンプレート以外の無線にバインドします。

手順

1. システムビューに入ります。

   system-view
2. 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fail-permit テンプレートとして指定します。

   fail-permit template

   デフォルトでは、fail-permit サービステンプレートとして指定されているサービステンプレートはありません。

サービステンプレートでの802.1X EAP終了のイネーブル化

このタスクについて

認証サーバーがクライアントで使用される認証方式をサポートしていない場合、クライアントはEAPリレーモードで認証に失敗します。認証の失敗を回避するには、この機能を使用して、クライアントのサービステンプレートでEAP終端をイネーブルにし、デバイスが認証サーバーと通信するための認証方式を指定します。

制限事項とガイドライン

PEAP-GTC認証方式を使用するクライアントがサービステンプレートに含まれている場合は、この機能をサービステンプレートで使用します。この機能により、デバイスはサービステンプレート内のすべてのクライアントに対してEAP終了を実行します。

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. サービステンプレートで802.1X EAP終端をイネーブルにし、デバイスと認証サーバー間の認証方式を指定します。

   dot1x eap-termination authentication-method { chap | pap }

   デフォルトでは、CHAPが使用されます。

WLAN認証用の表示およびメンテナンスコマンド

任意のビューで表示コマンドを実行し、ユーザービューでコマンドをリセットします。

タスク	コマンド
802.1Xセッション接続情報、統計情報、または設定情報を表示します。	**display dot1x [sessions | statistics] [ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]
オンラインの802.1Xクライアント情報を表示します。	スタンドアロンモードの場合: **display dot1x connection [ap** *ap-name* [**radio** *radio-id]* | **interface** *interface-type interface-number* | **user-mac** *mac-address* | **user-name** *name-string*] IRFモードの場合: **display dot1x connection [ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** name-string]
MAC認証情報を表示します。	**display mac-authentication [ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]
MAC認証接続を表示します。	スタンドアロンモードの場合: **display mac-authentication connection [ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number* | **user-mac** *mac-address* | **user-name** *name-string*] IRFモードの場合: **display mac-authentication connection [ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number* | **slot** *slot-number* | **user-mac** *mac-address* | **user-name** *name-string*]
ブロックされたMACアドレス情報を表示します。	**display wlan client-security block-mac [ap** *ap-name* [**radio** *radio-id*]]
無線クライアントに関するRADIUSアカウンティングパケット統計情報を表示します。	**display wlan statistics accounting**
802.1X統計情報をクリアします。	**reset dot1x statistics [ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type* interface-number]
MAC認証統計情報を消去します。	**reset mac-authentication statistics [ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number*]

注:

display dot1x connectionコマンド、**display dot1x**コマンド、および**reset dot1x statistics**コマンドの詳細については、『User Access and Authentication Command Reference』の802.1Xを参照してください。

display mac-authentication connection、**display mac-authentication**、および**reset mac-authentication statistics**コマンドの詳細については、『User Access and Authentication Command Reference』の「MAC authentication」を参照してください。

WLAN認証の設定例

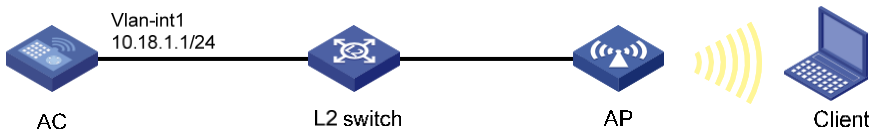
この文書のAPモデルとシリアル番号は、例としてのみ使用されています。APモデルとシリアル番号のサポートは、ACモデルによって異なります。

例:802.1X CHAPローカル認証の設定

ネットワーク構成

図3に示すように、CHAPを使用してクライアントの802.1Xローカル認証を実行するようにACを設定します。

図3 ネットワーク図



手順

この例では、ローカルユーザーを含む基本的なAAA設定だけを提供します。AAAコマンドの詳細については、『User Access and Authentication Command Reference』を参照してください。

1. 802.1Xおよびローカルクライアントを設定します。

   #EAP終了を実行し、CHAPを使用するようにACを設定します。

   <AC> system-view

   [AC] dot1x authentication-method chap

   #ユーザー名chap1およびパスワード123456をプレーンテキストで入力して、ローカルネットワークアクセスユーザーを追加します。

   [AC] local-user chap1 class network

   [AC-luser-network-chap1] password simple 123456

   #サービスタイプをlan-accessに設定します。

   [AC-luser-network-chap1] service-type lan-access

   [AC-luser-network-chap1] quit

2. ISPドメインのAAA方式を設定します。

   #localという名前のISPドメインを作成します。

   [AC] domain local

   #ローカル認証、ローカル許可、およびLANクライアントのローカルアカウンティングを使用するようにISPドメインを設定します。

[AC-isp-local] authentication lan-access local

[AC-isp-local] authorization lan-access local

[AC-isp-local] accounting lan-access local

[AC-isp-local] quit

3. サービステンプレートを設定します。

#wlas_local_chapという名前のサービステンプレートを作成します。

[AC] wlan service-template wlas_local_chap

#認証モードを802.1Xに設定します。

[AC-wlan-st-wlas_local_chap] client-security authentication-mode dot1x

#サービステンプレートのISPドメインローカルを指定します。

[AC-wlan-st-wlas_local_chap]dot1x domain local

#SSIDをwlas_local_chapに設定します。

[AC-wlan-st-wlas_local_chap] ssid wlas_local_chap

#サービステンプレートを有効にします。

[AC-wlan-st-wlas_local_chap] service-template enable

[AC-wlan-st-wlas_local_chap] quit

4. 手動AP ap1を設定し、サービステンプレートをAP無線にバインドします。

#ap1を作成し、APのモデルとシリアルIDを指定します。

[AC] wlan ap ap1 model WA4320i-ACN

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

#チャネル149をAPの無線1の作業チャネルとして設定し、無線1をイネーブルにします。

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel 149

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

#サービステンプレートwlas_local_chapをradio 1にバインドします。

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

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

[AC-wlan-ap-ap1] quit

設定の確認

#802.1Xの設定を確認します。

[AC] display wlan service-template

[AC] display dot1x

#802.1Xクライアントが認証に合格した後に、クライアント接続情報を表示します。

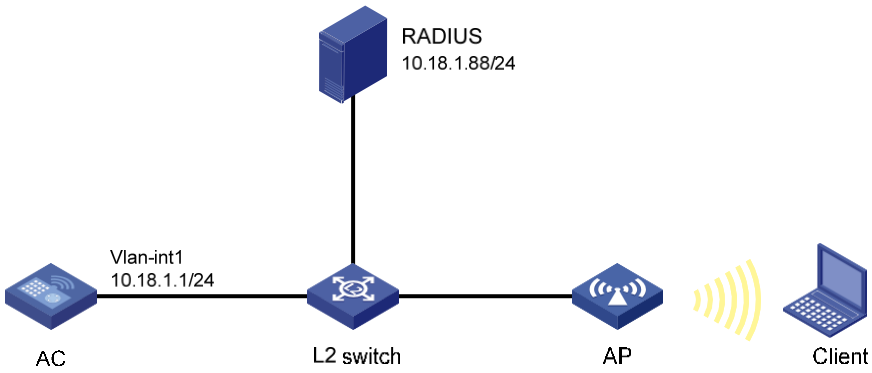
[AC] display dot1x connection

例:802.1X EAP-PEAP RADIUS認証の設定

ネットワーク構成

図4に示すように、EAP-PEAPを使用してクライアントに802.1X RADIUS認証を実行するようにACを設定します。

図4 ネットワーク図



手順

この例では、RADIUSを含む基本的なAAA設定だけを示します。AAAコマンドの詳細については、『User Access and Authentication Command Reference』を参照してください。

1. ACを設定します。
   a. 802.1XおよびRADIUSスキームを設定します。

      #EAPリレーを使用して802.1Xクライアントを認証するようにACを設定します。

      <AC> system-view

      [AC] dot1x authentication-method eap

      #RADIUSスキームを作成します。

      [AC] radius scheme imcc

      #プライマリ認証サーバーとプライマリアカウンティングサーバーを指定します。

      [AC-radius-imcc] primary authentication 10.18.1.88 1812

      [AC-radius-imcc] primary accounting 10.18.1.88 1813

      #サーバーとの安全な通信のための共有キーをプレーンテキストで12345678に設定します。

      [AC-radius-imcc] key authentication simple 12345678

      [AC-radius-imcc] key accounting simple 12345678

      #RADIUSサーバーに送信されたユーザー名のドメイン名を除外します。

      [AC-radius-imcc] user-name-format without-domain

      [AC-radius-imcc] quit

   b. ISPドメインのAAA方式を設定します。#imccという名前のISPドメインを作成します。

      [AC] domain imc

      #LANクライアントの認証、認可、およびアカウンティングにRADIUSスキームimccを使用

するようにISPドメインを設定します。

[AC-isp-imc] authentication lan-access radius-scheme imcc

[AC-isp-imc] authorization lan-access radius-scheme imcc

[AC-isp-imc] accounting lan-access radius-scheme imcc

[AC-isp-imc] quit

c. サービステンプレートを設定します。

#wlas_imc_peapという名前のサービステンプレートを作成します。

[AC] wlan service-template wlas_imc_peap

#認証モードを802.1Xに設定します。

[AC-wlan-st-wlas_imc_peap] client-security authentication-mode dot1x

#サービステンプレートのISPドメインimccを指定します。

[AC-wlan-st-wlas_imc_peap]dot1x domain imc

#SSIDをwlas_imc_peapに設定します。

[AC-wlan-st-wlas_imc_peap] ssid wlas_imc_peap

#AKMモードを802.1Xに設定します。

[AC-wlan-st-wlas_imc_peap] akm mode dot1x

#CCMP暗号スイートを設定します。

[AC-wlan-st-wlas_imc_peap] cipher-suite ccmp

#ビーコン応答とプローブ応答でRSN-IEをイネーブルにします。

[AC-wlan-st-wlas_imc_peap] security-ie rsn

#サービステンプレートを有効にします。

[AC-wlan-st-wlas_imc_peap] service-template enable

[AC-wlan-st-wlas_imc_peap] quit

d. 手動AP ap1を設定し、サービステンプレートをAP無線にバインドします。

#ap1を作成し、APのモデルとシリアルIDを指定します。

[AC] wlan ap ap1 model WA4320i-ACN

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

#チャネル149をAPの無線1の作業チャネルとして設定し、無線1をイネーブルにします。

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel 149

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

#サービステンプレートwlas_imc_peapをradio 1にバインドします。

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

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

[AC-wlan-ap-ap1] quit

2. RADIUSサーバーを設定します。

この例では、RADIUSサーバーはIMC PLAT 7.1およびIMC UAM 7.1を実行し、EAP-PEAP証明書がインストールされています。

#アクセスデバイスを追加します。

a. **user**タブをクリックします。

b. ナビゲーションツリーで、User Access Policy>Access Device Management>Access Device.

c. Addをクリックします。

   Add Access Deviceページが表示されます。

d. Access Configuration領域で、図5に示すように、次のパラメータを設定します。

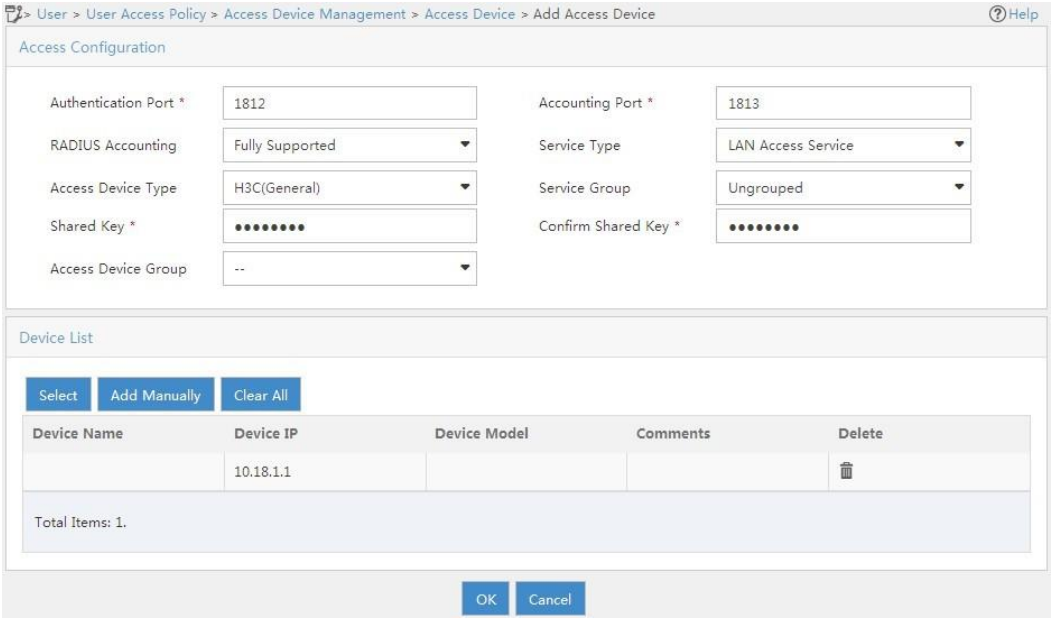
   – **Shared Key**フィールドおよび**Confirm Shared Key**フィールドに**12345678**と入力します。

   – その他のパラメータにはデフォルト値を使用します。

e. Device List領域で、**Select**または**Add Manually**をクリックして、**10.18.1.1**のデバイスをアクセスデバイスとして追加します。

f. OKをクリックします。

図5 アクセスデバイスの追加



#アクセスポリシーを追加します。

a. **user**タブをクリックします。

b. ナビゲーションツリーで、**User Access Policy > Access Policy**を選択します。

c. **Add**をクリックします。

d. **Add Access Policy**ページで、図6に示すように、次のパラメータを設定します。

   – **Access Policy Name**フィールドに**dot1x**と入力します。

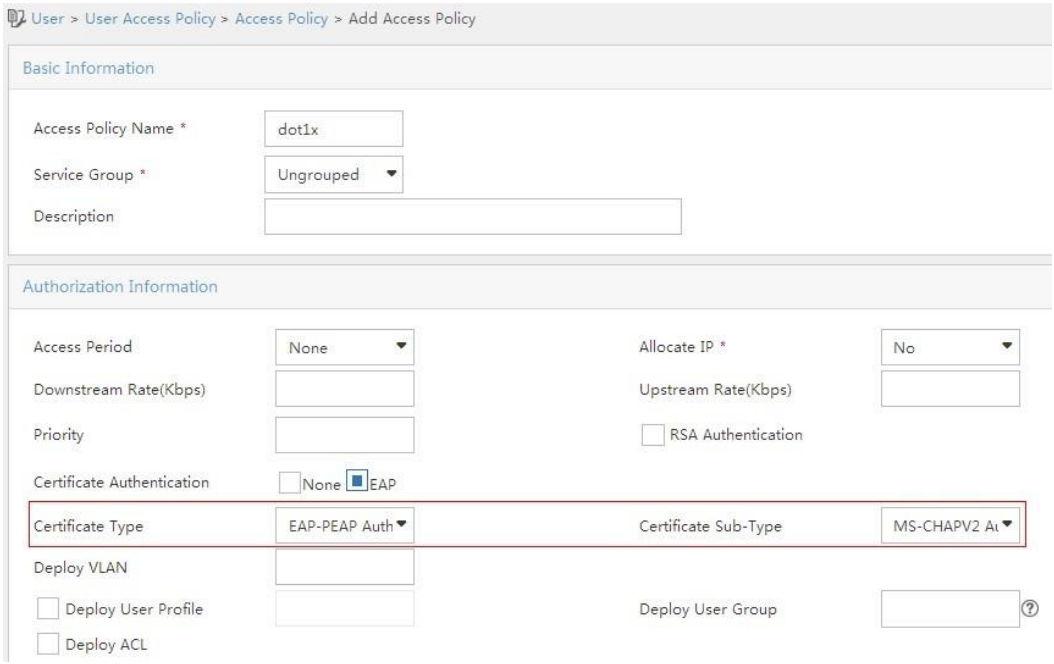
   – **Certificate Authentication**フィールドで**EAP**を選択します。

   – **Certificate Type**リストからEAP-PEAP Authを選択し、MS-CHAPV2 Authを選択します。リストから選択します。

IMCサーバー上の証明書サブタイプは、クライアント上で設定されたアイデンティティ認証方式と同じである必要があります。

e. OKをクリックします。

図6 アクセスポリシーの追加



#アクセスサービスを追加します。

a. **user**タブをクリックします。

b. ナビゲーションツリーで、**User Access Policy > Access Service**を選択します。

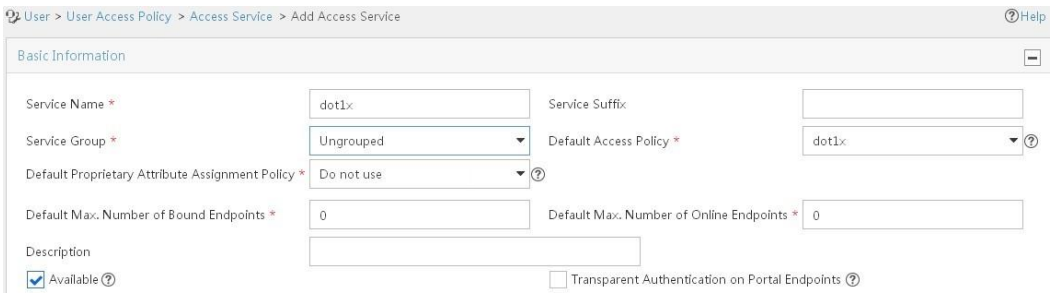
c. **Add**をクリックします。

d. **Add Access Service**ページで、図7に示すように、次のパラメータを設定します。

- Service Nameフィールドに**dot1x**と入力します。
- Default Access Policyリストから**dot1x**を選択します。

e. OKをクリックします。

図7 アクセスサービスの追加



#アクセスユーザーを追加します。

a. **user**タブをクリックします。

b. ナビゲーションツリーで、**Access User > All Access Users**を選択します。

アクセスユーザーリストが表示されます。

c. **Add**をクリックします。

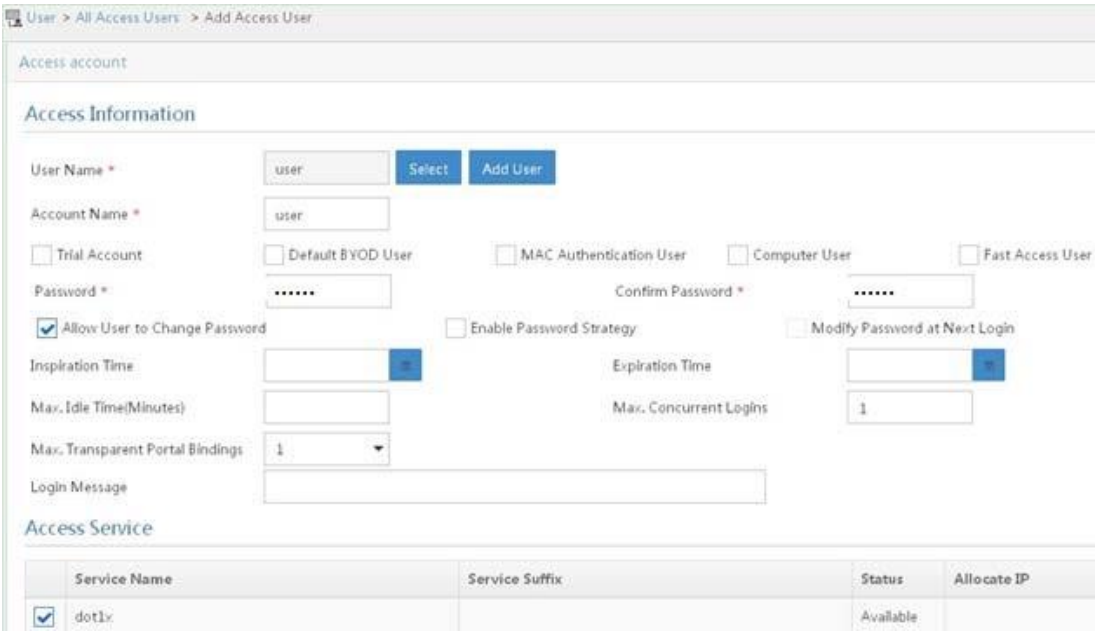
Add Access Userページが表示されます。

d. **Access Information**領域で、図8に示すように、次のパラメータを設定します。
   - **Select**または**Add User**をクリックして、ユーザー**user**をIMCプラットフォームサーバーに関連付けます。
   - **Account Name**フィールドに**user**と入力します。
   - **Password**フィールドと**Confirm Password**フィールドに**dot1x**と入力します。

e. **Access Service**領域で、リストから**dot1x**を選択します。

f. **OK**をクリックします。

図8 アクセスユーザーアカウントの追加



3. 次のようにWLANクライアントを設定します。

   WLANクライアントは、EAP-PEAP証明書とともにインストールされています。

   WLANクライアントを設定するには、次の作業を実行します(詳細は省略します)。

   - ID認証にPEAPを選択します。
   - クライアントがサーバー証明書を確認できないようにします。
   - Windowsのログイン名とパスワードを使用してクライアントが自動的にログインできないようにします。

設定の確認

1. クライアントで、ユーザー名userとパスワードdot1xを使用してネットワークにアクセスできることを確認します(詳細は表示されていません)。
2. ACで次の作業を実行して、ユーザーが認証に合格し、オンラインになったことを確認します。

   #オンラインの802.1Xクライアント情報を表示します。

   [AC] display dot1x connection

   User MAC address: 0023-8933-2090

   AP name: ap1

   Radio ID: 1

   SSID: wlas_imc_peap

BSSID: 000f-e201-0003

```
User name: user
```

Authentication domain: imc

Authentication method: EAP

Initial VLAN: 1

Authorization VLAN: N/A Authorization

ACL number: N/A Authorization user

profile : N/A Termination action: Default

Session timeout period: 6001 s

Online from: 2014/04/18 09:25:18

Online duration: 0h 1m 1s

Total connections: 1.

#WLANクライアント情報を表示します。

[AC] display wlan client

Total number of clients: 1

MAC addressUsernameAP nameR IP addressVLAN 0023-8933-2090 userap11

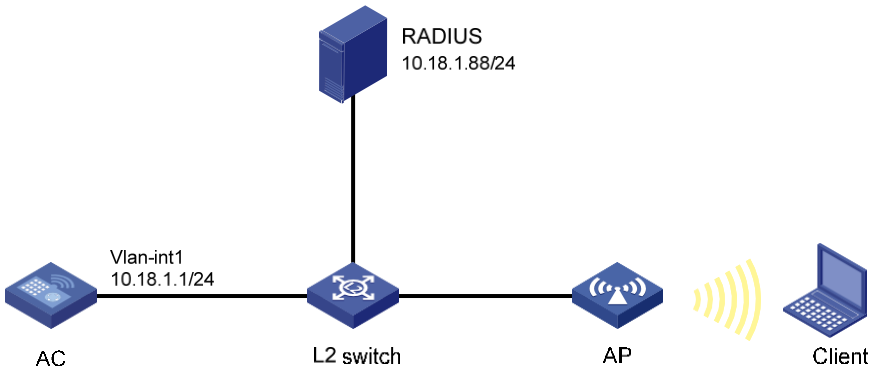
10.18.1.1001

例:RADIUSベースのMAC認証の設定

ネットワーク構成

図9に示すように、RADIUSサーバーを使用してクライアントのMAC認証を実行するようにACを設定します。

図9 ネットワーク図



手順

RADIUSサーバー、AC、AP、およびクライアントが互いに到達できることを確認します(詳細は省略します)。

1. ACを設定します。
   a. RADIUSスキームを設定します。

#RADIUSスキームを作成します。

<AC> system-view

[AC] radius scheme imcc

#プライマリ認証サーバーとプライマリアカウンティングサーバーを指定します。

[AC-radius-imcc] primary authentication 10.18.1.88 1812

[AC-radius-imcc] primary accounting 10.18.1.88 1813

#サーバーとの安全な通信のための共有キーをプレーンテキストで12345678に設定します。

[AC-radius-imcc] key authentication simple 12345678

[AC-radius-imcc] key accounting simple 12345678

#RADIUSサーバーに送信されたユーザー名のドメイン名を除外します。

[AC-radius-imcc] user-name-format without-domain

[AC-radius-imcc] quit

b. ISPドメインのAAA方式を設定します。

#imccという名前のISPドメインを作成します。

[AC] domain imc

#LANクライアントの認証、認可、およびアカウンティングにRADIUSスキームimccを使用するようにISPドメインを設定します。

[AC-isp-imc] authentication lan-access radius-scheme imcc

[AC-isp-imc] authorization lan-access radius-scheme imcc

[AC-isp-imc] accounting lan-access radius-scheme imcc

[AC-isp-imc] quit

c. MAC認証クライアントが共有するアカウントには、ユーザー名123とパスワードaaa_macaをプレーンテキストで指定します。

[AC] mac-authentication user-name-format fixed account 123 password simple aaa_maca

d. サービステンプレートを設定します。

#maca_imccという名前のサービステンプレートを作成します。

[AC] wlan service-template maca_imc

#SSIDをmaca_imccに設定します。

[AC-wlan-st-maca_imc] ssid maca_imc

#認証モードをMAC認証に設定します。

[AC-wlan-st-maca_imc] client-security authentication-mode mac

#サービステンプレートのISPドメインファイルを指定します。

[AC-wlan-st-maca_imc] mac-authentication domain imc

#サービステンプレートを有効にします。

[AC-wlan-st-maca_imc] service-template enable

[AC-wlan-st-maca_imc] quit

e. 手動AP ap1を設定し、サービステンプレートをAP無線にバインドします。

#ap1という名前の手動APを作成し、APのモデルとシリアルIDを指定します。

[AC] wlan ap ap1 model WA4320i-ACN

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

#チャネル149をAPの無線1の作業チャネルとして設定し、無線1をイネーブルにします。

[AC-wlan-ap-ap1] radio 1

[AC-wlan-ap-ap1-radio-1] channel 149

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

#サービステンプレートmaca_imcをradio 1にバインドします。

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

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

[AC-wlan-ap-ap1] quit

2. RADIUSサーバーを設定します。

この例では、RADIUSサーバーはIMC PLAT 7.1およびIMC UAM 7.1を実行します。

#アクセスデバイスを追加します。

a. **user**タブをクリックします。

b. ナビゲーションツリーで、User Access Policy>Access Device Management>Access Device.

c. Addをクリックします。

Add Access Deviceページが表示されます。

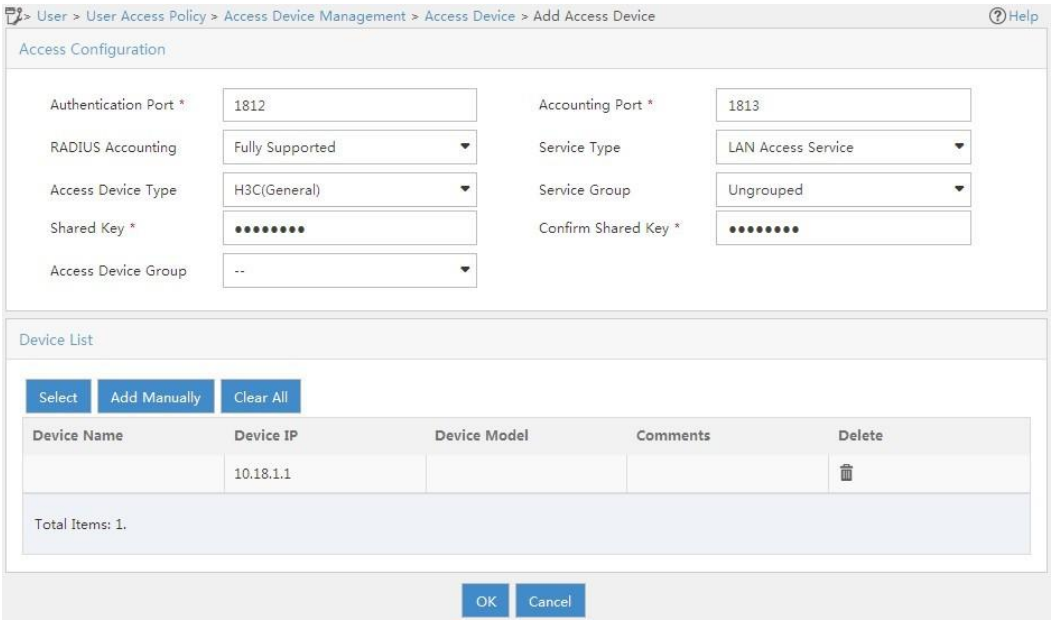
d. Access Configuration領域で、図10に示すように、次のパラメータを設定します。

- Shared KeyフィールドおよびConfirm Shared Keyフィールドに12345678と入力します。
- その他のパラメータにはデフォルト値を使用します。

e. Device List領域で、SelectまたはAdd Manuallyをクリックして、10.18.1.1のデバイスをアクセスデバイスとして追加します。

f. OKをクリックします。

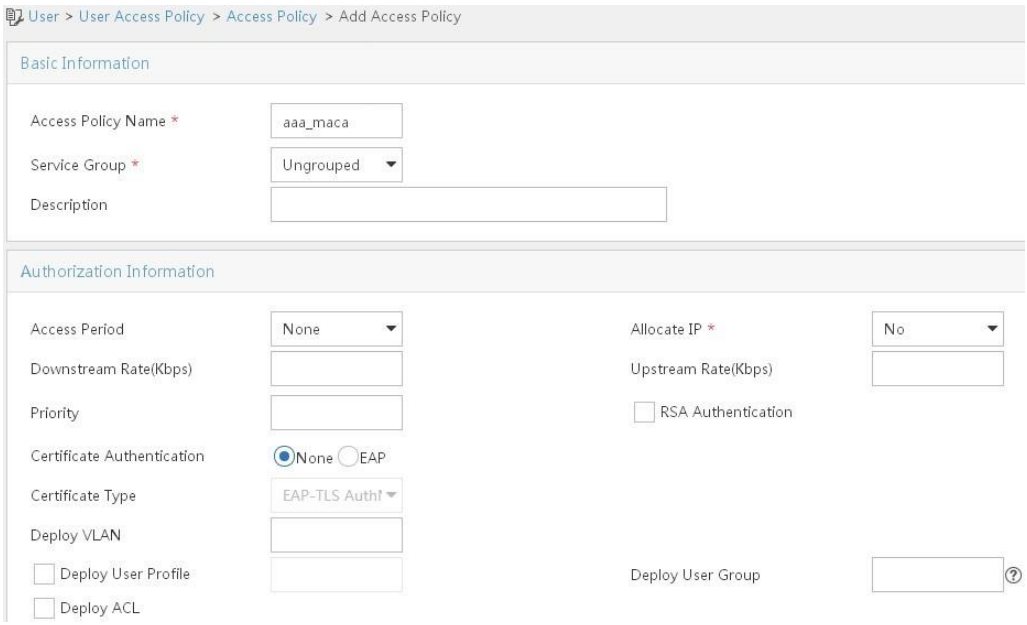
図10 アクセスデバイスの追加



#アクセスポリシーを追加します。

a. **user**タブをクリックします。
b. ナビゲーションツリーで、User Access Policy>Access Policyを選択します。
c. Addをクリックします。
d. Add Access Policyページで、図11に示すように、次のパラメータを設定します。
   - Access Policy Nameフィールドにaaa_macaと入力します。
   - その他のパラメータにはデフォルト値を使用します。
e. OKをクリックします。

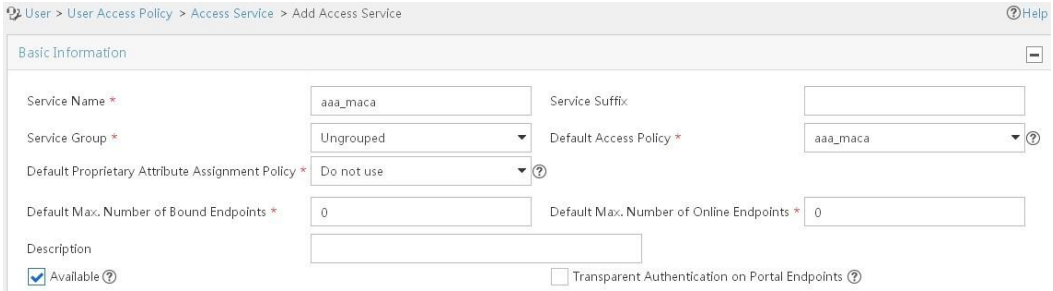
図11 アクセスポリシーの追加



#アクセスサービスを追加します。

a. **user**タブをクリックします。
b. ナビゲーションツリーで、User Access Policy>Access Serviceを選択します。
c. Addをクリックします。
d. Add Access Serviceページで、図12に示すように、次のパラメータを設定します。
   - Service Nameフィールドにaaa_macaと入力します。
   - Default Access Policyリストからaaa_macaを選択します。
e. OKをクリックします。

図12 アクセスサービスの追加



#アクセスサーバーを追加します。

a. **user**タブをクリックします。

b. ナビゲーションツリーで、**Access User > All Access Users**を選択します。アクセスユーザーリストが表示されます。

c. **Add**をクリックします。

Add Access Userページが表示されます。

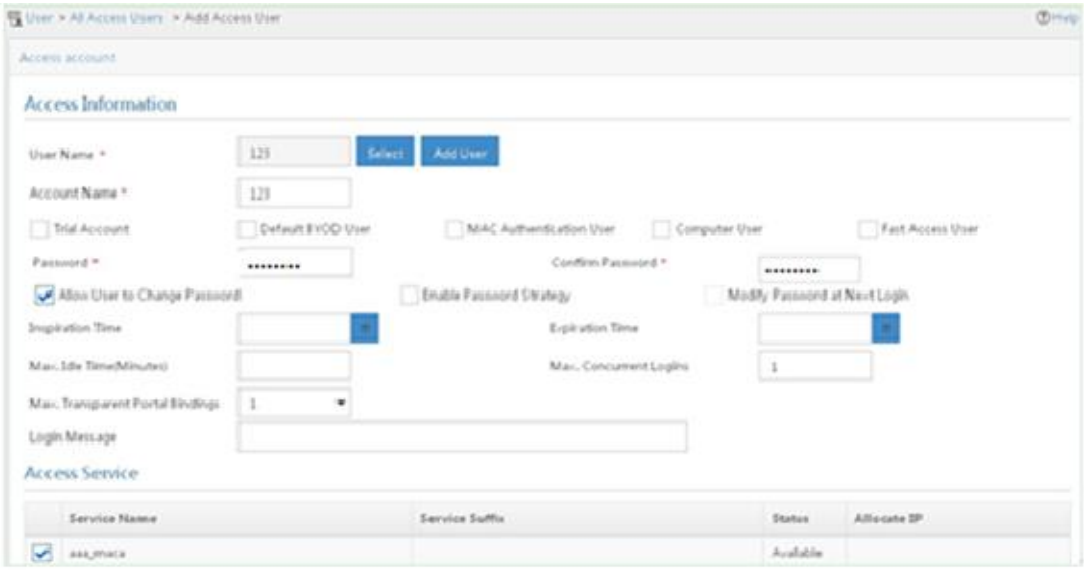
d. Access Information領域で、図13に示すように、次のパラメータを設定します。

- SelectまたはAdd Userをクリックして、ユーザーをIMC Platform user 123に関連付けます。
- Account Nameフィールドに123と入力します。
- PasswordフィールドとConfirm Passwordフィールドにaaa_macaと入力します。

e. Access Service領域で、リストからaaa_macaを選択します。

f. OKをクリックします。

図13 アクセスユーザーアカウントの追加



設定の確認

1. クライアントで、ユーザー名123とパスワードaaa_macaを使用してネットワークにアクセスできることを確認します(詳細は省略します)。
2. ACで次の作業を実行して、ユーザーが認証に合格し、オンラインになったことを確認します。

#オンラインMAC認証クライアント情報を表示します。

[AC] display mac-authentication connection User MAC address: 0023-8933-2098
AP name: ap1
Radio ID: 1
SSID: maca_imc
BSSID: 000f-e201-0001
User name: 123
Authentication domain: imc
Initial VLAN: 1
Authorization VLAN: N/A Authorization ACL number : N/A Authorization user profile : N/A
Authorization URL: N/A

Termination action: Default
Session timeout period: 6001 s
Online from: 2014/04/17 17:21:12
Online duration: 0h 0m 30s Total connections: 1.

#WLANクライアント情報を表示します。

[AC] display wlan client
Total number of clients: 1

MAC address	Username	AP name	R	IP address	VLAN
0023-8933-2098	123	ap1	1	10.18.1.100	1