H3Cアクセスコントローラ

802.1X認証設定ガイド

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

802.1Xの概要

802.1Xプロトコルについて

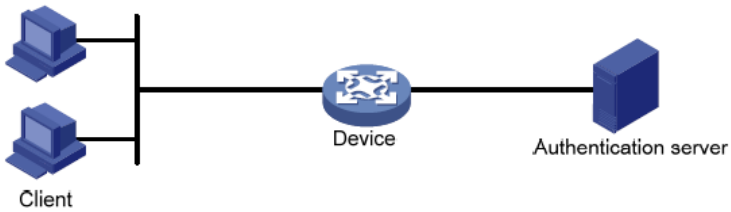
802.1Xは、イーサネットネットワークで広く使用されているポートベースのネットワークアクセスコントロールプロトコルです。このプロトコルは、802.1X対応のLANポートに接続されたデバイスを認証することによってネットワークアクセスを制御します。

802.1Xアーキテクチャ

802.1Xはクライアント/サーバーモデルで動作します。図1に示すように、802.1X認証には次のエンティティが含まれます:

- クライアント(サプリカント):LANへのアクセスを求めるサーバー端末。アクセスデバイスに対して認証を行うには、端末に802.1Xソフトウェアが必要です。
- アクセスデバイス(オーセンティケータ):LANへのアクセスを制御するためにクライアントを認証します。一般的な802.1X環境では、アクセスデバイスは認証サーバーを使用して認証を実行します。
- 認証サーバー:アクセスデバイスに認証サービスを提供します。認証サーバーは、まずアクセスデバイスから送信されたデータを使用して802.1Xクライアントを認証します。次に、アクセスデバイスに認証結果を返してアクセス決定を行います。認証サーバーは通常、RADIUSサーバーです。小規模なLANでは、アクセスデバイスを認証サーバーとして使用できます。

図1 802.1Xアーキテクチャ

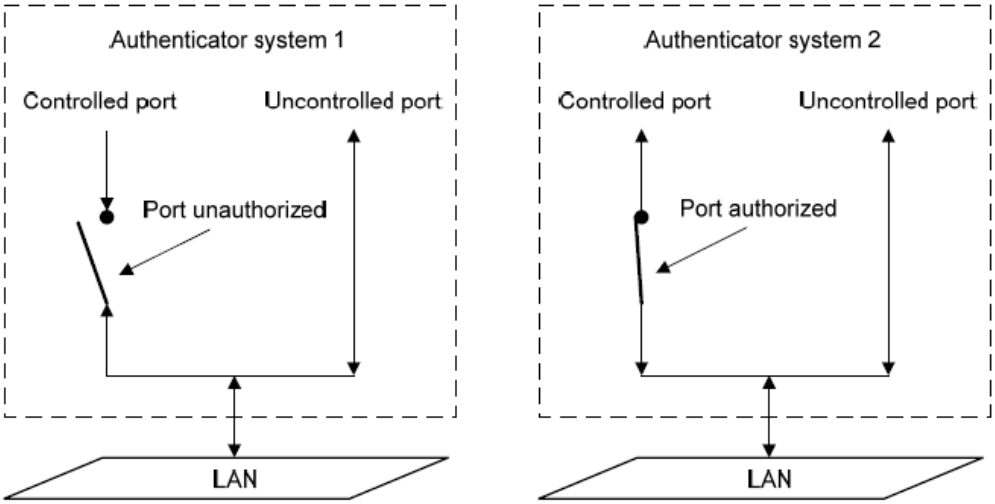


制御/非制御ポートおよびポート認可ステータス

802.1Xは、ネットワークアクセスポートに2つの論理ポート(制御ポートと非制御ポート)を定義します。ネットワークアクセスポートに到着したパケットは、両方の論理ポートから認識されます。

- 非制御ポート:認証パケットを送受信するために常にオープンです。
- 制御ポートポートの状態に応じてパケットをフィルタリングします。
  - 認可ステート:クライアントが認証を通過した場合、制御ポートは認可ステートです。ポートはトラフィックの通過を許可します。
  - 無許可ステート:クライアントが認証に失敗した場合、ポートは無許可ステートになります。ポートは、次のいずれかの方法を使用してトラフィックを制御します。
    - 双方向トラフィック制御を実行して、クライアントとのトラフィックを拒否します。
    - 単一方向トラフィック制御を実行して、クライアントからのトラフィックを拒否します。デバイスは単一方向トラフィック制御だけをサポートします。

図2 制御対象ポートの許可ステート



パケット交換方式

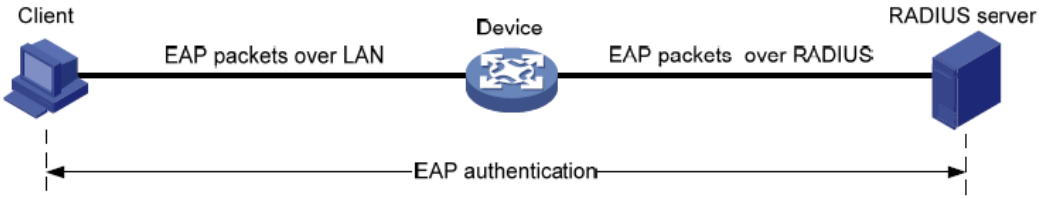
802.1Xでは、Extensible Authentication Protocol(EAP)を使用して、クライアント、アクセスデバイス、および認証サーバーの認証情報を転送します。EAPは、クライアント/サーバーモデルを使用する認証フレームワークです。このフレームワークでは、MD5-Challenge、EAP-Transport Layer Security(EAP-TLS)、Protected EAP(PEAP)などのさまざまな認証方法がサポートされています。

802.1Xでは、有線または無線LANを介してクライアントとアクセスデバイス間でEAPパケットを渡すためのEAP over LAN(EAPOL)を定義しています。アクセスデバイスと認証サーバー間では、802.1XはEAPリレーまたはEAPターミネーションによって認証情報を提供します。

EAPリレー

EAPリレーはIEEE 802.1Xで定義されています。このモードでは、ネットワークデバイスはEAP over RADIUS(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(図3を参照)。

図3 EAPリレー



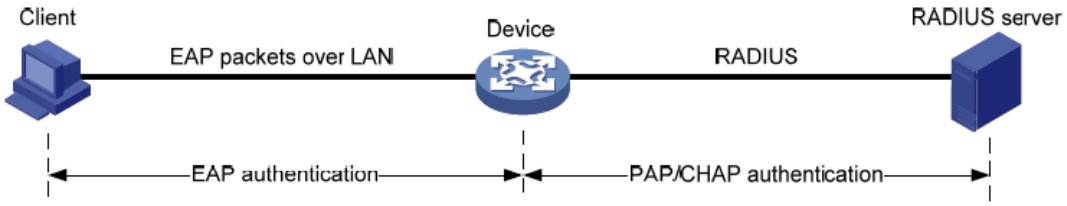
EAPリレーモードでは、クライアントはRADIUSサーバーと同じ認証方式を使用する必要があります。アクセスデバイスでは、dot1x authentication-method eapコマンドを使用するだけで、EAPリレーをイネーブルにできます。

EAP終了

図4に示すように、アクセスデバイスはEAP終了モードで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サーバーへの認証を行います。

図4 EAPの終了



EAPリレーとEAPターミネーションの比較

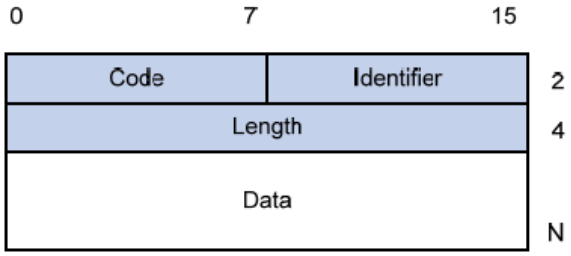
パケット交換方式	メリット	制限事項
EAPリレー	• さまざまなEAP認証方式をサポートします。 • アクセスデバイスでの設定と処理は簡単です。	RADIUSサーバーは、EAP-Messageとメッセージオーセンティケータアトリビュート、およびクライアントで使用されるEAP認証方式。
EAP終了	PAPまたはCHAP認証をサポートする任意のRADIUSサーバーで動作します。	• 次のEAP認証方式だけをサポートします。 ○ MD 5:Challenge EAP認証。 ○ INode 802.1Xクライアントによって開始されるEAP認証のサーバー名とパスワード。 • アクセスデバイスでの処理は複雑です。

パケットフォーマット

EAPパケット形式

図5に、EAPパケットのフォーマットを示します。

図5 EAPパケットフォーマット

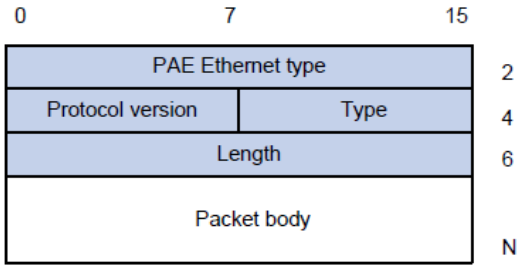


- コード:EAPパケットのタイプ。オプションには、Request(1)、Response(2)、Success(3)、またはFailure(4)があります。
- 識別子-応答と要求を照合するために使用されます。
- 長さ:EAPパケットの長さ(バイト単位)。EAPパケット長は、コード、識別子、長さ、およびデータフィールドの合計です。
- データ:EAPパケットの内容。このフィールドは、要求または応答EAPパケットにのみ表示されます。データフィールドには、要求タイプ(または応答タイプ)とタイプデータが含まれます。タイプ1(識別)とタイプ4(MD 5-チャレンジ)は、タイプフィールドの2つの例です。

EAPOLパケット形式

図6に、EAPOLパケットフォーマットを示します。

図6 EAPOLパケットフォーマット



- PAE Ethernet typeプロトコル・タイプ。EAPOLの値は0x888Eです。
- プロトコルバージョン:EAPOLパケット送信者によって使用されるEAPOLプロトコルバージョン。
- タイプ-EAPOLパケットのタイプ。表1に、デバイスの802.1X実装でサポートされているEAPOLパケットのタイプを示します。

  表1 EAPOLパケットのタイプ

[値]	種類	説明
0x00	EAPパケット	クライアントとアクセスデバイスは、EAPパケットを使用して認証情報を転送します。
0x01	EAPOL開始	クライアントはEAPOL-Startメッセージを送信して、アクセスデバイスへの802.1X認証を開始します。
0x02	EAPOL-ログオフ	クライアントはEAPOL-Logoffメッセージを送信して、クライアントがログオフ中であることをアクセスデバイスに通知します。

- 長サーバーイト単位のデータ長、またはパケット本体の長さ。パケットタイプがEAPOL-StartまたはEAPOL-Logoffの場合、このフィールドは0に設定され、パケット本体フィールドは続きません。
- Packet body:パケットの内容。EAPOLパケットタイプがEAP-Packetの場合、Packet bodyフィールドにはEAPパケットが含まれます。

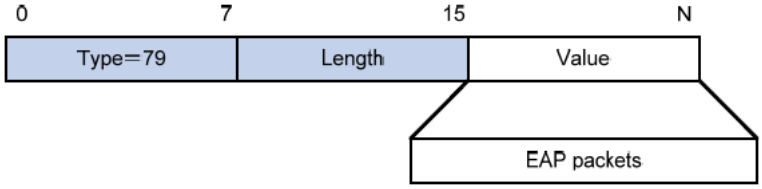
EAP over RADIUS

RADIUSでは、EAP認証をサポートするためにEAP-MessageとMessage-Authenticatorの2つのアトリビュートが追加されています。RADIUSパケットフォーマットの詳細については、「AAAの設定」を参照してください。

- EAP:メッセージ。

  図7に示すように、RADIUSはEAPパケットをEAP-Message属性にカプセル化します。Typeフィールドは79で、Valueフィールドは最大253バイトです。EAPパケットが253バイトを超える場合、RADIUSは複数のEAP-Message属性にカプセル化します。

  図7 EAP-Message属性のフォーマット

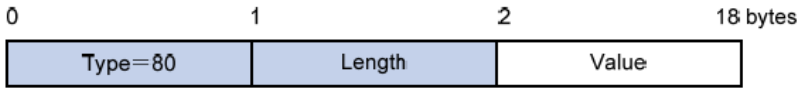


- メッセージオーセンティケータ。

  図8に示すように、RADIUSは、完全性をチェックするためにEAP-Message属性を持つすべてのパケットにMessage-Authenticator属性を含めます。計算されたパケット完全性チェックサムがMessage-Authenticator属性の値と異なる場合、パケット受信側はパケットをドロップします。

Message-Authenticatorは、EAP認証中にEAP認証パケットが改ざんされるのを防ぎます。

図8 メッセージオーセンティケータ属性フォーマット



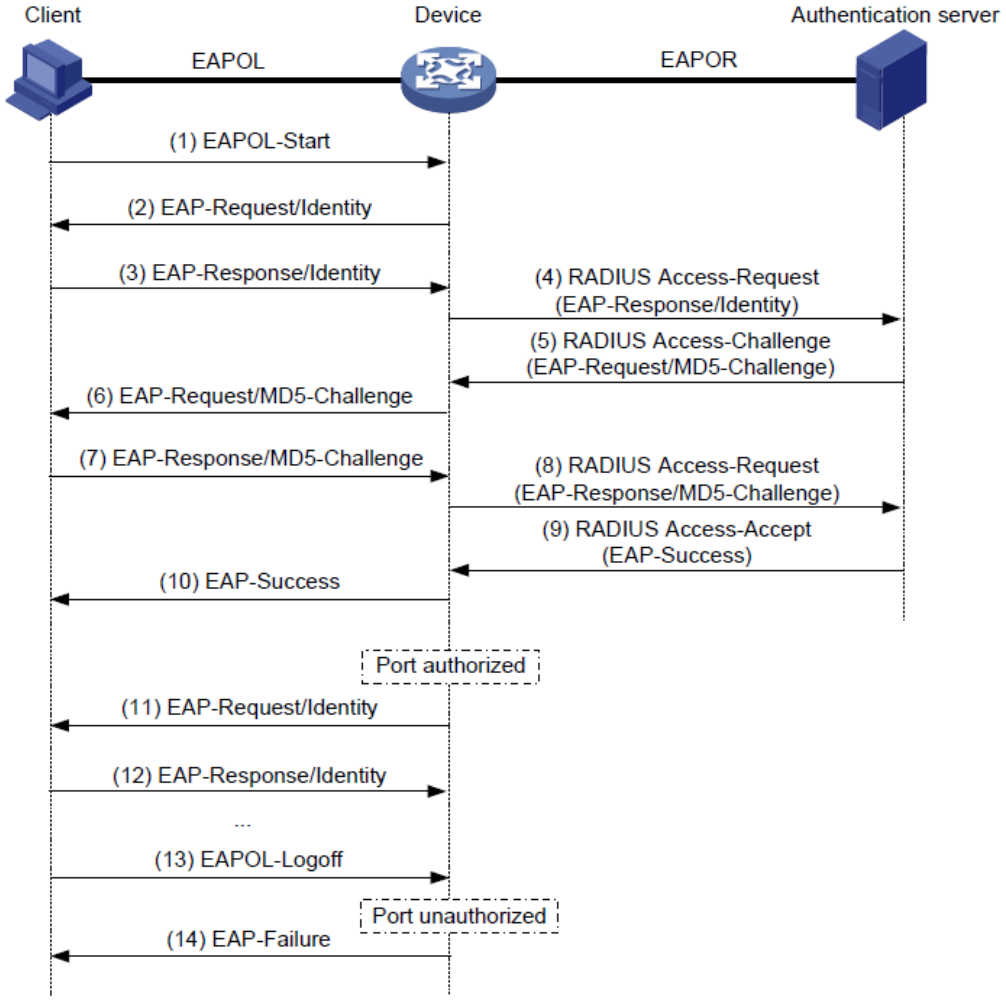
802.1X認証手順

802.1X認証には、EAPリレーとEAPターミネーションの2つの方式があります。EAPパケットに対するRADIUSサーバーのサポートとEAP認証方式に応じて、いずれかのモードを選択します。

EAPリレー

図9は、MD5-Challenge EAP認証が使用されていると想定した、EAPリレーモードでの基本的な802.1X認証手順を示しています。

図9 EAPリレーモードでの802.1X認証手順



次のステップでは、802.1X認証手順について説明します。

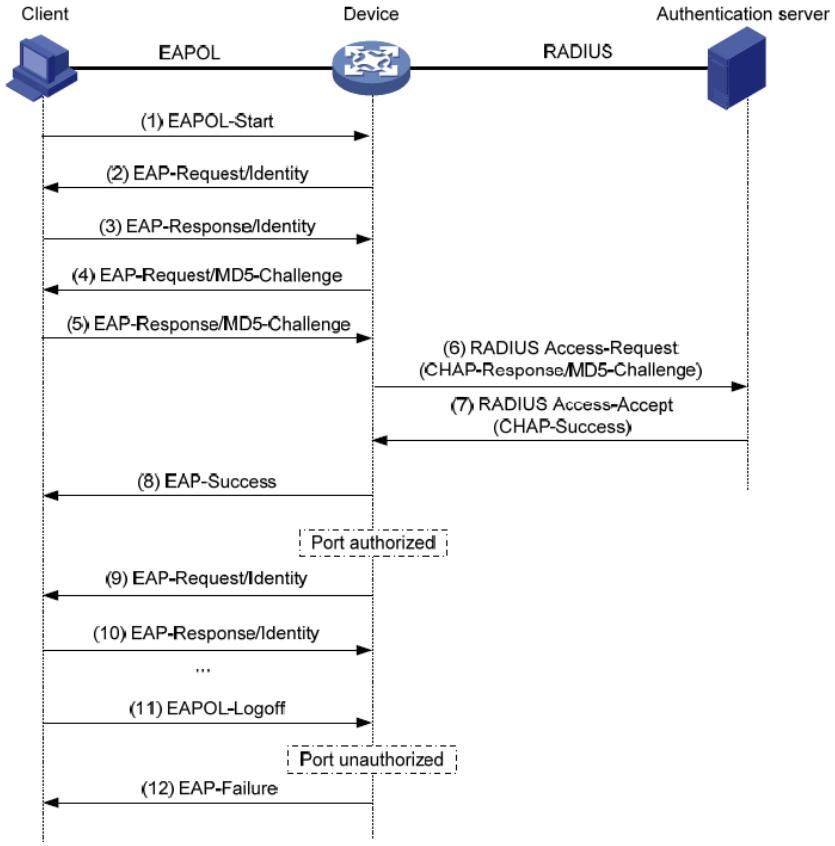
1. サーバーが802.1Xクライアントを起動し、登録されたサーバー名とパスワードを入力すると、802.1XクライアントはEAPOL-Startパケットをアクセスデバイスに送信します。
2. アクセスデバイスはEAP-Request/Identityパケットで応答し、クライアントのサーバー名を要求します。

3. EAP-Request/Identityパケットに応答して、クライアントはEAP-Response/Identityパケットでサーバー名をアクセスデバイスに送信します。
4. アクセスデバイスは、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ID情報を使用してサーバ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ると、ランダムに生成されたチャレンジ(EAP-Request/MD5-Challenge)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、RADIUS Access-Challengeパケットでアクセスデバイスにチャレンジを送信します。
6. アクセスデバイスは、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、EAP-Response/MD5-Challengeパケットで暗号化されたパスワードをアクセスデバイスに送信します。
8. アクセスデバイスは、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の場合、サーバーはクライアントが有効であると見なし、RADIUS Access-Acceptパケットをアクセスデバイスに送信します。
10. RADIUS Access-Acceptパケットを受信すると、アクセスデバイスは次の動作を実行します。
    a. EAP-Successパケットをクライアントに送信します。
    b. 制御ポートを許可ステートに設定します。クライアントはネットワークにアクセスできます。
11. クライアントがオンラインになった後、アクセスデバイス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確認します。デフォルトでは、2回連続してハンドシェイクに失敗すると、デバイスはクライアントをログオフします。
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。連続したハンドシェイク試行回数(デフォルトでは2回)後にクライアントが応答を返さなかった場合、アクセスデバイス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サーバーによって使用されているネットワークリソースを適時に解放できます。
13. クライアントは、EAPOL-Logoffパケットを送信して、アクセスデバイスにログオフを要求することもできます。
14. EAPOL-Logoffパケットに応答して、アクセスデバイスは制御ポートのステータスを許可から無許可に変更します。次に、アクセスデバイスはEAP-Failureパケットをクライアントに送信します。

EAP終了

図10は、CHAP認証が使用されていると仮定して、EAP終了モードでの基本的な802.1X認証手順を示しています。

図10 EAP終了モードでの802.1X認証手順



EAP終了モードでは、認証サーバーではなくアクセスデバイスが、パスワード暗号化のためのMD5チャレンジを生成します。次に、アクセスデバイスは、MD5チャレンジを、サーバー名および暗号化されたパスワードとともに標準RADIUSパケットでRADIUSサーバーに送信します。

802.1X認証の開始

802.1Xクライアントとアクセスデバイスの両方が802.1X認証を開始できます。

802.1 イニシエータとしてのXクライアント

クライアントはEAPOL-Startパケットをアクセスデバイスに送信して、802.1X認証を開始します。パケットの宛先MACアドレスは、IEEE 802.1Xで指定されたマルチキャストアドレス01-80-C2-00-00-03またはブロードキャストMACアドレスです。クライアントと認証サーバー間の中間デバイスがマルチキャストアドレスをサポートしていない場合は、ブロードキャストEAPOL-Startパケットを送信できる802.1Xクライアントを使用する必要があります。たとえば、INode 802.1Xクライアントを使用できます。

イニシエータとしてのアクセスデバイス

クライアントがEAPOL-Startパケットを送信できない場合は、認証を開始するようにアクセスデバイスを設定します。たとえば、Windows XPで使用できる802.1Xクライアントがあります。

アクセスデバイスは、次のモードをサポートします。

- マルチキャストトリガーモード:アクセスデバイスはEAP-Request/Identityパケットをマルチキャストし、ID要求間隔で802.1X認証を開始します。
- ユニキャストトリガーモードアクセスデバイスは、不明なMACアドレスからフレームを受信すると、受信ポートからMACアドレスにEAP-Request/Identityパケットを送信します。ID要求タイムアウト時間内に応答が受信されなかった場合、デバイスはパケットを再送信します。このプロセスは、dot1x retryコマンドを使用して設定された最大要求試行回数に達するまで継続されます。

サーバー名要求タイムアウトタイマーは、マルチキャストトリガーのID要求間隔とユニキャストトリガーのID要求タイムアウト間隔の両方を設定します。

アクセス制御方式

H3Cは、802.1Xプロトコルで定義されているポートベースのアクセスコントロールを実装し、MACベースのアクセスコントロールをサポートするようにプロトコルを拡張します。

- ポートベースのアクセス制御802.1Xサーバーがポートで認証を通過すると、後続のサーバーは認証なしでポートを介してネットワークにアクセスできます。認証されたサーバーがログオフすると、他のすべてのサーバーがログオフされます。
- MACベースのアクセス制御各サーバーはポート上で個別に認証されます。サーバーがログオフしても、他のオンラインサーバーは影響を受けません。

802.1X VLANの操作

認可VLAN

認可VLANは、認可されたネットワークリソースへの802.1Xサーバーのアクセスを制御します。デバイスは、ローカルまたはリモートサーバーによって割り当てられた認可VLANをサポートします。

重要:

タグ付き認可VLANを割り当てることができるのはリモートサーバーだけです。

リモートVLAN許可

リモートVLAN認可では、リモートサーバー上でサーバーの認可VLANを設定する必要があります。サーバーがサーバーに対して認証されると、サーバーは認可VLAN情報をデバイスに割り当てます。次に、デバイスはサーバークセスポートをタグ付きまたはタグなしメンバーとして認可VLANに割り当てます。

デバイスは、リモートサーバーによる次の認可VLAN情報の割り当てをサポートしています。

- VLAN ID。
- VLAN名。アクセスデバイスのVLANの説明と同じである必要があります。
- VLAN IDとVLAN名のストリング。

  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。
- 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設定」を参照してください。
- tまたはuのサフィックスを持つVLAN ID。

  サフィックスtおよびuは、デバイスがアクセスポートをそれぞれタグ付きメンバーまたはタグなしメンバーとしてVLANに割り当てる必要があります。たとえば、2uはポートをタグなしメンバーとしてVLAN 2に割り当てることを示します。

VLAN名またはVLANグループ名が割り当てられている場合、デバイスはVLAN割り当ての前に情報をVLAN IDに変換します。

重要:

VLAN名で表されるVLANを正常に割り当てるには、そのVLANがデバイス上に作成されていることを確認する必要があります。

サフィックス付きのVLAN IDを割り当てるには、サーバークセスポートがポートベースのアクセスコントロールを実行するハイブリッドポートまたはトランクポートであることを確認します。

割り当てを成功させるために、リモートサーバーによって割り当てられた認可VLANは、次のタイプのいずれにもできません。

- ダイナミックに学習されたVLAN。
- 予約済みVLAN。

サーバーがVLANのグループを割り当てる場合、アクセスデバイスは表2で説明するようにVLANを選択します。

表2 VLANグループからの認可VLANの選択

VLAN情報	認可VLANの選択
IDによるVLAN名前によるVLAN VLANグループ名	802.1 X対応ポートがMACベースのアクセスコントロールを実行する場合、デバイスは次の規則に従って、サーバーのVLANグループから認可VLANを選択します。 • ポートにオンラインサーバーがない場合、デバイスは最も小さいIDを持つVLANを選択します。 • ポートにオンラインサーバーが存在する場合、デバイスはVLANグループでオンラインサーバーのVLANを調べます。VLANが検出されると、そのVLANは認可VLANとしてサーバーに割り当てられます。VLANが検出されない場合、VLAN認可は失敗します。 802.1X対応ポートがポートベースのアクセスコントロールを実行する場合、デバイスはIDが最も小さいVLANをVLANグループから選択します。後続のすべての802.1Xサーバーはそのに割り当てられます。
サフィックス付きのVLAN ID	1. デバイスは、一番左のVLAN ID(サフィックスなし)、またはuがサフィックスとして付加された一番左のVLAN ID(タグなしVLAN)のうち、最も左にある方を選択します。 2. デバイスは、タグなしVLANをPVIDとしてポートに割り当て、残りをタグ付きVLANとして割り当てます。タグなしVLANが割り当てられていない場合、ポートのPVIDは変更されません。ポートは、これらのタグ付きおよびタグなしVLANからのトラフィックの通過を許可します。 たとえば、認証サーバーはストリング1u 2t 3をサーバーのアクセスデバイスに送信します。デバイスはVLAN 1をタグなしVLANとして割り当て、残りのすべてのVLAN(VLAN 3を含む)をタグ付きVLANとして割り当てます。VLAN 1はPVIDになります。

ローカルVLAN許可

サーバーに対してローカルVLAN認可を実行するには、そのサーバーのローカルサーバーカウントの認可アトリビュートリストにVLAN IDを指定します。ローカルサーバーごとに、1つの認可VLAN IDだけを指定できます。サーバークセスポートは、タグなしメンバーとしてVLANに割り当てられます。

重要:

ローカルVLAN認可では、タグ付きVLANの割り当てはサポートされません。

ローカルサーバー設定の詳細については、「AAAの設定」を参照してください。

802.1 X対応ポートでの許可VLANの操作

表3に、アクセスデバイスが802.1 X対応ポート上でVLAN(サフィックスで指定されたVLANを除く)を処理する方法を示します。

表3 VLANの操作

ポートアクセス制御方式	VLAN操作
ポートベース	デバイスは、最初に認証されたサーバーの認可VLANにポートを割り当てます。後続のすべての802.1Xサーバーは、認証なしでVLANにアクセスできます。 認可VLANにタグなしアトリビュートがある場合、デバイスはポートをタグなしメンバーとして認可VLANに割り当て、そのVLANをPVIDとして設定します。 認可VLANにタグ付きアトリビュートがある場合、デバイスはPVIDを変更せずに、ポートをタグ付きメンバーとしてVLANに割り当てます。 **注:** タグ付きアトリビュートは、トランクポートおよびハイブリッドポートだけでサポートされます。
MACベース	• デバイスは、最初に認証されたサーバーの認可VLANにポートを割り当て、その認可VLANにタグなしアトリビュートがある場合は、そのVLANをPVIDとして設定します。 • 認可VLANにタグ付きアトリビュートがある場合、デバイスはPVIDを変更せずにポートを認可VLANに割り当てます。

重要:

- サーバーがリンクタイプがアクセスであるポートに接続されている場合は、サーバーによって割り当てられた認可VLANにタグなしアトリビュートが設定されていることを確認してください。サーバーがタグ付きアトリビュートを持つVLANを発行すると、VLAN割り当ては失敗します。
- トランクポートまたはハイブリッドポートに接続されているサーバーにVLANを割り当てる場合は、タグなしVLANが1つだけであることを確認してください。別のタグなしVLANが後続のサーバーに割り当てられている場合、そのサーバーは認証を通過できません。
- ネットワークセキュリティを強化するためのベストプラクティスとして、port hybrid vlanコマンドを使用して、ハイブリッドポートをタグ付きメンバーとして認可VLANに割り当てないでください。

サーバーに認可VLANが設定されていない場合に、802.1X認証サーバーがハイブリッドポート上のネットワークにアクセスするには、次のいずれかの作業を行います。

- ポートがVLAN内のサーバーからタグ付き認証パケットを受信する場合は、port hybrid vlanコマンドを使用して、ポートをVLAN内のタグ付きメンバーとして設定します。
- ポートがVLAN内のサーバーからタグなし認証パケットを受信する場合は、port hybrid vlanコマンドを使用して、ポートをVLAN内のタグなしメンバーとして設定します。

ゲストVLAN

ポート上の802.1Xゲスト VLANは、802.1X認証を実行していないサーバーに対応します。ゲストVLAN内のサーバーは、ソフトウェアサーバーなどの限られたネットワークリソースセットにアクセスして、アンチウイルスソフトウェアおよびシステムパッチをダウンロードできます。ゲストVLAN内のサーバーが802.1X認証を通過すると、そのサーバーはゲストVLANから削除され、許可されたネットワークリソースにアクセスできます。

アクセスデバイスは、802.1Xアクセスコントロール方式に基づいて、802.1X対応ポート上でVLANを処理します。

ポートベースのアクセス制御

認証ステータス	VLAN操作
ポートがautoステートの場合、サーバーは802.1 X対応ポートにアクセスします。	デバイスはポートを802.1Xゲスト VLANに割り当てます。このポート上のすべての802.1Xサーバーは、ゲストVLAN内のリソースだけにアクセスできます。 ゲストVLANの割り当ては、ポートリンクモードによって異なります。詳細は、「認可VLAN」の表3を参照してください。
802.1Xゲスト VLANのサーバーは、802.1X認証に失敗します。	802.1X Auth-fail VLAN(認証失敗VLAN)が使用可能な場合、デバイスはポートを認証失敗VLANに割り当てます。このポート上のすべてのサーバーは、認証失敗VLAN内のリソースだけにアクセスできます。 Auth-fail VLAN(認証失敗VLAN)が設定されていない場合、ポートはまだ802.1Xゲスト VLANにあります。ポート上のすべてのサーバーはゲストVLANにあります。 802.1X Auth-fail VLAN(認証失敗VLAN)については、「認証失敗VLAN」を参照してください。
802.1Xゲスト VLANのサーバーは、802.1X認証を通過します。	デバイスは802.1Xゲスト VLANからポートを削除し、そのポートをサーバーの認可VLANに割り当てます。 認証サーバーが認可VLANを割り当てない場合、ポートの初期PVIDが適用されます。サーバーと後続のすべての802.1Xサーバーは、初期ポートVLANに割り当てられます。 サーバーがログオフした後、ポートはゲストVLANに再度割り当てられます。 **注:** 802.1X対応ポートの初期PVIDとは、ポートが802.1X VLANに割り当てられる前にポートで使用されるPVIDのことです。

MACベースのアクセス制御

認証ステータス	VLAN操作
サーバーが802.1X対応ポートにアクセスし、802.1X認証を実行していない。	デバイスは、サーバーのMACアドレスと802.1Xゲスト VLAN間のマッピングを作成します。サーバーは、ゲストVLAN内のリソースだけにアクセスできます。
802.1Xゲスト VLANのサーバーは、802.1X認証に失敗します。	802.1X Auth-fail VLAN(認証失敗VLAN)が使用可能な場合、デバイスはサーバーのMACアドレスをAuth-fail VLAN(認証失敗VLAN)に再マップします。サーバーはAuth-fail VLAN(認証失敗VLAN)内のリソースだけにアクセスできます。 802.1X Auth-fail VLAN(認証失敗VLAN)が設定されていない場合、サーバーは802.1Xゲスト VLANから削除され、最初のPVIDに追加されます。

802.1XゲストVLANのサーバーは、802.1X認証を通過します。	デバイスは、サーバーのMACアドレスを認可VLANに再マップします。 認証サーバーが認可VLANを割り当てない場合、デバイスはサーバーのMACアドレスをポートの最初のPVIDに再マップします。

Auth-fail VLAN(認証失敗VLAN)

ポート上の802.1X認証失敗VLANは、組織のセキュリティ方針に従わなかったために802.1X認証に失敗したサーバーX認証に失敗したサーバーに対応します。たとえば、VLANは、誤ったパスワードを入力したサーバーに対応します。認証失敗VLAN内のサーバーは、ソフトウェアサーバーなどの限られたネットワークリソースにアクセスして、ウイルス対策ソフトウェアおよびシステムパッチをダウンロードできます。

アクセスデバイスは、802.1Xアクセスコントロール方式に基づいて、802.1X対応ポート上でVLANを処理します。

ポートベースのアクセス制御

認証ステータス	VLAN操作
サーバーがポートにアクセスし、802.1X認証に失敗しました。	デバイスはポートをAuth-fail VLAN(認証失敗VLAN)に割り当てます。このポート上のすべての802.1Xサーバーは、Auth-fail VLAN(認証失敗VLAN)内のリソースだけにアクセスできます。 Auth-fail VLAN(認証失敗VLAN)の割り当ては、ポートリンクモードによって異なります。詳細については、「認可VLAN」の表3を参照してください。
802.1Xのサーバー Auth-fail VLAN(認証失敗VLAN)は802.1X認証に失敗します。	ポートはまだAuth-fail VLAN(認証失敗VLAN)にあり、このポートのすべての802.1Xサーバーはこのvlanに属しています。
802.1X Auth-fail VLAN(認証失敗VLAN)のサーバーは、802.1X認証を通過します。	デバイスはポートをサーバーの認可VLANに割り当て、そのポートをAuth-fail VLAN(認証失敗VLAN)から削除します。 認証サーバーが認可VLANを割り当てない場合は、ポートの初期PVIDが適用されます。サーバーと後続のすべての802.1Xサーバーが初期PVIDに割り当てられます。 サーバーがログオフした後、ポートはゲストVLANに割り当てられます。ゲストVLANが設定されていない場合、ポートはポートの初期PVIDに割り当てられます。

MACベースのアクセス制御

認証ステータス	VLAN操作
サーバーがポートにアクセスし、802.1X認証に失敗しました。	デバイスは、サーバーのMACアドレスを802.1X Auth-fail VLAN(認証失敗VLAN)にマッピングします。サーバーがアクセスできるのは、認証失敗VLAN内のリソースだけです。
802.1Xのサーバー Auth-fail VLAN(認証失敗VLAN)は802.1X認証に失敗します。	サーバーはまだAuth-fail VLAN(認証失敗VLAN)にあります。

802.1X Auth-fail VLAN(認証失敗VLAN)のサーバーは、802.1X認証を通過します。	デバイスは、サーバーのMACアドレスを認可VLANに再マップします。 認証サーバーが認可VLANを割り当てない場合、デバイスはサーバーのMACアドレスをポートの最初のPVIDに再マップします。

クリティカルVLAN

ポート上の802.1Xクリティカル VLANは、ISPドメイン内のどのRADIUSサーバーも到達できないために認証に失敗した802.1Xサーバーに対応します。クリティカルVLAN内のサーバーは、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。

クリティカルVLAN機能は、802.1X認証がRADIUSサーバーを介してのみ実行される場合に有効になります。RADIUS認証後に802.1Xサーバーがローカル認証に失敗した場合、サーバーはクリティカルVLANに割り当てられません。認証方式の詳細については、「AAAの設定」を参照してください。

アクセスデバイスは、802.1Xアクセスコントロール方式に基づいて、802.1X対応ポート上でVLANを処理します。

ポートベースのアクセス制御

認証ステータス	VLAN操作
すべてのRADIUSサーバーが到達不能であるため、サーバーがポートにアクセスし、802.1X認証に失敗します。	デバイスはポートをクリティカルVLANに割り当てます。このポート上の802.1Xサーバーおよび後続のすべての802.1Xサーバーは、802.1Xクリティカル VLAN内のリソースだけにアクセスできます。 クリティカルVLAN割り当ては、ポートリンクモードによって異なります。詳細は、「認可VLAN」の表3を参照してください。
すべてのRADIUSサーバーが到達不能であるため、802.1Xクリティカル VLAN内のサーバーは認証に失敗します。	ポートはまだクリティカルVLAN内にあります。
802.1Xクリティカル VLAN内のサーバーは、到達不能サーバー以外の理由で認証に失敗します。	802.1X Auth-fail VLAN(認証失敗VLAN)が設定されている場合、ポートは認証失敗VLANに割り当てられます。802.1X Auth-fail VLAN(認証失敗VLAN)が設定されていない場合、ポートはポートの初期PVIDに割り当てられます。
802.1Xクリティカル VLANのサーバーは、802.1X認証を通過します。	デバイスはポートをサーバーの認可VLANに割り当て、802.1Xクリティカル VLANからポートを削除します。 認証サーバーが認可VLANを割り当てない場合、ポートの初期PVIDが適用されます。サーバーと後続のすべての802.1Xサーバーは、このポートVLANに割り当てられます。 サーバーがログオフした後、ポートはゲストVLANに割り当てられます。802.1Xゲスト VLANが設定されていない場合、ポートの初期PVIDが復元されます。
すべてのRADIUSサーバーが到達不能であるため、802.1Xゲスト VLAN内のサーバーは認証に失敗します。	デバイスはポートを802.1Xクリティカル VLANに割り当て、このポート上のすべての802.1Xサーバーはこの VLANに属します。
802.1X Auth-fail VLAN(認証失敗VLAN)のサーバーは、すべてのRADIUSサーバーが到達不能であるため、認証に失敗します。	ポートはまだ802.1X Auth-fail VLAN(認証失敗VLAN)にあります。このポート上のすべての802.1Xサーバーは、802.1X Auth-fail VLAN(認証失敗VLAN)内のリソースだけにアクセスできます。
認証を通過したサーバーは再認証に失敗します。これは、すべてのRADIUSサーバーが到達不能であり、サーバーがデバイスからログアウトしているためです。	デバイスはポートを802.1Xクリティカル VLANに割り当てます。

到達可能なRADIUSサーバーがないためにポートがクリティカルVLANに追加された場合、デバイスは到達可能なRADIUSサーバーを検出した後に次の動作を実行します。

1. クリティカルVLANからポートを削除します。
2. 認証をトリガーするために、マルチキャストEAP-Request/Identityメッセージをポートから送信します。

MACベースのアクセス制御

認証ステータス	VLAN操作
すべてのRADIUSサーバーが到達不能であるため、サーバーがポートにアクセスし、802.1X認証に失敗します。	デバイスは、サーバーのMACアドレスを802.1Xクリティカル VLANにマッピングします。サーバーは、802.1Xクリティカル VLAN内のリソースだけにアクセスできます。
すべてのRADIUSサーバーが到達不能であるため、802.1Xクリティカル VLAN内のサーバーは認証に失敗します。	サーバーはまだクリティカルVLANに存在します。
802.1Xクリティカル VLAN内のサーバーは、到達不能サーバー以外の理由で802.1X認証に失敗します。	802.1X Auth-fail VLAN(認証失敗VLAN)が設定されている場合、デバイスはサーバーのMACアドレスを認証失敗VLAN IDに再マップします。 802.1X Auth-fail VLAN(認証失敗VLAN)が設定されていない場合、デバイスはサーバーのMACアドレスを初期PVIDに再マップします。
802.1Xクリティカル VLANのサーバーは、802.1X認証を通過します。	デバイスは、サーバーのMACアドレスを認可VLANに再マップします。 認証サーバーがサーバーに認可VLANを割り当てない場合、デバイスはサーバーのMACアドレスをポートの最初のPVIDに再マップします。
すべてのRADIUSサーバーが到達不能であるため、802.1Xゲスト VLAN内のサーバーは認証に失敗します。	デバイスは、サーバーのMACアドレスを802.1Xクリティカル VLANに再マップします。サーバーは、802.1Xクリティカル VLAN内のリソースだけにアクセスできます。
802.1X Auth-fail VLAN(認証失敗VLAN)のサーバーは、すべてのRADIUSサーバーが到達不能であるため、認証に失敗します。	サーバーは802.1X Auth-fail VLAN(認証失敗VLAN)にとどまります。

到達可能なRADIUSサーバーがないためにサーバーがクリティカルVLANに追加された場合、デバイスは到達可能なRADIUSサーバーを検出した後に次の動作を実行します。

1. クリティカルVLANからサーバーを削除します。
2. 再認証のために、ポートからサーバーにユニキャストEAP-Request/Identityメッセージを送信します。

ACL割り当て

認証サーバーで802.1Xサーバーの ACLを指定して、ネットワークリソースへのサーバーのアクセスを制御できます。サーバーが802.1X認証に合格すると、認証サーバーはACLをサーバーのサーバークセスポートに割り当てます。次に、ポートは、ACLに構成されたルールに応じて、サーバーの一致するトラフィックを許可またはドロップします。

認証サーバーはは、ローカルアクセスデバイスまたはRADIUSサーバーを使用できます。いずれの場合も、サーバーはACL番号のみを指定します。ACLを作成し、アクセスデバイスでそのルールを設定する必要があります。

サーバー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。

- アクセスデバイスのACLルールを変更します。
- 認証サーバーで別の許可ACLを指定します。サポートされてい

る許可ACLには、次のタイプがあります。

- 2000～2999の範囲の番号が付けられた基本ACL。
- 3000～3999の範囲で番号付けされた拡張ACL。
- 4000～4999の範囲で番号付けされたレイヤ2 ACL。

認可ACLを有効にするには、ACLがルールとともに存在し、どのルールにもcounting、established、fragment、source-mac、またはloggingキーワードが含まれていないことを確認します。

ACLの詳細については、『Security Command Reference』を参照してください。

サーバープロファイルの割り当て

認証サーバー上で802.1Xサーバーのサーバープロファイルを指定して、ネットワークリソースへのサーバーのアクセスを制御できます。サーバーが802.1X認証に合格すると、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サーバープロファイルをサーバーに割り当てます。

認証サーバーはは、ローカルアクセスデバイスまたはRADIUSサーバーを使用できます。いずれの場合も、サーバーはサーバープロファイル名のみを指定します。アクセスデバイスでサーバープロファイルを設定する必要があります。

サーバーのアクセス権を変更するには、次のいずれかの方法を使用できます。

- アクセスデバイスのサーバープロファイル設定を変更します。
- 認証サーバー上のサーバーに別のサーバープロファイルを指定しま

す。サーバープロファイルの詳細は、「サーバープロファイルの構成」を参照

してください。

定期的な802.1X再認証

定期的な802.1X再認証は、オンラインサーバー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(ACLやVLANなど)を更新します。

定期的なオンラインサーバー再認証機能がイネーブルになっている場合、デバイスは定期的な再認証間隔でオンライン802.1Xサーバーを再認証します。間隔はタイマーによって制御され、タイマーはサーバーが設定できます。定期的な再認証タイマーへの変更は、古いタイマーが期限切れになり、サーバーが認証を通過した後にだけオンラインサーバーに適用されます。

サーバーによって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)と終了アクション(Termination-Actionアトリビュート)の両方が、定期的なオンラインサーバー再認証機能に影響を与える場合があります。サーバーによって割り当てられたSession-TimeoutアトリビュートとTermination-Action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(logoff)の場合、デバイスでの定期的なオンラインサーバー再認証は、定期的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も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サーバ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が満了した後にオンライン802.1Xサーバーを再認証します。

サーバーによってセッションタイムアウトタイマーが割り当てられていない場合、デバイスが定期的な

802.1X再認証を実行するかどうかは、デバイスの定期的再認証設定によって決まります。Session-Timeoutアトリビュートおよび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。

デフォルトでは、802.1X再認証のために到達可能なサーバーがない場合、デバイスはオンライン802.1Xサーバーをログオフします。keep-online機能は、802.1X再認証のために到達可能なサーバーがない場合、認証された802.1Xサーバーをオンラインに維持します。

再認証の前後にオンラインサーバーに割り当てられるVLANは、同じであっても異なっていてもかまいません。

EADアシスタント

Endpoint Admission Defense(EAD)は、ネットワークの脅威防御能力を向上させるためのH3C統合エンドポイントアクセスコントロールソリューションです。このソリューションにより、セキュリティクライアント、セキュリティポリシーサーバー、アクセスデバイス、およびサードパーティサーバーが一緒に動作できるようになります。端末デバイスがEADネットワークにアクセスしようとする場合は、802.1X認証を実行するEADクライアントが必要です。

EADアシスタント機能を使用すると、アクセスデバイスは、EADクライアントをダウンロードおよびインストールするために、サーバーのHTTP要求をリダイレクトURLにリダイレクトできます。この機能により、EADクライアントを展開するための管理タスクが不要になります。

EADアシスタントは、次の機能によって実装されます。

- 無料IP。

  フリーIPは、自由にアクセス可能なネットワークセグメントであり、ソフトウェアやDHCPサーバーなどのネットワークリソースのセットが制限されています。セキュリティ戦略への準拠を保証するために、未認証サーバーはこのセグメントにのみアクセスして操作を実行できます。たとえばサーバーは、ソフトウェアサーバーからEADクライアントをダウンロードしたり、DHCPサーバーからダイナミックIPアドレスを取得したりできます。

- リダイレクトURL。

  非認証802.1XサーバーがWebブラウザーを使用してネットワークにアクセスしている場合、EADアシスタントはサーバーのネットワークアクセス要求を特定のURLにリダイレクトします。たとえば、この機能を使用して、サーバーをEADクライアントソフトウェアのダウンロード・ページにリダイレクトできます。

EADアシスタント機能は、リダイレクトされた各サーバーのリダイレクトURLへのアクセスを開くために、ACLベースのEADルールを自動的に作成します。

EADルールは、ACLリソースを使用して実装されます。EADルールタイマーが期限切れになるか、サーバーが認証を通過すると、ルールは削除されます。サーバーがEADクライアントのダウンロードに失敗した場合、またはタイマーが期限切れになる前にサーバーが認証を通過できなかった場合は、ネットワークに再接続して空きIPにアクセスする必要があります。

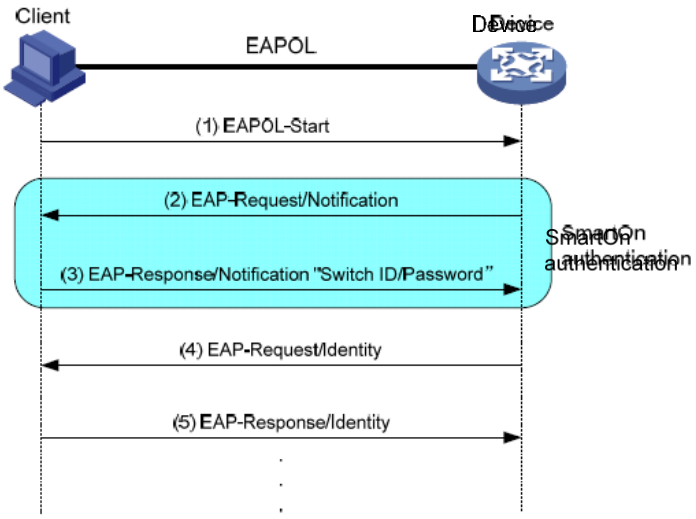
SmartOn

SmartOn機能は、NEC 802.1Xクライアントをサポートするために開発されました。

図11に示すように、アクセスデバイスは802.1X認証の前にSmartOn認証を実行します。次に、認証プロセスを示します。

1. SmartOn対応ポートは、802.1XクライアントからEAPOL-Startパケットを受信すると、SmartOn認証のためにユニキャストEAP-Request/Notificationパケットをクライアントに送信します。
2. クライアントからEAP-Response/Notificationを受信すると、デバイスはパケット内のスイッチIDとパスワードを、デバイスに設定されているスイッチIDとパスワードと比較します。
   - 同じ場合は、802.1X認証を続行できます。
   - 一致しない場合、SmartOn認証は失敗します。アクセスデバイスは、クライアントの802.1X認証を停止します。

図11 SmartOn機能を使用した802.1X認証プロセス



サーバーが別の802.1Xクライアントを認証に使用しようとすると、SmartOn認証に失敗します。アクセスデバイスは、サーバーの802.1X認証を停止します。

注:

SmartOnクライアントソフトウェアをインストールしたら、2つの値QX_IDとQX_PASSWORDをWindowsレジストリキー [HKEY_LOCAL_MACHINE\SOFTWARE\Soliton Systems K.K.\SmartOnClient\Clients\1XGate] に追加します。QX_IDとQX_PASSWORDには、それぞれスイッチIDとパスワードを指定します。スイッチIDとパスワードは、デバイスに設定されているスイッチIDとパスワードと同じである必要があります。

802.1Xの設定

制約事項および注意事項:802.1X設定

802.1Xを実行するようにポートセキュリティ機能を設定できます。ポートセキュリティは、802.1X認証とMAC認証を組み合わせて拡張します。ポートセキュリティは、ポート上のサーバーごとに異なる認証方法を必要とするネットワーク(WLANなど)に適用されます。ポートセキュリティ機能の詳細は、「ポートセキュリティの設定」を参照してください。

ポート上の802.1XゲストVLAN、Auth-fail VLAN(認証失敗VLAN)、またはクリティカルVLANにサーバーが存在する場合は、ポートのリンクタイプを変更しないでください。

802.1X タスク一覧

802.1X認証を設定するには、次のタスクを実行します。

1. 802.1Xのイネーブル化
2. 基本的な802.1X機能の設定
   - EAPリレーまたはEAPターミネーションのイネーブル化
   - ポート許可ステートの設定
   - アクセス制御方式の指定
   - (任意)ポートでの必須認証ドメインの指定
   - (オプション)802.1X認証タイムアウトタイマーの設定
   - (オプション)802.1X再認証の設定
   - (オプション)待機タイマーの設定
3. (任意)802.1X VLAN割り当ての設定
   - 802.1XゲストVLANの設定
   - 802.1X Auth-fail VLAN(認証失敗VLAN)設定
   - 802.1Xクリティカル VLANの設定
4. (オプション)その他の802.1X機能の設定
   - 認証トリガー機能の設定

     802.1Xクライアントが認証を開始できない場合は、次の作業を実行します。
   - ポート上の同時802.1Xサーバーの最大数の設定
   - 認証要求の最大試行回数の設定
   - オンラインサーバーハンドシェイクの設定
   - サポートされているドメイン名区切り文字の指定
   - EADアシスタント機能の設定
   - 802.1X SmartOnの設定

802.1Xの前提条件

802.1Xを設定する前に、次の作業を完了してください。

- 802.1Xサーバー用にISPドメインとAAA方式(ローカルまたはRADIUS認証)を設定します。

- RADIUS認証を使用する場合は、RADIUSサーバー上にサーバーカウントを作成します。
- ローカル認証を使用する場合は、アクセスデバイスでローカルサーバーカウントを作成し、サービスタイプをlan-accessに設定します。

802.1Xのイネーブル化

制約事項およびガイドライン

ポートで802.1Xを有効にするには、グローバルとポートの両方でイネーブルにする必要

があります。リンク集約グループ内のポートでは802.1Xをイネーブルにしないでください。

手順

1. system viewと入力します。
   System-view
2. 802.1Xをグローバルにイネーブルにします。
   dot1x
   デフォルトでは、802.1Xはグローバルにディセーブルです。
3. インタフェースビューを入力してください
   interface *interface-type interface-number*
4. ポートで802.1Xをイネーブルにします。
   dot1x
   デフォルトでは、802.1Xはポート上でディセーブルです。

EAPリレーまたはEAPターミネーションのイネーブル化

このタスクについて

適切なEAPモードを選択するには、次の要素を考慮してください。

- EAPパケットに対するRADIUSサーバーのサポート。
- 802.1XクライアントとRADIUSサーバーでサポートされている認証方式。

制約事項およびガイドライン

- EAPリレーモードが使用されている場合、RADIUSスキームビューで設定されたuser-name-formatコマンドは有効になりません。アクセスデバイスは、クライアントからサーバーに認証データを変更せずに送信します。の詳細については
  user-name-formatコマンド。『User Access and Authentication Command Reference』のAAAコマンドを参照してください。
- 次のいずれかの状況では、EAP終了とEAPリレーの両方を使用できます。
  - クライアントはMD5-Challenge EAP認証だけを使用しています。EAP終了を使用する場合は、アクセスデバイスでCHAP認証をイネーブルにする必要があります。
  - クライアントはINode 802.1Xクライアントであり、サーバー名とパスワードのEAP認証のみを開始します。EAP終了を使用する場合は、アクセスデバイスでPAP認証またはCHAP認証を有効にできます。ただし、セキュリティ上の理由から、アクセスデバイスでCHAP認証を使用する必要があります。
- EAP-TLS、PEAP、またはその他のEAP認証方法を使用するには、EAPリレーを使用する必要

があります。決定する際には、「EAPリレーとEAP終了の比較」を参照してください。

手順

1. system viewと入力します。

   system-view
2. EAPリレーまたはEAPターミネーションを設定します。

   dot1xauthentication-method { **chap** | **eap** | **pap** }

   デフォルトでは、アクセスデバイスはEAP終了を実行し、CHAPを使用してRADIUSサーバーと通信します。

ポート許可ステートの設定

このタスクについて

ポート認可ステートは、クライアントにネットワークへのアクセス権を付与するかどうかを決定します。ポートの次の認可ステートを制御できます。

- Authorized:ポートを許可ステートにして、ポート上のサーバーが認証なしでネットワークにアクセスできるようにします。
- Unauthorized:ポートを無許可ステートにして、ポート上のサーバーからのアクセス要求を拒否します。
- auto:ポートを最初に無許可ステートにして、EAPOLパケットだけが通過できるようにします。サーバーが認証を通過した後、はポートを許可ステートに設定してネットワークへのアクセスを許可します。このオプションは、ほとんどのシナリオで使用できます。

手順

1. system viewと入力します。

   System-view
2. インタフェースビューを入力してください

   interface *interface-type interface-number*
3. ポート認可ステートを設定します。

   dot1x port-control {**authorized-force**|**auto**|**unauthorized-force**}

   デフォルトでは、auto状態が適用されます。

アクセス制御方式の指定

このタスクについて

デバイスは、ポートベースおよびMACベースのアクセス制御方式をサポートします。

手順

1. system viewと入力します。

   System-view
2. インタフェースビューを入力してください

   interface *interface-type interface-number*
3. アクセス制御方式を指定します。

   dot1x port-method {**macbased** | **portbased** }

   デフォルトでは、MACベースのアクセスコントロールが適用されます。

ポート上の必須認証ドメインの指定

このタスクについて

ポートでの認証、認可およびアカウンティングのために、すべての802.1Xサーバーを必須認証ドメインに配置できます。サーバーは、他のドメインのアカウントを使用してポート経由でネットワークにアクセスすることはできません。必須認証ドメインを実装すると、802.1Xアクセス制御配置の柔軟性が向上します。

手順

1. system viewと入力します。

   System-view
2. インタフェースビューを入力してください

   interface *interface-type interface-number*
3. ポートに必須の802.1X認証ドメインを指定します。

   dot1x mandatory-domain *domain-name*

   デフォルトでは、必須の802.1X認証ドメインは指定されていません。

802.1X認証タイムアウトタイマーの設定

このタスクについて

ネットワークデバイスは、次の802.1X認証タイムアウトタイマーを使用します。

- クライアントタイムアウトタイマー:アクセスデバイスが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。このタイマーが経過しても応答が受信されない場合、アクセスデバイスはクライアントに要求を再送信します。
- サーバータイムアウトタイマー:アクセスデバイスが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応答が受信されない場合、802.1X認証は失敗します。

制約事項およびガイドライン

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。

- 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があ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. system viewと入力します。

   System-view
2. クライアントタイムアウトタイマーを設定します。

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

   デフォルトは30秒です。
3. サーバータイムアウトタイマーを設定します。

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

   デフォルトは100秒です。

802.1X再認証の設定

制約事項およびガイドライン

必須認証ドメインまたはEAPメッセージ処理方法の設定を変更しても、オンライン802.1Xサーバーの再認証には影響しません。変更した設定は、変更後にオンラインになった802.1Xサーバーに対してのみ有効です。

手順

1. system viewと入力します。

   System-view
2. (任意)定期的な再認証タイマーを設定します。

   dot1x timerreauth-period *reauth-period-value*

   デフォルト設定は3600秒です。
3. インタフェースビューを入力してください

   interface *interface-type interface-number*
4. 定期的なオンラインサーバー再認証をイネーブルにします。

   dot1x re-authenticate

   デフォルトでは、この機能はディセーブルです。
5. (オプション)802.1Xサーバーに対してキープオンライン機能をイネーブルにします。

   dot1x re-authenticate server-unreachable keep-online

   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再認証のために到達可能な認証サーバーがない場合、デバイスはオンライン802.1Xサーバーをログオフします。

   実際のネットワーク状況に合わせてオンライン状態を維持する機能を使用します。高速回復ネットワークでは、オンライン状態を維持する機能を使用して、802.1Xサーバーが頻繁にオンライン状態になったりオフライン状態になったりするのを防ぐことができます。

待機タイマーの設定

このタスクについて

待機タイマーを使用すると、アクセスデバイスは、802.1X認証に失敗したクライアントからの認証要求を処理できるようになるまで、一定時間待機できます。

制約事項およびガイドライン

ネットワークの状態に応じて、待機タイマーを編集できます。

- 脆弱なネットワークでは、待機タイマーを高い値に設定します。
- 認証応答が迅速な高性能ネットワークでは、待機タイマーを低い値に設定します。

手順

1. system viewと入力します。

   System-view
2. 待機タイマーをイネーブルにします。

   dot1x quiet-period

   デフォルトでは、タイマーはディセーブルです。
3. (任意)待機タイマーを設定します。

   dot1x timer quiet-period *quiet-period-value*

   デフォルトは60秒です。

802.1XゲストVLANの設定

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	ゲストVLANの互換性
WX1800Hシリーズ	WX1804H	EWP-WX1804H-PWR-CN	ない
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	ない
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	ある
WX3500Hシリーズ	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H	しない
WX5500Eシリーズ	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	ある
WX5500Hシリーズ	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	ある
アクセスコントローラモジュール	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM･1 MAC 0 F	LSUM1WCME0 EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM･1 MAC 0 F	ある

ハードウェアシリーズ	モデル	製品コード	ゲストVLANの互換性
WX1800Hシリーズ	WX1804H WX1810H WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	ない
WX3800Hシリーズ	WX3820H	EWP-WX3820H-GL	ある

ハードウェアシリーズ	モデル	製品コード	ゲストVLANの互換性
	WX3840H	EWP-WX3840H-GL	
WX5800Hシリーズ	WX5860H	EWP-WX5860H-GL	ある

制約事項およびガイドライン

- 1つのポートに設定できる802.1XゲストVLANは1つだけです。異なるポート上の802.1XゲストVLANは異なっていてもかまいません。
- ポート上のポートVLANと802.1XゲストVLANに異なるIDを割り当てます。この割り当てにより、ポートが着信VLANタグ付きトラフィックを正しく処理できるようになります。
- ハイブリッドポートでは、ゲストVLANはタグなしVLANだけにできます。
- ポートに複数のセキュリティ機能を設定する場合は、表4のガイドラインに従ってください。

表4 802.1XゲストVLANとその他のセキュリティ機能の関係

機能	リレーションシップの説明	リファレンス
MACベースのアクセスコントロールを実行するポート上の802.1X認証失敗VLAN	802.1X認証失敗VLANには、802.1Xゲスト VLANより高いプライオリティが設定されています。	「802.1X VLAN」を参照 "操作"
MACベースのアクセスコントロールを実行するポートでのポート侵入防御アクション	802.1XゲストVLAN機能は、ブロックMACアクションよりも高いプライオリティを持ちます。 802.1XゲストVLAN機能のプライオリティは、ポート侵入保護機能のshutdown portアクションよりも低くなります。	「ポートセキュリティの設定」を参照してください。

前提条件

802.1XゲストVLANを設定する前に、次の作業を完了してください。

- 802.1XゲストVLANとして指定するVLANを作成します。
- ポートタイプがハイブリッドの場合は、ゲストVLANとして指定されるVLANがポートのタグ付きVLANリストにないことを確認します。

手順

1. system viewと入力します。

   System-view

2. インタフェースビューを入力してください

   interface *interface-type interface-number*

3. ポートで802.1XゲストVLANを設定します。

   dot1x guest-vlan *guest-vlan-id*

   デフォルトでは、ポート上に802.1XゲストVLANは存在しません。

802.1X Auth-fail VLAN(認証失敗VLAN)設定

制約事項およびガイドライン

- ポート上のポートVLAN、音声VLAN、および802.1X Auth-Fail VLAN(認証失敗VLAN)に異なるIDを割り当てます。この割り当てにより、ポートがVLANタグ付き着信トラフィックを正しく処理できるようになります。
- 1つのポートに設定できる802.1X Auth-fail VLAN(認証失敗VLAN)は1つだけです。異なるポート上の802.1X Auth-fail VLAN(認証失敗VLAN)は異なる場合があります。
- ハイブリッドポートでは、Auth-fail VLAN(認証失敗VLAN)はタグなしVLANにしかできません。
- ポートに複数のセキュリティ機能を設定する場合は、表5のガイドラインに従ってください。

表5 802.1X Auth-fail VLAN(認証失敗VLAN)と他の機能との関係

機能	リレーションシップの説明	リファレンス
を実行するポート上のMAC認証 ゲストVLAN MACベースのアクセス制御	802.1X Auth-fail VLAN(認証失敗VLAN)には高いプライオリティがあります。	「MAC認証の設定」を参照してください。
を実行するポートでのポート侵入防御アクション MACベースのアクセス制御	802.1X Auth-fail VLAN(認証失敗VLAN)機能のプライオリティは、block MACアクションよりも高くなります。 802.1X Auth-fail VLAN(認証失敗VLAN)機能のプライオリティは、ポート侵入保護機能のshutdown portアクションよりも低くなります。	「ポートセキュリティの設定」を参照してください。

前提条件

802.1X Auth-fail VLAN(認証失敗VLAN)を設定する前に、次の作業を完了します。

- 802.1X Auth-fail VLAN(認証失敗VLAN)として指定するVLANを作成します。
- ポートタイプがハイブリッドの場合は、Auth-fail VLAN(認証失敗VLAN)として指定されるVLANが、ポートのタグ付きVLANリストにないことを確認します。

手順

1. system viewと入力します。

   System-view
2. インタフェースビューを入力してください

   interface *interface-type interface-number*
3. ポートに802.1X Auth-fail VLAN(認証失敗VLAN)を設定します。

   dot1x auth-fail vlan*authfail-vlan-id*

   デフォルトでは、ポートに802.1X Auth-fail VLAN(認証失敗VLAN)は存在しません。

802.1Xクリティカル VLANの設定

802.1Xクリティカル VLAN設定の制約事項およびガイドライン

- ポート上のPVIDと802.1Xクリティカル VLANに異なるIDを割り当てます。この割り当てにより、ポートがVLANタグ付き着信トラフィックを正しく処理できるようになります。
- 1つのポートに設定できる802.1Xクリティカル VLANは1つだけです。異なるポート上の802.1Xクリティカル VLANは異なる可能性があります。
- ハイブリッドポートでは、クリティカル VLANはタグなしVLANだけにできます。

前提条件

802.1Xクリティカル VLANを設定する前に、次の作業を完了してください。

- クリティカル VLANとして指定するVLANを作成します。
- ポートタイプがハイブリッドの場合は、クリティカル VLANとして指定されるVLANがポートのタグ付きVLANリストにないことを確認します。

手順

1. system viewと入力します。

   System-view

2. インタフェースビューを入力してください

   interface *interface-type interface-number*
3. ポートに802.1Xクリティカル VLANを設定します。

   dot1x critical vlan*critical-vlan-id*

   デフォルトでは、ポートに802.1Xクリティカル VLANは存在しません。

認証トリガー機能の設定

このタスクについて

認証トリガー機能を使用すると、802.1Xクライアントが認証を開始できない場合にアクセスデバイスが802.1X認証を開始できます。

この機能は、マルチキャストトリガーとユニキャストトリガーを提供します(「802.1X概要」の802.1X認証の開始を参照)。

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	ユニキャストトリガーの互換性
WX1800Hシリーズ	WX1804H	EWP-WX1804H-PWR-CN	ない
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	ない
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	ある
WX3500Hシリーズ	WX3508H WX3510H WX3520H WX3520H-F WX3540H	EWP-WX3508H EWP-WX3510H EWP-WX3520H EWP-WX3520H-F EWP-WX3540H	ない
WX5500Eシリーズ	WX5510E WX5540E	EWP-WX5510E EWP-WX5540E	ある
WX5500Hシリーズ	WX5540H WX5560H WX5580H	EWP-WX5540H EWP-WX5560H EWP-WX5580H	ある
アクセスコントローラモジュール	LSUM1WCME0	LSUM1WCME0	ある

ハードウェアシリーズ	モデル	製品コード	ユニキャストトリガーの互換性
	EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM・1 MAC 0 F	EWPXM1WCME0 LSQM1WCMX20 LSUM1WCMX20RT LSQM1WCMX40 LSUM1WCMX40RT EWPXM2WCMD0F EWPXM・1 MAC 0 F	

ハードウェアシリーズ	モデル	製品コード	ユニキャストトリガーの互換性
WX1800Hシリーズ	WX1804H WX1810H WX1820H WX1840H	EWP-WX1804H-PWR EWP-WX1810H-PWR EWP-WX1820H EWP-WX1840H-GL	ない
WX3800Hシリーズ	WX3820H WX3840H	EWP-WX3820H-GL EWP-WX3840H-GL	ある
WX5800Hシリーズ	WX5860H	EWP-WX5860H-GL	ある

制約事項およびガイドライン

- ポートに接続されたクライアントがEAPOL-Startパケットを送信して802.1X認証を開始できない場合に、ポートでマルチキャストトリガーをイネーブルにします。
- 無線LANでマルチキャストトリガーを無効にします。無線クライアントとアクセスデバイスの無線モジュールはどちらも802.1X認証を開始できます。
- 少数の802.1Xクライアントだけがポートに接続されていて、これらのクライアントが認証を開始できない場合は、ポートでユニキャストトリガーをイネーブルにします。
- 認証パケットの重複を避けるために、ポート上で両方のトリガーをイネーブルにしないでください。

手順

1. system viewと入力します。

   System-view
2. (任意)サーバー名要求タイムアウトタイマーを設定します。

   dot1x timer tx-period *tx-period-value*

   デフォルトは30秒です。
3. インタフェースビューを入力してください

   interface *interface-type interface-number*
4. 認証トリガーをイネーブルにします。

   dot1x {**multicast-trigger** |**unicast-trigger**}

   デフォルトでは、マルチキャストトリガーはイネーブルで、ユニキャストトリガーはディセーブルです。

ポート上の同時802.1Xサーバーの最大数の設定

このタスクについて

システムリソースが過剰に使用されないようにするには、次の作業を実行します。

手順

1. system viewと入力します。
   System-view
2. インタフェースビューを入力してください
   interface *interface-type interface-number*
3. ポート上の同時802.1Xサーバーの最大数を設定します。
   dot1xmax-user *max-number*
   デフォルトは4294967295です。

認証要求の最大試行回数の設定

このタスクについて

アクセスデバイスは、クライアントから一定期間内に要求に対する応答を受信しなかった場合、認証要求を再送信します。時間を設定するには、dot1x timer tx-period tx-period-valueコマンドまたはdot1x timer supp-timeout supp-timeout-valueコマンドを使用します。アクセスデバイスは、最大回数の要求送信を試行したにもかかわらず応答がない場合、要求の再送信を停止します。

手順

1. system viewと入力します。
   System-view
2. 認証要求の送信の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。

オンラインサーバーハンドシェイクの設定

このタスクについて

オンラインサーバーハンドシェイク機能は、オンライン802.1Xサーバーの接続ステータスをチェックします。アクセスデバイスは、dot1x timer handshake-periodコマンドで指定された間隔で、オンラインサーバーにハンドシェイク要求(EAP-Request/Identity)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サーバーからEAP-Response/Identityパケットを受信しない場合、デバイスはサーバーをオフライン状態に設定します。最大ハンドシェイク試行を設定するには、dot1x retryコマンドを使用します。

通常、デバイスは802.1XクライアントのEAP-XクライアントのEAP-Response/Identityパケットに応答しません。一部の802.1Xクライアントは、ハンドシェイク用のEAP-Successパケットを受信しないとオフラインになります。この問題を回避するには、オンラインサーバーハンドシェイク応答機能を有効にします。

INodeクライアントがデプロイされている場合は、オンラインサーバーハンドシェイクセキュリティ機能を有効にして、クライアントからのハンドシェイクパケット内の認証情報をチェックすることもできます。この機能により、不正なクライアントソフトウェアを使用する802.1Xサーバーが、デュアルネットワークインタフェースカード(NIC)検出などのINodeセキュリティチェックをバイパスすることを防止できます。サーバ

ーがハンドシェイクセキュリティチェックに失敗した場合、デバイスはサーバーをオフライン状態に設定します。

制約事項およびガイドライン

- ネットワークに、アクセスデバイスとハンドシェイクパケットを交換できない802.1Xクライアントがある場合は、オンラインサーバーハンドシェイク機能をディセーブルにします。この操作により、802.1X接続が誤って切断されるのを防ぎます。
- SmartOn機能とオンラインサーバーハンドシェイク機能は相互に排他的です。オンラインサーバーハンドシェイク機能を有効にする前に、SmartOn機能が無効になっていることを確認してください。
- オンラインサーバーハンドシェイクセキュリティ機能を使用するには、オンラインサーバーハンドシェイク機能が有効になっていることを確認します。
- オンラインサーバーハンドシェイクセキュリティ機能は、INodeクライアントとIMCサーバーが使用されているネットワークでのみ有効です。
- 802.1Xクライアントがデバイスから EAP-Successパケットを受信せずにオフラインになる場合に限り、オンラインサーバーハンドシェイク応答機能をイネーブルにします。

手順

1. system viewと入力します。

   System-view
2. (任意)ハンドシェイクタイマーを設定します。

   dot1x timerhandshake-period *handshake-period-value*

   デフォルトは15秒です。
3. インタフェースビューを入力してください

   interface *interface-type interface-number*
4. オンラインサーバーハンドシェイク機能をイネーブルにします。

   dot1x handshake

   デフォルトでは、この機能はイネーブルです。
5. (オプション)オンラインサーバ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

   デフォルトでは、この機能はディセーブルです。
6. (任意)802.1Xオンラインサーバーハンドシェイク応答機能をイネーブルにします。

   dot1x handshake reply enable

   デフォルトでは、デバイスは、オンラインハンドシェイクプロセス中に802.1XクライアントのEAP-Response/Identityパケットに応答しません。

サポートされているドメイン名区切り文字の指定

このタスクについて

デフォルトでは、アクセスデバイスは区切り文字としてアットマーク(@)をサポートしています。他のドメイン名区切り文字を使用する802.1Xサーバーに対応するようにアクセスデバイスを設定することもできます。設定可能な区切り文字には、アットマーク(@)、バックスラッシュ(\)、ドット(.)、スラッシュ(/)があります。ドメイン名を含むサーバー名は、username@domain-name、domain-name\username、username.domain-name、またはusername/domain-nameの形式を使用できます。

802.1Xサーバー名文字列に複数の構成済デリミタが含まれている場合、右端のデリミタはドメイン名デリミタです。たとえば、バックスラッシュ(\)、ドット(.)およびスラッシュ(/)を構成した場合デリミタとして、

サーバー名文字列121.123/22\@abcのドメイン名デリミタはバックスラッシュ(\)です。サーバー名は@abc、ドメイン名は121.123/22です。

制約事項およびガイドライン

サーバー名ストリングに区切り文字が含まれていない場合、アクセスデバイスは、必須またはデフォルトのISPドメインでサーバーを認証します。

ドメイン名を含むサーバー名をRADIUSサーバーに送信するようにアクセスデバイスを設定する場合は、RADIUSサーバーがドメインデリミタを認識できることを確認します。サーバー名フォーマットの設定については、『User Access and Authentication Command Reference』のuser-name-formatコマンドを参照してください。

手順

1. system viewと入力します。

   System-view
2. 802.1Xサーバーのドメイン名区切り文字のセットを指定します。

   dot1x domain-delimiter *string*

   デフォルトでは、アットマーク(@)デリミタのみがサポートされています。

EADアシスタント機能の設定

制約事項およびガイドライン

- EADアシスタント機能をイネーブルにする前に、MAC認証とポートセキュリティをグローバルにディセーブルにする必要があります。
- 802.1 X対応ポートでEADアシスタント機能を有効にするには、ポート認可モードをautoに設定する必要があります。
- グローバルMAC認証またはポートセキュリティがイネーブルの場合、フリーIPは有効になりません。
- 802.1XゲストVLAN機能を正しく動作させるには、EADアシスタントを802.1XゲストVLAN機能とともにイネーブルにしないでください。
- フリーIPとAuth-fail VLAN(認証失敗VLAN)機能を一緒に使用する場合は、認証失敗VLAN内のリソースがフリーIPセグメント上にあることを確認してください。
- サーバーが802.1X認証を通過する前にダイナミックIPアドレスを取得できるようにするには、DHCPサーバーが空きIPセグメント上にあることを確認します。
- リダイレクトURLを提供するサーバーは、非認証サーバーがアクセスできるフリーIP上にある必要があります。

手順

1. system viewと入力します。

   System-view
2. EADアシスタント機能を有効にします。

   dot1x ead-assistant enable

   デフォルトでは、この機能は無効です。
3. フリーIPを設定します。

   dot1x ead-assistant free-ip *ip-address* {*mask-length*|*mask-address* }

デフォルトでは、空きIPは存在しません。

複数の空きIPを設定するには、このコマンドを繰り返します。

4. (オプション)サーバーがWebブラウザーを使用してネットワークにアクセスする場合は、リダイレクトURLを設定します。

   dot1x ead-assistant url *url-string*

   デフォルトでは、リダイレクトURLは存在しません。

5. (任意)EADルールタイマーを設定します。

   dot1x timer ead-timeout *ead-timeout-value*

   デフォルト設定は30分です。

   多数のEADサーバーが存在する場合にACLリソースの使用を回避するには、EADルールタイマーを短縮します。

802.1X SmartOnの設定

このタスクについて

デバイスがユニキャストEAP-Request/Notificationパケットをクライアントに送信すると、SmartOnクライアントタイムアウトタイマー(dot1x smarton timer supp-timeoutコマンドを使用して設定)が開始されます。

- デバイスがタイムアウトタイマー内にクライアントからEAP-Response/Notificationパケットを受信しなかった場合、デバイスはEAP-Request/Notificationパケットをクライアントに再送信します。デバイスは最大再送信試行を行い、応答を受信しなかった後、クライアントの802.1X認証プロセスを停止します。
- デバイスがEAP-Response/Notificationパケットを受信したEAP-Response/Notificationパケットを受信した場合、デバイスはSmartOn認証を開始します。パケット内のSmartOnスイッチIDとSmartOnパスワードのMD5ダイジェストがデバイス上のものと一致する場合、クライアントの802.1X認証は継続されます。一致しない場合、デバイスはクライアントの802.1X認証要求を拒否します。

制約事項およびガイドライン

SmartOn機能は、802.1Xオンラインサーバーハンドシェイク機能と相互に排他的です。

手順

1. system viewと入力します。

   System-view

2. インタフェースビューを入力してください

   interface *interface-type interface-number*

3. ポートでSmartOn機能をイネーブルにします。

   dot1x smarton

   デフォルトでは、この機能はディセーブルです。

4. システムビューに戻ります。

   quit

5. SmartOnスイッチIDを設定します。

   dot1x smarton switched *switch-string*

   デフォルトでは、SmartOnスイッチIDは存在しません。

6. SmartOnパスワードを設定します。

dot1x smarton password{**cipher**|**simple**}*string*

デフォルトでは、SmartOnパスワードは存在しません。

7. (任意)SmartOnクライアントのタイムアウトタイマーを設定します。
   dot1x smarton timer supp-timeout *supp-timeout-value*

   デフォルトのタイマーは30秒です。

8. (任意)EAP-Request/Notificationパケットをクライアントに再送信する最大試行回数を設定します。

   dot1x smarton retry *retries*

   デフォルトでは、デバイスはEAP-Request/Notificationパケットをクライアントに再送信する最大3回の試行を許可します。

802.1Xの表示および保守コマンド

重要:

WX1800Hシリーズ、WX2500Hシリーズ、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。

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

タスク	コマンド
指定されたポートまたはすべてのポートの802.1Xセッション情報、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802.1Xサーバー情報を表示します。	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: 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]*
ポート上の802.1Xゲスト VLANからサーバーを削除します。	reset dot1x guest-vlan interface interface-type interface-number [mac-address mac-address]
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]

802.1Xのトラブルシューティング

EADアシスタントURLリダイレクションの失敗

症状

非認証サーバーは、Webブラウザーに外部Webサイトアドレスを入力した後、指定されたリダイレクトURLにリダイレクトされません。

解析

リダイレクトは、次のいずれかの理由で実行されません。

- アドレスは文字列フォーマットです。ホストのオペレーティングシステムは文字列をWebサイト名とみなし、文字列を解決しようとします。解決に失敗した場合、オペレーティンシステムはARP要求を送信しますが、ターゲットアドレスはドット付き10進表記ではありません。リダイレクション機能は、この種のARP要求をリダイレクトします。
- アドレスは空きIPセグメント内にあります。アドレスにホストが存在しない場合でも、リダイレクトは行われません。
- リダイレクトURLがフリーIPセグメント内にありません。
- リダイレクトURLを使用しているサーバーがないか、URLを持つサーバーがWebサービスを提供していません。

ソリューション

この問題を解決するには、次の手順に従います

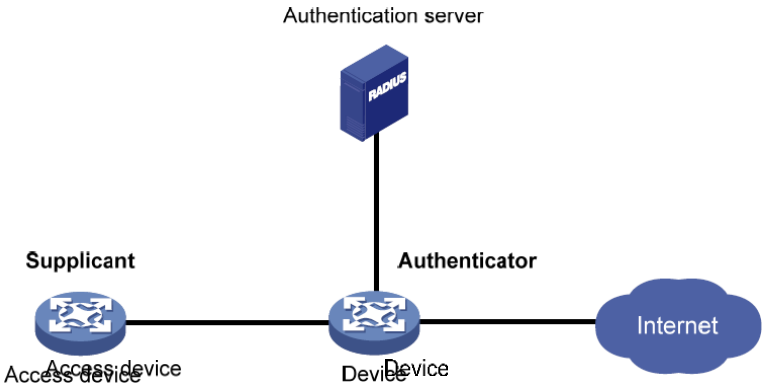
1. 空きIPセグメントに含まれないドット付き10進IPアドレスを入力します。
2. アクセスデバイスとサーバーが正しく設定されていることを確認します。
3. 問題が解決しない場合は、H3Cサポートに連絡してください。

802.1Xクライアントの設定

802.1Xクライアントについて

図1に示すように、802.1Xクライアント機能により、アクセスデバイスは802.1Xアーキテクチャでサプリカントとして動作できます。802.1Xアーキテクチャの詳細は、「802.1Xの概要」を参照してください。

図1 802.1Xクライアントのネットワーク図



制約事項および注意事項:802.1Xクライアント設定

注意して802.1Xクライアント機能を無効にしてください。この操作により、すべてのオンラインユーザーがログオフされます。

802.1Xクライアントタスクの一覧表示

802.1Xクライアントを設定するには、次のタスクを実行します。

1. 802.1Xクライアント機能の有効化
2. 802.1Xクライアントのユーザ名とパスワードの設定
3. 802.1XクライアントのEAP認証方式の指定
4. (オプション)802.1Xクライアント匿名IDの設定

802.1Xクライアント機能の有効化

1. system viewと入力します。
   System-view
2. 手動APを作成し、APビューを開始します。
   wlan ap *ap-name* [**model** *model-name*]
   APを作成するときは、モデル名を指定する必要があります。
3. APプリプロビジョニングをイネーブルにし、APプロビジョニングビューを開始します。
   provision
   デフォルトでは、APプリプロビジョニングはディセーブルです。

4. 802.1Xクライアント機能をイネーブルにします。

   dot1x supplicant enable

   デフォルトでは、802.1Xクライアント機能はディセーブルです。

802.1Xクライアントのユーザ名とパスワードの設定

制約事項およびガイドライン

認証を成功させるには、デバイスに設定されているユーザ名とパスワードが、認証サーバーに設定されているユーザ名とパスワードと一致していることを確認します。

手順

1. system viewと入力します。

   System-view

2. 手動APを作成し、APビューを開始します。

   wlan ap *ap-name* [**model** *model-name*]

3. APプリプロビジョニングをイネーブルにし、APプロビジョニングビューを開始します。

   provision

4. 802.1Xクライアントユーザ名を設定します。

   dot1x supplicant username *username*

   デフォルトでは、802.1Xクライアントユーザ名は設定されていません。

5. 802.1Xクライアントパスワードを設定します。

   dot1x supplicant password {**cipher** | **simple** } *string*

   デフォルトでは、802.1Xクライアントパスワードは設定されていません。

802.1XクライアントのEAP認証方式の指定

このタスクについて

802.1Xクライアント機能では、次のEAP認証方式を使用できます。

- MD 5-チャレンジ
- PEAP-MSCHAPv2.
- PEAP-GTC.
- TTLS-MSCHAPv2.
- TTLS-GTC.

制約事項およびガイドライン

- 次の表は、802.1Xクライアントおよびオーセンティケータでの認証方式の選択に関する制約事項を示しています。

802.1Xクライアントで指定された認証方式	オーセンティケータで指定されたパケット交換方式
MD 5-チャレンジ	• EAPリレー • EAP終了
• PEAP-MSCHAPv2	EAPリレー

802.1Xクライアントで指定された認証方式	オーセンティケータで指定されたパケット交換方式
• PEAP-GTC • TTLS-MSCHAPv2 • TTLS-GTC(TTLS-GTC)	

802.1Xパケット交換方式について詳しくは、「802.1Xの設定」を参照してください。

- 指定された802.1XクライアントEAP認証方式が認証サーバーでサポートされていることを確認します。

手順

1. system viewと入力します。

   System-view
2. 手動APを作成し、APビューを開始します。

   wlan ap *ap-name* [**model** *model-name*]
3. APプリプロビジョニングをイネーブルにし、APプロビジョニングビューを開始します。

   provision
4. 802.1XクライアントEAP認証方式を指定します。

   dot1x supplicant eap-method { **md5** | **peap-gtc** | **peap-mschapv2** | **ttls-gtc** | **ttls-mschapv2** }

   デフォルトでは、802.1Xクライアント対応デバイスはMD5-Challenge EAP認証を使用します。

802.1Xクライアント匿名IDの設定

このタスクについて

最初の認証フェーズでは、オーセンティケータに送信されるパケットは暗号化されません。802.1Xクライアントの匿名IDを使用すると、最初のフェーズで802.1Xクライアントのユーザ名が開示されるのを防ぐことができます。802.1Xクライアント対応デバイスは、802.1Xクライアントのユーザ名ではなく匿名IDをオーセンティケータに送信します。802.1Xクライアントのユーザ名は、2番目のフェーズで暗号化されたパケットでオーセンティケータに送信されます。

802.1Xクライアントの匿名IDが設定されていない場合、デバイスは最初の認証フェーズで802.1Xクライアントのユーザ名を送信します。

設定された802.1Xクライアント匿名IDは、次のいずれかのEAP認証方式が使用されている場合にだけ有効になります。

- PEAP-MSCHAPv2.
- PEAP-GTC.
- TTLS-MSCHAPv2.
- TTLS-GTC.

MD 5チャレンジEAP認証が使用されている場合、設定された802.1Xクライアントの匿名IDは有効になりません。デバイスは最初の認証フェーズで802.1Xクライアントのユーザ名を使用します。

制約事項およびガイドライン

ベンダー固有の認証サーバーが匿名IDを識別できない場合は、802.1Xクライアントの匿名IDを設定しないでください。

手順

1. system viewと入力します。
   System-view
2. 手動APを作成し、APビューを開始します。
   wlan ap *ap-name* [**model** *model-name*]
3. APプリプロビジョニングをイネーブルにし、APプロビジョニングビューを開始します。
   provision
4. 802.1Xクライアントの匿名IDを設定します。
   dot1x supplicant anonymous identify *identifier*
   デフォルトでは、802.1Xクライアントの匿名IDは設定されていません。

802.1Xクライアントの設定例

このドキュメントに記載されている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クライアントの設定

ネットワーク構成

図2に示すように、スイッチはオーセンティケータとして動作し、ポートGigabitEthernet 1/0/1に接続するAPに対して802.1X認証を実行します。

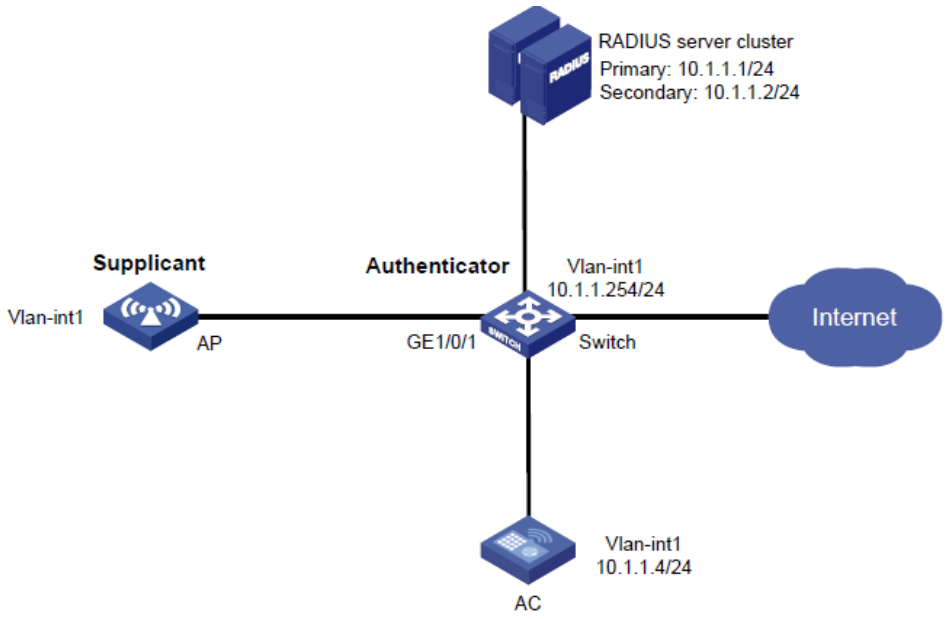
ACで次のタスクを実行します。

- APの802.1Xクライアント機能をイネーブルにします。
- APに次の802.1Xクライアントパラメータを設定します。
  - 認証ユーザ名をaaaとして設定します。
  - パスワードをプレーンテキスト形式で123456に設定します。
  - EAP認証方式としてPEAP-MSCHAPv2を指定します。
- 802.1Xクライアント設定をAP上のコンフィギュレーションファイルに保存します。

次の要件を満たすようにスイッチを設定します。

- RADIUSサーバーを使用して、APの認証と認可を実行します。
- スイッチがRADIUSサーバーと通信するためのEAPリレーをイネーブルにします。
- APをISPドメインbbbに割り当てます。
- 共有キーをnameに設定して、スイッチとRADIUSサーバー間のセキュアな通信を実現します。
- APに802.1Xポートベースのアクセスコントロールを実装します。

図2 ネットワーク図



ACの設定

1. 各インターフェイスにIPアドレスを割り当てます(詳細は省略)。
2. 802.1Xクライアント機能を設定します。

#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> system-view

[AC] wlan ap ap1 model WA6638-JP

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

#APプリプロビジョニングを有効にして、APプロビジョニングビューに入ります。

[AC-wlan-ap-ap1] provision

#802.1Xクライアントの EAP認証方式としてPEAP-MSCHAPv2を指定します。

[AC-wlan-ap-ap1-prvs] dot1x supplicant eap-method peap-mschapv2

#802.1Xクライアントのユーザ名をaaaに設定し、パスワードをプレーンテキスト形式で123456に設定します。

[AC-wlan-ap-ap1-prvs] dot1x supplicant username aaa

[AC-wlan-ap-ap1-prvs] dot1x supplicant password simple 123456

#802.1Xクライアントの匿名IDをbbbに設定します。

[AC-wlan-ap-ap1-prvs] dot1x supplicant anonymous identify bbb

#802.1Xクライアント機能を有効にします。

[AC-wlan-ap-ap1-prvs] dot1x supplicant enable

#APプロビジョニングビューの802.1Xクライアント設定をAP ap1上のwlan_ap_prvs.xml設定ファイルに保存する

[AC-wlan-ap-ap1-prvs] save wlan ap provision name ap1

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

[AC-wlan-ap-ap1] quit

スイッチの設定

ここでは、RADIUSを設定するためのコマンドについて説明します。これらのコマンドの詳細については、『User Access and Authentication Command Reference』のAAAコマンドを参照してください。

1. RADIUSサーバーを設定し、ユーザアカウントを追加して、認証および許可サービスが正しく機能することを確認します(詳細は省略)。
2. 各インターフェイスにIPアドレスを割り当てます(詳細は省略)。
3. RADIUSスキームを設定します。

   #radius1という名前のRADIUSスキームを作成し、RADIUSスキームビューに入ります。

   <Switch> system-view

   [Switch] radius scheme radius1

   #プライマリ認証RADIUSサーバーのIPアドレスを指定します。

   [Switch-radius-radius1] primary authentication 10.1.1.1

   #セカンダリ認証RADIUSサーバーのIPアドレスを指定します。

   [Switch-radius-radius1] secondary authentication 10.1.1.2

#スイッチと認証RADIUSサーバー間の共有キーを指定します。

[Switch-radius-radius1] key authentication simple name

4. 次のようにISPドメインを設定します。

#bbbという名前のISPドメインを作成し、ISPドメインビューに入ります。

[Switch] domain name bbb

#ISPドメインbbbの802.1Xクライアントに対して、RADIUSスキームradius1に基づいて認証と認可を実行します。

[Switch-isp-bbb] authentication lan-access radius-scheme radius1

[Switch-isp-bbb] authorization lan-access radius-scheme radius1

[Switch-isp-bbb] accounting lan-access none

[Switch-isp-bbb] quit

5. 802.1Xを設定します。

#EAPリレーを有効にします。

[Switch] dot1x authentication-method eap

#ポートGigabitEthernet 1/0/1でポートベースのアクセスコントロールをイネーブルにします。

[Switch] interface gigabitethernet 1/0/1

[Switch-GigabitEthernet1/0/1] dot1x port-method portbased

#ISPドメインbbbを必須ドメインとして指定します。

[Switch-GigabitEthernet1/0/1] dot1x mandatory-domain bbb

#GigabitEthernet 1/0/1で802.1xをイネーブルにします。

[Switch-GigabitEthernet1/0/1] dot1x

[Switch-GigabitEthernet1/0/1] quit

#802.1Xをグローバルにイネーブルにします。

[Switch] dot1x

設定の確認

オンラインの 802.1X クライアント情報を表示します。

[Switch] display dot1x connection

Total connections: 1

User MAC address: 70f9-6dd7-d1e0

Access interface: GigabitEthernet1/0/1

Username: aaa

Authentication domain: bbb

Authentication method: EAP Initial VLAN: 1

Authorization untagged VLAN: N/A

Authorization tagged VLAN list: N/A

Authorization ACL ID: N/A

Authorization user profile: N/A

Termination action: N/A

Session timeout period: N/A

Online from: 2015/06/16 19:10:32

Online duration: 0h 1m 1s