



# H3C S5560X-EI スイッチシリーズ セキュリティコンフィギュレーションガイド



New H3C Technologies Co., Ltd.  
<http://www.h3c.com>

ソフトウェアバージョン: Release 1118、Release 1118P07  
文書バージョン: 6W101-20180821

**無断転載を禁じます。**

本書のいかなる部分も、New H3C Technologies Co.,Ltd.の書面による事前の同意なしに、いかなる形式または手段によっても複製または配布することはできません。

**商標**

H3C, **H3C**, H3CS, H3CIE, H3CNE, Aolynk, , H<sup>3</sup>Care, , IRF, NetPilot, Netflow, SecEngine, SecPath, SecCenter, SecBlade, Comware, ITCMM および HUASAN は、New H3C Technologies Co.,Ltd.の商標です。

その他のすべての商標は、各所有権者の財産です。

**注意**

このドキュメントの情報は、予告なく変更されることがあります。このドキュメントのすべての内容(説明、情報、推奨事項を含む)は正確であると考えられますが、明示的であるか黙示的であるかを問わず、いかなる種類の保証もなく提示されます。H3C は、このドキュメントに含まれる技術的または編集上の誤りや脱落について責任を負いません。

# はじめに

このコンフィギュレーションガイドでは、スイッチの導入に役立つ次の機能と作業について説明します。

- AAA や PKI などの ID 認証機能。
- 公開鍵管理、IPsec、SSH などのデータ セキュリティ機能。
- IP ソース ガードや ARP 攻撃保護などの攻撃保護機能。

ここでは、マニュアルに関する次のトピックについて説明します。

- 対象者
- 表記法
- 文書のフィードバック

## 対象者

このマニュアルの対象者:

- ネットワークプランナー。
- フィールドテクニカルサポート/サービスエンジニア
- S5560X-EI スイッチシリーズを使用するネットワーク管理者

## 表記法

ここでは、マニュアルで使用されている表記法について説明します。

コマンドの表記法





規約	説明
太字	太字のテキストは、文字どおりに入力したコマンドとキーワードを示します。
イタリック体	斜体のテキストは、実際の値に置き換える引数を表します。
[ ]	角カッコは、オプションの構文選択(キーワードまたは引数)を囲みます。
{ x   y   ... }	中カッコは、必要な構文の選択肢を縦棒で区切って囲みます。この中から1つを選択します。
[ x   y   ... ]	角カッコは、オプションの構文選択のセットを縦棒で区切って囲みます。この中から1つまたは何も選択しません。
{ x   y   ... } *	アスタリスクの付いた中括弧は、必須構文の選択肢を縦棒で区切って囲みます。この中から少なくとも1つを選択します。
[ x   y   ... ] *	アスタリスクの付いた角括弧は、オプションの構文選択肢を縦棒で区切って囲みます。選択肢は1つ、複数、または何も選択しません。
&<1-n>	アンパサンド(&)記号の前の引数またはキーワードと引数の組み合わせは、1～n回入力できます。
#	シャープ記号(#)で始まる行はコメントです。

## GUI のルール













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

規約	説明
>	マルチレベルメニューは、File > Create > Folderのように、山かっこで区切られています。

## シンボル

規約	説明
 <b>警告!</b>	重要な情報を理解していない場合や、その情報に従っていない場合に、けがをするおそれがある場合に注意を促す警告。
 <b>注意:</b>	重要な情報が理解されていない場合、または情報が理解されていない場合に、データの損失、データの破損、またはハードウェアやソフトウェアの損傷につながる可能性がある場合に、注意を促す警告。
 <b>重要:</b>	重要な情報への注意を喚起するアラート。
<b>注:</b>	追加情報または補足情報を含むアラート。
 <b>ヒント:</b>	役立つ情報を提供するアラート。

## ネットワークポロジアイコン

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

## **本書に記載されている例**

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

## **文書のフィードバック**

製品マニュアルに関するコメントは、[info@h3c.com](mailto:info@h3c.com) まで電子メールでお送りください。

ご意見をお寄せください。

# 目次

AAA の設定 .....	13
AAA について .....	13
AAA 実装 .....	13
AAA ネットワーク図 .....	13
RADIUS .....	14
HWTACACS .....	17
LDAP .....	20
ISPドメインとユーザーアクセスデータベースのユーザー管理 .....	23
認証、許可と会計方法 .....	24
AAA 拡張機能 .....	25
VPN 用 AAA .....	25
デバイスの RADIUS サーバー機能 .....	25
プロトコルおよび標準 .....	26
FIPS 準拠 .....	28
AAA タスクの概要 .....	28
ローカルユーザーの構成 .....	28
ローカルユーザーについて .....	28
ローカルユーザー設定タスクの概要 .....	29
ユーザーグループ属性の構成 .....	32
ローカルユーザー自動削除機能の設定 .....	33
ローカルユーザーおよびローカルユーザーグループの表示およびメンテナンスコマンド .....	33
RADIUS タスクの概要 .....	34
RADIUS 設定の制約事項およびガイドライン .....	35
RADIUS サーバーステータス検出用のテストプロファイルの設定 .....	35
RADIUS スキームの作成 .....	35
セキュア RADIUS 通信用の共有キーの指定 .....	37
RADIUS スキームの MPLS L3VPN インスタンスの指定 .....	38
RADIUS サーバーのステータスの設定 .....	38
RADIUS タイマーの設定 .....	39
発信 RADIUS パケットの送信元 IP アドレスの指定 .....	41
RADIUS 要求送信の最大試行回数の設定 .....	42
SSH、FTP、および端末ユーザーのログインサービス属性チェック方法の設定 .....	43
RADIUS クラス属性の CAR パラメーターとしての解釈 .....	44
Remanent_Volume 属性のデータ測定単位の設定 .....	44
強制的に stop-accounting パケットを送信できるようにする .....	47
RADIUS アカウンティングオン機能の設定 .....	48
RADIUS の表示およびメンテナンスコマンド .....	50
RADIUS サーバー機能の設定 .....	51
RADIUS サーバーの機能タスクの概要 .....	51
RADIUS サーバー機能の制約事項およびガイドライン .....	51
RADIUS ユーザーの設定 .....	51
RADIUS ユーザーおよびクライアントの表示およびメンテナンスコマンド .....	52
接続記録ポリシーの設定 .....	52
接続記録ポリシーについて .....	52
制約事項とガイドライン .....	52
手順 .....	52
接続記録ポリシーの表示およびメンテナンスコマンド .....	53
AAA 設定例 .....	53
例:HWTACACS サーバーによる SSH ユーザー用の AAA の設定 .....	53
例:SSH ユーザーのローカル認証、HWTACACS 許可、および RADIUS アカウンティングの設定 .....	54
例:RADIUS サーバーによる SSH ユーザーの認証および認可の設定 .....	56

例:LDAP サーバーによる SSH ユーザーの認証の設定	59
例:RADIUS サーバーによる 802.1X ユーザーの AAA の設定	63
例:デバイスを RADIUS サーバーとして 802.1X ユーザーの認証と許可設定する	68
AAA のトラブルシューティング	71
RADIUS 認証の失敗	71
RADIUS パケット配信障害	71
RADIUS アカウティングエラー	72
HWTACACS のトラブルシューティング	72
LDAP 認証エラー	72
付録	73
付録 A 一般的に使用される RADIUS アトリビュート	73
付録 B 一般的に使用される標準 RADIUS アトリビュートの説明	74
付録 C RADIUS サブアトリビュート(ベンダーID25506)	76
<b>802.1X の概要</b>	<b>80</b>
802.1X プロトコルについて	80
802.1X アーキテクチャ	80
制御/非制御ポートおよびポート許可ステータス	80
パケット交換方式	81
パケット形式	82
802.1X 認証手順	84
802.1X 認証の開始	86
アクセス制御方式	87
802.1X VLAN 操作	87
認証 VLAN	87
ゲスト VLAN	90
認証失敗 VLAN	91
クリティカル VLAN	92
クリティカル Voice VLAN	94
802.1X VSI 操作	94
VXLAN の 802.1X サポート	94
認証 VSI	95
ゲスト VSI	95
認証失敗 VSI	96
クリティカル VSI	96
ACL の割り当て	97
ユーザープロファイルの割り当て	97
リダイレクト URL の割り当て	98
CAR アトリビュートの割り当て	98
定期的な 802.1X 再認証	98
EAD アシスタント	99
802.1X の設定	100
制約事項および注意事項:802.1X 設定	100
802.1X タスクの概要	100
802.1X の前提条件	101
802.1X のイネーブル化	101
EAP リレーまたは EAP 終了のイネーブル化	102
ポート許可状態の設定	102
アクセス制御方式の指定	103
ポート上の必須認証ドメインの指定	103
802.1X 認証タイムアウトタイマーの設定	104
802.1X 再認証の設定	104
待機タイマーの設定	105
802.1X ゲスト VLAN の設定	106
802.1X ゲスト VLAN 割り当て遅延のイネーブル化	107

802.1X 認証失敗 VLAN の設定	107
802.1X クリティカル VLAN の設定	108
ポートでの 802.1X クリティカル VLAN の設定	108
802.1X クリティカル VLAN 内のユーザーへの EAP-Success パケットの送信	109
802.1X クリティカル Voice VLAN 機能のイネーブル化	109
802.1X ゲスト VSI の設定	110
802.1X ゲスト VSI 割り当て遅延のイネーブル化	111
802.1X 認証失敗 VSI の設定	111
802.1X クリティカル VSI の設定	112
認証トリガー機能の設定	112
ポート上の同時 802.1X ユーザーの最大数の設定	113
認証要求の最大試行回数	113
オンラインユーザーハンドシェイクの設定	114
サポートされているドメイン名デリミタの指定	115
ポートから送信された 802.1X プロトコルパケットの VLAN タグの削除	115
MAC 認証ユーザーに対する 802.1X 認証の最大試行回数	116
802.1X ユーザー IP フリーズのイネーブル化	116
802.1X MAC アドレスバインディングの設定	117
EAD Assistant 機能の設定	118
802.1X ユーザーのロギングのイネーブル化	118
802.1X の表示およびメンテナンスコマンド	119
802.1X 認証の設定例	120
例:基本 802.1X 認証の設定	120
例:802.1X ゲスト VLAN および認証 VLAN の設定	122
例:ACL 割り当てを使用した 802.1X の設定	124
例:802.1X ゲスト VSI および認可 VSI の設定	126
例:EAD アシスタントを使用する 802.1X の設定(DHCP リレーエージェントを使用)	128
例:EAD アシスタントを使用した 802.1X の設定(DHCP サーバーを使用)	131
802.1X のトラブルシューティング	133
EAD アシスタント URL リダイレクションの失敗	133

## MAC 認証の設定 ..... 134

MAC 認証について	134
ユーザーカウントポリシー	134
認証方式	135
VLAN 割り当て	135
VSI 操作	139
ACL 割り当て	141
ユーザープロファイルの割り当て	142
リダイレクト URL の割り当て	142
CAR アトリビュートの割り当て	142
Blackhole MAC 属性の割り当て	143
定期的な MAC 再認証	143
制約事項および注意事項:MAC 認証の設定	144
MAC 認証タスクの概要	144
MAC 認証の前提条件	145
MAC 認証のイネーブル化	145
MAC 認証ドメインの指定	146
ユーザーアカウントフォーマットの構成	146
MAC 認証タイマーの設定	146
MAC 認証ゲスト VLAN の設定	147
MAC 認証クリティカル VLAN の設定	148
MAC 認証クリティカル音声 VLAN 機能のイネーブル化	149
MAC 認証ゲスト VSI の設定	149
MAC 認証クリティカル VSI の設定	150



MAC 認証オフライン検出のイネーブル化 .....	151
ポート上の同時 MAC 認証ユーザーの最大数の設定 .....	151
ポート上での MAC 認証マルチ VLAN モードの有効化 .....	151
MAC 認証遅延の設定 .....	152
定期的な MAC 再認証の設定 .....	152
MAC 認証要求へのユーザー IP アドレスの追加 .....	153
MAC 認証と 802.1X 認証の並列処理の有効化 .....	154
MAC 認証ユーザーのロギングのイネーブル化 .....	155
MAC 認証用の表示およびメンテナンスコマンド .....	155
MAC 認証の設定例 .....	156
例:ローカル MAC 認証の設定 .....	156
例:RADIUS ベースの MAC 認証の設定 .....	158
例: サーバー割り当て MAC ベース VLAN .....	161
例:MAC 認証用の ACL 割り当ての設定 .....	166
例:MAC 認証認可 VSI 割り当ての設定 .....	168
<b>ポータル認証の設定 .....</b>	<b>171</b>
ポータル認証について .....	171
ポータル認証の利点 .....	171
拡張ポータル機能 .....	171
ポータルシステム .....	171
リモートポータルサーバーを使用したポータル認証 .....	172
ローカルポータルサービス .....	173
ポータル認証モード .....	173
ポータル認証プロセス .....	174
EAP のポータルサポート .....	176
ポータルフィルタールール .....	177
制約事項および注意事項:ポータル設定 .....	177
ポータル認証タスクの概要 .....	178
ポータル認証の前提条件 .....	179
リモートポータル認証サーバーの設定 .....	179
ポータル Web サーバーを構成する .....	180
ポータル Web サーバータスクの概要 .....	180
ポータル Web サーバーの基本パラメーターを構成する .....	180
キャプティブバイパス機能のイネーブル化 .....	181
URL リダイレクションの一致ルールの設定 .....	181
ローカルポータルサービス機能を構成する .....	182
ローカルポータルサービスについて .....	182
ローカルポータルサービス機能を設定するための制約事項とガイドライン .....	182
認証ページのカスタマイズ .....	182
ローカルポータル Web サービスを構成する .....	185
インターフェースでのポータル認証のイネーブル化 .....	185
インターフェース上のポータル Web サーバーの指定 .....	186
事前認証 IP アドレスプールの指定 .....	186
ポータル認証ドメインの指定 .....	187
ポータル認証ドメインについて .....	187
ポータル認証ドメインを指定するための制限およびガイドライン .....	188
インターフェース上のポータル認証ドメインの指定 .....	188
ポータルユーザーアクセスの制御 .....	188
ポータルフリー規則の設定 .....	188
認証送信元サブネットの設定 .....	189
認証先サブネットの設定 .....	190
ポータルユーザーの最大数の設定 .....	191
ポータル許可情報の厳密な検査の使用可能化 .....	191
DHCP で割り当てられた IP アドレスを持つユーザーだけがポータル認証を通過できるようにする .....	192

ポータル認証のための Web プロキシのサポートの構成	192
ポータルローミングを有効にする	193
ポータルの失敗許容機能の設定	194
ポータル検出機能の設定	194
ポータルユーザーのオンライン検出の設定	194
ポータル認証サーバー検出の設定	195
ポータル Web サーバーの検出の構成	196
ポータルユーザー同期の構成	197
ポータルパケット属性の設定	198
BAS-IP または BAS-IPv6 アトリビュートの設定	198
デバイス ID の指定	199
RADIUS パケットの属性の設定	199
NAS-Port-Id 属性のフォーマットの指定	199
インターフェースへの NAS-ID プロファイルの適用	199
ポータルクライアントのルール ARP または ND エントリ機能の無効化	200
オンラインポータルユーザーのログアウト	201
ポータルユーザーのログイン/ログアウトロギングの使用可能化	201
Web リダイレクトの構成	201
ポータルの表示および保守コマンド	202
ポータル構成の例	203
例:ダイレクトポータル認証の設定	203
例:再 DHCP ポータル認証の設定	211
例:クロスサブネットポータル認証の設定	214
例:拡張ダイレクトポータル認証の設定	217
例:拡張 re-DHCP ポータル認証の設定	221
例:拡張クロスサブネットポータル認証の設定	225
例:ポータルサーバーの検出とポータルユーザーの同期化の構成	228
例:ローカルポータル Web サービスを使用した直接ポータル認証の構成	236
ポータルのトラブルシューティング	239
ユーザーのポータル認証ページはプッシュされません。	239
アクセスデバイスのポータルユーザーをログアウトできません	239
RADIUS サーバー上のポータルユーザーをログアウトできない	240
アクセスデバイスによってログアウトされたユーザーは、ポータル認証サーバーにまだ存在しています。	240
Re-DHCP ポータルで認証されたユーザーが正常にログインできない	240

## Web 認証の設定 ..... 242

Web 認証について	242
Web 認証のメリット	242
Web 認証システム	242
Web 認証プロセス	243
VLAN 割り当ての Web 認証サポート	243
認可 ACL の Web 認証サポート	244
制限事項とガイドライン: Web 認証の構成	244
Web 認証タスクの概要	245
Web 認証の前提条件	245
Web 認証サーバーの設定	246
Web 認証を有効にする	246
Web 認証ドメインの指定	247
リダイレクト待ち時間の設定	247
Web 認証フリーのサブネットの構成	248
Web 認証ユーザーの最大数を設定する	248
オンライン Web 認証ユーザー検出の構成	248
認証失敗 VLAN の設定	249
Web プロキシをサポートするための Web 認証の構成	249
Web 認証の表示・保守コマンド	250

Web 認証の設定例 .....	250
例: ローカル認証方式を使用した Web 認証の構成 .....	250
例: RADIUS 認証方式を使用した Web 認証の設定 .....	252
Web 認証のトラブルシューティング .....	254
オンラインにならない (デフォルトの ISP ドメインを使用するローカル認証 インターフェース) .....	254
<b>トリプル認証について .....</b>	<b>255</b>
トリプル認証の典型的なネットワーク .....	255
トリプル認証メカニズム .....	255
VLAN 割り当てのトリプル認証サポート .....	256
認可 VLAN .....	256
認証失敗 VLAN .....	256
サーバー到達不能 VLAN .....	256
ACL 許可のトリプル認証サポート .....	257
オンラインユーザー検出のためのトリプル認証サポート .....	257
制約事項および注意事項: トリプル認証 .....	257
トリプル認証タスクの概要 .....	257
トリプル認証の設定例 .....	258
例: 基本トリプル認証の設定 .....	258
手順 .....	258
設定の確認 .....	260
例: 許可 VLAN および認証失敗 VLAN をサポートするためのトリプル認証の設定 .....	262
ネットワーク構成 .....	262
手順 .....	263
設定の確認 .....	266
<b>ポートセキュリティの設定 .....</b>	<b>269</b>
ポートセキュリティについて .....	269
主な機能 .....	269
ポートセキュリティ機能 .....	269
ポートセキュリティモード .....	269
制約事項および注意事項: ポートセキュリティ設定 .....	272
ポートセキュリティタスクの概要 .....	273
ポートセキュリティのイネーブル化 .....	273
ポートセキュリティモードの設定 .....	274
ポート上のセキュア MAC アドレス数に対するポートセキュリティの制限の設定 .....	275
セキュア MAC アドレスの設定 .....	276
セキュア MAC アドレスについて .....	276
前提条件 .....	277
セキュア MAC アドレスの追加 .....	277
セキュア MAC アドレスの非アクティブエージングのイネーブル化 .....	278
ダイナミックセキュア MAC 機能のイネーブル化 .....	278
NTK の設定 .....	278
侵入保護の設定 .....	279
サーバーからの許可情報を無視する .....	280
MAC 移動の有効化 .....	280
authorization-fail-offline 機能のイネーブル化 .....	280
ポート上の特定の VLAN の MAC アドレス数に対するポートセキュリティの制限の設定 .....	281
オープン認証モードの有効化 .....	282
ポートセキュリティのためのフリー-VLAN の設定 .....	283
ポートセキュリティへの NAS-ID プロファイルの適用 .....	283
エスケープクリティカル VSI 機能の設定 .....	284
ポートセキュリティの SNMP 通知のイネーブル化 .....	286
ポートセキュリティユーザーのロギングのイネーブル化 .....	286
ポートセキュリティの表示およびメンテナンスコマンド .....	287

ポートセキュリティの設定例 .....	287
例:autoLearn モードでのポートセキュリティの設定 .....	287
例:userLoginWithOUI モードでのポートセキュリティの設定 .....	290
例:macAddressElseUserLoginSecure モードでのポートセキュリティの設定 .....	293
ポートセキュリティのトラブルシューティング .....	298
ポートセキュリティモードを設定できません .....	298
セキュア MAC アドレスを設定できません .....	298
<b>攻撃の検出と防御の設定 .....</b>	<b>300</b>
概要 .....	300
デバイスが防止できる攻撃 .....	300
TCP フラグメント攻撃 .....	300
ログイン辞書攻撃 .....	300
TCP フラグメント攻撃防止の設定 .....	300
ログイン遅延の有効化 .....	301
<b>TCP 攻撃防止の設定 .....</b>	<b>302</b>
TCP 攻撃防止について .....	302
Naphtha 攻撃防止の設定 .....	302
<b>IP ソースガードの設定 .....</b>	<b>303</b>
IPSG について .....	303
IPSG 動作メカニズム .....	303
スタティック IPSG バインディング .....	303
ダイナミック IPSG バインディング .....	304
IPSG タスクの概要 .....	305
IPv4SG 機能の設定 .....	305
インターフェイスでの IPv4SG のイネーブル化 .....	305
静的 IPv4SG バインディングの設定 .....	306
IPSG フィルタリングからの IPv4 パケットの除外 .....	306
IPv6SG 機能の設定 .....	307
インターフェイスでの IPv6SG のイネーブル化 .....	307
静的 IPv6SG バインディングの設定 .....	308
IPSG の表示コマンドおよびメンテナンスコマンド .....	308
IPSG の設定例 .....	309
例:スタティック IPv4SG の設定 .....	309
例:DHCP スヌーピングベースのダイナミック IPv4SG の設定 .....	311
例:DHCP リレーエージェントベースのダイナミック IPv4SG の設定 .....	312
例:スタティック IPv6SG の設定 .....	313
例:DHCPv6 スヌーピングベースのダイナミック IPv6SG アドレスバインディングの設定 .....	313
例:DHCPv6 スヌーピングベースのダイナミック IPv6SG プレフィクスバインディングの設定 .....	314
例:DHCPv6 リレーエージェントベースのダイナミック IPv6SG の設定 .....	315
<b>ARP 攻撃からの保護の設定 .....</b>	<b>316</b>
ARP 攻撃からの保護について .....	316
ARP 攻撃からの保護タスクの概要 .....	317
解決不可能な IP 攻撃からの保護の設定 .....	317
解決不可能な IP 攻撃からの保護について .....	317
ARP 送信元抑制の設定 .....	318
ARP ブラックホールルーティングの設定 .....	318
解決不可能な IP 攻撃から保護するための表示コマンドとメンテナンスコマンド .....	319
例:解決不可能な IP 攻撃からの保護の設定 .....	319
ARP パケットレート制限の設定 .....	320
送信元 MAC ベース ARP 攻撃検出の設定 .....	321
送信元 MAC ベースの ARP 攻撃検出について .....	321

制限事項およびガイドライン .....	321
手順 .....	321
送信元 MAC ベース ARP 攻撃検出用の表示およびメンテナンスコマンド .....	322
例:送信元 MAC ベース ARP 攻撃検出の設定 .....	322
ARP パケットの送信元 MAC 整合性チェックの設定 .....	323
ARP パケットの送信元 MAC 整合性チェックについて .....	323
手順 .....	323
ARP アクティブ確認応答の設定 .....	323
許可 ARP の設定 .....	324
認可 ARP について .....	324
手順 .....	324
例:DHCP サーバーでの許可 ARP の設定 .....	324
例:DHCP リレーエージェントでの許可 ARP の設定 .....	325
ARP 攻撃検出の設定 .....	327
ARP 攻撃の検出について .....	327
ユーザー妥当性検査の構成 .....	327
ARP パケットの有効性チェックの設定 .....	329
ARP 制限付き転送の設定 .....	330
ユーザー有効性チェック中に ARP パケットの入力ポートを無視する .....	330
VSI の ARP 攻撃検出の設定 .....	331
ARP 攻撃検出ロギングのイネーブル化 .....	332
ARP 攻撃検出用の表示およびメンテナンスコマンド .....	332
例:ユーザー妥当性検査の構成 .....	333
例:ユーザー有効性チェックおよび ARP パケット有効性チェックの設定 .....	334
例:ARP 制限付きフォワーディングの設定 .....	335
ARP スキャンおよび固定 ARP の設定 .....	337
ARP ゲートウェイ保護の設定 .....	338
ARP ゲートウェイ保護について .....	338
制限事項およびガイドライン .....	338
手順 .....	338
例:ARP ゲートウェイ保護の設定 .....	339
ARP フィルタリングの設定 .....	339
ARP フィルタリング .....	339
制限事項およびガイドライン .....	340
手順 .....	340
例:ARP フィルタリングの設定 .....	340
ARP 送信元 IP アドレスチェックの設定 .....	341
ARP 送信元 IP アドレスの確認について .....	341
制限事項およびガイドライン .....	341
手順 .....	341
例:ARP 送信元 IP アドレスチェックの設定 .....	342
<b>ND 攻撃防御の設定 .....</b>	<b>344</b>
ND 攻撃防御について .....	344
ND 攻撃防御タスク一覧 .....	344
ND メッセージの送信元 MAC 整合性チェックのイネーブル化 .....	345
ND 攻撃検出の設定 .....	345
ND 攻撃検出について .....	345
制限事項およびガイドライン .....	346
手順 .....	346
ND 攻撃検出用の表示およびメンテナンスコマンド .....	347
例:ND 攻撃検出の設定 .....	347
<b>uRPF の設定 .....</b>	<b>349</b>
uRPF について .....	349

uRPF アプリケーションのシナリオ .....	349
uRPF チェックモード .....	349
ネットワークアプリケーション .....	350
uRPF のグローバルなイネーブル化 .....	350
インターフェイスでの uRPF のイネーブル化 .....	350
uRPF の表示およびメンテナンスコマンド .....	351

# AAA の設定

## AAAについて

### AAA 実装

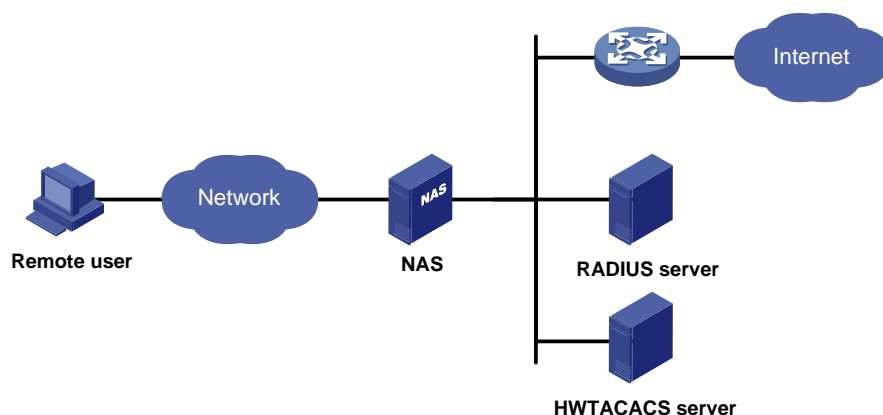
Authentication(認証), Authorization(許可), and Accounting(会計)(AAA)は、ネットワークアクセス管理を実装するための統一されたフレームワークを提供します。この機能は、次のセキュリティ機能を指定します。

- **認証:** ユーザーを識別し、その有効性を確認します。
- **許可:** 異なるユーザーに異なる権限を付与し、リソースおよびサービスへのユーザーのアクセスを制御します。たとえば、オフィスユーザーにファイルの読み取りと印刷を許可し、ゲストがデバイス上のファイルにアクセスできないようにすることができます。
- **会計:** サービスタイプ、開始時刻、トラフィックなど、ユーザーのネットワーク使用状況の詳細を記録します。この機能により、時間ベースおよびトラフィックベースの課金とユーザー動作の監査が可能になります。

### AAA ネットワーク図

AAA はクライアント/サーバーモデルを使用します。クライアントはアクセスデバイスまたはネットワークアクセスサーバー(NAS)上で実行されます。NAS はユーザーIDを認証し、ユーザーアクセスを制御します。サーバーはユーザー情報を集中管理します。図1を参照してください。

図1 AAA ネットワーク図



NAS 以外のネットワークまたはリソースにアクセスするには、ユーザーがその ID 情報を NAS に送信します。NAS は透過的にユーザー情報を AAA サーバーに渡し、認証、認可およびアカウントिंगの結果を待ちます。その結果に基づいて、NAS はアクセス要求を許可するか拒否するかを決定します。

AAA には、HWTACACS、LDAP、RADIUS などのさまざまな実装があります。RADIUS が最もよく使用されます。

異なるサーバーを使用して、異なるセキュリティ機能を実装できます。たとえば、認証および認可に HWTACACS サーバーを使用し、会計に RADIUS サーバーを使用できます。

必要に応じて、AAA が提供するセキュリティ機能を選択できます。たとえば、特定のリソースにアクセスする前に従業員を認証する場合は、認証サーバーを配置します。ネットワーク使用情報が必要な場合は、アカウントリングサーバーも構成します。

デバイスは動的パスワード認証を実行します。

## RADIUS

Remote Authentication Dial-In User Service(RADIUS)は、クライアント/サーバーモデルを使用する分散情報対話プロトコルです。このプロトコルは、不正アクセスからネットワークを保護でき、高度なセキュリティとリモートユーザーアクセスの両方を必要とするネットワーク環境でよく使用されます。

RADIUS 認可プロセスは RADIUS 認証プロセスと組み合わせられ、ユーザー認可情報は認証応答に載せられます。RADIUS は認証に UDP ポート 1812 を使用し、アカウントリングに UDP ポート 1813 を使用します。

RADIUS はもともとダイヤルインユーザーアクセス用に設計されており、イーサネットや ADSL などの追加のアクセス方法をサポートするように拡張されています。

### クライアント/サーバーモデル

RADIUS クライアントは、ネットワーク全体に配置された NAS 上で実行されます。RADIUS サーバーにユーザー情報を渡し、ユーザーアクセス要求の拒否や受け入れなどの応答に対して動作します。

RADIUS サーバーは、ネットワークセンターのコンピュータまたはワークステーション上で動作し、ユーザー認証およびネットワークサービスアクセスに関連する情報を保持します。

RADIUS サーバーは、次のプロセスを使用して動作します。

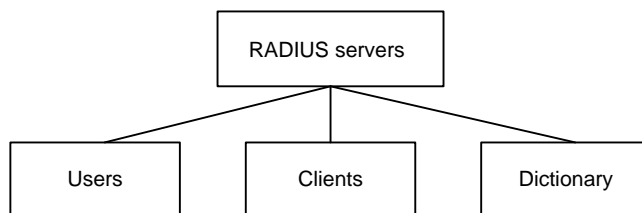
1. RADIUS クライアントから認証、認可、アカウントリング要求を受信します。
2. ユーザー認証、認可、またはアカウントリングを実行します。
3. ユーザーアクセス制御情報(ユーザーアクセス要求の拒否または受け入れなど)をクライアントに返します。

RADIUS サーバーは、別の RADIUS サーバーのクライアントとして動作し、認証プロキシサービスを提供することもできます。

RADIUS サーバーは、次のデータベースを管理します。

- **Users:** ユーザー名、パスワード、適用されたプロトコル、IP アドレスなどのユーザー情報を格納します。
- **Clients:** 共有キーや IP アドレスなど、RADIUS クライアントに関する情報を格納します。
- **Dictionary:** RADIUS プロトコルのアトリビュートとその値を格納します。

図2 RADIUS サーバーデータベース



### 情報交換セキュリティメカニズム

RADIUS クライアントとサーバーは、クライアントとサーバーに事前に設定されている共有キーを使用して、クライアントとサーバー間で情報を交換します。RADIUS パケットには、オーセンティケータと呼ばれる 16 バイトのフィールドがあります。このフィールドには、MD5 アルゴリズムを使用して生成されたシングニチャ、



共有キー、およびその他の情報が含まれます。パケットの受信側は、シグニチャを確認し、シグニチャが正しい場合にのみパケットを受け入れます。このメカニズムにより、RADIUS クライアントとサーバー間で交換される情報のセキュリティが確保されます。

共有キーは、RADIUS パケットに含まれるユーザーパスワードの暗号化にも使用されます。

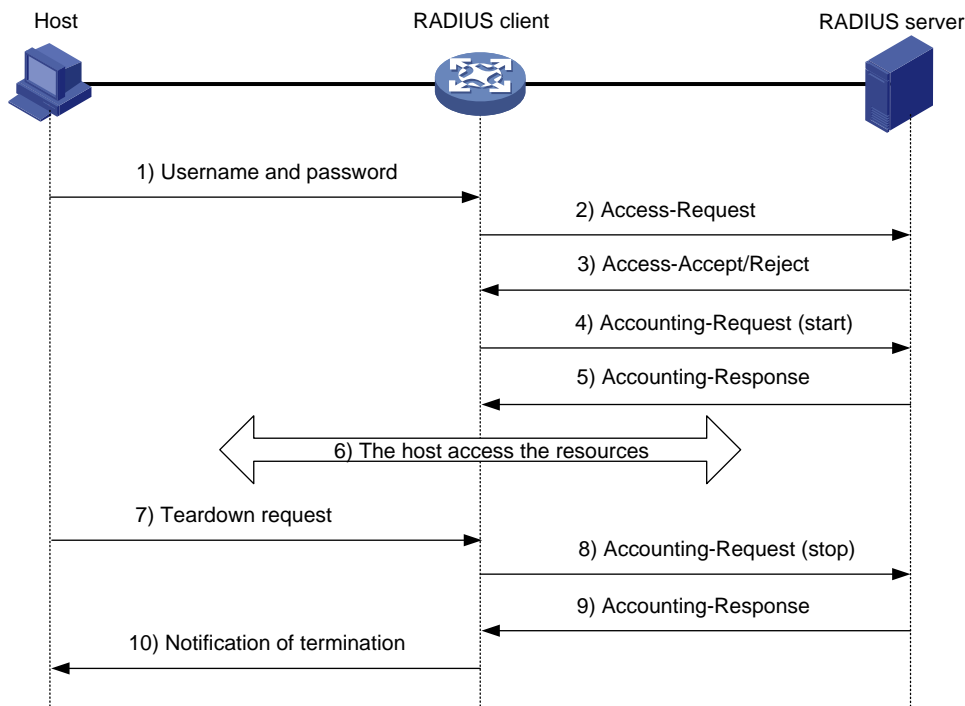
## ユーザー認証方法

RADIUS サーバーは、PAP、CHAP、EAP などの複数のユーザー認証方式をサポートしています。

## 基本的な RADIUS パケット交換プロセス

図3に、ユーザーホスト、RADIUS クライアント、および RADIUS サーバー間の相互作用を示します。

図3 基本的な RADIUS パケット交換プロセス



RADIUS は次のワークフローで使われます。

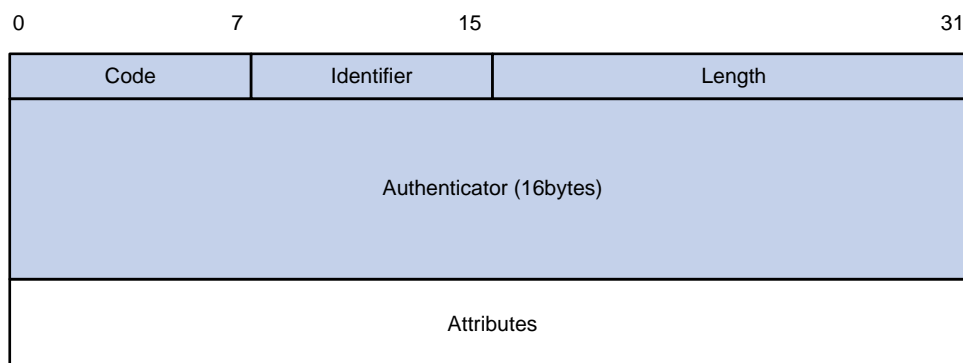
1. ホストは、ユーザーのユーザー名とパスワードを含む接続要求を RADIUS クライアントに送信します。
2. RADIUS クライアントは、認証要求(Access-Request)を RADIUS サーバーに送信します。この要求には、MD5 アルゴリズムで処理されたユーザーのパスワードと共有キーが含まれます。
3. RADIUS サーバーはユーザー名とパスワードを認証します。認証が成功すると、サーバーはユーザーの認証情報を含む Access-Accept パケットを送り返します。認証が失敗すると、サーバーは Access-Reject パケットを送り返します。
4. RADIUS クライアントは、認証結果に従ってユーザーを許可または拒否します。結果がユーザーを許可する場合、RADIUS クライアントはアカウント開始要求(Accounting-Request)パケットを RADIUS サーバーに送信します。
5. RADIUS サーバーは確認応答(Accounting-Response)パケットを返し、アカウントを開始します。
6. ユーザーがネットワークリソースにアクセスする。
7. ホストは RADIUS クライアントに接続の切断を要求します。

8. RADIUS クライアントは、アカウント停止要求(Accounting-Request)パケットを RADIUS サーバーに送信します。
9. RADIUS サーバーは確認応答(Accounting-Response)を返し、ユーザーのアカウント停止をします。
10. RADIUS クライアントは、ユーザーに終了を通知します。

## RADIUS パケット形式

RADIUS は、UDP を使用してパケットを送信します。また、RADIUS サーバーとクライアント間のスムーズなパケット交換を保証するために、一連のメカニズムを使用します。これらのメカニズムには、タイマーメカニズム、再送信メカニズム、およびバックアップサーバーメカニズムが含まれます。

図4 RADIUS パケット形式



フィールドの説明は次のとおりです。

- コードフィールド(1 バイト長)は、RADIUS パケットのタイプを示します。表 1 に、主な値とその意味を示します。

表1 コードフィールドの主な値

コード	パケットタイプ	説明
1	Access-Request	クライアントからサーバー。このタイプのパケットには、サーバーがユーザーを認証するためのユーザー情報が含まれます。このパケットにはUser-Name属性を含める必要があり、オプションでNAS-IP-Address、User-PasswordおよびNAS-Port属性を含めることができます。
2	Access-Accept	サーバーからクライアント。Access-Requestに含まれるすべての属性値が許容可能な場合、認証は成功し、サーバーはAccess-Accept応答を送信します。
3	Access-Reject	サーバーからクライアント。Access-Requestに含まれるいずれかの属性値が許容できない場合、認証は失敗し、サーバーはAccess-Reject応答を送信します。
4	Accounting-Request	クライアントからサーバー。このタイプのパケットには、サーバーがユーザーのアカウントを開始または停止するためのユーザー情報が含まれます。パケット内のAcct-Status-Type属性は、アカウントを開始または停止するかどうかを示します。
5	Accounting-Response	サーバーからクライアントへ。サーバーは、このタイプのパケットを送信して、Accounting-Requestを受信し、アカウント情報を正常に記録したことをクライアントに通知します。

- 識別子フィールド(長さ 1 バイト)は、応答パケットを要求パケットと一致させ、重複する要求パケットを検出するために使用されます。同じ目的(認証やアカウントリングなど)の同じ交換プロセスの要求パケットと応答パケットは、同じ識別子を持ちます。
- Length フィールド(長さ 2 バイト)は、Code、Identifier、Length、Authenticator、および Attributes フィールドを含むパケット全体の長さ(バイト単位)を示します。この長さを超えるバイトはパディングと見なされ、受信側では無視されます。受信パケットの長さがこの長さ未満の場合、パケットはドロップされます。
- Authenticator フィールド(長さ 16 バイト)は、RADIUS サーバーからの応答を認証し、ユーザーパスワードを暗号化するために使用されます。オーセンティケーターには、要求オーセンティケーターと応答オーセンティケーターの 2 種類があります。
- **Attributes フィールド(長さは可変)には、認証、認可およびアカウントリング情報が含まれます。このフィールドには複数の属性を含めることができ、各属性には次のサブフィールドがあります。**
  - Type: 属性のタイプ。
  - Length: Type、Length、および Value サブフィールドを含む、バイト単位の属性の長さ。
  - Value: 属性の値。フォーマットおよび内容は、Type サブフィールドによって異なります。

## 拡張 RADIUS アトリビュート

RADIUS プロトコルは拡張性に優れています。ベンダー固有属性(属性 26)を使用すると、ベンダーは拡張属性を定義できます。拡張属性は、標準 RADIUS プロトコルが提供しない機能を実装できます。

ベンダーは、拡張機能を提供するために、属性 26 に複数のサブ属性を TLV 形式でカプセル化できます。図5に示すように、属性 26 にカプセル化されたサブ属性は、次の部分で構成されます。

- Vendor-ID: ベンダーの ID。最上位バイトは 0 です。残りの 3 バイトには RFC1700 に準拠したコードが含まれています。
- Vendor-Type: サブアトリビュートのタイプ。
- Vendor-Length: サブアトリビュートの長さ。
- Vendor-Data: サブアトリビュートの内容。

デバイスは、ベンダーID25506 の RADIUS サブアトリビュートをサポートしています。

図5 属性 26 のフォーマット

0	7	15	23	31
Type		Length		Vendor-ID
Vendor-ID (continued)			Vendor-Type	Vendor-Length
Vendor-Data (Specified attribute value.....)				
.....				

## HWTACACS

HW Terminal Access Controller Access Control System(HWTACACS)は、TACACS(RFC1492)に基づく拡張セキュリティプロトコルです。HWTACACS は RADIUS に似ており、NAS と HWTACACS サーバー間の情報交換にクライアント/サーバーモデルを使用します。

HWTACACS は通常、PPP、VPDN およびターミナルユーザーに対して AAA サービスを提供します。一般的な HWTACACS のシナリオでは、ターミナルユーザーは NAS にログインする必要があります。NAS は HWTACACS クライアントとして機能し、ユーザーのユーザー名とパスワードを認証のために

HWTACACS のサーバーに送信します。認証を渡し、承認された権限を取得した後、ユーザーはデバイスにログインして操作を実行します。HWTACACS サーバーは各ユーザーが実行する操作を記録します。

## HWTACACS と RADIUS の違い

HWTACACS と RADIUS には、クライアント/サーバーモデルの使用、データ暗号化のための共有キーの使用、柔軟性とスケーラビリティの提供など、多くの共通機能があります。に、HWTACACS と RADIUS の主な相違点を示します。

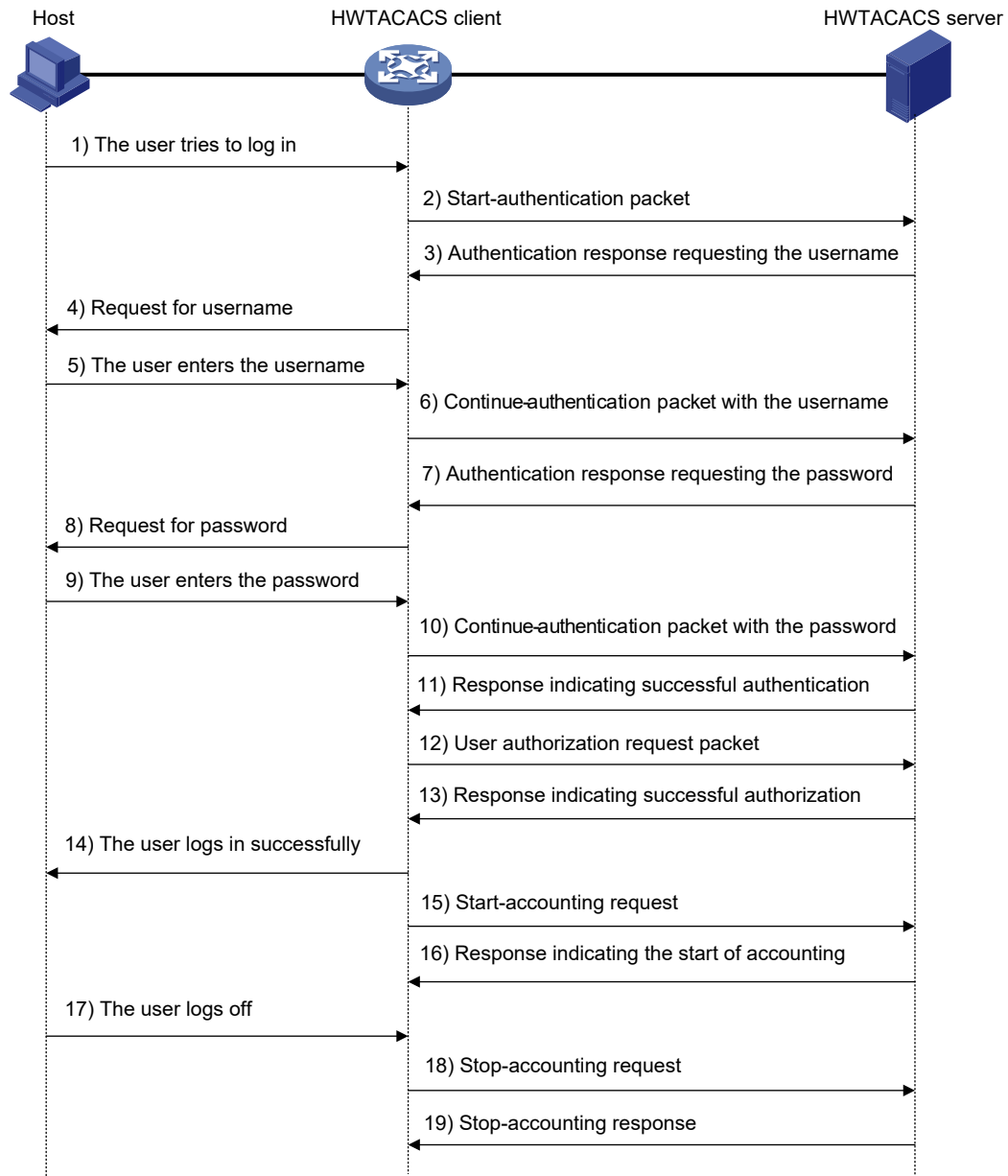
表2 HWTACACS と RADIUS の主な違い

HWTACACS	RADIUS
信頼性の高いネットワーク伝送を提供するTCPを使用します。	転送効率の高いUDPを使用しています。
HWTACACSヘッダーを除くパケット全体を暗号化します。	認証パケットのユーザーパスワードフィールドだけを暗号化します。
プロトコルパケットは複雑で、許可は認証とは独立しています。認証と許可は異なるHWTACACSサーバーに展開できます。	プロトコルパケットは単純で、認可プロセスは認証プロセスと組み合わせられます。
構成コマンドの認可をサポートします。コマンドへのアクセスは、ユーザーのロールと認可の両方に依存します。ユーザーは、ユーザーロールによって許可され、HWTACACSサーバーによって認可されたコマンドのみ使用できます。	構成コマンドの認可はサポートされていません。コマンドへのアクセスは、ユーザーのロールのみに依存します。ユーザーロールの詳細は、「基本構成ガイド」を参照してください。

## 基本的な HWTACACS パケット交換プロセス

図6に、HWTACACS が Telnet ユーザーのユーザー認証、許可、アカウントングを実行する方法を示します。

図6 Telnet ユーザーのための基本的な HWTACACS パケット交換プロセス



HWTACACS は、次のワークフローを使用して動作します。

1. Telnet ユーザーが HWTACACS クライアントにアクセス要求を送信します。
2. HWTACACS クライアントは、要求を受信すると、開始認証パケットを HWTACACS サーバーに送信します。
3. HWTACACS サーバーは、ユーザー名を要求する認証応答を返します。
4. 応答を受信すると、HWTACACS クライアントはユーザーにユーザー名を要求します。
5. ユーザー名を入力します。
6. ユーザーからユーザー名を受信すると、HWTACACS クライアントはユーザー名を含む継続認証パケットをサーバーに送信します。
7. HWTACACS サーバーは、ログインパスワードを要求するために認証応答を送り返します。
8. 応答を受信すると、HWTACACS クライアントはユーザーにログインパスワードを要求します。

9. ユーザーがパスワードを入力します。
10. ログインパスワードを受信すると、HWTACACS クライアントはログインパスワードを含む継続認証パケットを HWTACACS サーバーに送信します。
11. 認証が成功すると、HWTACACS サーバーはユーザーが認証に合格したことを示す認証応答を返します。
12. HWTACACS クライアントは、ユーザー認証要求パケットを HWTACACS サーバーに送信します。
13. 認証が成功すると、HWTACACS サーバーは、ユーザーが現在許可されていることを示す許可応答を返します。
14. ユーザーが許可されたことを認識すると、HWTACACS クライアントはその CLI をユーザーにプッシュし、ユーザーのログインを許可します。
15. HWTACACS クライアントは、HWTACACS サーバーにアカウント開始要求を送信します。
16. HWTACACS サーバーは、アカウント開始要求を受信したことを示すアカウント開始応答を返します。
17. ユーザーがログオフします。
18. HWTACACS クライアントは、アカウント停止要求を HWTACACS サーバーに送信します。
19. HWTACACS サーバーから stop-accounting 応答が返され、stop-accounting 要求が受信されたことが示されます。

## LDAP

Lightweight Directory Access Protocol(LDAP)は、標準的なマルチプラットフォームディレクトリサービスを提供します。LDAP は、X.500 プロトコルに基づいて開発されました。X.500 の次の機能が拡張されています。

- 読み取り/書き込みの対話型アクセス
- 参照
- 検索

LDAP は、頻繁に変更されないデータの格納に適しています。このプロトコルは、ユーザー情報の格納に使用されます。たとえば、LDAP サーバーソフトウェアの Active Directory サーバーは、Microsoft Windows オペレーティングシステムで使用されます。このソフトウェアは、ユーザーログイン認証および認可のユーザー情報およびユーザーグループ情報を格納します。

### LDAP ディレクトリサービス

LDAP では、ディレクトリを使用して組織情報、人事情報およびリソース情報を保守します。ディレクトリはツリー構造に編成され、エントリが含まれます。エントリは、識別名(DN)を持つ属性のセットです。属性は、ユーザー名、パスワード、電子メール、コンピュータ名および電話番号などの情報の格納に使用されます。

LDAP はクライアント/サーバーモデルを使用し、すべてのディレクトリ情報は LDAP サーバーに保管されます。一般的に使用される LDAP サーバー製品には、Microsoft Active Directory Server、IBM Tivoli Directory Server、および Sun ONE Directory Server があります。

### LDAP 認証および許可

AAA は、LDAP を使用してユーザーに認証サービスおよび認可サービスを提供できます。LDAP は、その機能を実装する一連の操作を定義します。認証および認可の主な操作は、バインド操作および検索操作です。

- バインド操作により、LDAP クライアントは次の操作を実行できます。
  - LDAP サーバーとの接続を確立します。
  - LDAP サーバーへのアクセス権を取得します。

- ユーザー情報の妥当性を確認します。
- 検索操作では、検索条件を作成し、LDAP サーバーのディレクトリリソース情報を取得します。

LDAP 認証では、クライアントは次のタスクを完了します。

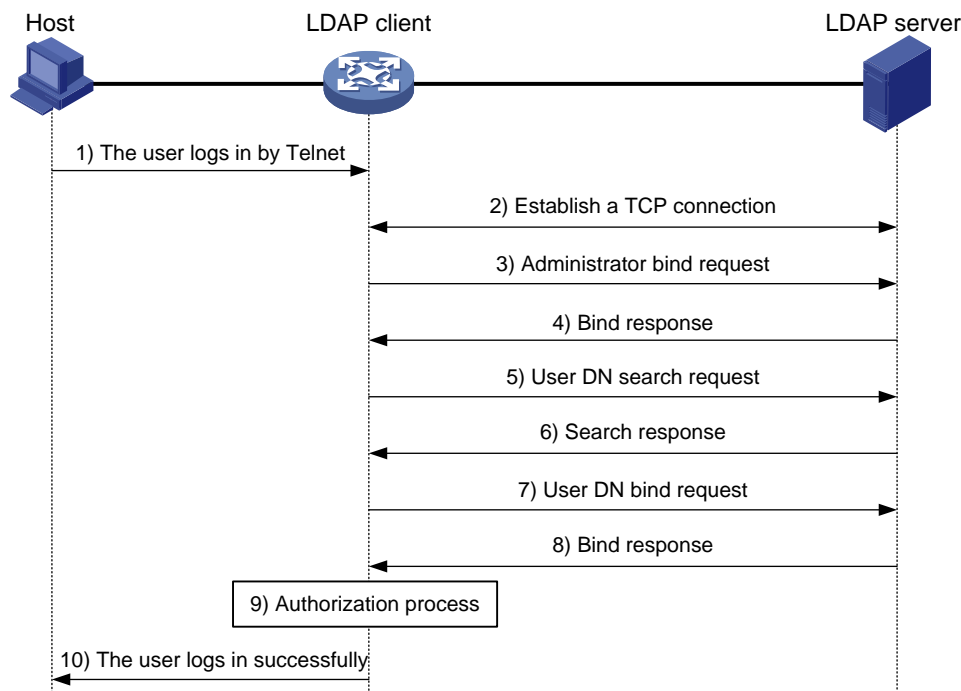
1. LDAP サーバー管理者 DN を使用して LDAP サーバーとバインドします。バインドが作成されると、クライアントはサーバーへの接続を確立し、検索権限を取得します。
2. ユーザーの認証情報内のユーザー名を使用して検索条件を作成します。サーバーの指定されたルートディレクトリが検索され、ユーザーDN リストが生成されます。
3. 各ユーザーDN およびパスワードを使用して LDAP サーバーとバインドします。バインドが作成された場合、ユーザーは合法とみなされます。

LDAP 認可では、クライアントは LDAP 認証と同じタスクを実行します。クライアントが検索条件を構築すると、認可情報とユーザーDN リストの両方が取得されます。

## 基本的な LDAP 認証プロセス

次に、Telnet ユーザーの基本的な LDAP 認証プロセスの例を示します。

図7 Telnet ユーザーの基本的な LDAP 認証プロセス



次に、基本的な LDAP 認証プロセスを示します。

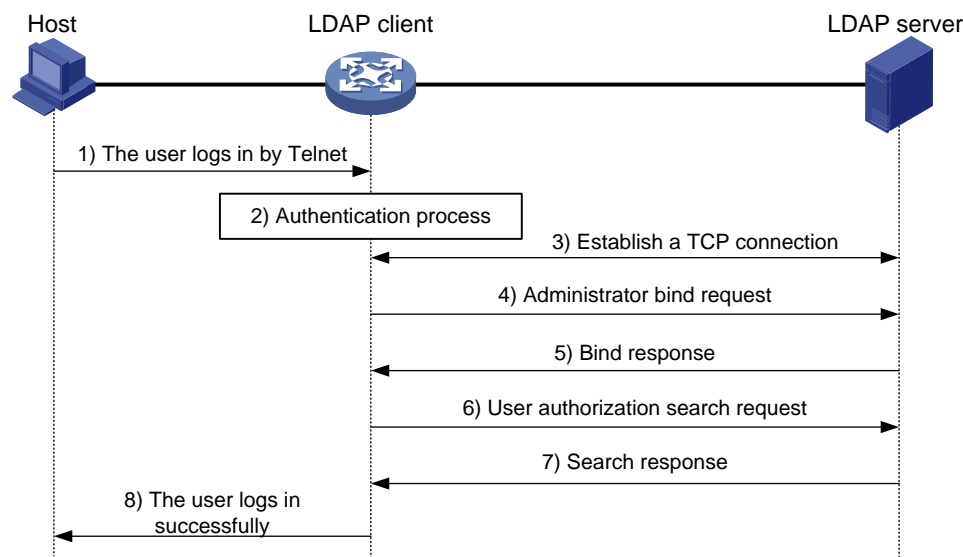
1. Telnet ユーザーは接続要求を開始し、ユーザー名とパスワードを LDAP クライアントに送信します。
2. 要求を受信すると、LDAP クライアントは LDAP サーバーとの TCP 接続を確立します。
3. 検索権限を取得するために、LDAP クライアントは管理者 DN とパスワードを使用して、管理者バインド要求を LDAP サーバーに送信します。
4. LDAP サーバーが要求を処理します。バインド操作が成功すると、LDAP サーバーは LDAP クライアントに確認応答を送信します。
5. LDAP クライアントは、Telnet ユーザーのユーザー名を持つユーザーDN 検索要求を LDAP サーバーに送信します。

6. 要求を受信すると、LDAP サーバーはベース DN、検索範囲およびフィルタ条件によってユーザー DN を検索します。一致が検出されると、LDAP サーバーは LDAP クライアントに検索が成功したことを通知する応答を送信します。1 つ以上のユーザー DN が検出される場合があります。
7. LDAP クライアントは、取得したユーザー DN と入力したユーザーパスワードをパラメーターとして使用して、ユーザー DN バインド要求を LDAP サーバーに送信します。サーバーは、ユーザーパスワードが正しいかどうかをチェックします。
8. LDAP サーバーは要求を処理し、バインド操作の結果を LDAP クライアントに通知するための応答を送信します。バインド操作が失敗すると、LDAP クライアントは取得した別のユーザー DN をパラメーターとして使用し、ユーザー DN バインド要求を LDAP サーバーに送信します。このプロセスは、DN が正常にバインドされるか、すべての DN がバインドに失敗するまで続行されます。すべてのユーザー DN がバインドに失敗すると、LDAP クライアントはログイン失敗をユーザーに通知し、ユーザーのアクセス要求を拒否します。
9. LDAP クライアントは、バインドされたユーザー DN を保存し、認証サーバーと認証パケットを交換します。
  - LDAP 認証を使用する場合は、に示す認可プロセスを参照してください。
  - 認可に別の方式が必要な場合は、その方式の認可プロセスが適用されます。
10. 認証が成功すると、LDAP クライアントはユーザーにログイン成功を通知します。

## 基本的な LDAP 認証プロセス

次に、Telnet ユーザーの基本的な LDAP 認可プロセスの例を示します。

図8 Telnet ユーザーの基本的な LDAP 認証プロセス



次に、基本的な LDAP 認可プロセスを示します。

1. Telnet ユーザーは接続要求を開始し、ユーザー名とパスワードをデバイスに送信します。デバイスは認可中に LDAP クライアントとして動作します。
2. 要求を受信すると、デバイスはユーザーの認証サーバーと認証パケットを交換します。
  - LDAP 認証を使用する場合は、図7に示す認証プロセスを参照してください。
    - デバイス(LDAP クライアント)が認証と認可に同じ LDAP サーバーを使用する場合は、手順 6 に進みます。
    - デバイス(LDAP クライアント)が認証と認可に異なる LDAP サーバーを使用する場合は、ステップ 4 に進みます。



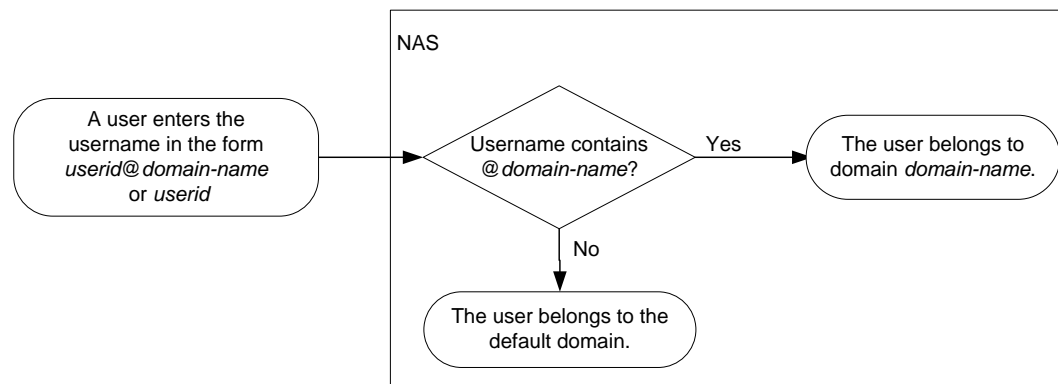
- 別の認証方式を使用する場合は、その方式の認証プロセスが適用されます。デバイスは LDAP クライアントとして動作します。手順 3 に進みます。
- 3. LDAP クライアントは、LDAP 認証サーバーとの TCP 接続を確立します。
- 4. 検索権限を取得するために、LDAP クライアントは管理者 DN とパスワードを使用して、管理者バインド要求を LDAP サーバーに送信します。
- 5. LDAP サーバーが要求を処理します。バインド操作が成功すると、LDAP サーバーは LDAP クライアントに確認応答を送信します。
- 6. LDAP クライアントは、Telnet ユーザーのユーザー名を持つ認証検索要求を LDAP サーバーに送信します。ユーザーが認証と許可に同じ LDAP サーバーを使用する場合、クライアントは、Telnet ユーザーの保存されたユーザー DN を持つ要求を LDAP サーバーに送信します。
- 7. 要求を受信すると、LDAP サーバーはベース DN、検索範囲、フィルタ条件および LDAP 属性によってユーザー情報を検索します。一致が検出されると、LDAP サーバーは LDAP クライアントに検索が成功したことを通知する応答を送信します。
- 8. 認証が成功すると、LDAP クライアントはユーザーにログイン成功を通知します。

## ISP ドメインとユーザーアクセスタイプベースのユーザー管理

AAA は、ユーザーの ISP ドメインおよびアクセスタイプに基づいてユーザーを管理します。

NAS では、各ユーザーは 1 つの ISP ドメインに属します。NAS は、ログイン時にユーザーが入力したユーザー名に基づいて、ユーザーが属する ISP ドメインを決定します。

図9 ユーザー名によるユーザーの ISP ドメインの決定



AAA は、ユーザーのアクセスタイプに基づいて同じ ISP ドメイン内のユーザーを管理します。デバイスは、次のユーザーアクセスタイプをサポートします。

- **LAN:** LAN ユーザーがオンラインになるには、802.1X または MAC 認証に合格する必要があります。
- **LOG IN:** ログインユーザーには、デバイスにログインする SSH、Telnet、FTP、および端末ユーザーが含まれます。端末ユーザーは、コンソールポートからアクセスできます。
- **ポータル:** ポータルユーザーは、ネットワークにアクセスするためにポータル認証に合格する必要があります。
- **HTTP/HTTPS:** ユーザーは HTTP または HTTPS を介してデバイスにログインします。

デバイスには、ユーザー認証管理ポリシーを実装するための認証モジュール(802.1X など)も用意されています。これらの認証モジュールを設定する場合、アクセスタイプのユーザーの ISP ドメインは認証モジュールの設定によって異なります。

# 認証、許可と会計方法

AAA は、ISP ドメイン内の異なるタイプのユーザーに対して、異なる認証、認可、アカウントング方式の設定をサポートします。NAS は、ユーザーの ISP ドメインとアクセスタイプを決定します。また、NAS は、ユーザーのアクセスを制御するために、ドメイン内のアクセスタイプに対して設定された方式を使用します。

AAA では、ISP ドメインの一連のデフォルト方式の設定もサポートされています。これらのデフォルト方式は、AAA 方式が設定されていないユーザーに適用されます。

## 認証方式

デバイスは次の認証方式をサポートしています。

- **認証なし:** この方法ではすべてのユーザーが信頼され、認証は実行されません。セキュリティ上の理由から、この方法は使用しないでください。
- **ローカル認証:** NAS は、ユーザー名、パスワード、アトリビュートなどのローカルに設定されたユーザー情報に基づいて、ユーザーを自身で認証します。ローカル認証では、高速かつ低コストが可能ですが、保存できる情報量はストレージスペースのサイズによって制限されます。
- **リモート認証:** NAS はリモートサーバーと連携してユーザーを認証します。NAS は RADIUS、LDAP または HWTACACS プロトコルを介してリモートサーバーと通信します。サーバーはユーザー情報を集中管理します。リモート認証は、複数の NAS に対して大容量で信頼性の高い集中認証サービスを提供します。リモートサーバーが使用できない場合に使用するバックアップ方法を構成できます。

## 許可方式

デバイスは、次の認可方式をサポートしています。

- **認可なし:** NAS は認可交換を実行しません。次のデフォルトに合格すると、次のデフォルトの認可情報が適用されます。
  - ログインユーザーは、レベル 0 のユーザーロールを取得します。レベル 0 のユーザーロールの詳細については、『Fundamentals Configuration Guide』の「RBAC configuration」を参照してください。
  - FTP、SFTP および SCP ログインユーザーの作業ディレクトリは、NAS のルートディレクトリです。ただし、ユーザーにはルートディレクトリへのアクセス権はありません。
  - ログインしていないユーザーもネットワークにアクセスできます。
- **ローカル認可:** NAS は、ユーザーに対してローカルに設定されたユーザートリビュートに従って認可を実行します。
- **リモート認証:** NAS はリモートサーバーと連携してユーザーを認証します。RADIUS 認証は RADIUS 認証とバインドされます。RADIUS 認証は、RADIUS 認証が成功した後にのみ機能し、認可情報は Access-Accept パケットに含まれます。HWTACACS または LDAP 認可は認証とは別個のものであり、認可情報は認証成功後の認可応答に含まれます。リモートサーバーが使用できない場合に使用するバックアップ方法を設定できます。

## 会計処理方法

デバイスは、次のアカウントング方式をサポートしています。

- **アカウントングなし:** NAS はユーザーのアカウントングを実行しません。
- **ローカルアカウントング:** ローカルアカウントングは NAS に実装されます。ローカルアカウントングは、同じローカルユーザーカウントを使用する同時ユーザー数をカウントおよび制御しますが、課金の統計情報は提供しません。
- **リモートアカウントング:** NAS はアカウントング用の RADIUS サーバーまたは HWTACACS サーバーと連動します。リモートサーバーが使用できない場合に使用するバックアップ方法を設定できます。

## AAA 拡張機能

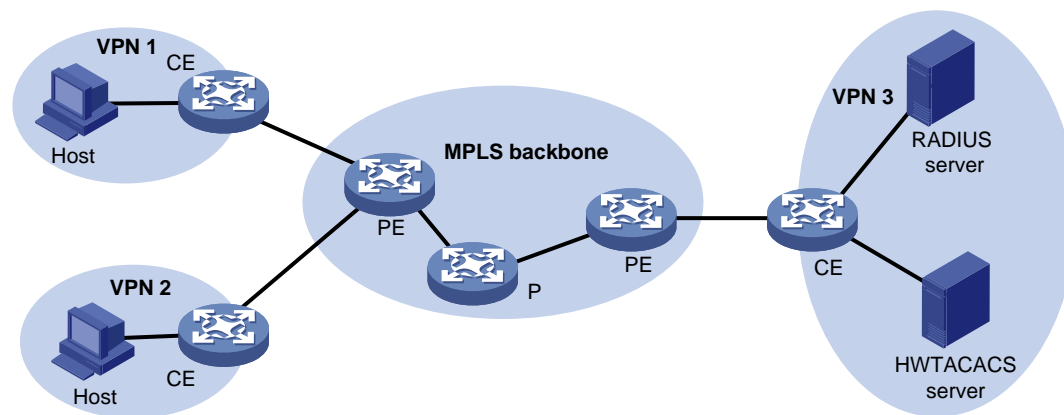
デバイスは、デバイスセキュリティを強化するために次のログインサービスを提供します。

- **コマンド認可**: ログインユーザーが入力したコマンドが許可されているかどうかを NAS が認可サーバーに判断できるようにします。ログインユーザーは、認可サーバーで許可されているコマンドのみ実行できます。コマンド認可の詳細は、「基本構成ガイド」を参照してください。
- **コマンドアカウンティング**: コマンド認可がディセーブルの場合、コマンドアカウンティングにより、アカウンティングサーバーはデバイスで実行されたすべての有効なコマンドを記録できます。コマンド認可がイネーブルの場合、コマンドアカウンティングにより、アカウンティングサーバーはすべての認可されたコマンドを記録できます。コマンドアカウンティングの詳細については、『Fundamentals Configuration Guide』を参照してください。
- **ユーザーロール認証**: ログアウトまたは切断せずに別のユーザーロールを取得する各ユーザーを認証します。ユーザーロール認証の詳細については、『Fundamentals Configuration Guide』を参照してください。

## VPN 用 AAA

VPN 間で認証、認可、およびアカウンティングパケットの転送をイネーブルにするために、VPN 間に AAA を展開できます。たとえば、図 10 に示すように、MPLS バックボーン の左側にある CE は NAS として機能します。NAS は、VPN1 および VPN2 のプライベートユーザーの AAA パケットを VPN3 の AAA サーバーに透過的に配信して、一元的な認証を行います。異なる VPN のプライベートユーザーの認証パケットは相互に影響しません。

図 10 ネットワーク図

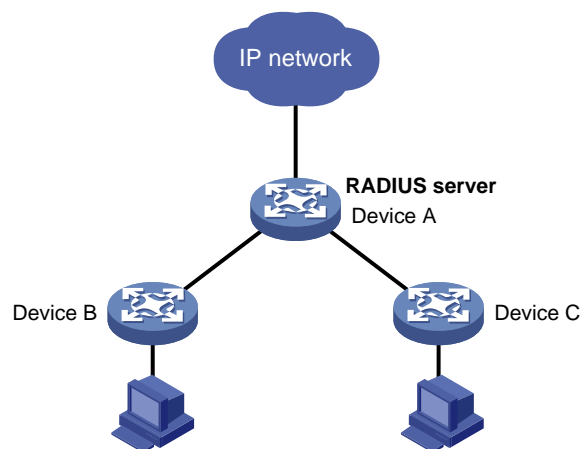


この機能は、MCE が VPN 用のポータル認証を実装するのにも役立ちます。MCE の詳細については、「MCE Configuration Guide」を参照してください。

## デバイスの RADIUS サーバー機能

デバイスの RADIUS サーバー機能をイネーブルにして、ユーザーの認証および認可のために RADIUS クライアントと連携できるようにします。デバイスは、専用 RADIUS サーバーとして、または RADIUS サーバーと RADIUS クライアントの両方として同時に動作できます。

図11 ネットワーク図



RADIUS サーバー機能は、次の操作をサポートしています。

- ローカルユーザー情報から生成される RADIUS ユーザーデータを管理します。このデータには、ユーザー名、パスワード、説明、認可 ACL、認可 VLAN、および有効期限が含まれます。
- RADIUS クライアントを追加、変更および削除できます。RADIUS クライアントは IP アドレスで識別され、共有キーなどの属性情報を含みます。RADIUS サーバー機能は、記録された RADIUS クライアントからの認証要求だけを処理し、不明なクライアントからの要求は無視します。
- ネットワークアクセスタイプのユーザーを認証および認可します。サーバーはアカウントングを提供しません。

RADIUS サーバーは、RADIUS パケットを受信すると、次のアクションを実行します。

1. パケットが記録された RADIUS クライアントから送信されることを確認します。
2. 共有キーを使用してパケットを確認します。
3. ユーザーカウントが存在し、パスワードが正しいこと、およびその他の属性が要件を満たしていること (たとえば、アカウントが有効期間内にあること)を確認します。
4. 認証結果を判別し、認証されたユーザーに特定の権限を付与します。

デバイスの RADIUS サーバー機能には、次の制約事項があります。

- 認証ポートは UDP1812 に固定されており、変更できません。
- この機能は IPv4 ネットワークではサポートされていますが、IPv6 ネットワークではサポートされていません。
- サーバーは、PAP および CHAP 認証方式だけを提供します。
- RADIUS サーバーに送信されるユーザー名にドメイン名を含めることはできません。

## プロトコルおよび標準

- RFC2865『Remote Authentication Dial In User Service(RADIUS)』
- RFC2866、RADIUS Accounting
- RFC2867『RADIUS Accounting Modifications for Tunnel Protocol Support』
- RFC2868『RADIUS Attributes for Tunnel Protocol Support』
- RFC2869、RADIUS Extensions
- RFC3576『Dynamic Authorization Extensions to Remote Authentication Dial In User Service(RADIUS)』

- RFC4818、RADIUS Delegated-IPv6-Prefix Attribute
- RFC5176『Dynamic Authorization Extensions to Remote Authentication Dial In User Service(RADIUS)』
- RFC1492、Access Control Protocol、Sometimes Called TACACS
- RFC1777、Lightweight Directory Access Protocol
- RFC2251、Lightweight Directory Access Protocol(v3)

# FIPS準拠

デバイスは、NIST FIPS140-2 要件に準拠した FIPS モードをサポートしています。機能、コマンド、およびパラメーターのサポートは、FIPS モードと非 FIPS モードで異なる場合があります。

## AAAタスクの概要

AAAを設定するには、次の作業を実行します。

### 1. AAAスキームの設定

ローカル認証を使用する場合は、ローカルユーザーと関連アトリビュートを設定します。リモート認証を使用する場合は、必要な RADIUS、LDAP、または HWTACACS スキームを設定します。

- ローカルユーザーの構成
- RADIUS の構成
- HWTACACS の構成
- LDAP の構成

### 2. ISPドメインの設定

- a. ISPドメインの作成
- b. ISPドメイン属性の構成

### 3. ISPドメインの AAA 方式の設定

必要に応じて、ISPドメインの認証、認可、アカウントング方式を設定します。これらの方式では、既存の AAA 方式が使用されます。

- ISPドメインの認証方法の構成
- ISPドメインの承認方法の構成
- ISPドメインのアカウントング方法の構成

### 4. (オプション)高度な AAA 機能の設定

- 同時ログインユーザーの最大数の設定
- NAS-ID の構成
- デバイス ID の構成
- RADIUS サーバー機能の構成
- 接続記録ポリシーの構成

## ローカルユーザーの構成

### ローカルユーザーについて

ローカル認証、認可およびアカウントングを実装するには、ローカルユーザーを作成し、デバイス上でユーザー属性を構成します。ローカルユーザーと属性は、デバイス上のローカルユーザーデータベースに格納されます。ローカルユーザーは、ユーザー名とユーザータイプの組み合わせによって一意に識別されません。

ローカルユーザーは、次のタイプに分類されます。

- Device management user: デバイス管理のためにデバイスにログインするユーザー。

- Network access user: デバイスを介してネットワークリソースにアクセスするユーザー。

次に、設定可能なローカルユーザートリビュートを示します。

- Description: ユーザーの説明情報。
- Service type: ユーザーが利用できるサービス。ローカル認証では、ローカルユーザーのサービスタイプがチェックされます。使用可能なサービスタイプがない場合、ユーザーは認証をパスできません。
- User state: ローカルユーザーがネットワークサービスを要求できるかどうか。ユーザー状態には、アクティブとブロックの2つがあります。アクティブ状態のユーザーはネットワークサービスを要求できますが、ブロック状態のユーザーはネットワークサービスを要求できません。
- Upper limit of concurrent logins using the same user name: 同じユーザー名を使用してデバイスに同時にアクセスできるユーザーの最大数。この数が上限に達すると、そのユーザー名を使用してデバイスにアクセスできるローカルユーザーはなくなります。
- User group: 各ローカルユーザーはローカルユーザーグループに属し、グループのすべての属性を持ちます。属性には、パスワード制御属性および許可属性が含まれます。ローカルユーザーグループの詳細は、Configuring user group attributes を参照してください。
- Binding attributes: バインド属性はユーザーの範囲を制御し、ユーザーのローカル認証時にチェックされます。ユーザーの属性がローカルユーザーアカウントに構成されたバインド属性と一致しない場合、ユーザーは認証をパスできません。
- Authorization attributes: 許可属性は、ユーザーがローカル認証した後のユーザーの権限を示します。

ローカルユーザーのサービスタイプに基づいて認可アトリビュートを設定します。

認可属性は、ユーザーグループビューまたはローカルユーザービューで構成できます。ローカルユーザービューでの認可属性の設定は、ユーザーグループビューでの属性設定より優先されます。

- ユーザーグループビューで設定されたアトリビュートは、ユーザーグループ内のすべてのローカルユーザーに対して有効になります。
- ローカルユーザービューで設定された属性は、ローカルユーザーに対してのみ有効です。
- Password control attributes: パスワード制御属性は、デバイス管理ユーザーのパスワードセキュリティの制御に役立ちます。パスワード制御属性には、パスワードのエージングタイム、最小パスワード長、パスワード構成チェック、パスワード複雑度チェックおよびログイン試行制限が含まれます。  
パスワード制御属性は、システムビュー、ユーザーグループビューまたはローカルユーザービューで構成できます。有効範囲が小さいパスワード制御属性の方が優先度が高くなります。パスワード管理およびグローバルパスワード構成の詳細は、ユーザーグループ属性の構成を参照してください。
- Validity period: ネットワークアクセスユーザーが認証に対して有効と見なされる期間。

## ローカルユーザー設定タスクの概要

ローカルユーザーを設定するには、次の作業を実行します。

1. ローカルユーザー属性の設定
  - デバイス管理ユーザーの属性の構成
  - ネットワークアクセスユーザーの属性の構成
2. (オプション) ユーザーグループ属性の構成
3. (オプション) ローカルユーザーの自動削除機能の構成

### 制約事項とガイドライン

**password-control enable** コマンドを使用してパスワード制御機能をグローバルにイネーブルにすると、ローカルユーザーパスワードは表示されません。

認可属性およびパスワード制御属性は、ローカルユーザービューまたはユーザーグループビューで構成できます。ローカルユーザービューの設定は、ユーザーグループビューの設定より優先されます。

## 手順

1. システムビューに入ります。  
**system-view**
2. デバイス管理ユーザーを追加し、デバイス管理ユーザービューに入ります。  
**local-user user-name class manage**
3. デバイス管理ユーザーのパスワードを設定します。  
非 FIPS モードの場合:  
**password [ { hash | simple } string ]**  
FIPS モードの場合:  
**password**  
非 FIPS モードでは、パスワードで保護されていないユーザーが正しいユーザー名を入力し、属性チェックに合格すると、そのユーザーは認証に合格します。セキュリティを強化するには、ローカルユーザーごとにパスワードを構成します。  
FIPS モードでは、パスワードで保護されたユーザーのみが認証を通過できます。デバイス管理ユーザーの場合は、パスワードを対話モードで設定する必要があります。
4. デバイス管理ユーザーにサービスを割り当てます。  
非 FIPS モードの場合:  
**service-type { ftp | { http | https | ssh | telnet | terminal } \* }**  
FIPS モードの場合:  
**service-type { https | ssh | terminal } \***  
デフォルトでは、デバイス管理ユーザーに許可されるサービスはありません。
5. (オプション)デバイス管理ユーザーのステータスを設定します。  
**state { active | block }**  
デフォルトでは、デバイス管理ユーザーはアクティブ状態にあり、ネットワークサービスを要求できません。
6. (オプション)デバイス管理ユーザー名を使用して同時ログインの上限を設定します。  
**access-limit max-user-number**  
デフォルトでは、デバイス管理ユーザーの同時ログイン数は制限されていません。  
このコマンドは、デバイス管理ユーザーにローカルアカウントが設定されている場合にだけ有効です。このコマンドは、アカウントをサポートしていない FTP、SFTP、または SCP ユーザーには適用されません。
7. (オプション)デバイス管理ユーザーの認可アトリビュートを設定します。  
**authorization-attribute { idle-cut minutes | user-role role-name | work-directory directory-name } \***  
次のデフォルト設定が適用されます。
  - FTP、SFTP および SCP ユーザーの作業ディレクトリは、NAS のルートディレクトリです。ただし、ユーザーにはルートディレクトリへのアクセス権はありません。
  - network-operator ユーザーロールは、network-admin ユーザーまたはレベル 15 ユーザーによって作成されたローカルユーザーに割り当てられます。
8. (オプション)デバイス管理ユーザーのパスワード制御アトリビュートを設定します。必要に応じて、次のタスクを選択します。
  - パスワードのエージングタイムを設定します。



**password-control aging** *aging-time*

- パスワードの最小長を設定します。

**password-control length** *length*

- パスワード構成ポリシーを構成します。

**password-control composition type-number** *type-number* [ **type-length** *type-length* ]

- パスワード複雑度チェックポリシーを設定します。

**password-control complexity** { **same-character** | **user-name** } **check**

- 最大ログイン試行回数およびログイン失敗時のアクションを設定します。

**password-control login-attempt** *login-times* [ **exceed** { **lock** | **lock-time** *time* | **unlock** } ]

デフォルトでは、デバイス管理ユーザーは、そのユーザーが属するユーザーグループのパスワード制御アトリビュートを使用します。

9. (オプション)デバイス管理ユーザーをユーザーグループに割り当てます。

**group** *group-name*

デフォルトでは、デバイス管理ユーザーはユーザーグループシステムに属します。

## 制約事項とガイドライン

認可属性は、ローカルユーザービューまたはユーザーグループビューで構成できます。ローカルユーザービューの設定は、ユーザーグループビューの設定より優先されます。

ユーザーのサービスタイプに基づいて *location* バインディングアトリビュートを設定します。

- 802.1X ユーザーの場合、ユーザーがデバイスにアクセスするための 802.1X 対応レイヤー2 イーサネットインターフェースまたはレイヤー2 集約インターフェースを指定します。
- MAC 認証ユーザーの場合、ユーザーがデバイスにアクセスするための MAC 認証対応レイヤー2 イーサネットインターフェースまたはレイヤー2 集約インターフェースを指定します。
- Web 認証ユーザーの場合、ユーザーがデバイスにアクセスするための Web 認証対応レイヤー2 イーサネットインターフェースを指定します。
- ポータルユーザーの場合は、ユーザーがデバイスにアクセスするためのポータル対応インターフェースを指定します。VLAN インターフェース上でポータルがイネーブル、*portal roaming enable* コマンドが設定されていない場合は、レイヤー2 イーサネットインターフェースを指定します。

## 手順

1. システムビューに入ります。

**system-view**

2. ネットワークアクセスユーザーを追加し、ネットワークアクセスユーザービューを入力します。

**local-user** *user-name* **class** **network**

3. (オプション)ネットワークアクセスユーザーのパスワードを設定します。

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

4. (オプション)ネットワークアクセスユーザーの説明を設定します。

**description** *text*

デフォルトでは、ローカルユーザーの説明は設定されていません。

5. ネットワークアクセスユーザーにサービスを割り当てます。

**service-type** { **lan-access** | **portal** }

デフォルトでは、ネットワークアクセスユーザーに許可されるサービスはありません。

6. (オプション)ネットワークアクセスユーザーのステータスを設定します。

**state** { **active** | **block** }

デフォルトでは、ネットワークアクセスユーザーはアクティブ状態にあり、ネットワークサービスを要求できます。

7. (オプション)ネットワークアクセスユーザー名を使用して同時ログインの上限を設定します。

**access-limit** *max-user-number*

デフォルトでは、ネットワークアクセスユーザーの同時ログイン数は制限されていません。

8. (オプション)ネットワークアクセスユーザーのバインディングアトリビュートを設定します。

**bind-attribute** { **ip** *ip-address* | **location interface** *interface-type interface-number* | **mac** *mac-address* | **vlan** *vlan-id* } \*

デフォルトでは、ネットワークアクセスユーザーのバインディングアトリビュートは設定されていません。

9. (オプション)ネットワークアクセスユーザーの認可アトリビュートを設定します。

**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minutes* | **ip-pool** *ipv4-pool-name* | **ipv6-pool** *ipv6-pool-name* | **session-timeout** *minutes* | **user-profile** *profile-name* | **vlan** *vlan-id* } \*

デフォルトでは、ネットワークアクセスユーザーには認可アトリビュートがありません。

10. (オプション)ネットワークアクセスユーザーをユーザーグループに割り当てます。

**group** *group-name*

デフォルトでは、ネットワークアクセスユーザーはユーザーグループシステムに属します。

11. (オプション)ローカルユーザーの有効期間を指定します。

**validity-datetime** { **from** *start-date start-time* **to** *expiration-date expiration-time* | **from** *start-date start-time* | **to** *expiration-date expiration-time* }

デフォルトでは、ネットワークアクセスユーザーの有効期間は満了しません。

## ユーザーグループ属性の構成

### ユーザーグループ属性について

ユーザーグループを使用すると、ローカルユーザーの構成と管理が簡素化されます。ユーザーグループには、ローカルユーザーのグループが含まれており、一連のローカルユーザー属性があります。ユーザーグループのローカルユーザー属性を構成して、グループ内のローカルユーザーの集中ユーザー属性管理を実装できます。管理可能なローカルユーザー属性には、認可属性が含まれます。

### 手順

1. システムビューに入ります。

**system-view**

2. ユーザーグループを作成し、ユーザーグループビューを入力します。

**user-group** *group-name*

デフォルトでは、システム定義のユーザーグループが存在します。グループ名は `system` です。

3. ユーザーグループの認可アトリビュートを設定します。

**authorization-attribute** { **acl** *acl-number* | **idle-cut** *minutes* | **ip-pool** *ipv4-pool-name* | **ipv6-pool** *ipv6-pool-name* | **session-timeout** *minutes* | **user-profile** *profile-name* | **vlan** *vlan-id* | **work-directory** *directory-name* } \*

デフォルトでは、ユーザーグループに認可アトリビュートは設定されていません。

4. (オプション)ユーザーグループのパスワード制御アトリビュートを設定します。必要に応じて、次のタスクを選択します。

- パスワードのエージングタイムを設定します。

**password-control aging** *aging-time*

- パスワードの最小長を設定します。

**password-control length** *length*

- パスワード構成ポリシーを構成します。

**password-control composition type-number** *type-number* [ **type-length** *type-length* ]

- パスワード複雑度チェックポリシーを設定します。

**password-control complexity** { **same-character** | **user-name** } **check**

- ログイン試行回数およびログイン失敗時のアクションを設定します。

**password-control login-attempt** *login-times* [ **exceed** { **lock** | **lock-time** *time* | **unlock** } ]

デフォルトでは、ユーザーグループはグローバルパスワード制御設定を使用します。詳細は、パスワード制御の構成を参照してください。

パスワード制御アトリビュートは、デバイス管理ユーザーだけに適用できます。

## ローカルユーザー自動削除機能の設定

### ローカルユーザーの自動削除機能について

この機能を使用すると、デバイスは 10 分間の固定時間でローカルユーザーの有効性を検査し、期限切れのローカルユーザーを自動的に削除できます。

#### 手順

1. システムビューに入ります。

**system-view**

2. ローカルユーザー自動削除機能をイネーブルにします。

**local-user auto-delete enable**

デフォルトでは、ローカルユーザー自動削除機能はディセーブルです。

## ローカルユーザーおよびローカルユーザーグループ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ます。

タスク	コマンド
ローカルユーザー設定およびオンラインユーザー統計情報を表示します。	<b>display local-user</b> [ <b>class</b> { <b>manage</b>   <b>network</b> }   <b>idle-cut</b> { <b>disable</b>   <b>enable</b> }   <b>service-type</b> { <b>ftp</b>   <b>http</b>   <b>https</b>   <b>lan-access</b>   <b>portal</b>   <b>ssh</b>   <b>telnet</b>   <b>terminal</b> }   <b>state</b> { <b>active</b>   <b>block</b> }   <b>user-name</b> <i>user-name</i> <b>class</b> { <b>manage</b>   <b>network</b> }   <b>vlan</b> <i>vlan-id</i> ]
ユーザーグループ設定を表示します。	<b>display user-group</b> { <b>all</b>   <b>name</b> <i>group-name</i> }

# RADIUS タスクの概要

RADIUS を設定するには、次の作業を実行します。

1. RADIUS サーバーステータス検出用のテストプロファイルの構成  
RADIUS サーバーステータスを検出するには、テストプロファイルを設定し、RADIUS スキームでテストプロファイルを使用するように RADIUS サーバーを設定する必要があります。
2. RADIUS スキームの作成
3. RADIUS 認証サーバーの指定
4. RADIUS アカウンティングサーバーの指定
5. 安全な RADIUS 通信のための共有キーの指定  
RADIUS 認証サーバーはアカウンティングサーバーの設定時に共有キーが指定されていない場合は、この作業を実行します。
6. RADIUS スキームの MPLS L3VPN インスタンスの指定  
RADIUS 認証サーバーまたはアカウンティングサーバーの設定時に MPLS L3VPN インスタンスが指定されていない場合、この作業を実行します。
7. (オプション)RADIUS サーバーのステータスの設定
8. (オプション)RADIUS タイマーの設定
9. (オプション)RADIUS パケットのパラメーターの設定
  - 発信 RADIUS パケットの送信元 IP アドレスの指定
  - ユーザー名の形式とトラフィック統計単位の設定
  - RADIUS 要求送信の最大試行回数の設定
  - リアルタイムアカウンティングの最大試行回数の設定
  - RADIUS パケットの DSCP 優先度の設定
10. (オプション)RADIUS アトリビュートのパラメーターの設定
  - SSH、FTP、およびターミナルユーザーの Login-Service 属性チェック方法の構成
  - RADIUS クラス属性を CAR パラメーターとして解釈する
  - RADIUS 属性 31 の MAC アドレス形式の構成
  - Remanent\_Volume 属性のデータ測定単位の設定
  - RADIUS 属性変換機能の構成
11. (オプション)拡張 RADIUS 機能の設定
  - RADIUS ストップアカウンティングパケットバッファリングの設定
  - アカウンティング停止パケットの強制送信を有効にする
  - RADIUS サーバーの負荷分散機能を有効にする
  - RADIUS アカウンティング機能の設定
  - RADIUS セッション制御機能の設定
  - RADIUSDAS 機能の構成
  - RADIUS の SNMP 通知を有効にする

# RADIUS 設定の制約事項およびガイドライン

RADIUS スキームの認証サーバーがデバイスの RADIUS サーバー機能によって提供される場合、RADIUS スキームには次の設定だけが含まれます。

- RADIUS 認証サーバー。
- RADIUS 通信用の共有キー。
- RADIUS サーバーと対話するためのユーザー名形式。

## RADIUS サーバーステータス検出用のテストプロファイルの設定

### RADIUS サーバーステータス検出用のテストプロファイルについて

テストプロファイルを使用して、検出間隔で RADIUS 認証サーバーが到達可能かどうかを検出します。RADIUS サーバーのステータスを検出するには、RADIUS スキームでこのテストプロファイルを使用するように RADIUS サーバーを設定する必要があります。

テストプロファイルを指定すると、デバイスは各検出間隔内に検出パケットを RADIUS サーバーに送信します。検出パケットは、テストプロファイル内に指定されたユーザー名とパスワードを含む、シミュレートされた認証要求です。

- デバイスは、インターバル内にサーバーから応答を受信すると、サーバーをアクティブ状態に設定します。
- デバイスがインターバル内にサーバーから応答を受信しない場合、デバイスはサーバーをブロックステートに設定します。

デバイスは、検出結果に従って、検出間隔ごとに RADIUS サーバーのステータスをリフレッシュします。

### 制約事項とガイドライン

システムに複数のテストプロファイルを設定できます。

RADIUS 認証サーバーに既存のテストプロファイルが指定されている場合に限り、デバイスは RADIUS サーバーのステータスの検出を開始します。

次のいずれかの操作が実行されると、デバイスは RADIUS サーバーのステータスの検出を停止します。

- RADIUS サーバーが RADIUS スキームから削除されます。
- RADIUS スキームビューの RADIUS サーバーのテストプロファイル設定が削除されます。
- テストプロファイルが削除されます。
- RADIUS サーバーは手動でブロックステートに設定されます。
- RADIUS スキームが削除されます。

### 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS 認証サーバーのステータスを検出するためのテストプロファイルを設定します。  
**radius-server test-profile profile-name username name [ password { cipher | simple } string ] [ interval interval ]**

## RADIUS スキームの作成

### 制約事項とガイドライン

最大 16 の RADIUS スキームを設定できます。RADIUS スキームは複数の ISP ドメインで使用できます。

## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームを作成し、RADIUS スキームビューに入ります。  
**radius scheme** *radius-scheme-name*

## RADIUS 認証サーバーについて

RADIUS 認証サーバーはクライアントに送信される認証応答に載せられるため、RADIUS 認証サーバーは認証と認可を同時に完了します。

RADIUS スキームには、1 つのプライマリ認証サーバーと最大 16 のセカンダリ認証サーバーを指定できます。セカンダリサーバーは、プライマリサーバーが到達不能になったときに AAA サービスを提供します。デバイスは、セカンダリサーバーが設定されている順序でアクティブサーバーを検索します。

RADIUS サーバーのロードシェアリングが有効になっている場合、デバイスはプライマリサーバーとセカンダリサーバーの役割を考慮せずに、すべてのサーバーにワークロードを分散します。デバイスは、アクティブなサーバーごとに現在サービスされているユーザーの重み値と数をチェックし、認証要求を受信するために最適なサーバーをパフォーマンスで決定します。

## 制約事項とガイドライン

冗長性が不要な場合は、プライマリサーバーだけを指定します。

RADIUS 認証サーバーは、ある方式のプライマリ認証サーバーと別の方式のセカンダリ認証サーバーとして同時に機能できます。

スキーム内の 2 つの認証サーバー(プライマリまたはセカンダリ)は、VPN インスタンス、ホスト名、IP アドレス、およびポート番号の同じ組み合わせを持つことはできません。

## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームビューに入ります。  
**radius scheme** *radius-scheme-name*
3. プライマリ RADIUS 認証サーバーを指定します。  
**primary authentication** { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [ *port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **vpn-instance** *vpn-instance-name* | **weight** *weight-value* ] \*  
デフォルトでは、プライマリ RADIUS 認証サーバーは指定されていません。  
*weight* キーワードが有効になるのは、RADIUS サーバーロードシェアリング機能が RADIUS スキームに対してイネーブルになっている場合だけです。
4. (オプション)セカンダリ RADIUS 認証サーバーを指定します。  
**secondary authentication** { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [ *port-number* | **key** { **cipher** | **simple** } *string* | **test-profile** *profile-name* | **vpn-instance** *vpn-instance-name* | **weight** *weight-value* ] \*  
デフォルトでは、セカンダリ RADIUS 認証サーバーは指定されていません。  
*weight* キーワードが有効になるのは、RADIUS サーバーロードシェアリング機能が RADIUS スキームに対してイネーブルになっている場合だけです。

## RADIUS アカウンティングサーバーについて

RADIUS スキームには、1 つのプライマリアカウンティングサーバーと最大 16 のセカンダリアカウンティングサーバーを指定できます。セカンダリサーバーは、プライマリサーバーが使用できなくなったときに AAA

サービスを提供します。デバイスは、セカンダリサーバーが設定されている順序でアクティブサーバーを検索します。

RADIUS サーバーのロードシェアリングが有効になっている場合、デバイスはプライマリサーバーとセカンダリサーバーの役割を考慮せずに、すべてのサーバーにワークロードを分散します。デバイスは、アクティブサーバーごとに現在サービスされているユーザーの重み値と数をチェックし、アカウントリング要求を受信するために最適なサーバーをパフォーマンスで決定します。

## 制約事項とガイドライン

冗長性が不要な場合は、プライマリサーバーだけを指定します。

RADIUS アカウンティングサーバーは、ある方式のプライミアカウンティングサーバーと別の方式のセカンダリアカウンティングサーバーとして同時に機能できます。

スキーム内の 2 つのアカウントリングサーバー(プライマリまたはセカンダリ)は、VPN インスタンス、ホスト名、IP アドレス、およびポート番号の同じ組み合わせを持つことはできません。

RADIUS は、FTP、SFTP、および SCP ユーザーのアカウントリングをサポートしていません。

## 手順

1. システムビューに入ります。

**system-view**

2. RADIUS スキームビューに入ります。

**radius scheme** *radius-scheme-name*

3. プライマリ RADIUS アカウンティングサーバーを指定します。

**primary accounting** { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [ *port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name* | **weight** *weight-value* ] \*

デフォルトでは、プライマリ RADIUS アカウンティングサーバーは指定されていません。

**weight** キーワードが有効になるのは、RADIUS サーバーロードシェアリング機能が RADIUS スキームに対してイネーブルになっている場合だけです。

4. (オプション)セカンダリ RADIUS アカウンティングサーバーを指定します。

**secondary accounting** { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [ *port-number* | **key** { **cipher** | **simple** } *string* | **vpn-instance** *vpn-instance-name* | **weight** *weight-value* ] \*

デフォルトでは、セカンダリ RADIUS アカウンティングサーバーは指定されていません。

**weight** キーワードが有効になるのは、RADIUS サーバーロードシェアリング機能が RADIUS スキームに対してイネーブルになっている場合だけです。

## セキュア RADIUS 通信用の共有キーの指定

### セキュア RADIUS 通信用の共有キーについて

RADIUS クライアントおよびサーバーは、MD5 アルゴリズムおよび共有キーを使用して、パケット認証およびユーザーパスワード暗号化用のオーセンティケーター値を生成します。クライアントおよびサーバーは、通信のタイプごとに同じキーを使用する必要があります。

このタスクで設定されるキーは、スキーム内の同じタイプ(アカウントリングまたは認証)のすべてのサーバー一用です。キーのプライオリティは、RADIUS サーバー用に個別に設定されるキーよりも低くなります。

## 制約事項とガイドライン

デバイスに設定されている共有キーは、RADIUS サーバーに設定されている共有キーと同じである必要があります。

## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームビューに入ります。  
**radius scheme** *radius-scheme-name*
3. セキュア RADIUS 通信用の共有キーを指定します。  
**key** { **accounting** | **authentication** } { **cipher** | **simple** } *string*  
デフォルトでは、セキュア RADIUS 通信用の共有キーは指定されていません。

# RADIUS スキームの MPLS L3VPN インスタンスの指定

## RADIUS スキームの MPLS L3VPN インスタンスについて

RADIUS スキームに指定された VPN インスタンスは、そのスキーム内のすべての認証およびアカウントリングサーバーに適用されます。VPN インスタンスが個々の RADIUS サーバーにも設定されている場合、RADIUS スキームに指定された VPN インスタンスはそのサーバーには適用されません。

## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームビューに入ります。  
**radius scheme** *radius-scheme-name*
3. RADIUS スキームの VPN インスタンスを指定します。  
**vpn-instance** *vpn-instance-name*  
デフォルトでは、RADIUS スキームはパブリックネットワークに属します。

# RADIUS サーバーのステータスの設定

## RADIUS サーバーのステータスについて

現在のサーバーが使用できなくなったときにデバイスが通信する RADIUS サーバーを制御するには、RADIUS サーバーのステータスをブロックまたはアクティブに設定します。1 つのプライマリ RADIUS サーバーと複数のセカンダリ RADIUS サーバーを指定できます。セカンダリサーバーはプライマリサーバーのバックアップとして機能します。RADIUS サーバーの負荷分散機能が無効になっている場合、デバイスは次のルールに基づいてサーバーを選択します。

- プライマリサーバーがアクティブ状態の場合、デバイスは最初にプライマリサーバーとの通信を試みます。プライマリサーバーが到達不能の場合、デバイスはサーバーが設定されている順序でアクティブなセカンダリサーバーを検索します。
- 1 つまたは複数のサーバーがアクティブ状態の場合、デバイスはこれらのアクティブサーバーとのみ通信しようとします。サーバーが使用できない場合も同様です。
- すべてのサーバーがブロック状態の場合、デバイスはプライマリサーバーとの通信だけを試みます。
- サーバーに到達できない場合、デバイスは次の操作を実行します。
  - サーバーステータスをブロック済みに変更します。
  - サーバーの待機タイマーを開始します。
  - 最も高いプライオリティを持つアクティブ状態の次のセカンダリサーバーと通信しようとします。



- サーバーの待機タイマーが期限切れになるか、サーバーを手動でアクティブ状態に設定すると、サーバーのステータスがアクティブに戻ります。認証またはアカウントングプロセス中に、デバイスはサーバーを再度チェックしません。
- デバイスが使用可能なセカンダリサーバーを検出するか、すべてのセカンダリサーバーのセカンダリサーバーをチェックするまで、検索プロセスが続行されます。到達可能なサーバーがない場合、デバイスは認証またはアカウントングの試行を失敗と見なします。
- 使用中のサーバーを削除すると、そのサーバーとの通信がタイムアウトします。デバイスは、最初にプライマリサーバーをチェックし、次にセカンダリサーバーを設定順にチェックすることによって、アクティブ状態のサーバーを探します。
- RADIUS サーバーのステータスが自動的に変更されると、デバイスは、このサーバーが指定されているすべての RADIUS スキームに従ってこのサーバーのステータスを変更します。
- RADIUS サーバーが手動でブロックに設定されている場合、サーバーにテストプロファイルが指定されているかどうかに関係なく、サーバー検出は無効になります。RADIUS サーバーがアクティブ状態に設定されている場合、サーバー検出は既存のテストプロファイルが指定されているサーバーに対して有効になります。

デフォルトでは、デバイスはすべての RADIUS サーバーのステータスをアクティブに設定します。ただし、状況によっては、サーバーのステータスを変更する必要があります。たとえば、サーバーに障害が発生した場合、サーバーへの通信試行を避けるために、サーバーのステータスをブロックに変更できます。

## 制約事項とガイドライン

設定されたサーバーステータスは、どの設定ファイルにも保存できず、`display radius scheme` コマンドを使用しないと表示できません。

デバイスの再起動後、すべてのサーバーがアクティブ状態に復元されます。

## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームビューに入ります。  
**radius scheme** *radius-scheme-name*
3. RADIUS サーバーのステータスを設定します。必要に応じて、次のタスクを選択します。
  - プライマリ RADIUS 認証サーバーのステータスを設定します。  
**state primary authentication** { **active** | **block** }
  - プライマリ RADIUS アカウントングサーバーのステータスを設定します。  
**state primary accounting** { **active** | **block** }
  - セカンダリ RADIUS 認証サーバーのステータスを設定します。  
**state secondary authentication** [ { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [ *port-number* | **vpn-instance** *vpn-instance-name* ] \* ] { **active** | **block** }
  - セカンダリ RADIUS アカウントングサーバーのステータスを設定します。  
**state secondary accounting** [ { *host-name* | *ipv4-address* | **ipv6** *ipv6-address* } [ *port-number* | **vpn-instance** *vpn-instance-name* ] \* ] { **active** | **block** }

デフォルトでは、RADIUS サーバーはアクティブステートです。

# RADIUS タイマーの設定

## RADIUS タイマーについて

デバイスは、次のタイプのタイマーを使用して RADIUS サーバーとの通信を制御します。

- サーバー応答タイムアウトタイマー(応答タイムアウト): RADIUS 要求の再送信間隔を定義します。タイマーは、RADIUS 要求が送信された直後に開始されます。タイマーの期限が切れる前にデバイスが RADIUS サーバーからの応答を受信しなかった場合、デバイスは要求を再送信します。
- サーバー待機タイマー(待機): 到達不能なサーバーをブロック状態に維持する期間を定義します。あるサーバーに到達できない場合、デバイスはサーバステータスをブロックに変更し、そのサーバーに対してこのタイマーを開始し、アクティブ状態の別のサーバーとの通信を試みます。サーバー待機タイマーの期限が切れると、デバイスはサーバステータスをアクティブに戻します。
- リアルタイムアカウントングタイマー(realtime-accounting): デバイスがオンラインユーザーの RADIUS アカウントングサーバーにリアルタイムアカウントングパケットを送信する間隔を定義します。

RADIUS パケット送信の最大試行回数および RADIUS サーバー応答タイムアウトタイマーを設定する場合は、セカンダリサーバーの数を考慮してください。RADIUS スキームにセカンダリサーバーが多数含まれている場合、再送信プロセスが長すぎる可能性があり、Telnet などのアクセスモジュールのクライアント接続がタイムアウトする可能性があります。

クライアント接続のタイムアウト時間が短い場合、多数のセカンダリサーバーが最初の認証またはアカウントングの試行を失敗させる可能性があります。この場合、RADIUS パケット送信試行およびサーバー応答タイムアウトタイマーを調整するのではなく、クライアントを再接続してください。通常、次の試行は成功します。これは、デバイスが到達不能なサーバーをブロックして到達可能なサーバーを見つける時間を短縮したためです。

サーバー待機タイマーが正しく設定されていることを確認してください。タイマーが短すぎると、認証またはアカウントングの失敗が頻繁に発生する可能性があります。これは、デバイスがアクティブ状態の到達不能なサーバーとの通信を試み続けるためです。タイマーが長すぎると、障害から回復した到達可能なサーバーが一時的にブロックされる可能性があります。これは、サーバーがタイマーの期限が切れるまでブロック状態にとどまるためです。

短いリアルタイムのアカウントング間隔は、アカウントングの精度を向上させますが、多くのシステムリソースを必要とします。ユーザー数が 1000 人以上の場合は、間隔を 15 分以上に設定します。

## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームビューに入ります。  
**radius scheme radius-scheme-name**
3. RADIUS タイマーを設定します。必要に応じて、次のタスクを選択します。
  - RADIUS サーバー応答タイムアウトタイマーを設定します。  
**timer response-timeout seconds**  
デフォルト設定は 3 秒です。
  - サーバーの待機タイマーを設定します。  
**timer quiet minutes**  
デフォルト設定は 5 分です。
  - リアルタイムアカウントングタイマーを設定します。  
**timer realtime-accounting interval [ second ]**  
デフォルト設定は 12 分です。

# 発信 RADIUS パケットの送信元 IP アドレスの指定

## 発信 RADIUS パケットの送信元 IP アドレスについて

NAS が送信する RADIUS パケットの送信元 IP アドレスは、RADIUS サーバー上設定されている NAS の IP アドレスと一致する必要があります。RADIUS サーバーは、IP アドレスによって NAS を識別します。RADIUS サーバーは、RADIUS パケットを受信すると、パケットの送信元 IP アドレスが管理対象 NAS の IP アドレスかどうかをチェックします。

- 管理対象 NAS の IP アドレスの場合、サーバーはパケットを処理します。
- 管理対象 NAS の IP アドレスでない場合、サーバーはパケットをドロップします。

NAS は、RADIUS パケットを送信する前に、次の順序で送信元 IP アドレスを選択します。

1. RADIUS スキームに指定された送信元 IP アドレス。
2. RADIUS サーバーが存在する場所に応じて、VPN またはパブリックネットワークのシステムビューで指定された送信元 IP アドレス。
3. ルートで指定された発信インターフェースの IP アドレス。

## 送信元 IP アドレス設定の制約事項およびガイドライン

発信 RADIUS パケットの送信元 IP アドレスは、RADIUS スキームビューまたはシステムビューで指定できます。

- RADIUS スキームビューで指定された IP アドレスは、1 つの RADIUS スキームだけに適用されます。
- システムビューで指定された IP アドレスは、すべての RADIUS スキームに適用されます。

NAS が送信する RADIUS パケットの送信元 IP アドレスは、RADIUS サーバーに設定されている NAS の IP アドレスと一致する必要があります。

物理ポートエラーによる RADIUS パケット損失を避けるために、発信 RADIUS パケットの送信元 IP アドレスとしてループバックインターフェースアドレスを指定することをお勧めします。

通常、発信 RADIUS パケットの送信元アドレスは、RADIUS サーバーと通信する NAS 上の出カインターフェースの IP アドレスです。ただし、場合によっては、送信元 IP アドレスを変更する必要があります。たとえば、VRRP がステートフルフェールオーバー用に設定されている場合、アップリンク VRRP グループの仮想 IP を送信元アドレスとして設定します。

## すべての RADIUS スキームの送信元 IP アドレスの指定

1. システムビューに入ります。

**system-view**

2. 発信 RADIUS パケットの送信元 IP アドレスを指定します。

```
radius nas-ip { ipv4-address | ipv6 ipv6-address } [ vpn-instance vpn-instance-name ]
```

デフォルトでは、RADIUS パケット発信インターフェースのプライマリ IP アドレスが送信元 IP アドレスとして使用されます。

## RADIUS スキームの送信元 IP アドレスの指定

1. システムビューに入ります。

**system-view**

2. RADIUS スキームビューに入ります。

```
radius scheme radius-scheme-name
```

3. 発信 RADIUS パケットの送信元 IP アドレスを指定します。

```
nas-ip { ipv4-address | ipv6 ipv6-address }
```

デフォルトでは、システムビューで `radius nas-ip` コマンドを使用して指定された送信元 IP アドレスが使用されます。送信元 IP アドレスが指定されていない場合は、アウトバウンドインターフェースのプライマリ IP アドレスが使用されます。

## ユーザー名フォーマットとトラフィック統計ユニットについて

ユーザー名は `userid@isp-name` 形式です。isp-name 部分はユーザーの ISP ドメイン名を表します。デフォルトでは、ISP ドメイン名がユーザー名に含まれます。ただし、古い RADIUS サーバーでは、ISP ドメイン名を含むユーザー名が認識されない場合があります。この場合、送信する各ユーザー名のドメイン名を削除するようにデバイスを構成できます。

デバイスは、アカウントングパケットでオンラインユーザートラフィック統計情報を報告します。トラフィック測定単位は設定可能です。

## 制約事項とガイドライン

2 つ以上の ISP ドメインが同じ RADIUS スキームを使用する場合は、RADIUS スキームを設定して、ドメイン識別用のユーザー名に ISP ドメイン名を保持します。

アカウントングを正確に行うために、デバイスと RADIUS アカウントングサーバーで設定されているトラフィック統計情報ユニットが同じであることを確認してください。

## 手順

1. システムビューに入ります。

**system-view**

2. RADIUS スキームビューに入ります。

**radius scheme radius-scheme-name**

3. RADIUS サーバーに送信するユーザー名の形式を設定します。

**user-name-format { keep-original | with-domain | without-domain }**

デフォルトでは、ISP ドメイン名はユーザー名に含まれています。

デバイスがスキームで RADIUS サーバーとして指定されている場合は、ユーザー名の形式を `without-domain` に設定する必要があります。

4. トラフィック統計情報のデータフローおよびパケット測定単位を設定します。

**data-flow-format { data { byte | giga-byte | kilo-byte | mega-byte } | packet { giga-packet | kilo-packet | mega-packet | one-packet } }**\*

デフォルトでは、トラフィックはバイト単位およびパケット単位でカウントされます。

# RADIUS 要求送信の最大試行回数の設定

## RADIUS 要求送信の最大試行回数設定について

RADIUS は UDP パケットを使用してデータを転送します。UDP 通信は信頼できないため、RADIUS は信頼性を向上させるために再送信メカニズムを使用します。NAS が応答タイムアウトタイマー内に要求に対するサーバー応答を受信しない場合、RADIUS 要求は再送信されます。RADIUS サーバー応答タイムアウトタイマーの詳細については、「」を参照してください。RADIUS サーバーの状態の設定。

NAS が同じサーバーに RADIUS 要求を再送信する最大数を設定できます。最大数に達すると、NAS はアクティブ状態の他の RADIUS サーバーとの通信を試行します。その時点でアクティブ状態の他のサーバーがない場合、NAS は認証またはアカウントングの試行を失敗と見なします。

## 手順

1. システムビューに入ります。

**system-view**

2. RADIUS スキームビューに入ります。

**radius scheme** *radius-scheme-name*

3. RADIUS 要求送信の最大試行回数を設定します。

**retry** *retries*

デフォルトでは、RADIUS 要求送信試行の最大数は 3 です。

### リアルタイムアカウントングの最大試行回数の設定について

リアルタイムアカウントングの最大試行回数を設定した場合、デバイスは、許可された試行回数内にアカウントング応答を受信しなかったユーザーの接続を解除します。

#### 手順

1. システムビューに入ります。

**system-view**

2. RADIUS スキームビューに入ります。

**radius scheme** *radius-scheme-name*

3. リアルタイムアカウントングの最大試行回数を設定します。

**retry realtime-accounting** *retries*

デフォルトでは、リアルタイムアカウントング試行の最大数は 5 です。

### RADIUS パケットの DSCP プライオリティについて

ToS フィールドの DSCP プライオリティによって、RADIUS パケットの送信プライオリティが決まります。値が大きいほど、プライオリティが高くなります。

#### 手順

1. システムビューに入ります。

**system-view**

2. RADIUS パケットの DSCP プライオリティを設定します。

**radius [ ipv6 ] dscp** *dscp-value*

デフォルトでは、RADIUS パケットの DSCP プライオリティは 0 です。

## SSH、FTP、および端末ユーザーのログインサービス属性チェック方法の設定

### ログインサービス属性チェック方法について

デバイスは、SSH、FTP、および端末ユーザーの Login-Service アトリビュート(RADIUS アトリビュート 15) に対して次のチェック方式をサポートしています。

- Strict: SSH、FTP、およびターミナルサービスの Login-Service アトリビュート値 50、51、および 52 します。
- Loose: SSH、FTP、およびターミナルサービスの標準ログインサービス属性値 0 と一致します。

ユーザーに対して受信した Access-Accept パケットには、一致するアトリビュート値が含まれている必要があります。一致しない場合、ユーザーはデバイスにログインできません。

### 制約事項とガイドライン

ルーズチェック方式は、サーバーが SSH、FTP、および端末ユーザーに対して Login-Service アトリビュート値 50、51、および 52 を発行しない場合にだけ使用してください。

#### 手順

1. システムビューに入ります。

### **system-view**

2. RADIUS スキームビューに入ります。

**radius scheme** *radius-scheme-name*

3. SSH、FTP、および端末ユーザーのログインサービスアトリビュートチェック方法を設定します。

**attribute 15 check-mode** { **loose** | **strict** }

デフォルトのチェック方法は **strict** です。

## RADIUS クラス属性の CAR パラメーターとしての解釈

### RADIUS クラス属性の CAR パラメーターとしての解釈について

RADIUS サーバーは、RADIUS パケット内の RADIUS クラス属性(属性 25)を使用して、ユーザーベースのトラフィックモニタリングおよび制御用の CAR パラメーターを配信できます。CAR パラメーターに対するクラス属性を解釈するようにデバイスを設定できます。

#### 手順

1. システムビューに入ります。

**system-view**

2. RADIUS スキームビューに入ります。

**radius scheme** *radius-scheme-name*

3. RADIUS クラスアトリビュートを CAR パラメーターとして解釈します。

**attribute 25 car**

デフォルトでは、RADIUS クラス属性は CAR パラメーターとして解釈されません。

### 制約事項とガイドライン

タイプが異なる RADIUS サーバーは、RADIUS アトリビュート 31 の MAC アドレスフォーマットに対して異なる要件を持つ場合があります。RADIUS サーバーの要件を満たすように、RADIUS アトリビュート 31 の MAC アドレスフォーマットを設定します。

#### 手順

1. システムビューに入ります。

**system-view**

2. RADIUS スキームビューに入ります。

**radius scheme** *radius-scheme-name*

3. RADIUS アトリビュート 31 の MAC アドレスフォーマットを設定します。

**attribute 31 mac-format section** { **six** | **three** } **separator** *separator-character* { **lowercase** | **uppercase** }

デフォルトでは、MAC アドレスは HH-HH-HH-HH-HH-HH の形式になっています。MAC アドレスはハイフン(-)で区切られ、大文字の 6 つのセクションに分けられています。

## Remanent\_Volume 属性のデータ測定単位の設定

### Remanent\_Volume 属性のデータ測定単位について

RADIUS サーバーは、認証またはリアルタイムアカウントリング応答で Remanent\_Volume アトリビュートを使用して、オンラインユーザーが使用できる現在のデータ量をデバイスに通知します。

## 制約事項とガイドライン

設定されている測定単位が、RADIUS サーバーのユーザーデータ測定単位と同じであることを確認します。

### 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームビューに入ります。  
**radius scheme radius-scheme-name**
3. Remanent\_Volume 属性のデータ測定単位を設定します。  
**attribute remanent-volume unit { byte | giga-byte | kilo-byte | mega-byte }**  
デフォルトのデータ測定単位はキロバイトです。

## RADIUS アトリビュート変換について

RADIUS アトリビュート変換機能を使用すると、デバイスと互換性のない RADIUS アトリビュートをサポートするさまざまなベンダーの RADIUS サーバーとデバイスを正しく動作させることができます。

RADIUS アトリビュート変換には、次の実装があります。

- アトリビュート変換: RADIUS アトリビュート変換規則に基づいて、送信元 RADIUS アトリビュートを宛先 RADIUS アトリビュートに変換します。
- アトリビュート拒否: RADIUS 属性拒否規則に基づいて RADIUS 属性を拒否します。

RADIUS アトリビュート変換機能がイネーブルの場合、デバイスは RADIUS パケットを次のように処理します。

- 送信された RADIUS パケットの場合:
  - 拒否されたアトリビュートをパケットから削除します。
  - 宛先 RADIUS アトリビュートを使用して、パケット内の RADIUS アトリビュート変換ルールに一致するアトリビュートを置き換えます。
- 受信した RADIUS パケットの場合:
  - パケット内の拒否されたアトリビュートを無視します。
  - RADIUS アトリビュート変換規則に一致するアトリビュートを宛先 RADIUS アトリビュートとして解釈します。

独自の RADIUS アトリビュートを識別するには、アトリビュートを拡張 RADIUS アトリビュートとして定義し、拡張 RADIUS アトリビュートをデバイスサポートアトリビュートに変換します。

## RADIUS アトリビュート変換設定の制約事項およびガイドライン

RADIUS アトリビュートに変換ルールまたは拒否ルールを設定します。

RADIUS アトリビュートに方向ベースのルールまたはパケットタイプベースのルールを設定します。

RADIUS アトリビュートの方向ベースの変換では、方向(インバウンドまたはアウトバウンド)ごとにルールを設定できます。RADIUS アトリビュートのパケットタイプベースの変換では、RADIUS パケットタイプ(RADIUS Access-Accept、RADIUS Access-Request、または RADIUS アカウンティング)ごとにルールを設定できます。

1. システムビューに入ります。  
**system-view**
2. (オプション)拡張 RADIUS アトリビュートを定義します。  
**radius attribute extended attribute-name [ vendor vendor-id ] code attribute-code type { binary | date | integer | interface-id | ip | ipv6 | ipv6-prefix | octets | string }**

3. RADIUS スキームビューに入ります。  
**radius scheme** *radius-scheme-name*
4. RADIUS アトリビュート変換機能をイネーブルにします。  
**attribute translate**  
デフォルトでは、この機能は無効になっています。
5. RADIUS アトリビュート変換ルールまたは RADIUS アトリビュート拒否ルールを設定します。必要に応じて、次のタスクを選択します。
  - RADIUS アトリビュート変換ルールを設定します。  
**attribute convert** *src-attr-name* **to** *dest-attr-name* { { **access-accept** | **access-request** | **accounting** } \* | { **received** | **sent** } \* }  
デフォルトでは、RADIUS アトリビュート変換ルールは設定されていません。
  - RADIUS アトリビュート拒否ルールを設定します。  
**attribute reject** *attr-name* { { **access-accept** | **access-request** | **accounting** } \* | { **received** | **sent** } \* }  
デフォルトでは、RADIUS アトリビュート拒否規則は設定されていません。

1. システムビューに入ります。  
**system-view**
2. (オプション)拡張 RADIUS アトリビュートを定義します。  
**radius attribute extended** *attribute-name* [ **vendor** *vendor-id* ] **code** *attribute-code* **type** { **binary** | **date** | **integer** | **interface-id** | **ip** | **ipv6** | **ipv6-prefix** | **octets** | **string** }
3. RADIUS DAS ビューに入ります。  
**radius dynamic-author server**
4. RADIUS アトリビュート変換機能をイネーブルにします。  
**attribute translate**  
デフォルトでは、この機能は無効になっています。
5. RADIUS アトリビュート変換ルールまたは RADIUS アトリビュート拒否ルールを設定します。必要に応じて、次のタスクを選択します。
  - RADIUS アトリビュート変換ルールを設定します。  
**attribute convert** *src-attr-name* **to** *dest-attr-name* { { **coa-ack** | **coa-request** } \* | { **received** | **sent** } \* }  
デフォルトでは、RADIUS アトリビュート変換ルールは設定されていません。
  - RADIUS アトリビュート拒否ルールを設定します。  
**attribute reject** *attr-name* { { **coa-ack** | **coa-request** } \* | { **received** | **sent** } \* }  
デフォルトでは、RADIUS アトリビュート拒否規則は設定されていません。

## RADIUS stop-accounting パケットバッファリングについて

デバイスは、ホストから接続ティアダウン要求を受信したとき、または管理者から接続ティアダウンコマンドを受信したときに、RADIUS stop-accounting 要求を送信します。ただし、デバイスは、stop-accounting 要求に対する応答を 1 回の送信で受信できない場合があります。デバイスが、アカウントングサーバーから応答を受信していない RADIUS stop-accounting 要求をバッファできるようにします。デバイスは、応答を受信するまで要求を再送します。

送信時間を制限するには、個々の RADIUS stop-accounting 要求に対して送信できる最大試行回数を設定します。要求に対して最大試行回数を設定すると、デバイスはバッファされた要求を廃棄します。



## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームビューに入ります。  
**radius scheme radius-scheme-name**
3. 応答を受信していない RADIUS stop-accounting 要求のバッファリングをイネーブルにします。  
**stop-accounting-buffer enable**  
デフォルトでは、バッファリング機能は有効になっています。
4. (オプション)個々の RADIUS stop-accounting 要求の最大送信試行回数を設定します。  
**retry stop-accounting retries**  
デフォルト設定は 500 です。

## 強制的に stop-accounting パケットを送信できるようにする

### 強制的に stop-accounting パケットを送信することについて

通常、デバイスは、認証されたユーザーの開始アカウントングパケットを RADIUS サーバーに送信しない場合、ユーザーがオフラインになったときに停止アカウントングパケットを送信しません。サーバーが開始アカウントングパケットなしでユーザーのユーザーエントリを生成した場合、ユーザーがオフラインになったときにユーザーエントリを解放しません。この機能により、ユーザーがオフラインになったときに、デバイスは停止アカウントングパケットを RADIUS サーバーに送信するように強制されます。

## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームビューを有効にします。  
**radius scheme radius-scheme-name**
3. 開始アカウントングパケットが送信されていないユーザーがオフラインになった場合に、デバイスが停止アカウントングパケットを送信できるようにします。  
**stop-accounting-packet send-force**  
デフォルトでは、強制的に stop-accounting パケットを送信することになっています。start-accounting パケットが送信されていないユーザーがオフラインになった場合、デバイスは stop-accounting パケットを送信しません。

### RADIUS サーバーのロードシェアリングについて

デフォルトでは、デバイスはサーバーロールに基づいて RADIUS サーバーと通信します。最初にプライマリサーバーとの通信が試行され、プライマリサーバーに到達できない場合は、構成されている順序でセカンダリサーバーが検索されます。アクティブ状態の最初のセカンダリサーバーが通信に使用されます。このプロセスでは、ワークロードは常にアクティブサーバーに置かれます。

RADIUS サーバーの負荷分散機能を使用して、サーバーの役割に関係なく複数のサーバーにワークロードを動的に分散します。デバイスは、重み値と現在サービスされているユーザーの数を比較した後、スキーム内のすべてのアクティブサーバーの最も適切なサーバーに AAA 要求を転送します。サーバーの AAA 容量に基づいて各 RADIUS サーバーの重み値を指定します。重み値が大きいほど、AAA 容量が大きいことを示します。

RADIUS サーバーのロードシェアリングでは、デバイスがユーザーの開始アカウントング要求をサーバーに送信すると、そのユーザーの以降のすべてのアカウントング要求が同じサーバーに転送されます。アカウントングサーバーに到達できない場合、デバイスは別のアクティブなアカウントングサーバーを検索するのではなく、アカウントング失敗メッセージを返します。

## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS スキームビューに入ります。  
`radius-scheme-name`
3. RADIUS サーバーロードシェアリング機能をイネーブルにします。  
**サーバー負荷分散イネーブル**  
デフォルトでは、この機能は無効になっています。

# RADIUS アカウンティングオン機能の設定

## RADIUS アカウンティングオンについて

アカウンティングオン機能が有効になっている場合、デバイス全体がリブートした後、デバイスは自動的にアカウンティングオンパケットを RADIUS サーバーに送信します。アカウンティングオンパケットを受信すると、RADIUS サーバーはすべてのオンラインユーザーをログアウトし、デバイス経由で再度ログインできるようにします。この機能がないと、RADIUS サーバーはユーザーがオンラインになったと判断するため、ユーザーはリブート後に再度ログインできません。

デバイスがアカウンティングオンパケットの再送信を待機する間隔と最大再試行回数を設定できます。

拡張アカウンティングオン機能は、分散アーキテクチャのアカウンティングオン機能を拡張します。

拡張アカウンティングオン機能は、LAN ユーザーに適用できます。ユーザーデータは、ユーザーがシステムにアクセスする際に経由する IRF メンバーデバイスに保存されます。拡張アカウンティングオン機能が有効な場合、メンバーデバイスのリブート後に、システムは自動的にアカウンティングオンパケットを RADIUS サーバーに送信します。パケットには、メンバーデバイス識別子が含まれます。アカウンティングオンパケットを受信すると、RADIUS サーバーは、メンバーデバイスを介してシステムにアクセスするすべてのオンラインユーザーをログアウトします。メンバーデバイスを介してオンラインになったユーザーがいない場合、IRF ファブリックはメンバーデバイスのリブート後にアカウンティングオンパケットを送信しません。

## 制約事項とガイドライン

拡張アカウンティング機能を有効にするには、RADIUS サーバーを IMC 上で実行し、アカウンティング機能を有効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. RADIUS スキームビューに入ります。  
**radius scheme** `radius-scheme-name`
3. アカウンティングを有効にします。  
**accounting-on enable** [ `interval interval` | `send send-times` ] \*  
デフォルトでは、アカウンティング機能はディセーブルです。
4. (オプション)拡張アカウンティングをイネーブルにします。  
**accounting-on extended**  
デフォルトでは、拡張アカウンティングはディセーブルです。

## RADIUS セッション制御について

セッション制御パケットを使用して、認可情報を動的に変更したり、ユーザーを強制的に接続解除したりするには、RADIUS サーバーに対してこの機能をイネーブルにします。このタスクは、デバイスが UDP ポート 1812 で RADIUS セッション制御パケットを受信できるようにします。

RADIUS サーバーから送信されるセッション制御パケットを確認するには、RADIUS サーバーをデバイスのセッション制御クライアントとして指定します。

RADIUS セッション制御機能は、IMC 上で動作する RADIUS サーバーでのみ動作します。セッション制御クライアントの設定は、セッション制御機能がイネーブルになっている場合にだけ有効になります。

### 手順

1. システムビューに入ります。

#### **system-view**

2. セッション制御機能をイネーブルにします。

#### **radius session-control enable**

デフォルトでは、セッション制御機能はディセーブルです。

3. セッション制御クライアントを指定します。

**radius session-control client** { ip *ipv4-address* | ipv6 *ipv6-address* } [ key { cipher | simple } string | vpn-instance *vpn-instance-name* ] \*

デフォルトでは、セッション制御クライアントは指定されていません。

## RADIUS DAS 機能について

RFC5176 で定義されている RADIUS への Dynamic Authorization Extension(DAE;動的認可拡張)では、オンラインユーザーをログオフし、オンラインユーザー認可情報を変更できます。

RADIUS ネットワークでは、通常、RADIUS サーバーが DAE クライアント(DAC)として機能し、NAS が DAE サーバー(DAS)として機能します。

RADIUS DAS 機能を有効にすると、NAS は次の操作を実行します。

1. デフォルトまたは指定された UDP ポートで DAE 要求を受信します。
2. 要求の基準に一致するオンラインユーザーのログオフ、許可情報の変更、アクセスポートのシャットダウンまたはリポート、またはユーザーの再認証を行います。
3. DAE 応答を DAC に送信します。

DAE は次のタイプのパケットを定義します。

- 切断メッセージ(DM): DAC は DM 要求を DAS に送信し、特定のオンラインユーザーをログオフします。
- 認可メッセージの変更(CoA メッセージ): DAC は、特定のオンラインユーザーの認可情報を変更するために、CoA 要求を DAS に送信します。

### 手順

1. システムビューに入ります。

#### **system-view**

2. RADIUS DAS 機能を有効にし、RADIUS DAS ビューに入ります。

#### **radius dynamic-author server**

デフォルトでは、RADIUS DAS 機能はディセーブルです。

3. RADIUS DAC を指定します。

```
client { ip ipv4-address | ipv6 ipv6-address } [ key { cipher | simple } string | vpn-instance vpn-instance-name ] *
```

デフォルトでは、RADIUS DAC は指定されていません。

4. (オプション)RADIUS DAS ポートを指定します。

```
port port-number
```

デフォルトでは、RADIUS DAS ポートは 3799 です。

## RADIUS の SNMP 通知について

SNMP 通知が RADIUS に対してイネーブルになっている場合、SNMP エージェントは RADIUS によって生成される次の通知をサポートします。

- RADIUS サーバー到達不能通知: RADIUS サーバーに到達できません。RADIUS は、指定された数の RADIUS 要求送信試行内にアカウントing要求または認証要求に対する応答を受信しない場合、この通知を生成します。
- RADIUS サーバー到達可能通知: RADIUS サーバーに到達できます。RADIUS は、待機タイマーの期限が切れた後、以前ブロックされていた RADIUS サーバーに対してこの通知を生成します。
- 過度の認証失敗の通知: 認証試行の合計数と比較した認証失敗数が、指定したしきい値を超えています。

RADIUS SNMP 通知を正しく送信するには、デバイス上で SNMP も構成する必要があります。SNMP 構成の詳細は、『Network Management and Monitoring 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. RADIUS の SNMP 通知をイネーブルにします。

```
snmp-agent trap enable radius [ accounting-server-down | accounting-server-up | authentication-error-threshold | authentication-server-down | authentication-server-up ] *
```

デフォルトでは、すべての SNMP 通知は RADIUS に対してディセーブルです。

## RADIUS 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、ユーザービューでリセットコマンドを実行します。

タスク	コマンド
RADIUSスキーム設定を表示します。	<b>display radius scheme</b> [ <i>radius-scheme-name</i> ]
RADIUSパケット統計情報を表示します。	<b>display radius statistics</b>
応答を受信していないバッファRADIUS stop-accounting要求に関する情報を表示します。	<b>display stop-accounting-buffer</b> { <b>radius-scheme</b> <i>radius-scheme-name</i>   <b>session-id</b> <i>session-id</i>   <b>time-range</b> <i>start-time end-time</i>   <b>user-name</b> <i>user-name</i> }
RADIUS統計情報をクリアします。	<b>reset radius statistics</b>
応答を受信していないバッファRADIUS stop-accounting要求をクリアします。	<b>reset stop-accounting-buffer</b> { <b>radius-scheme</b> <i>radius-scheme-name</i>   <b>session-id</b> <i>session-id</i>   <b>time-range</b> <i>start-time end-time</i>   <b>user-name</b> <i>user-name</i> }

# RADIUS サーバー機能の設定

## RADIUSサーバーの機能タスクの概要

RADIUS サーバー機能を設定するには、次の作業を実行します。

1. RADIUS ユーザーの設定
2. RADIUS クライアントの指定について
3. RADIUS サーバーの設定のアクティブ化について

## RADIUSサーバー機能の制約事項およびガイドライン

RADIUS サーバー機能が正しく動作するようにするには、デバイスで RADIUS セッション制御をディセーブルにします。

## RADIUSユーザーの設定

RADIUS ユーザーを設定するには、RADIUS ユーザーデータの基礎となるネットワークアクセスユーザーを設定する必要があります。

RADIUS ユーザーには、ユーザー名、パスワード、説明、認可 ACL、認可 VLAN、および有効期限の各アトリビュートがあります。

### RADIUS クライアントの指定について

集中管理用の RADIUS クライアントおよび共有キーを指定するには、次の作業を実行します。RADIUS サーバー機能は、システムによって管理されていない RADIUS クライアントからの要求を受け入れません。

### 制約事項とガイドライン

RADIUS クライアントの IP アドレスは、RADIUS クライアントで指定された発信 RADIUS パケットの送信元 IP アドレスと同じである必要があります。

RADIUS クライアントの共有キーは、RADIUS クライアントの設定と同じである必要があります。

### 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS クライアントを指定します。  
**radius-server client ip ipv4-address key { cipher | simple } string**

### RADIUS サーバーの設定のアクティブ化について

デバイスの起動時に、RADIUS ユーザーと RADIUS クライアントを含む RADIUS サーバー設定が自動的にアクティブになります。RADIUS ユーザーデータが生成される RADIUS クライアントとネットワークアクセスユーザーを追加、変更、または削除した場合は、最新の RADIUS サーバー設定をすぐにアクティブにできます。

## 手順

1. システムビューに入ります。  
**system-view**
2. RADIUS サーバー設定をアクティブにします。  
**radius-server activate**  
このコマンドを実行すると、RADIUS サーバープロセスが再起動され、再起動中に認証サービスの中断が発生します。

## RADIUS ユーザーおよびクライアントの表示およびメンテナンス コマンド

任意のビューで display コマンドを実行します。

タスク	コマンド
アクティブなRADIUSユーザーに関する情報を表示します。	<b>display radius-server active-user [ user-name ]</b>
アクティブ化されたRADIUSクライアントに関する情報を表示します。	<b>display radius-server active-client</b>

## 接続記録ポリシーの設定

### 接続記録ポリシーについて

この機能は、デバイスが FTP、SSH、SFTP または Telnet ログインクライアントとして動作し、ログインサーバーとの接続を確立するシナリオで使用します。この機能により、デバイスは接続の開始および終了情報をアカウントサーバーに提供できます。ログインクライアントがログインサーバーとの接続を確立すると、システムはアカウント開始要求をアカウントサーバーに送信します。接続が終了すると、システムはアカウント停止要求をアカウントサーバーに送信します。

## 制約事項とガイドライン

デバイスには、接続記録のために AAA サーバーに送信されるアカウントリングパケットにユーザーが入力したユーザー名が含まれています。アカウントリング方式で user-name-format コマンドを使用して設定されたユーザー名フォーマット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. 接続記録ポリシーを作成し、そのビューを入力します。  
**aaa connection-recording policy**

3. 接続記録ポリシーのアカウントング方式を指定します。

`accounting hwtacacs-scheme hwtacacs-scheme-name`

## 接続記録ポリシーの表示およびメンテナンスコマンド

任意のビューで `display` コマンドを実行します。

タスク	コマンド
接続記録ポリシー設定を表示します。	<code>display aaa connection-recording policy</code>

## AAA設定例

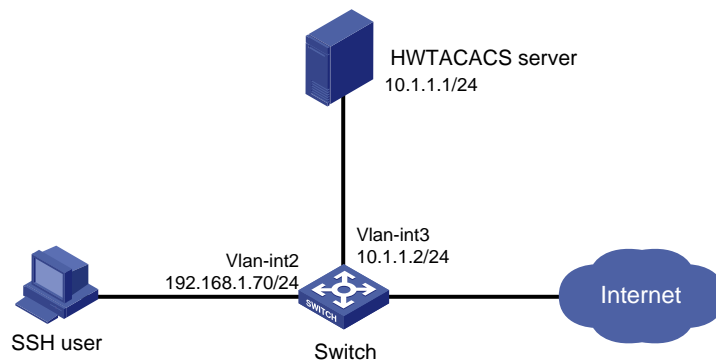
### 例:HWTACACS サーバーによる SSH ユーザー用の AAA の設定

#### ネットワーク構成

図1に示すように、次の要件を満たすようにスイッチを設定します。

- SSH ユーザー認証、許可、およびアカウントングに HWTACACS サーバーを使用します。
- デフォルトのユーザーロール `network-operator` を、SSH ユーザーが認証に合格した後割り当てます。
- HWTACACS サーバーに送信されるユーザー名からドメイン名を除外します。
- セキュアな HWTACACS 通信の共有キーとしてエキスパートを使用します。

図1 ネットワーク図



#### HWTACACS サーバーの構成

#スイッチとのセキュアな通信のために共有キーを `expert` に設定し、SSH ユーザーのアカウントを追加し、パスワードを指定します(詳細は省略します)。

#### スイッチの設定

#インターフェースの IP アドレスを設定します(詳細は省略します)。

#HWTACACS スキームを作成します。

```
<Switch> system-view
```

```
[Switch] hwtacacs scheme hwtac
```

```

#プライマリ認証サーバーを指定します。
[Switch-hwtacacs-hwtac] primary authentication 10.1.1.1 49
#プライマリ許可サーバーを指定します。
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.1 49
#プライマリアカウンティングサーバーを指定します。
[Switch-hwtacacs-hwtac] primary accounting 10.1.1.1 49
#安全な HWTACACS 通信のために、共有鍵を平文形式の expert に設定します。
[Switch-hwtacacs-hwtac] key authentication simple expert
[Switch-hwtacacs-hwtac] key authorization simple expert
[Switch-hwtacacs-hwtac] key accounting simple expert
#HWTACACS サーバーに送信されるユーザー名からドメイン名を除外します。
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
#bbb という名前の ISP ドメインを作成し、ログインユーザーの認証、許可、アカウンティングに HWTACACS
スキームを使用するようにドメインを設定します。
[Switch-isp-bbb] authentication login hwtacacs-scheme hwtac
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting login hwtacacs-scheme hwtac
[Switch-isp-bbb] quit
#ローカル RSA キーと DSA キーのペアを作成します。
[Switch] public-key local create rsa
[Switch] public-key local create dsa
#Stelnet サーバーを有効にします。
[Switch] ssh server enable
#ユーザー回線 VTY0~VTY63 のスキーム認証をイネーブルにします。
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
#認証済み SSH ユーザーにデフォルトユーザーロール network-operator を割り当てるデフォルトユーザー
ロール機能をイネーブルにします。
[Switch] role default-role enable

```

## 設定の確認

#スイッチへの SSH 接続を開始し、正しいユーザー名とパスワードを入力します。ユーザーはスイッチにログインします(詳細は省略します)。

#ユーザーが network-operator ユーザーロールで許可されたコマンドを使用できることを確認します(詳細は省略します)。

## 例:SSH ユーザーのローカル認証、HWTACACS 許可、および RADIUS アカウンティングの設定

### ネットワーク構成

図2に示すように、次の要件を満たすようにスイッチを設定します。

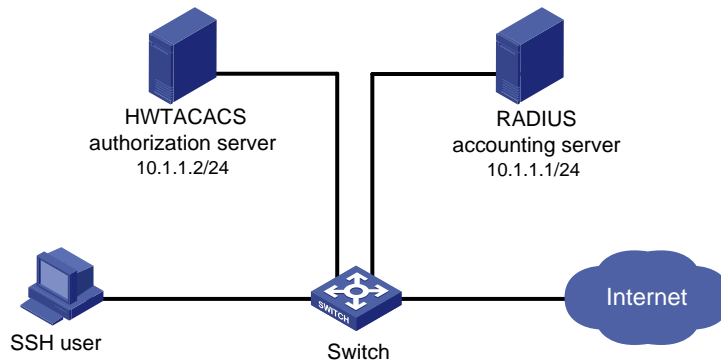
- SSH ユーザーのローカル認証を実行します。



- SSH ユーザー認可とアカウントिंगには、それぞれ HWTACACS サーバーと RADIUS サーバーを使用します。
- サーバーに送信されるユーザー名からドメイン名を除外します。
- デフォルトのユーザーロール network-operator を、SSH ユーザーが認証に合格した後割り当てます。

SSH ユーザーに hello という名前のアカウントを設定します。HWTACACS サーバーおよび RADIUS サーバーとのセキュアな通信のために、expert を共有キーを設定します。

図2 ネットワーク図



## HWTACACS サーバーの構成

#スイッチとのセキュアな通信のために共有キーを expert に設定し、SSH ユーザーのアカウントを追加し、パスワードを指定します(詳細は省略します)。

## RADIUS サーバーの設定

#スイッチとのセキュアな通信のために共有キーを expert に設定し、SSH ユーザーのアカウントを追加し、パスワードを指定します(詳細は省略します)。

## スイッチの設定

#インターフェースの IP アドレスを設定します(詳細は省略します)。

#ローカル RSA キーと DSA キーのペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
```

#Stelnet サーバーを有効にします。

```
[Switch] ssh server enable
```

#ユーザー回線 VTY0~VTY63 のスキーム認証をイネーブルにします。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
```

#HWTACACS スキームを設定します。

```
[Switch] hwtacacs scheme hwtac
[Switch-hwtacacs-hwtac] primary authorization 10.1.1.2 49
[Switch-hwtacacs-hwtac] key authorization simple expert
[Switch-hwtacacs-hwtac] user-name-format without-domain
[Switch-hwtacacs-hwtac] quit
```

#RADIUS スキームを設定します。

```

[Switch] radius scheme rd
[Switch-radius-rd] primary accounting 10.1.1.1 1813
[Switch-radius-rd] key accounting simple expert
[Switch-radius-rd] user-name-format without-domain
[Switch-radius-rd] quit

#デバイス管理ユーザーを作成します。
[Switch] local-user hello class manage

#SSH サービスをローカルユーザーに割り当てます。
[Switch-luser-manage-hello] service-type ssh

#ローカルユーザーのパスワードを平文形式で 123456TESTplat&!に設定します。FIPS モードでは、パスワードを対話モードで設定する必要があります。
[Switch-luser-manage-hello] password simple 123456TESTplat&!
[Switch-luser-manage-hello] quit

#bbb という名前の ISP ドメインを作成し、ローカル認証、HWTACACS 許可、および RADIUS アカウンティングを使用するようにログインユーザーを設定します。
[Switch] domain bbb
[Switch-isp-bbb] authentication login local
[Switch-isp-bbb] authorization login hwtacacs-scheme hwtac
[Switch-isp-bbb] accounting login radius-scheme rd
[Switch-isp-bbb] quit

#認証済み SSH ユーザーにデフォルトユーザーロール network-operator を割り当てるデフォルトユーザーロール機能をイネーブルにします。
[Switch] role default-role enable

```

## 設定の確認

#スイッチへの SSH 接続を開始し、ユーザー名 hello@bbb と正しいパスワードを入力します。ユーザーはスイッチにログインします(詳細は省略)。

#ユーザーが network-operator ユーザーロールで許可されたコマンドを使用できることを確認します(詳細は省略)。

## 例:RADIUS サーバーによる SSH ユーザーの認証および認可の設定

### ネットワーク構成

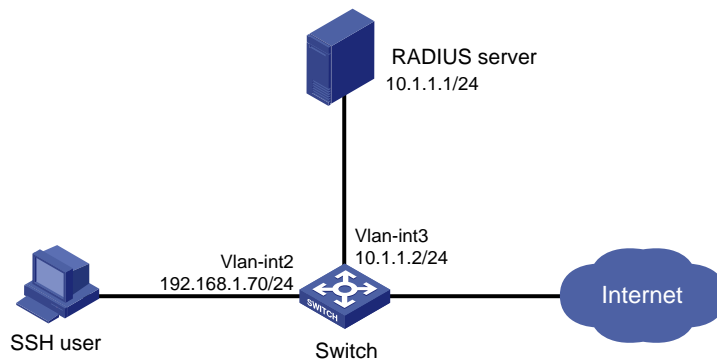
図3に示すように、次の要件を満たすようにスイッチを設定します。

- SSH ユーザー認証および認可に RADIUS サーバーを使用します。
- RADIUS サーバーに送信されるユーザー名にドメイン名を含めます。
- デフォルトのユーザーロール network-operator を、SSH ユーザーが認証に合格した後割り当てます。

RADIUS サーバーは、IMC Plat5.0(E0101)および IMC UAM5.0(E0101)上で動作します。RADIUS サーバーにユーザー名 hello@bbb のアカウントを追加します。

RADIUS サーバーとスイッチは、セキュアな RADIUS 通信の共有キーとしてエキスパートを使用します。認証およびアカウンティング用のポートは、それぞれ 1812 と 1813 です。

図 3 ネットワーク図



## RADIUS サーバーの設定

1. スイッチをアクセスデバイスとして IMC プラットフォームに追加します。  
 IMC にログインし、Service タブをクリックし、ナビゲーションツリーから User Access Manager > Access Device Management > Access Device を選択します。次に、Add をクリックして、アクセスデバイスを次のように設定します。
    - a. セキュア RADIUS 通信用の共有キーを expert に設定します。
    - b. 認証およびアカウンティング用のポートをそれぞれ 1812 および 1813 に設定します。
    - c. Service Type リストから Device Management Service を選択します。
    - d. Access Device Type リストから H3C を選択します。
    - e. デバイスリストからアクセスデバイスを選択するか、アクセスデバイスを手動で追加します。この例では、デバイスの IP アドレスは 10.1.1.2 です。
    - f. 他のパラメーターのデフォルト値を使用し、OK をクリックします。
- ここで指定するアクセスデバイスの IP アドレスは、スイッチから送信される RADIUS パケットの送信元 IP アドレスと同じである必要があります。送信元 IP アドレスは、スイッチ上で次の順序で選択されます。
- nas-ip コマンドを使用して指定した IP アドレス。
  - radius nas-ip コマンドを使用して指定した IP アドレス。
  - 発信インターフェースの IP アドレス(デフォルト)。

図4 スイッチのアクセスデバイスとしての追加

Service >> User Access Manager >> Access Device >> Add Access Device

Access Configuration			
* Shared Key	expert	* Authentication Port	1812
* Accounting Port	1813	Service Type	Device Management S
Access Device Type	H3C	RADIUS Accounting	Fully Supported
Service Group	Ungrouped	Access Area	--

Device List

Select Add Manually Clear All Click OK to save your change.

Total Items: 1.

Device Name	Device IP	Device Model	Delete
	10.1.1.2		✖

OK Cancel

2. デバイス管理用のアカウントを追加します。

User タブをクリックし、ナビゲーションツリーから Access User View>Device Mgmt User を選択します。次に、Add をクリックして、デバイス管理アカウントを次のように設定します。

- a. アカウント名 hello@bbb を入力し、パスワードを指定します。
- b. Service Type リストから SSH を選択します。
- c. 管理するホストの IP アドレス範囲として 10.1.1.0~10.1.1.255 を指定します。
- d. OK をクリックします。

注:

IP アドレス範囲には、スイッチの IP アドレスが含まれている必要があります。

図5 デバイス管理用アカウントの追加

User >> Device Management User >> Add Device Management User

**Add Device Management User**

Basic Information of Device Management User

\* Account Name: hello@bbb

\* User Password: [masked]

\* Confirm Password: [masked]

Service Type: SSH

EXEC Priority: 3

Bound User IP List

Add Delete

No match found.

<input type="checkbox"/>	Start IP	End IP	Delete
--------------------------	----------	--------	--------

IP Address List of Managed Devices

Add Delete

Total Items: 1.

<input type="checkbox"/>	Start IP	End IP	Delete
<input type="checkbox"/>	10.1.1.0	10.1.1.255	✖

OK Cancel

スイッチの設定

#インターフェースの IP アドレスを設定します(詳細は省略します)。

#ローカル RSA キーと DSA キーのペアを作成します。

```
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
```

#Stelnet サーバーを有効にします。

```
[Switch] ssh server enable
```

#ユーザー回線 VTY0~VTY63 のスキーム認証をイネーブルにします。

```
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
```

```

[Switch-line-vty0-63] quit
#認証済み SSH ユーザーにデフォルトユーザーロール network-operator を割り当てるデフォルトユーザー
#ロール機能をイネーブルにします。
[Switch] role default-role enable
#RADIUS スキームを作成します。
[Switch] radius scheme rad
#プライマリ認証サーバーを指定します。
[Switch-radius-rad] primary authentication 10.1.1.1 1812
#サーバーとの安全な通信のために、共有鍵を平文形式の expert に設定します。
[Switch-radius-rad] key authentication simple expert
#RADIUS サーバーに送信されるユーザー名にドメイン名を含めます。
[Switch-radius-rad] user-name-format with-domain
[Switch-radius-rad] quit
#bbb という名前の ISP ドメインを作成し、ログインユーザーの認証、認可、アカウントング方式を設定しま
#す。
[Switch] domain bbb
[Switch-isp-bbb] authentication login radius-scheme rad
[Switch-isp-bbb] authorization login radius-scheme rad
[Switch-isp-bbb] accounting login none
[Switch-isp-bbb] quit

```

## 設定の確認

#スイッチへの SSH 接続を開始し、ユーザー名 hello@bbb と正しいパスワードを入力します。ユーザーはスイッチにログインします(詳細は省略します)。

#ユーザーが network-operator ユーザーロールで許可されたコマンドを使用できることを確認します(詳細は省略します)。

## 例:LDAP サーバーによる SSH ユーザーの認証の設定

### ネットワーク構成

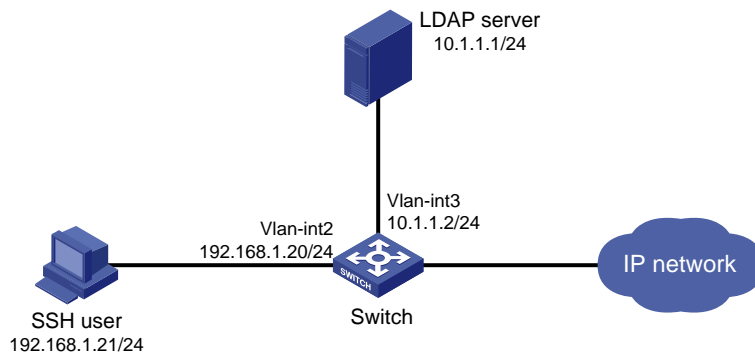
図6に示すように、LDAP サーバーはドメイン ldap.com を使用し、Microsoft Windows2003Server Active Directory を実行します。

次の要件を満たすようにスイッチを設定します。

- LDAP サーバーを使用して SSH ユーザーを認証します。
- SSH 合格した SSH ユーザーにレベル 0 ユーザーロールを割り当てます。

LDAP サーバーで、管理者パスワードを admin!123456 に設定し、aaa という名前のユーザーを追加し、ユーザーのパスワードを ldap!123456 に設定します。

図6 ネットワーク図



## LDAP サーバーの構成

1. aaa という名前のユーザーを追加し、パスワードを ldap!123456 に設定します。
  - a. LDAP サーバーで、Start > Control Panel > Administrative Tools を選択します。
  - b. Active Directory Users and Computers をダブルクリックします。  
Active Directory Users and Computers ウィンドウが表示されます。
  - c. ナビゲーションツリーで、ldap.com ノードの下の Users をクリックします。
  - d. メニューから Action > New > User を選択して、ユーザーを追加するためのダイアログボックスを表示します。
  - e. ログオン名 aaa を入力し、next をクリックします。

図7 ユーザーaaa の追加

The screenshot shows the 'New Object - User' dialog box. The 'Create in' field is set to 'ldap.com/Users'. The 'First name' field contains 'aaa', 'Initials' is empty, 'Last name' is empty, and 'Full name' contains 'aaa'. The 'User logon name' field contains 'aaa' and '@ldap.com'. The 'User logon name (pre-Windows 2000)' field contains 'LDAP\' and 'aaa'. Buttons for '< Back', 'Next >', and 'Cancel' are visible at the bottom.

- f. ダイアログボックスに password ldap!123456 と入力し、必要に応じてオプションを選択し、Next をクリックします。

図8 ユーザーのパスワードの設定

New Object - User

Create in: ldap.com/Users

Password: [.....]

Confirm password: [.....]

User must change password at next logon

User cannot change password

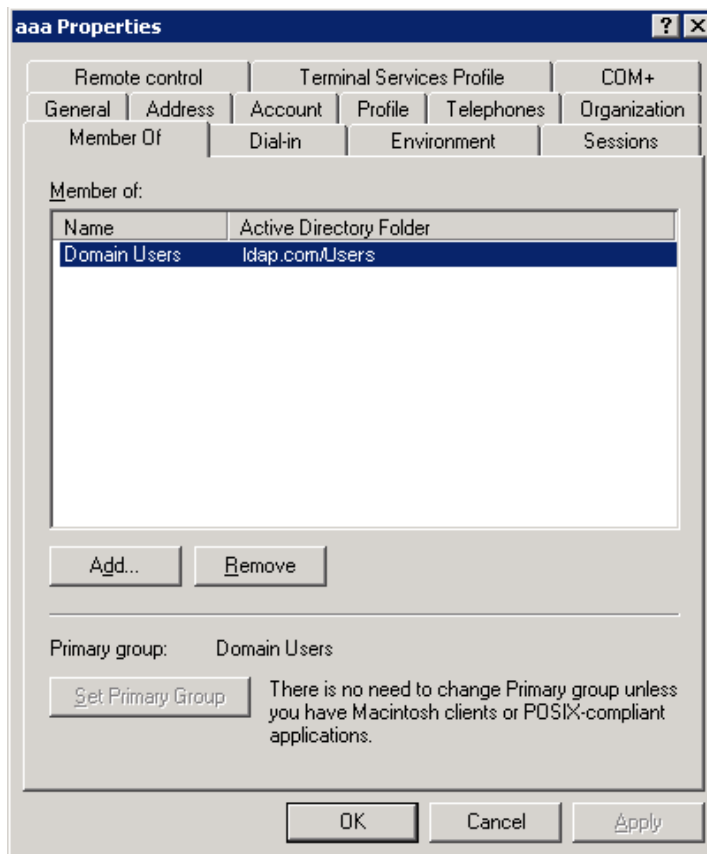
Password never expires

Account is disabled

< Back   Next >   Cancel

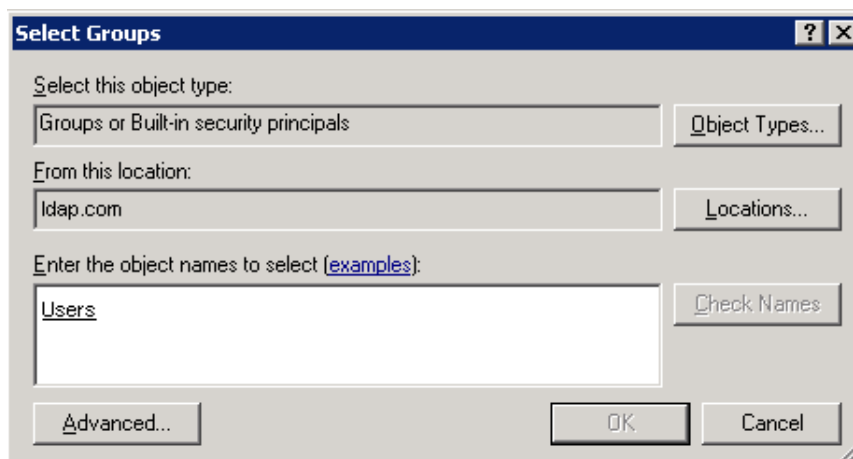
- g. OK をクリックします。
2. ユーザーaaaをグループ Users に追加:
  - a. ナビゲーションツリーで、ldap.com ノードの下の Users をクリックします。
  - b. 右側のペインで、user の aaa を右クリックし、Properties を選択します。
  - c. ダイアログボックスで、Member Of タブをクリックし、Add をクリックします。

図9 ユーザープロパティの変更



- d. Select Groups ダイアログボックスの enter Users in the Enter the object names to select フィールドに Users と入力し OK をクリックします。  
ユーザーaaa がグループ Users に追加されます。

図10 グループ Users へのユーザーaaa の追加



3. 管理者パスワードを設定します。  
a. 右側のペインで、user の Administrator を右クリックし、Set Password を選択します。  
b. ダイアログボックスで、管理者パスワードを入力します(詳細は省略します)。

## スイッチの設定



```

#インターフェースの IP アドレスを設定します(詳細は省略します)。
#ローカル RSA キーと DSA キーのペアを作成します。
<Switch> system-view
[Switch] public-key local create rsa
[Switch] public-key local create dsa
#Stelnet サーバーを有効にします。
[Switch] ssh server enable
#ユーザー回線 VTY0~VTY63 のスキーム認証をイネーブルにします。
[Switch] line vty 0 63
[Switch-line-vty0-63] authentication-mode scheme
[Switch-line-vty0-63] quit
#LDAP サーバーを構成します。
[Switch] ldap server ldap1
#LDAP 認証サーバーの IP アドレスを指定します。
[Switch-ldap-server-ldap1] ip 10.1.1.1
#管理者 DN を指定します。
[Switch-ldap-server-ldap1] login-dn cn=admin,cn=users,dc=ldap,dc=com
#管理者パスワードを指定します。
[Switch-ldap-server-ldap1] login-password simple admin!123456
#ユーザー検索用のベース DN を構成します。
[Switch-ldap-server-ldap1] search-base-dn dc=ldap,dc=com
[Switch-ldap-server-ldap1] quit
#LDAP スキームを作成します。
[Switch] ldap scheme ldap-shm1
#LDAP 認証サーバーを指定します。
[Switch-ldap-ldap-shm1] authentication-server ldap1
[Switch-ldap-ldap-shm1] quit
#bbb という名前の ISP ドメインを作成し、ログインユーザーの認証、認可、アカウントング方式を設定します。
[Switch] domain bbb
[Switch-isp-bbb] authentication login ldap-scheme ldap-shm1
[Switch-isp-bbb] authorization login none
[Switch-isp-bbb] accounting login none
[Switch-isp-bbb] quit

```

## 設定の確認

#スイッチへの SSH 接続を開始し、ユーザー名 aaa@bbb およびパスワード ldap!123456 を入力します。ユーザーはスイッチにログインします。(詳細は省略します)。

#ユーザーがレベル 0 ユーザーロールで許可されたコマンドを使用できることを確認します(詳細は省略します)。

## 例:RADIUS サーバーによる 802.1X ユーザーの AAA の設定

### ネットワーク構成

図111に示すように、次の要件を満たすようにスイッチを設定します。

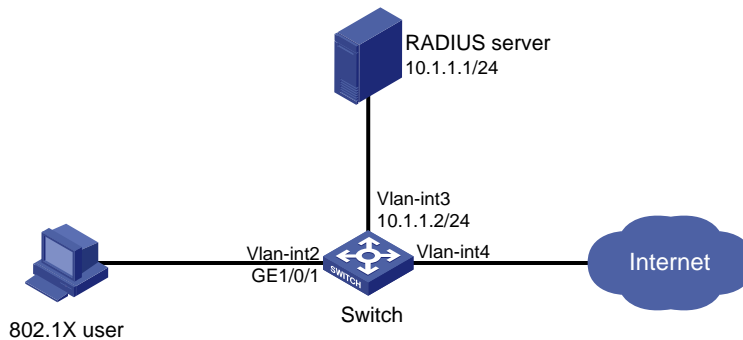
- 802.1X ユーザーの認証、認可、アカウントングに RADIUS サーバーを使用します。
- GigabitEthernet 1/0/1 で MAC ベースのアクセスコントロールを使用して、ポート上のすべての 802.1X ユーザーを個別に認証します。
- RADIUS サーバーに送信されるユーザー名にドメイン名を含めます。

この例では、RADIUS サーバーは IMC PLAT5.0(E0101)および IMC UAM5.0(E0101)上で動作します。RADIUS サーバー上で、次のタスクを実行します。

- 月に最大 120 時間 120ドルのサービスを追加し、**認証されたユーザーを VLAN4 に割り当てる**。
- dot1x@bbb という名前のユーザーを設定し、そのユーザーにサービスを割り当てます。

セキュア RADIUS 通信用の共有キーを expert に設定します。認証およびアカウントング用のポートをそれぞれ 1812 および 1813 に設定します。

図11 ネットワーク図



## RADIUS サーバーの設定

1. スイッチをアクセスデバイスとして IMC プラットフォームに追加します。  
IMC にログインし、Service タブをクリックし、ナビゲーションツリーから User Access Manager>(Access Device Management)>Access Device を選択します。次に、Add をクリックして、アクセスデバイスを次のように設定します。
  - a. セキュア認証およびアカウントング通信のために、共有キーを expert に設定します。
  - b. 認証およびアカウントング用のポートをそれぞれ 1812 および 1813 に設定します。
  - c. Service Type リストから LAN Access Service を選択します。
  - d. Access Device Type リストから H3C(一般的に)を選択します。
  - e. デバイスリストからアクセスデバイスを選択するか、アクセスデバイスを手動で追加します。この例では、デバイスの IP アドレスは 10.1.1.2 です。
  - f. 他のパラメーターのデフォルト値を使用し、OK をクリックします。

ここで指定するアクセスデバイスの IP アドレスは、スイッチから送信される RADIUS パケットの送信元 IP アドレスと同じである必要があります。送信元 IP アドレスは、スイッチ上で次の順序で選択されます。

  - nas-ip コマンドを使用して指定した IP アドレス。
  - radius nas-ip コマンドを使用して指定した IP アドレス。
  - 発信インターフェースの IP アドレス(デフォルト)。

図12 スイッチのアクセスデバイスとしての追加

Service >> User Access Manager >> Access Device Management >> Access Device >> Add Access Device Help

**Access Configuration**

* Shared Key: expert	* Authentication Port: 1812
* Accounting Port: 1813	Service Type: LAN Access Service
Access Device Type: H3C(General)	RADIUS Accounting: Fully Supported
Service Group: Ungrouped	Access Area: --

**Device List**

Select Add Manually Clear All Click OK to save your change.

Total Items: 1.

Device Name	Device IP	Device Model	Delete
	10.1.1.2		✖

2. 課金プランを追加する:

Service タブをクリックし、ナビゲーションツリーから Accounting Manager>Charging Plans を選択して、課金プラン設定ページに入ります。次に、Add をクリックして、次のように課金プランを設定します。

- a. UserAcct という名前のプランを追加します。
- b. Charging Template リストから Flat rate を選択します。
- c. Charge Based on に時間を選択し、Billing Term に Monthly を選択して、Fixed Fee フィールドに 120 と入力します。
- d. Usage Threshold フィールドに 120 と入力し、In フィールドで hr(hours) を選択します。この設定では、ユーザーは月に最大 120 時間インターネットにアクセスできます。
- e. 他のパラメーターのデフォルト値を使用し、OK をクリックします。

図13 課金プランの追加

Service >> Accounting Manager >> Charging Plans >> Add Charging Plan Help

**Charging Plan Setup**

**Basic Information**

\* Plan Name: UserAcct

Charging Template: Flat rate

Service Group: Ungrouped

Description:

**Basic Plan Settings**

Charge Based on: time

Billing Term: Monthly

\* Fixed Fee: 120 USD

**Service Usage Limit**

Usage Threshold: 120 in hr

3. サービスを追加する:

Service タブをクリックし、ナビゲーションツリーから User Access Manager>Service Configuration を選択します。次に、Add をクリックして、次のようにサービスを設定します。

- a. Dot1x auth という名前のサービスを追加し、サービスサフィックスを bbb(802.1X ユーザーの認証ドメイン)に設定します。サービスサフィックスが設定されている場合を含むユーザー名を 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必要があります。

- b. Charging Plan リストから UserAcct を選択します。
- c. **Deploy VLAN** を選択し、割り当てる VLAN の ID を 4 に設定します。
- d. 必要に応じて他のパラメーターを設定します。
- e. OK をクリックします。

図14 サービスの追加

Service >> User Access Manager >> Service Configuration >> Add Service Configuration

### Add Service Configuration

**Basic Information**

\* Service Name:  Service Suffix:

\* Service Group:

Charging Plan:

Billing Term Start Type:  Start Date:

Adaptive consecutive deduction  Charge Whole Term in Initial Term  Charge by Day in Initial Term  No Charge for Initial Term

Description:

LDAP Priority:   Available ?

---

**Authorization Information**

\* Access Period:  Allocate IP:

Downstream Rate:  Kbps Upstream Rate:  Kbps

Priority:

RSA Authentication

Certificate Authentication:  None  EAP

Certificate Type:

Deploy VLAN:   Deploy User Profile:

Deploy User Group:  ?

Deploy ACL

#### 4. ユーザーの追加:

User タブをクリックし、ナビゲーションツリーから Access User View > All Access Users を選択して All Access Users ページに移動します。次に、Add をクリックしてユーザーを次のように構成します。

- a. ユーザーを選択するか、hello という名前のユーザーを追加します。
- b. アカウント名を dot1x と指定し、パスワードを設定します。
- c. Access Service 領域で Dot1x auth を選択します。
- d. 必要に応じて他のパラメーターを設定し、OK をクリックします。

図15 アクセスユーザーアカウントの追加

	Service Name	Service Suffix	Status	Charging Plan	Allocate IP
<input checked="" type="checkbox"/>	Dot1x auth	bbb	Available	UserAcct	

## スイッチの設定

1. RADIUS スキームを設定します。

#rad という名前の RADIUS スキームを作成し、RADIUS スキームビューを入力します。

```
<Switch> system-view
```

```
[Switch] radius scheme rad
```

#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、サーバーとの通信用のキーを設定します。

```
[Switch-radius-rad] primary authentication 10.1.1.1
```

```
[Switch-radius-rad] primary accounting 10.1.1.1
```

```
[Switch-radius-rad] key authentication simple expert
```

```
[Switch-radius-rad] key accounting simple expert
```

#RADIUS サーバーに送信されるユーザー名にドメイン名を含めます。

```
[Switch-radius-rad] user-name-format with-domain
```

```
[Switch-radius-rad] quit
```

2. 認証ドメインを構成します。

#bbb という名前の ISP ドメインを作成し、ISP ドメインビューを入力します。

```
[Switch] domain bbb
```

#LAN ユーザーの認証、認可、アカウントングに RADIUS スキーム rad を使用するように ISP ドメインを設定します。

```
[Switch-isp-bbb] authentication lan-access radius-scheme rad
```

```
[Switch-isp-bbb] authorization lan-access radius-scheme rad
```

```
[Switch-isp-bbb] accounting lan-access radius-scheme rad
```

```
[Switch-isp-bbb] quit
```

3. 802.1X 認証を設定します。

#802.1X をグローバルに有効にします。

```
[Switch] dot1x
```

#GigabitEthernet 1/0/1 の 802.1X を有効にします。

```
[Switch] interface GigabitEthernet 1/0/1
```

```
[Switch-GigabitEthernet 1/0/1] dot1x
```

#アクセス制御方式を設定します。デフォルトでは、802.1X 対応ポートは MAC ベースのアクセス制御を使用します。

```
[Switch-GigabitEthernet 1/0/1] dot1x port-method macbased
```

## 設定の確認

1. ホストで、アカウント dot1x@bbb を使用して 802.1X 認証を渡します。  
#ホストで Windows XP802.1X クライアントが実行されている場合は、次のようにネットワーク接続プロパティを構成します。
  - a. プロパティウィンドウの Authentication タブをクリックします。
  - b. Enable IEEE802.1X authentication for this network オプションを選択します。
  - c. EAP タイプとして MD5challenge を選択します。
  - d. OK をクリックします。

ユーザーは、認証ページで正しいユーザー名とパスワードを入力した後で認証に合格します。

#ホストが INode クライアントを実行している場合、高度な認証オプションは必要ありません。ユーザーは、クライアントプロパティページでユーザー名 dot1x@bbb と正しいパスワードを入力した後、認証を渡すことができます。

---

### ❗ 重要:

クライアントが認証に合格した後に、許可された VLAN 内のリソースにアクセスするために IP アドレスを更新できることを確認します。

---

2. スイッチ上で、ユーザーが認証合格した後、サーバーがクライアントを接続するポートを VLAN4 に割り当てていることを確認します(詳細は省略します)。
3. スイッチの 802.1X 接続情報を表示します。  

```
[Switch] display dot1x connection
```

## 例: デバイスを RADIUS サーバーとして 802.1X ユーザーの認証と許可設定する

### ネットワーク構成

図16に示すように、スイッチ B は、NAS(スイッチ A)に接続された 802.1X ユーザーの認証および認可の RADIUS サーバーとして動作します。

次の要件を満たすようにスイッチを設定します。

- GigabitEthernet 1/0/1 の NAS の 802.1X ユーザー認証を実行します。
- 共有キーは expert で、認証ポートは 1812 です。
- RADIUS サーバーに送信されるユーザー名からドメイン名を除外します。
- 802.1X 認証のユーザー名は dot1x です。
- ユーザーが認証を合格すると、RADIUS サーバーはユーザーが接続している NAS ポートに VLAN4 を認可します。



```
[SwitchB-luser-network-dot1x] password simple 123456
#VLAN4 を認可 VLAN として設定します。
[SwitchB-luser-network-dot1x] authorization-attribute vlan 4
[SwitchB-luser-network-dot1x] quit

#RADIUS クライアントの IP アドレスを 10.1.1.2 に、共有キーを expert としてプレーンテキスト形式で設定
します。
[SwitchB] radius-server client ip 10.1.1.2 key simple expert

#RADIUS サーバーの設定を有効にします。
[SwitchB] radius-server activate
```

## 設定の確認

1. RADIUS サーバー上で、アクティブ化された RADIUS クライアントおよびユーザーを表示します。

```
[SwitchB] display radius-server active-client
Total 1 RADIUS clients.
Client IP: 10.1.1.2
[SwitchB] display radius-server active-user dot1x
Total 1 RADIUS users matched.
Username: dot1x
Description: Not configured
Authorization attributes:
  VLAN ID: 4
  ACL number: Not configured
Validity period:
Expiration time: Not configured
```
2. ホストで、802.1X 認証にアカウント dot1x を使用します。

ホストで Windows 組み込み 802.1X クライアントが実行されている場合は、次のようにネットワーク接続プロパティを構成します。

  - a. プロパティウィンドウの Authentication タブをクリックします。
  - b. Enable IEEE802.1X authentication for this network オプションを選択します。
  - c. EAP タイプとして MD5challenge を選択します。
  - d. OK をクリックします。

ホストが INode クライアントを実行している場合、高度な認証オプションは必要ありません。  
ユーザーは、認証ページまたは INode クライアントで正しいユーザー名とパスワードを入力した後に認証をパスします。

---

**① 重要:**  
クライアントが認証に合格した後に、許可された VLAN 内のリソースにアクセスするために IP アドレスを更新できることを確認します。

---
3. NAS で、ユーザーが認証に合格した後、RADIUS サーバーがポートを VLAN4 に割り当てることを確認します(詳細は省略します)。
4. NAS で、オンラインの 802.1X ユーザー情報を表示します。

```
[SwitchA] display dot1x connection
```



# AAAのトラブルシューティング

## RADIUS 認証の失敗

### 症状

ユーザー認証は常に失敗します。

### 解析

考えられる理由は次のとおりです。

- NASとRADIUSサーバーの間で通信障害が発生しています。
- ユーザー名がuserid@isp-name形式でないか、ISPドメインがNASで正しく設定されていません。
- ユーザーがRADIUSサーバー上で設定されていません。
- ユーザーが入力したパスワードが正しくありません。
- RADIUSサーバーとNASには異なる共有キーが設定されています。

### 解決策

この問題を解決するには、次の手順に従います

1. 次の項目を確認します。
  - NASとRADIUSサーバーは相互にpingできます。
  - ユーザー名がuserid@isp-name形式で、ISPドメインがNAS上で正しく設定されている。
  - ユーザーはRADIUSサーバー上で設定されます。
  - 正しいパスワードが入力されている。
  - RADIUSサーバーとNASの両方に同じ共有キーが設定されています。
2. 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。

## RADIUS パケット配信障害

### 症状

RADIUSパケットはRADIUSサーバーに到達できません。

### 解析

考えられる理由は次のとおりです。

- NASとRADIUSサーバーの間で通信障害が発生しています。
- NASがRADIUSサーバーのIPアドレスが設定されていません。
- NASに設定されている認証およびアカウントングUDPポートが正しくありません。
- RADIUSサーバーの認証およびアカウントングポート番号は、他のアプリケーションで使用されています。

### 解決策

この問題を解決するには、次の手順に従います

1. 次の項目を確認します。
  - NASとRADIUSサーバーの間のリンクは、物理層とデータリンク層の両方で正常に動作します。
  - RADIUSサーバーのIPアドレスがNASで正しく設定されている。

- NAS に設定されている認証およびアカウントング UDP ポート番号は、RADIUS サーバーのポート番号と同じです。
  - RADIUS サーバーの認証およびアカウントングポート番号を使用できます。
2. 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。

## RADIUS アカウントングエラー

### 症状

ユーザーは認証され、許可されていますが、ユーザーのアカウントングは正常ではありません。

### 解析

NAS のアカウントングサーバー構成が正しくありません。考えられる理由は次のとおりです。

- NAS に設定されているアカウントングポート番号が正しくありません。
- NAS に設定されているアカウントングサーバーの IP アドレスが正しくありません。たとえば、NAS は認証、認可、およびアカウントングサービスを提供するために単一のサーバーを使用するように設定されていますが、実際にはサービスは別のサーバーによって提供されています。

### 解決策

この問題を解決するには、次の手順に従います

1. 次の項目を確認します。
  - アカウントングポート番号が正しく設定されている。
  - アカウントングサーバーの IP アドレスが NAS 上で正しく設定されている。
2. 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。

RADIUS のトラブルシューティング似ています。「RADIUS 認証失敗」、「RADIUS パケット送信エラー」および「RADIUS アカウントエラー」を参照してください。

## HWTACACS のトラブルシューティング

RADIUS のトラブルシューティングに似ています。「RADIUS 認証の失敗」、「RADIUS パケット配信の失敗」、および「RADIUS アカウントングエラー」を参照してください。

## LDAP 認証エラー

### 症状

ユーザー認証が失敗する。

### 解析

考えられる理由は次のとおりです。

- NAS と LDAP サーバーの間で通信障害が発生しています。
- NAS に設定されている LDAP サーバーの IP アドレスまたはポート番号が正しくありません。
- ユーザー名が userid@isp-name 形式でないか、ISP ドメインが NAS で正しく設定されていません。
- ユーザーが LDAP サーバー上で構成されていません。
- ユーザーが入力したパスワードが正しくありません。
- 管理者 DN またはパスワードが設定されていません。

- NAS に設定されている一部のユーザートリビュート(username アトリビュートなど)が、サーバーに設定されているアトリビュートと一致しません。
- LDAP スキームにユーザー検索ベース DN が指定されていません。

## 解決策

この問題を解決するには、次の手順に従います

1. 次の項目を確認します。
  - NAS と LDAP サーバーは互いに ping できます。
  - NAS に設定された LDAP サーバーの IP アドレスとポート番号は、サーバーの IP アドレスとポート番号と一致します。
  - ユーザー名の形式が正しく、ユーザー認証用の ISP ドメインが NAS で正しく設定されている。
  - ユーザーは LDAP サーバー上で設定されます。
  - 正しいパスワードが入力されている。
  - 管理者 DN と管理者パスワードが正しく設定されている。
  - NAS に設定されたユーザートリビュート(ユーザー名アトリビュートなど)は、LDAP サーバーに設定されたユーザートリビュートと一貫性があります。
  - 認証用のユーザー検索ベース DN が指定されています。
2. 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。

## 付録

### 付録 A 一般的に使用される RADIUS アトリビュート

一般的に使用される RADIUS アトリビュートは、RFC2865、RFC2866、RFC2867、および RFC2868 で定義されています。

表1 一般的に使用される RADIUS アトリビュート

項番	属性	項番	属性
1	User-Name	45	Acct-Authentic
2	User-Password	46	Acct-Session-Time
3	CHAP-Password	47	Acct-Input-Packets
4	NAS-IP-Address	48	Acct-Output-Packets
5	NAS-Port	49	Acct-Terminate-Cause
6	Service-Type	50	Acct-Multi-Session-Id
7	Framed-Protocol	51	Acct-Link-Count
8	Framed-IP-Address	52	Acct-Input-Gigawords
9	Framed-IP-Netmask	53	Acct-Output-Gigawords
10	Framed-Routing	54	(unassigned)
11	Filter-ID	55	Event-Timestamp
12	Framed-MTU	56-59	(unassigned)
13	Framed-Compression	60	CHAP-Challenge
14	Login-IP-Host	61	NAS-Port-Type

項番	属性	項番	属性
15	Login-Service	62	Port-Limit
16	Login-TCP-Port	63	Login-LAT-Port
17	(unassigned)	64	Tunnel-Type
18	Reply-Message	65	Tunnel-Medium-Type
19	Callback-Number	66	Tunnel-Client-Endpoint
20	Callback-ID	67	Tunnel-Server-Endpoint
21	(unassigned)	68	Acct-Tunnel-Connection
22	Framed-Route	69	Tunnel-Password
23	Framed-IPX-Network	70	ARAP-Password
24	State	71	ARAP-Features
25	Class	72	ARAP-Zone-Access
26	Vendor-Specific	73	ARAP-Security
27	Session-Timeout	74	ARAP-Security-Data
28	Idle-Timeout	75	Password-Retry
29	Termination-Action	76	Prompt
30	Called-Station-Id	77	Connect-Info
31	Calling-Station-Id	78	Configuration-Token
32	NAS-Identifier	79	EAP-Message
33	Proxy-State	80	Message-Authenticator
34	Login-LAT-Service	81	Tunnel-Private-Group-ID
35	Login-LAT-Node	82	Tunnel-Assignment-id
36	Login-LAT-Group	83	Tunnel-Preference
37	Framed-AppleTalk-Link	84	ARAP-Challenge-Response
38	Framed-AppleTalk-Network	85	Acct-Interim-Interval
39	Framed-AppleTalk-Zone	86	Acct-Tunnel-Packets-Lost
40	Acct-Status-Type	87	NAS-Port-Id
41	Acct-Delay-Time	88	Framed-Pool
42	Acct-Input-Octets	89	(unassigned)
43	Acct-Output-Octets	90	Tunnel-Client-Auth-id
44	Acct-Session-Id	91	Tunnel-Server-Auth-id

## 付録 B 一般的に使用される標準 RADIUS アトリビュートの説明

項番	[属性]	説明
1	User-Name	認証されるユーザーの名前。
2	User-Password	PAP認証用のユーザーパスワード。PAP認証が使用されるAccess-Requestパケットにのみ存在します。
3	CHAP-Password	CHAP認証用のユーザーパスワードのダイジェスト。CHAP認証が使用さ

項番	[属性]	説明
		れている場合、Access-Requestパケットにのみ存在します。
4	NAS-IP-Address	クライアントの識別に使用するサーバーのIPアドレス。通常、クライアントはアクセスインターフェースのIPアドレスで識別されます。この属性は、アクセス要求パケットにのみ存在します。
5	NAS-Port	ユーザーがアクセスするNASの物理ポート。
6	Service-Type	ユーザーが要求したサービスのタイプまたは提供されるサービスのタイプ。
7	Framed-Protocol	フレームアクセスのカプセル化プロトコル。
8	Framed-IP-Address	ユーザーに割り当てられたIPアドレス。
11	Filter-ID	フィルタリストの名前。この属性は次のように解析されます。 <ul style="list-style-type: none"> <li>名前が数字で始まる場合は、ACL 番号を示します。</li> <li>名前が数字で始まらない場合は、ユーザープロファイル名を示します。</li> </ul>
12	Framed-MTU	ユーザーとNAS間のデータリンクのMTU。たとえば、このアトリビュートを使用して、802.1X EAP認証で処理できるEAPパケットの最大サイズを定義できます。
14	Login-IP-Host	ユーザーがアクセスするNASインターフェースのIPアドレス。
15	Login-Service	ユーザーがログインに使用するサービスのタイプ。
18	Reply-Message	ユーザーに表示されるテキスト。サーバーが情報(認証失敗の原因など)の通信に使用できます。
26	Vendor-Specific	ベンダー固有の固有属性。パケットには1つ以上の固有属性を含めることができ、各固有属性には1つ以上のサブ属性を含めることができます。
27	Session-Timeout	セッション終了前のユーザーの最大サービス継続時間。
28	Idle-Timeout	セッションの終了前にユーザーに許可される最大アイドル時間。
31	Calling-Station-Id	NASがサーバーに送信するユーザーID。H3Cデバイスによって提供されるLANアクセスサービスの場合、この属性にはユーザーのMACアドレスが含まれます。
32	NAS-Identifier	NASがRADIUSサーバーに対して自身を識別するために使用するID。
40	Acct-Status-Type	アカウント要求パケットのタイプ。次の値を指定できます。 <ul style="list-style-type: none"> <li>1-開始。</li> <li>2-停止</li> <li>3-中間-更新。</li> <li>4-リセット-充電。</li> <li>7-Accounting-On(第3世代パートナーシッププロジェクトで定義)</li> <li>8-Accounting-Off(第3世代パートナーシッププロジェクトで定義)</li> <li>9~14:トンネルアカウント用予約されています。</li> <li>15:予約が失敗しました。</li> </ul>
45 45	Acct-Authentic	ユーザーが使用する認証方式。次の値を指定できます。 <ul style="list-style-type: none"> <li>1:RADIUS</li> <li>2-ローカル。</li> <li>3-リモート。</li> </ul>
60	CHAP-Challenge	CHAP認証中にMD5計算のためにNASによって生成されるCHAPチャレンジ。
61	NAS-Port-Type	ユーザーを認証しているNASの物理ポートのタイプ。可能な値は次のとお

項番	[属性]	説明
		<p>リです。</p> <ul style="list-style-type: none"> <li>15-イーサネット。</li> <li>16:任意のタイプの ADSL。</li> <li>17-ケーブル(ケーブル TV 用ケーブル付き)</li> <li>19-WLAN-IEEE802.11</li> <li>201:VLAN。</li> <li>202-ATM</li> </ul> <p>ポートがATMまたはイーサネットポートで、VLANが実装されている場合、このアトリビュートの値は201です。</p>
64	Tunnel-Type	<p>Tunneling protocols used.</p> <p>値13はVLANを表します。値が13の場合、デバイスはTunnel-Type、Tunnel-Medium-Type、およびTunnel-Private-Group-IDアトリビュートをVLANに割り当てるアトリビュートとして解釈します。</p>
65	Tunnel-Medium-Type	<p>トンネルの作成に使用するトランスポートメディアタイプ。</p> <p>VLAN割り当ての場合、802メディア+イーサネットを示す値は6である必要があります。</p>
79	EAP-Message	<p>EAPパケットをカプセル化して、RADIUSがEAP認証をサポートできるようにするために使用します。</p>
80	Message-Authenticator	<p>Access-Requestのスプーフィングを防止するために、認証パケットの認証および検証に使用されます。このアトリビュートは、EAP認証が使用される場合に存在します。</p>
81	Tunnel-Private-Group-ID	<p>トンネルセッションのグループID。VLANを割り当てるために、NASはこの属性を使用してVLAN IDを伝達します。</p>
87	NAS-Port-Id	<p>ユーザーを認証するNASのポートを記述する文字列。</p>
168	Framed-IPv6-Address	<p>ホストに割り当てるNASのサーバー割り当てIPv6アドレス。アドレスは一意である必要があります。</p>

## 付録 C RADIUS サブアトリビュート(ベンダーID25506)

表2に、ベンダーIDが25506のすべてのRADIUSサブアトリビュートを示します。これらのサブアトリビュートのサポートは、デバイスモデルによって異なります。

表2 RADIUS サブアトリビュート(ベンダーID25506)

項番	サブ属性	説明
1	Input-Peak-Rate	ユーザーからNASへの方向のピークレート(bps)。
2	Input-Average-Rate	ユーザーからNASへの方向の平均レート(bps)。
3	Input-Basic-Rate	ユーザーからNASへの方向の基本レート(bps単位)。
4	Output-Peak-Rate	NASからユーザーへの方向のピークレート(bps単位)。
5	Output-Average-Rate	NASからユーザーへの方向の平均レート(bps)。
6	Output-Basic-Rate	NASからユーザーへの方向の基本レート(bps)。
15	Remanent_Volume	接続に使用できるデータの総量。サーバータイプごとに異なる単位が使用されます。
17	ISP-ID	ユーザーが認証情報を取得するISPドメイン。

項番	サブ属性	説明
20	command	セッションの操作。セッション制御に使用されます。可能な値は次のとおりです。 <ul style="list-style-type: none"> <li>• 1-トリガー-要求。</li> <li>• 2-終了要求。</li> <li>• 3-設定ポリシー。</li> <li>• 4-結果。</li> <li>• 5-PortalClear</li> </ul>
25	Result_Code	Trigger-RequestまたはSetPolicy操作の結果。成功の場合は0、失敗の場合はその他の値。
26	Connect_ID	ユーザー接続のインデックス。
27	PortalURL	PPPoEユーザーに割り当てられたPADMリダイレクトURL。
28	Ftp_Directory	FTP、SFTP、またはSCPユーザー作業ディレクトリ RADIUSクライアントがFTP、SFTP、またはSCPサーバーとして動作する場合、このアトリビュートはRADIUSクライアント上のFTP、SFTP、またはSCPユーザーの作業ディレクトリを設定するために使用されます。
29	Exec_Privilege	EXECユーザープライオリティ。
32	NAT-IP-Address	送信元IPアドレスとポートが変換されるときにユーザーに割り当てられるパブリックIPアドレス。
33	NAT-Start-Port	送信元IPアドレスおよびポートが変換されるときにユーザーに割り当てられるポート範囲の開始ポート番号。
34	NAT-End-Port	送信元IPアドレスおよびポートが変換されるときにユーザーに割り当てられるポート範囲の終了ポート番号。
59	NAS_Startup_Timestamp	NASの起動時間(秒)。1970年1月1日(UTC)の00:00:00からの経過時間で表されます。
60	Ip_Host_Addr	A.B.C.D hh:hh:hh:hh:hh:hh形式の認証要求およびアカウントティング要求に含まれるユーザーIPアドレスおよびMACアドレス。IPアドレスとMACアドレスの間にはスペースが必要です。
61	User_Notify	サーバーからクライアントに透過的に送信する必要がある情報。
62	User_HeartBeat	802.1Xユーザーが認証に合格した後に割り当てられるハッシュ値。32バイトの文字列です。このアトリビュートはNASのユーザーリストに格納され、802.1Xユーザーからのハンドシェイクパケットを確認します。このアトリビュートはAccess-AcceptパケットとAccounting-Requestパケットにのみ存在します。
98	Multicast_Receive_Group	ユーザーのホストが受信者として参加するマルチキャストグループのIPアドレス。このサブ属性は、ユーザーが複数のマルチキャストグループに属していることを示すために、マルチキャストパケット内に複数回現れることがあります。
100	IP6_Multicast_Receive_Group	ユーザーのホストが受信者として参加するマルチキャストグループのIPv6アドレス。このサブ属性は、ユーザーが複数のマルチキャストグループに属していることを示すために、マルチキャストパケット内に複数回現れることがあります。
101	MLD-Access-Limit	ユーザーが同時に加入できるMLDマルチキャストグループの最大数。
102	local-name	L2TPローカルトンネル名。

項番	サブ属性	説明
103	IGMP-Access-Limit	ユーザーが同時に加入できるIGMPマルチキャストグループの最大数。
104	VPN-Instance	ユーザーが属するMPLS L3VPNインスタンス。
105	ANCP-Profile	ANCPプロファイル名。
135	Client-Primary-DNS	プライマリDNSサーバーのIPアドレス。
136	Client-Secondary-DNS	セカンダリDNSサーバーのIPアドレス。
140	User_Group	SSL VPNユーザーが認証に合格した後に割り当てられたユーザーグループ。ユーザーは、セミコロンで区切られた複数のユーザーグループに属することができます。この属性は、SSL VPNデバイス进行操作するために使用されます。
144	Acct_IPv6_Input_Octets	インバウンド方向のIPv6パケットのバイト単位は、デバイスの設定によって異なります。
145	Acct_IPv6_Output_Octets	アウトバウンド方向のIPv6パケットのバイト数。測定単位はデバイスの設定によって異なります。
146	Acct_IPv6_Input_Packets	インバウンド方向のIPv6パケット数。測定単位は、デバイスの設定によって異なります。
147	Acct_IPv6_Output_Packets	発信方向のIPv6パケット数。測定単位は、デバイスの設定によって異なります。
148	Acct_IPv6_Input_Gigawords	インバウンド方向のIPv6パケットのバイト。測定単位は4Gバイトです。
149	Acct_IPv6_Output_Gigawords	アウトバウンド方向のIPv6パケットのバイト数。測定単位は4Gバイトです。
155	User-Roles	スペースで区切られたユーザー役割のリスト。
210	Av-Pair	<p>ユーザー定義属性ペア。使用可能な属性ペアは次のとおりです。</p> <ul style="list-style-type: none"> <li>• device-traffic-class=voice 形式のサーバー割り当て音声 VLAN。</li> <li>• shell:role=xxx の形式でサーバーに割り当てられたユーザーロール。</li> <li>• url-redirect-acl=xxx 形式のサーバー割り当て ACL。</li> <li>• url-redirect=xxx 形式のサーバー割り当て Web リダイレクト URL。</li> <li>• subscriber:command=bounce-host-port の形式で、ポートをリブートするサーバー展開コマンド。</li> <li>• bounce:seconds=xxx 形式のサーバー割り当てポートシャットダウン時間。</li> <li>• subscriber:command=disable-host-port 形式の、ポートをシャットダウンするサーバー展開コマンド。</li> <li>• vxlan:vsi-name=xxx 形式のサーバー割り当て VSI。</li> <li>• ACL:match-by-vsiindex=x 形式の VSI ベース ACL リソース割り当て機能。x の値 1 はこの機能がサポートされていることを示し、x の他の値は予約されています。</li> <li>• mac:block-mac=xxx 形式のサーバー割り当てブラックホール MAC アドレスアトリビュート</li> </ul>
230	NAS-Port-Name	ユーザーがNASに接続するためのインターフェース。
246	Auth_Detail_Result	アカウントの詳細。次の状況では、サーバーはサブアトリビュート246および250のAccess-Acceptパケットを送信します。



項番	サブ属性	説明
		<ul style="list-style-type: none"> <li>1-加入者の料金が期限切れです。加入者はホワイトリスト内のネットワークリソースにアクセスできます。加入者が他のネットワークリソースにアクセスする場合、デバイスはサブアトリビュート 250 で指定された URL にそのリソースをリダイレクトします。</li> <li>2-加入者のブロードバンドリソースが期限切れになります。加入者が初めて Web ページへのアクセスを要求すると、デバイスはサブアトリビュート 250 で指定された URL に加入者をリダイレクトします。</li> </ul>
247	Input-Committed-Burst-Size	<p>ユーザーからNASへの認定バーストサイズ(ビット単位)。このフィールドの合計長は4バイトを超えることはできません。</p> <p>このサブアトリビュートは、入力平均レート(Input-Average-Rate)アトリビュートと一緒に割り当てる必要があります。</p>
248	Output-Committed-Burst-Size	<p>NASからユーザーへの認定バーストサイズ(ビット単位)。このフィールドの合計長は4バイトを超えることはできません。</p> <p>このサブアトリビュートは、出力平均レート(Output-Average-Rate)アトリビュートとします。</p>
249	authentication-type	<p>認証タイプ。値は次のいずれかです。</p> <ul style="list-style-type: none"> <li>1-イントラネットアクセス認証。</li> <li>2-インターネットアクセス認証。</li> </ul> <p>パケットにこのサブアトリビュートが含まれていない場合は、共通認証が適用されます。</p>
250	WEB-URL	ユーザーのリダイレクトURL。
251	Subscriber-ID	ファミリープランID。
252	Subscriber-Profile	サブスクライバのファミリープランのQoSポリシー名。
255	Product_ID	製品名。

# 802.1X の概要

## 802.1X プロトコルについて

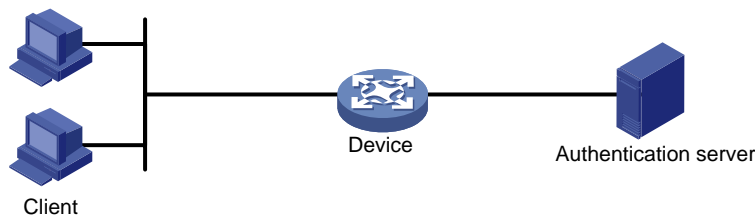
802.1X は、イーサネットネットワークで広く使用されているポートベースのネットワークアクセス制御プロトコルです。このプロトコルは、802.1X 対応の LAN ポートに接続されているデバイスを認証することによってネットワークアクセスを制御します。

## 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(サブリカント):** LAN へのアクセスを要求するユーザー端末。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):** クライアントを認証して、LAN へのアクセスを制御します。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、サーバーはアクセスデバイスに認証結果を返して、アクセスを決定します。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

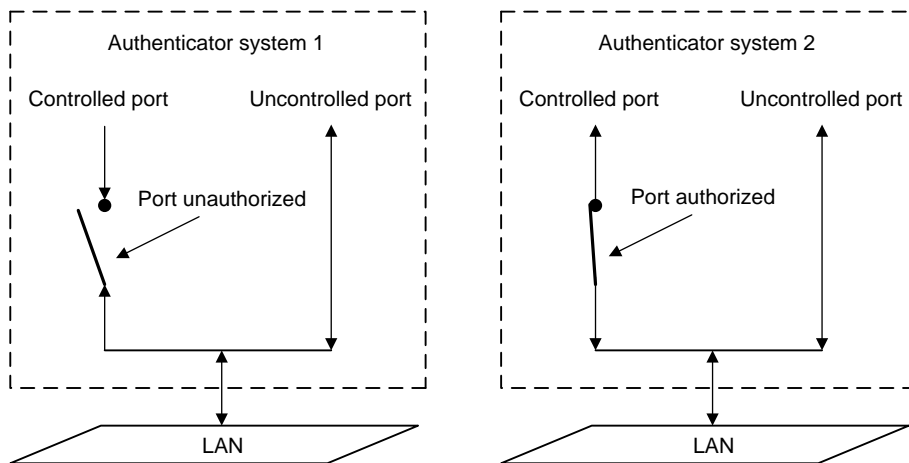


## 制御/非制御ポートおよびポート許可ステータス

802.1X では、ネットワークアクセスポートに対して、制御ポートと非制御ポートの 2 つの論理ポートが定義されています。ネットワークアクセスポートに到達したパケットは、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開いています。
- **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。
  - **許可ステート:** クライアントが認証に合格すると、制御ポートは許可ステートになります。ポートはトラフィックのパススルーを許可します。
  - **無許可ステート:** クライアントが認証に失敗すると、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、クライアントとの間のトラフィックを拒否します。
    - 単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。デバイスは単方向トラフィック制御だけをサポートします。

図 2 制御ポートの許可状態



## パケット交換方式

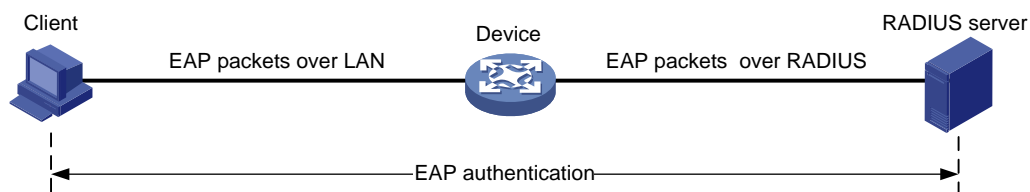
802.1X は、拡張認証プロトコル(EAP)を使用して、クライアント、アクセスデバイス、および認証サーバーの認証情報を転送します。EAP は、クライアント/サーバーモデルを使用する認証フレームワークです。このフレームワークは、MD5-Challenge、EAP-Transport Layer Security(EAP-TLS)、および Protected EAP(PEAP)などのさまざまな認証方法をサポートします。

802.1X 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の間で EAP パケットを渡すための EAP over LAN(EAPOL)を定義します。アクセスデバイスと認証サーバーの間では、802.1X は EAP リレーまたは EAP 終端のいずれかによって認証情報を配信します。

### 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、図 3 に示すように、ネットワークデバイスは EAP over RADIUS(EAPOR)パケットを使用して RADIUS サーバーに認証情報を送信します。

図 3 EAP リレー



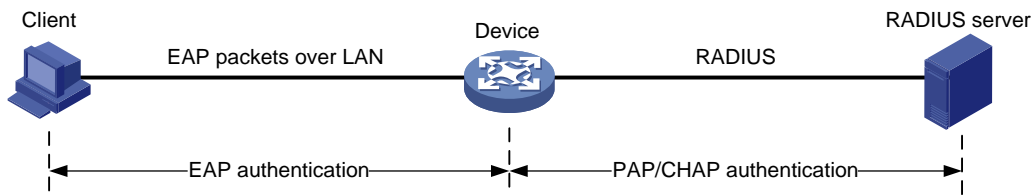
EAP リレーモードでは、クライアントは RADIUS サーバーと同じ認証方式を使用する必要があります。アクセスデバイスでは、`dot1x authentication-method eap` コマンドを使用するだけで EAP リレーをイネードルにできます。

### EAP 終端

図 4 に示すように、アクセスデバイスは EAP 終端モードで次の操作を実行します。

1. クライアントから受信した EAP パケットを終端します。
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. RADIUS サーバーへの認証に PAP または CHAP を使用します。

図 4 EAP 終端



## EAP リレーと EAP 終端の比較

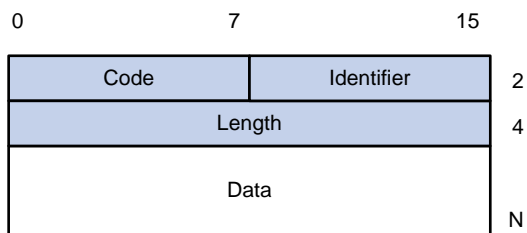
パケット交換方式	メリット	制限事項
EAPリレー	<ul style="list-style-type: none"> <li>さまざまな EAP 認証方式をサポートします。</li> <li>アクセスデバイスでの設定と処理は簡単です。</li> </ul>	RADIUSサーバーは、EAP-MessageアトリビュートとMessage-Authenticatorアトリビュート、およびクライアントが使用する EAP 認証方式をサポートする必要があります。
EAP終端	PAPまたはCHAP認証をサポートするすべてのRADIUSサーバーで動作します。	<ul style="list-style-type: none"> <li>次の EAP 認証方式だけをサポートします。 <ul style="list-style-type: none"> <li>MD 5:Challenge EAP 認証。</li> <li>iNode 802.1X クライアントによって開始されるユーザー名とパスワードの EAP 認証。</li> </ul> </li> <li>アクセスデバイスでの処理は複雑です。</li> </ul>

## パケット形式

### EAP パケット形式

図 5 に、EAP パケットフォーマットを示します。

図 5 EAP パケット形式

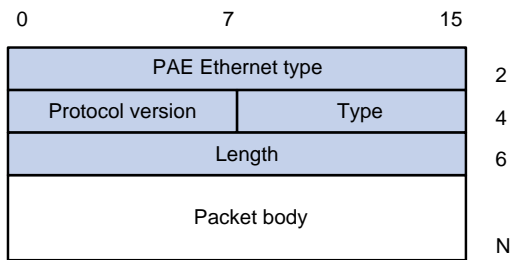


- **Code:** EAP パケットのコードタイプ。オプションには、Request(1)、Response(2)、Success(3)、または Failure(4)があります。
- **Identifier:** 応答と要求の照合に使用します。
- **Length:** EAP パケットの長さ(バイト単位)。EAP パケットの長さは、Code、Identifier、Length、および Data フィールドの合計です。
- **Data:** EAP パケットの内容。このフィールドは、Request または Response EAP パケットでのみ表示されます。Data フィールドには、要求タイプ(または応答タイプ)およびタイプデータが含まれます。タイプ 1(Identity)およびタイプ 4(MD5-Challenge)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 パケットの形式を示します。

図 6 EAPOL パケット形式



- **PAE Ethernet type:** プロトコルタイプ。EAPOL の場合は値 0x888E を取ります。
- **Protocol Version:** EAPOL パケット送信者が使用する EAPOL プロトコルのバージョン。
- **Type:** EAPOL パケットのタイプ。表 1 に、デバイス上の 802.1X の実装によってサポートされる 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秒	EAP-Packet	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秒	EAPOL-Start	クライアントはEAPOL-Startメッセージを送信して、アクセスデバイスに対して802.1X認証を開始します。
0x02秒	EAPOL-logoff	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していることをアクセスデバイスに通知します。

- **Length:** データ長(バイト単位)、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。

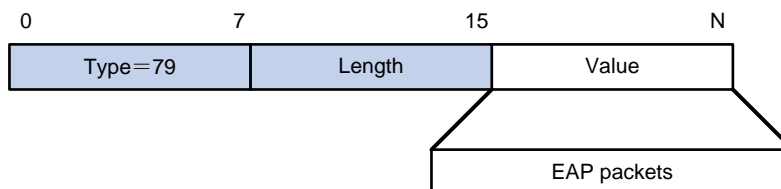
## RADIUS を介した EAP

RADIUS は、EAP 認証をサポートするために、EAP-Message と Message-Authenticator の 2 つの属性を追加します。RADIUS パケット形式については、「AAA の設定」を参照してください。

- EAP-Message。

RADIUS は、図 7 に示すように、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 バイトで、Value フィールドは最大 253 バイトです。EAP パケットが 253 バイトより長い場合、RADIUS はそれを複数の EAP-Message 属性にカプセル化します。

図 7 EAP-Message 属性フォーマット

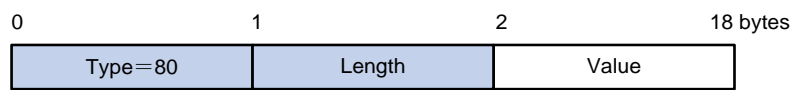


- Message-Authenticator。

図 8 に示すように、RADIUS では、整合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 属性が含まれます。計算されたパケット整合性チェックサムが Message-Authenticator 属性値と異なる場合、パケットレシーバはパケットを

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 メッセージ認証属性の形式



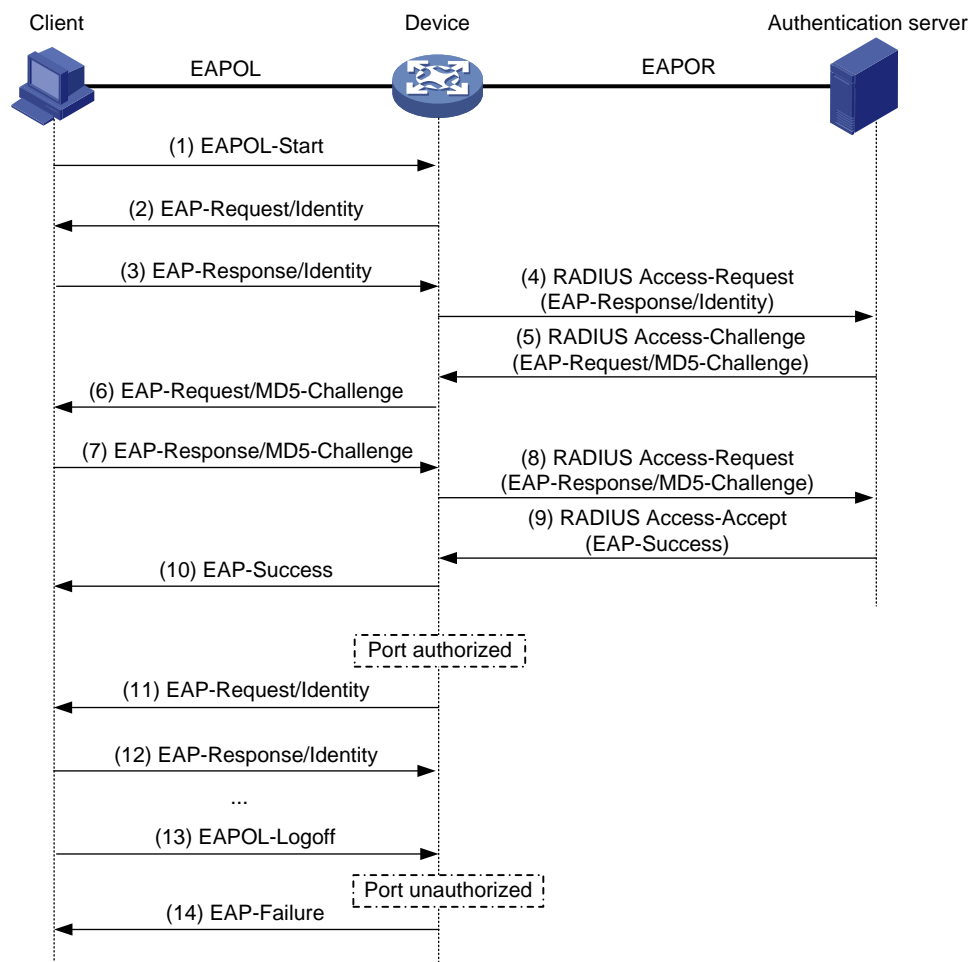
## 802.1X 認証手順

802.1X 認証には、EAP リレーと EAP 終端の 2 つの方式があります。EAP パケットおよび EAP 認証方式に対する RADIUS サーバーのサポートに応じて、いずれかのモードを選択します。

### EAP リレー

図 9 に、EAP リレーモードでの基本的な 802.1X 認証手順を示します。MD5-Challenge EAP 認証が使用されていることが前提です。

図 9 EAP リレーモードでの 802.1X 認証手順



次の手順では、802.1X 認証手順について説明します。

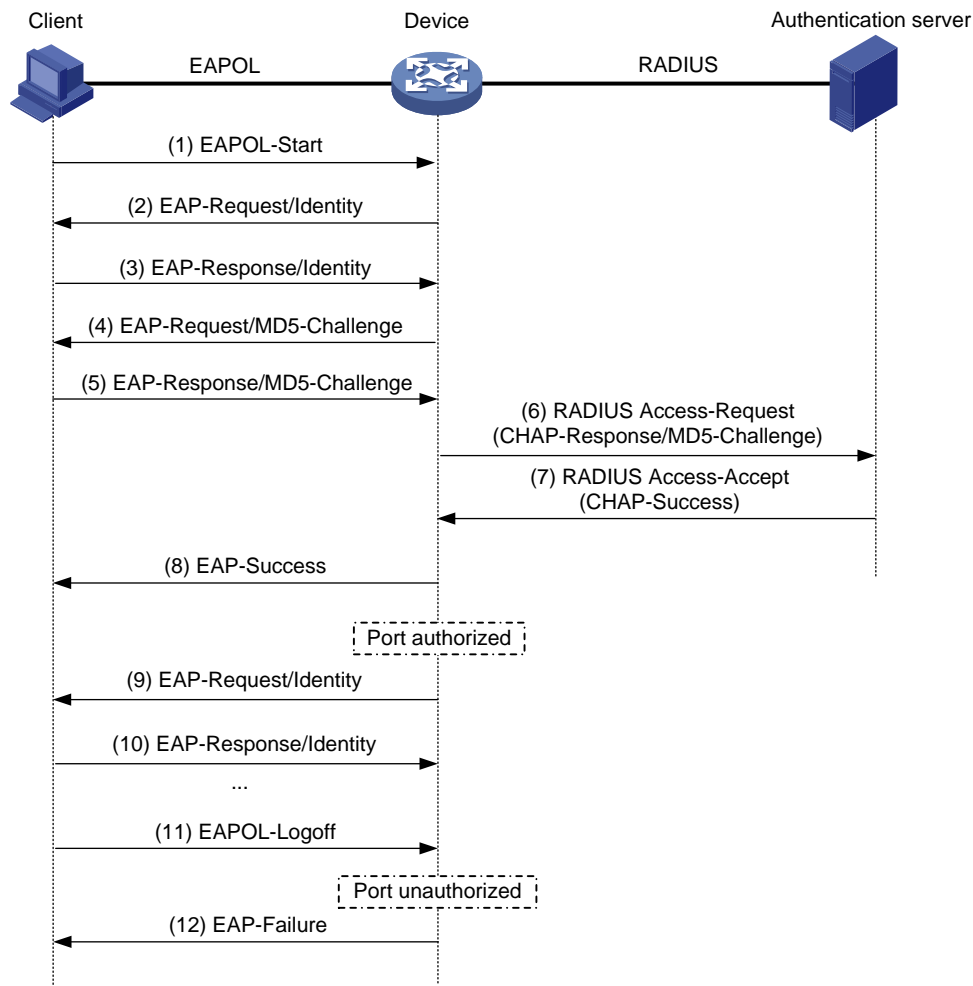
1. ユーザーが 802.1X クライアントを起動し、登録されたユーザー名とパスワードを入力すると、802.1X クライアントは EAPOL-Start パケットをアクセスデバイスに送信します。

2. アクセスデバイスは、EAP-Request/Identity パケットで応答し、クライアントユーザー名を要求します。
3. EAP-Request/Identity パケットに回答して、クライアントは EAP-Response/Identity パケットでユーザ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/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。その後、サーバーはチャレンジを RADIUS Access-Challenge パケットでアクセスデバイスに送信します。
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、暗号化されたパスワードを EAP-Response/MD5-Challenge パケットで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を有効と見なし、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処理を実行します。
  - 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タスに設定します。  
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からログオフします。
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。連続して何回かハンドシェイクを試みてもクライアントが応答を返さない場合(デフォルトでは 2 回)、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 ユーザー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、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 パケットに回答して、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 終端

図 10 に、EAP 終端モードでの基本的な 802.1X 認証手順を示します。CHAP 認証が使用されていることを前提としています。

図 10 EAP 終端モードでの 802.1X 認証手順



EAP 終端モードでは、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。アクセスデバイスは、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

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。

### イニシエータとしての 802.1X クライアント

クライアントは、802.1X 認証を開始するために EAPOL-Start パケットをアクセスデバイスに送信します。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 10 で使用可能な 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て、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:** 未知の MAC アドレスからフレームを受信すると、アクセスデバイスは受信ポートから MAC アドレスに EAP-Request/Identity パケットを送信します。ID 要求タイムアウト間隔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要求の最大試行回数に達するまで継続されます。

ユーザ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 要求インターバルとユニキャストトリガーの ID 要求タイムアウトインターバル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 ユーザーがポートで認証を渡すと、その後のユーザ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。認証されたユーザーがログオフすると、他のすべてのユーザーはログオフされます。
- **MAC ベースのアクセス制御:** 各ユーザーは、ポート上で個別に認証されます。ユーザーがログオフしても、他のオンラインユーザーは影響を受けません。

## 802.1X VLAN 操作

### 認証 VLAN

認証 VLAN は、認可されたネットワークリソースへの 802.1X ユーザ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証 VLAN をサポートします。

#### ❗重要:

タグ付き認証 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 認証

リモート VLAN 認証では、リモートサーバー上のユーザーの認証 VLAN を設定する必要があります。ユーザーがサーバーに対して認証されると、サーバーは認証 VLAN 情報をデバイスに割り当てます。次に、デバイスはユーザーア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証 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証 VLAN 情報の割り当てをサポートします。

- 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 および VLAN 名の文字列。

この文字列では、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、『レイヤー2 LAN スイッチングコンフィギュレーションガイド』を参照してください。

- サフィックス t または u が付いた VLAN ID。

- t および u サフィックスでは、デバイスがア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 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 を割り当てる前にその情報を VLAN ID に変換します。

**①重要:**

VLAN 名で表される VLAN を正常に割り当てるには、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、アクセスポートが、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。

**①重要:**

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る認証 VLAN は、次のいずれのタイプにもできません。

- ダイナミックに学習された VLAN。
- 予約済み VLAN。
- スーパーVLAN。
- プライベート 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 VLAN を選択します(表 2 を参照)。

**表 2 VLAN グループからの認証 VLAN の選択**

VLAN 情報	認証 VLAN の選択
IDによるVLAN 名前によるVLAN VLANグループ名	<p>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、デバイスは次のルールに従って、ユーザーのVLANグループから認証VLANを選択します。</p> <ul style="list-style-type: none"> <li>• MAC ベース VLAN がイネーブルになっているハイブリッドポートの場合:               <ul style="list-style-type: none"> <li>○ ポートにオンラインユーザーがいない場合、デバイスは最も小さい ID を持つ VLAN を選択します。</li> <li>○ ポートにオンラインユーザーがいる場合、デバイスはオンラインユーザーが最も少ない VLAN を選択します。2 つの VLAN に同じ数のオンライン 802.1X ユーザーがいる場合、デバイスはより低い ID の VLAN を選択します。</li> </ul> </li> <li>• アクセス、トランク、または MAC ベース VLAN がディセーブルになっているハイブリッドポートの場合:               <ul style="list-style-type: none"> <li>○ ポートにオンラインユーザーがいない場合、デバイスは最も小さい ID を持つ VLAN を選択します。</li> <li>○ ポートにオンラインユーザーがいる場合、デバイスはオンラインユーザーの VLAN の VLAN グループを調べます。VLAN が検出されると、その VLAN は認証 VLAN としてユーザーに割り当てられます。VLAN が検出されない場合、VLAN 認証は失敗します。</li> </ul> </li> </ul> <p>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VLANグループから最小のIDを持つVLANを選択します。後続のすべての802.1Xユーザーは、そのVLANに割り当てられます。</p>
サフィックス付きのVLAN ID	<ol style="list-style-type: none"> <li>1. デバイスは、サフィックスのない最も左側の VLAN ID、または u のサフィックスが付いた最も左側の VLAN ID のうち、より左側にある方をタグ</li> </ol>

VLAN 情報	認証 VLAN の選択
	<p>無 VLAN として選択します。</p> <p>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。</p> <p>たとえば、認証サーバーはユーザーのアクセスデバイスに文字列 1u 2t 3を送信します。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 が PVID になります。</p>

## ローカル VLAN 認証

ユーザーに対してローカル VLAN 認証を実行するには、そのユーザーのローカルユーザーカウントの認証アトリビュートリストに VLAN ID を指定します。各ローカルユーザーに指定できる認証 VLAN ID は 1 つだけです。ユーザーがデバイスにアクセスするために使用するポートは、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 認証では、タグ付き VLAN の割り当てはサポートされません。

ローカルユーザ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 対応ポートの認証 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 操作

ポートアクセスコントロール方式	VLAN 操作
ポートベース	<p>デバイスは、最初に認証されたユーザーの認証 VLAN にポートを割り当てます。その後のすべての 802.1X ユーザーは、認証なしで VLAN にアクセスできます。</p> <p>認証 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証 VLAN に割り当て、VLAN を PVID として設定します。認証 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。</p>
MAC ベース	<p>MAC ベース VLAN がイネーブルになっているハイブリッドポートでは、デバイスは各ユーザーの MAC アドレスを独自の認証 VLAN にマッピングします。ポートの PVID は変更されません。</p> <p>アクセス、トランク、または MAC ベース VLAN がディセーブルになっているハイブリッドポートの場合:</p> <ul style="list-style-type: none"> <li>デバイスは、最初に認証されたユーザーの認証 VLAN にポートを割り当て、その認証 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。</li> <li>認証 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証 VLAN に割り当てます。</li> </ul>

❗重要:

- アクセスポートに接続されたユーザーの場合、サーバーによって割り当てられた認証 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ます。サーバーがタグ付きアトリビュートを持つ VLAN を発行した場合、VLAN 割り当ては失敗します。
- トランクまたは MAC ベース VLAN がディセーブルのハイブリッドポートに接続されたユーザーに 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。後続のユーザーに別のタグなし VLAN が割り当てられた場合、そのユーザ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証 VLAN に割り当てないでください。

ユーザーに認証 VLAN が割り当てられていない場合に、802.1X 認証ユーザ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実行します。

- ポートが VLAN 内のユーザ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 内のユーザ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。

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ポートでは、MAC ベース VLAN 機能は、この機能がイネーブルになる前からオンラインであったユーザーに対しては有効になりません。アクセスデバイスは、次の要件が満たされた場合に、ユーザーの MAC/VLAN マッピングを作成します。

- ユーザーが再認証を通過しました。
- ユーザーの認証 VLAN が変更されます。

VLAN 設定および MAC ベース VLAN の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

## 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ユーザーに対応します。ゲスト VLAN 内のユーザーは、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、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 内のユーザーは、802.1X 認証を通過すると、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 対応ポート上の 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 状態の場合、ユーザーは 802.1X 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 ユーザーは、ゲスト VLAN 内のリソースにのみアクセスできます。 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。詳細については、「認証 VLAN」の表 7 を参照してください。
802.1X ゲスト VLAN のユーザーが 802.1X 認証に失敗しました。	802.1X 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。このポートのすべてのユーザーは、認証失敗 VLAN 内のリソースにだけアクセスできます。 認証失敗 VLAN が設定されていない場合、ポートは 802.1X ゲスト VLAN のままです。ポート上のすべてのユーザーはゲスト VLAN に属します。 802.1X 認証失敗 VLAN の詳細については、「認証失敗 VLAN」を参照してください。

認証ステータス	VLAN 操作
802.1XゲストVLANのユーザーは、802.1X認証を通過しません。	<p>デバイスは802.1XゲストVLANからポートを削除し、そのポートをユーザーの認証VLANに割り当てます。</p> <p>認証サーバーが認証VLANを割り当てない場合、ポートの最初のPVIDが適用されます。ユーザーおよび後続のすべての802.1Xユーザーは、最初のポートVLANに割り当てられます。</p> <p>ユーザーがログオフすると、ポートは再びゲストVLANに割り当てられます。</p> <p><b>注:</b></p> <p>802.1X 対応ポートの初期 PVID 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ていた PVID です。</p>

**❗重要:**

ポートが VLAN タグの付いたパケットを受信すると、VLAN がゲスト VLAN でない場合、パケットはタグ付き VLAN 内で転送されます。

### MAC ベースのアクセス制御

認証ステータス	VLAN 操作
ユーザーが802.1X対応ポートにアクセスし、802.1X認証を実行していません。	デバイスは、ユーザーの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。ユーザーは、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のユーザーが802.1X認証に失敗しました。	<p>802.1X認証失敗VLANが使用可能な場合、デバイスはユーザーのMACアドレスを認証失敗VLANに再マッピングします。ユーザーは、認証失敗VLAN内のリソースにだけアクセスできます。</p> <p>802.1X認証失敗VLANが設定されていない場合、ユーザーは802.1XゲストVLANから削除され、初期PVIDに追加されます。</p>
802.1XゲストVLANのユーザーは、802.1X認証を通過します。	<p>デバイスは、ユーザーのMACアドレスを認証VLANに再マッピングします。</p> <p>認証サーバーが認証VLANを割り当てない場合、デバイスはユーザーのMACアドレスをポート上の初期PVIDに再マッピングします。</p>

## 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準拠していないために 802.1X 認証に失敗したユーザーに対応します。たとえば、VLAN は、誤ったパスワードが入力されたユーザーに対応します。認証失敗 VLAN のユーザーは、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、アンチウイルスソフトウェアや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 対応ポート上の 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
ユーザーがポートにアクセスし、802.1X認証に失敗しました。	<p>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802.1Xユーザーは、認証失敗VLANのリソースにだけアクセスできます。</p> <p>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、「認証VLAN」の表7を参照してください。</p>
802.1XゲストVLANのユーザー	ポートはまだ認証失敗VLANにあり、このポートのすべての802.1Xユーザーはこ

認証ステータス	VLAN 操作
一は、802.1X認証に失敗しました。	のVLANに属しています。
802.1X認証失敗VLANのユーザーは、802.1X認証を通過しました。	<p>デバイスはユーザーの認証VLANにポートを割り当て、認証失敗VLANからポートを削除します。</p> <p>認証サーバーが認証VLANを割り当てない場合、ポートの最初のPVIDが適用されます。ユーザーおよび後続のすべての802.1Xユーザーは、最初のPVIDに割り当てられます。</p> <p>ユーザーがログオフすると、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。</p>

## MAC ベースのアクセス制御

認証ステータス	VLAN 操作
ユーザーが802.1X有効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、ユーザーのMACアドレスを802.1X認証失敗VLANにマッピングします。ユーザーは、認証失敗VLAN内のリソースにだけアクセスできます。
802.1X認証失敗VLANのユーザーは、802.1X認証に失敗しました。	ユーザーはまだ認証失敗VLANにいます。
802.1X認証失敗VLANのユーザーは、802.1X認証を通過しました。	<p>デバイスは、ユーザーのMACアドレスを認証VLANに再マッピングします。</p> <p>認証サーバーが認証VLANを割り当てない場合、デバイスはユーザーのMACアドレスをポート上の初期PVIDに再マッピングします。</p>

## クリティカル VLAN

ポート上の 802.1X クリティカル VLAN は、ISPドメイン内に到達可能な RADIUS サーバーがないために認証に失敗した 802.1X ユーザーに対応します。クリティカル VLAN のユーザーは、設定に応じて制限さ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。802.1X ユーザーが RADIUS 認証後にローカル認証に失敗した場合、そのユーザーはクリティカル 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 対応ポート上の 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
ユーザーはポートにアクセスしますが、すべてのRADIUSサーバーが到達不能であるため、802.1X認証に失敗します。	<p>デバイスはポートをクリティカルVLANに割り当てます。802.1Xユーザーおよびこのポート上のすべての後続の802.1Xユーザーは、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。</p> <p>クリティカル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、「AAAの設定」の表7を参照してください。</p>
802.1XクリティカルVLANのユーザーは、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。	ポートはまだクリティカルVLANにあります。
802.1XクリティカルVLANのユーザーは、到	802.1X認証失敗VLANが設定されている場合、ポートは認証失敗

認証ステータス	VLAN 操作
達不能なサーバー以外の理由で認証に失敗します。	VLANに割り当てられます。802.1X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のユーザーは、802.1X認証を通過します。	デバイスはユーザーの認証VLANにポートを割り当て、802.1XクリティカルVLANからポートを削除します。 認証サーバーが認証VLANを割り当てない場合は、ポートの最初のPVIDが適用されます。ユーザーおよび後続のすべての802.1Xユーザーは、このポートVLANに割り当てられます。 ユーザーがログオフすると、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は、ポートの初期PVIDが復元されます。
802.1XゲストVLANのユーザーは、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。	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ユーザーはこのVLANに属します。
802.1X認証失敗VLANのユーザーは、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認証失敗VLANにあります。このポートのすべての802.1Xユーザーは、802.1X認証失敗VLANのリソースにだけアクセスできます。
認証に合格したユーザーは、すべてのRADIUSサーバーが到達不能であるため再認証に失敗し、デバイスからログアウトされます。	デバイスはポートを802.1XクリティカルVLANに割り当てます。

## MAC ベースのアクセス制御

認証ステータス	VLAN 操作
ユーザーはポートにアクセスしますが、すべてのRADIUSサーバーが到達不能であるため、802.1X認証に失敗します。	デバイスは、ユーザーのMACアドレスを802.1XクリティカルVLANにマッピングします。ユーザーは、802.1XクリティカルVLAN内のリソースにだけアクセスできます。
802.1XクリティカルVLANのユーザーは、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。	ユーザーはまだクリティカルVLANに属しています。
802.1XクリティカルVLANのユーザーが、到達不能なサーバー以外の理由で802.1X認証に失敗しました。	802.1X認証失敗VLANが設定されている場合、デバイスはユーザーのMACアドレスを認証失敗VLAN IDに再マッピングします。 802.1X認証失敗VLANが設定されていない場合、デバイスはユーザーのMACアドレスを初期PVIDに再マッピングします。
802.1XクリティカルVLANのユーザーは、802.1X認証を通過します。	デバイスは、ユーザーのMACアドレスを認証VLANに再マッピングします。 認証サーバーがユーザーに認証VLANを割り当てない場合、デバイスはユーザーのMACアドレスをポート上の初期PVIDに再マッピングします。
802.1XゲストVLANのユーザーは、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。	デバイスは、ユーザーのMACアドレスを802.1XクリティカルVLANに再マッピングします。ユーザーは、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認証失敗VLANのユーザーは、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。	ユーザーは802.1X認証失敗VLANのままです。

到達可能な RADIUS サーバーが検出されると、デバイスは次の処理を実行します。

- MAC ベースのアクセスコントロールが使用されている場合、デバイスはクリティカル VLAN から 802.1X ユーザーを削除します。ポートは、認証をトリガーするために、これらのユーザーにユニキャスト EAP-Request/Identity を送信します。
- ポートベースのアクセスコントロールが使用されている場合、デバイスはクリティカル VLAN からポートを削除します。ポートは、認証をトリガーするために、ポート上のすべての 802.1X ユーザーにマルチキャスト EAP-Request/Identity を送信します。

## クリティカル Voice VLAN

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

クリティカル Voice 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。802.1X 音声ユーザーが RADIUS 認証後にローカル認証に失敗すると、その音声ユーザーはクリティカル Voice 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。

到達可能な RADIUS サーバーが検出されると、デバイスは 802.1X アクセスコントロール方式に基づいてポート上で動作を実行します。

### ポートベースのアクセス制御

到達可能な RADIUS サーバーが検出されると、デバイスはクリティカルな Voice VLAN からポートを削除します。ポートは、認証をトリガーするために、ポート上のすべての 802.1X 音声ユーザーにマルチキャスト EAP-Request/Identity パケットを送信します。

### MAC ベースのアクセス制御

到達可能な RADIUS サーバーが検出されると、デバイスはクリティカルな Voice VLAN から 802.1X 音声ユーザーを削除します。ポートは、認証をトリガーするために、クリティカルな Voice VLAN に割り当てられた各 802.1X 音声ユーザーにユニキャスト EAP-Request/Identity パケットを送信します。

## 802.1X VSI操作

この機能は、MAC ベースのアクセスコントロールを実行する 802.1 X 対応ポートだけでサポートされます。

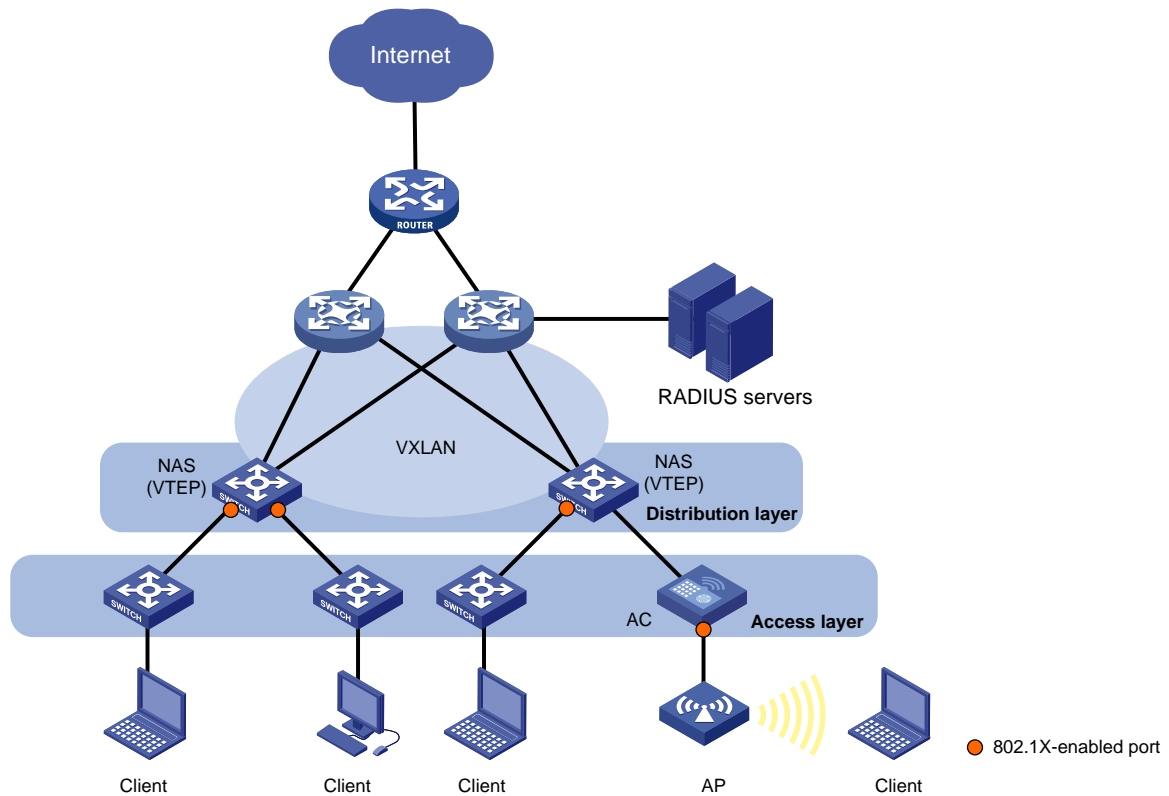
## VXLAN の 802.1X サポート

図 29 に示すように、デバイスが VXLAN VTEP と NAS の両方として動作する場合、ユーザーのサービス情報は VLAN によって識別できません。この問題を解決するには、認証された 802.1X ユーザーに VSI を割り当てるように RADIUS サーバーを設定する必要があります。NAS は、ユーザーのトラフィックを、ユーザーの認可 VSI に関連付けられた VXLAN にマッピングします。マッピング基準には、ユーザーのアクセス VLAN、アクセスポート、および MAC アドレスが含まれます。

VSI および VXLAN の詳細については、『VXLAN Configuration Guide』を参照してください。



図 29 802.1X 認証用の VXLAN ネットワーク図



## 認証 VSI

認可 VSI は、非認証ユーザーがアクセスできないネットワークリソースを持つ VXLAN に関連付けられています。

802.1X はリモート VSI 認可をサポートしています。ユーザーがリモート 802.1X 認証を渡すと、リモートサーバーはユーザーの認可 VSI 情報をユーザーのアクセスポートに割り当てます。認可 VSI 情報を受信すると、VTEP は次の操作を実行します。

1. ユーザーのアクセスポート、VLAN、および MAC アドレスに基づいて、イーサネットサービスインスタンスを動的に作成します。
2. イーサネットサービスインスタンスを認可 VSI にマッピングします。

これにより、ユーザーは認可 VSI に関連付けられた VXLAN 内のリソースにアクセスできます。

VTEP がリモートサーバーからユーザーの認可 VSI 情報を受信しない場合、ユーザーは認証を通過した後、どの VXLAN のリソースにもアクセスできません。

イーサネットサービスインスタンスの動的作成の詳細については、『VXLAN configuration Guide』を参照してください。

## ゲスト VSI

ポート上の 802.1X ゲスト VSI は、802.1X 認証を実行していないユーザーに対応します。ゲスト VSI に関連付けられた VXLAN には、限定されたネットワークリソースのセットを展開できます。たとえば、ユーザーが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するためのソフトウェアサーバーを展開します。ゲスト VSI のユーザーが 802.1X 認証を通過すると、そのユーザーはゲスト VSI 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。

次の表は、MAC ベースのアクセスコントロールを実行する 802.1X 対応ポートで VTEP が VSI を処理する方法を示しています。

認証ステータス	VSI 操作
ユーザーがポートにアクセスし、802.1X認証を実行していません。	VTEPは、ユーザーのMACアドレスとアクセスVLANをポート上の802.1XゲストVSIにマッピングします。ユーザーは、ゲストVSIに関連付けられたVXLAN内のリソースだけにアクセスできます。
802.1XゲストVSIのユーザーが802.1X認証に失敗しました。	802.1X認証失敗VSIがポートで使用可能な場合、VTEPはユーザーのMACアドレスとアクセスVLANを認証失敗VSIに再マッピングします。ユーザーは、認証失敗VSIに関連付けられたVXLAN内のリソースだけにアクセスできます。 ポートに802.1X Auth-Fail VSIが設定されていない場合、ユーザーは802.1XゲストVSIから削除されます。
802.1XゲストVSIのユーザーは、802.1X認証を通過します。	VTEPは802.1XゲストVSIからユーザーを削除し、ユーザーのMACアドレスとアクセスVLANを認可VSIに再マッピングします。

## 認証失敗 VSI

ポート上の 802.1X Auth-Fail VSI は、組織のセキュリティ方針に準拠していなかったために 802.1X 認証に失敗したユーザーに対応します。たとえば、VSI は、誤ったパスワードが入力されたユーザーに対応します。Auth-Fail VSI のユーザーは、この VSI に関連付けられた VXLAN 内の限られたネットワークリソースにアクセスできます。Auth-Fail VSI にソフトウェアサーバーを配置して、ユーザーが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るようにすることができます。

次の表は、MAC ベースのアクセスコントロールを実行する 802.1X 対応ポートで VTEP が VSI を処理する方法を示しています。

認証ステータス	VSI 操作
ユーザーがポートにアクセスし、802.1X認証に失敗しました。	VTEPは、ユーザーのMACアドレスとアクセスVLANをポート上の802.1X認証失敗VSIにマッピングします。ユーザーは、認証失敗VSIに関連付けられたVXLAN内のリソースだけにアクセスできます。
802.1X Auth-Fail VSIのユーザーは、到達不能サーバー以外の理由で802.1X認証に失敗します。	ユーザーはまだAuth-fail VSIの状態です。
802.1X認証失敗VSIのユーザーは、802.1X認証を通過します。	VTEPは802.1X認証失敗VSIからユーザーを削除し、ユーザーのMACアドレスとアクセスVLANを認可VSIに再マッピングします。

## クリティカル VSI

ポート上の 802.1X クリティカル VSI は、ISPドメイン内に到達可能な RADIUS サーバーがないために認証に失敗した 802.1X ユーザーに対応します。クリティカル VSI のユーザーは、この VSI に関連付けられた VXLAN 内の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 VSI 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。802.1XユーザーがRADIUS認証後にローカル認証に失敗した場合、そのユーザーはクリティカルVSI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。

次の表は、MAC ベースのアクセスコントロールを実行する 802.1X 対応ポートで VTEP が VSI を処理する方法を示しています。

認証ステータス	VSI 操作
ユーザーはポートにアクセスしますが、すべてのRADIUSサーバーが到達不能であるため、802.1X認証に失敗します。	VTEPは、ユーザーのMACアドレスとアクセスVLANをポート上の802.1XクリティカルVSIにマッピングします。ユーザーは、クリティカルVSIに関連付けられたVXLAN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VSIのユーザーは認証に失敗します。	ユーザーはまだクリティカルVSIにいます。
802.1XクリティカルVSIのユーザーは、到達不能なサーバー以外の理由で802.1X認証に失敗します。	802.1X認証失敗VSIがポートに設定されている場合、VTEPはユーザーのMACアドレスとアクセスVLANを認証失敗VSIに再マッピングします。 ポートに802.1X 認証失敗VSIが設定されていない場合、VTEPはユーザーをログオフします。
802.1XクリティカルVSIのユーザーは、802.1X認証を通過します。	VTEPは、ユーザーのMACアドレスとアクセスVLANを認可VSIに再マッピングします。
802.1X認証失敗VSIのユーザーは、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。	ユーザーは802.1X 認証失敗VSIのままです。

## ACLの割り当て

認証サーバー上の 802.1X ユーザーに ACL を指定して、ネットワークリソースへのユーザーのアクセスを制御できます。ユーザーが 802.1X 認証を通過すると、認証サーバーは ACL をアクセスポートに割り当てて、このユーザーのトラフィックをフィルタリングします。認証サーバーは、ローカルアクセスデバイスまたは RADIUS サーバーです。いずれの場合も、アクセスデバイスに ACL を設定する必要があります。

ユーザ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認証 ACL を指定します。

サポートされる認証 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 の範囲の番号が付けられた拡張 ACL。

認可 ACL を有効にするには、ACL が存在し、counting、established、fragment、または logging キーワードで設定されたルールを除く ACL ルールがあることを確認します。

ACL 設定の詳細については、『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

認証サーバーで 802.1X ユーザー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ユーザーのアクセスを制御できます。ユーザーが 802.1X 認証に合格すると、認証サーバーはユーザーにユーザープロファイルを割り当てて、トラフィックをフィルタリングします。認証サーバーは、ローカルアクセスデバイスまたは RADIUS サーバーです。いずれの場合も、アクセスデバイスでユーザープロファイルを設定する必要があります。

ユーザ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。

- 認証サーバー上のユーザー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については、「プロファイルの設定」を参照してください。

## リダイレクトURLの割り当て

802.1X 対応ポートが MAC ベースのアクセス制御を実行し、ポートの認証状態が auto の場合、デバイスは RADIUS サーバーによって割り当てられた URL 属性をサポートします。認証中、802.1X ユーザーの HTTP または HTTPS 要求は、サーバーに割り当てられた URL 属性によって指定された Web インターフェースにリダイレクトされます。ユーザーが Web 認証に合格すると、RADIUS サーバーはユーザーの MAC アドレスを記録し、DM(切断メッセージ)を使用してユーザーをログオフします。ユーザーが 802.1X 認証を再度開始すると、認証に合格し、正常にオンラインになります。

この機能は、EAD アシスタント機能と相互に排他的です。

802.1X ユーザーの HTTPS 要求をリダイレクトするには、デバイス上の HTTPS リダイレクトリスニングポートを指定します。詳細については、『レイヤー3 IP サービスコンフィギュレーションガイド』の「HTTP リダイレクト」を参照してください。

## CARアトリビュートの割り当て

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 ユーザ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、「AAA の設定」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-Peak-Rate:** 着信トラフィックのピークレート(bps)。
- **Input-Average-Rate:** 着信トラフィックの平均レート(bps)。
- **Output-Peak-Rate:** 発信トラフィックのピークレート(bps)。
- **Output-Average-Rate:** 発信トラフィックの平均レート(bps)。

サーバーがピークレートと平均レートの両方を制御するための CAR アトリビュートを割り当てる場合、デバイスはユーザートラフィックにダブルレートトラフィックポリシングを実装します。サーバーが Input-Peak-Rate または Output-Peak-Rate アトリビュートを割り当てない場合、デバイスはユーザートラフィックにシングルレートトラフィックポリシングを実装します。トラフィックポリシングの詳細については、『ACL and QoS Configuration Guide』の「QoS configuration」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、オンラインユーザ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ユーザーの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 ユーザーを再認証します。間隔はタイマーによって制御され、タイマーはユーザーが設定できます。定期的な再認証タイマーの変更は、古いタイマーが期限切れになり、ユーザーが認証に合格した後に限り、オンラインユーザーに適用されます。

サーバ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)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ユーザー再認証機能に影響を与える可能性があります。サーバーに割り当てられた 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ユーザー再認証は、定期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ユーザー再認証設定は有効になりません。セッションタイムアウトタイマーの期限が切れると、デバイスはオンラインの 802.1X ユーザーを再認証します。

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、デバイスの定期的な再認証設定によって決まります。Session-Timeout アトリビュートと 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。

RADIUS DAS 機能がイネーブルの場合、RADIUS 認証サーバーから再認証アトリビュートを含む CoA メッセージを受信すると、デバイスはただちにユーザーを再認証します。この場合、デバイスで 802.1X 定期再認証がイネーブルになっているかどうかに関係なく、再認証が実行されます。RADIUS DAS 設定の詳細については、「AAA の設定」を参照してください。

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の 802.1X ユーザ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に、認証された 802.1X ユーザーをオンラインに維持します。

再認証の前後でオンラインユーザーに割り当てられる VLAN は、同じでも異なってもかまいません。

## EADアシスタント

Endpoint Admission Defense(EAD)は、ネットワークの脅威防御機能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連携して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、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、ユーザーの HTTP 要求または HTTPS 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 Assistant は、次の機能によって実装されます。

- フリー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 サーバーなどの限られたネットワークリソースセットを持ちます。セキュリティ方針に準拠するために、非認証ユーザ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、ユーザ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 サーバーから動的 IP アドレスを取得したりできます。
- リダイレクト URL。  
認証されていない 802.1X ユーザーが 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、ユーザ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、ユーザーを 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、ACL ベースの EAD ルールを自動的に作成して、リダイレクトされた各ユーザーのリダイレクト URL へのアクセスを開きます。

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、ユーザーが認証に合格すると、ルールは削除されます。ユーザーが 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認証に合格しなかった場合、ユーザー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。

# 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 認証を組み合わせで拡張します。これは、ポート上のユーザーごとに異なる認証方式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については、「ポートセキュリティの設定」を参照してください。

認証サーバーが認可 VSI と認証 VLAN の両方をユーザーに割り当てる場合、デバイスは認証 VLAN だけを使用します。

ポートでは、ゲスト VLAN、Auth-fail VLAN(認証失敗 VLAN)、およびクリティカル VLAN 設定は、ゲスト VSI、Auth-fail VSI、およびクリティカル VSI 設定と相互に排他的です。

認証 VLAN または認可 VSI を正常に割り当てるには、次の注意事項に従ってください。

- 802.1X 対応ポートがゲスト VLAN、Auth-fail VLAN(認証失敗 VLAN)、またはクリティカル VLAN で設定されている場合は、認証サーバーを設定して、認証 VLAN を 802.1X ユーザーに割り当てます。
- 802.1X 対応ポートがゲスト VSI、Auth-Fail VSI、または重要な VSI で設定されている場合は、802.1X ユーザーに認可 VSI を割り当てるように認証サーバーを設定します。

802.1X ゲスト VSI 機能が正しく動作するように、この機能を EAD Assistant と一緒に設定しないでください。

ポートの 802.1X ゲスト VLAN、Auth-fail VLAN(認証失敗 VLAN)、またはクリティカル VLAN にユーザーがいる場合は、ポートのリンクタイプを変更しないでください。

802.1X 設定は、レイヤー2 イーサネットインターフェースおよびレイヤー2 集約インターフェースだけでサポートされます。

レイヤー2 イーサネットインターフェースが集約グループに追加されると、インターフェースの 802.1X 設定は有効になりません。

インターフェースにオンラインの 802.1X ユーザーがいる場合は、レイヤー2 集約インターフェースを削除しないでください。

## 802.1Xタスクの概要

802.1X 認証を設定するには、次の作業を実行します。

1. 802.1X を有効にする
2. 基本的な 802.1X 機能の設定
  - EAP リレーまたは EAP 終了の有効化
  - ポート認証状態の設定
  - アクセス制御方法の指定
  - (任意) ポートでの必須認証ドメインの指定。
  - (任意) 802.1X 認証タイムアウト タイマーの設定。
  - (任意) 802.1X 再認証の構成。
  - (任意) 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 の構成
  - 802.1X ゲスト VLAN 割り当て遅延の有効化

- 802.1X 認証失敗 VLAN の設定
- 802.1X クリティカル VLAN の構成
- 802.1X クリティカル Voice VLAN 機能の有効化
- 4. (任意)802.1X VSI 割り当ての設定
  - 802.1X ゲスト VSI の構成
  - 802.1X ゲスト VSI 割り当て遅延の有効化
  - 802.1X 認証失敗 VSI の構成
  - 802.1X クリティカル VSI の構成
- 5. (任意)その他の 802.1X 機能の設定
  - 認証トリガー機能の構成  
この作業は、802.1X クライアントが認証を開始できない場合に実行します。
  - ポートでの同時 802.1X ユーザーの最大数の設定
  - 認証リクエストの最大試行回数の設定
  - オンライン ユーザー ハンドシェイクの構成
  - サポートされているドメイン名区切り文字の指定
  - ポートから送信された 802.1X プロトコル パケットの VLAN タグの削除
  - MAC 認証ユーザーの 802.1X 認証試行の最大回数の設定
  - 802.1X ユーザー IP フリーズの有効化
  - 802.1X MAC アドレス バインドの構成
  - EAD アシスタント機能の構成
  - 802.1X ユーザーのロギングを有効にする

## 802.1Xの前提条件

802.1X を設定する前に、次の作業を実行します。

- 802.1X ユーザー用の 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。
- RADIUS 認証を使用する場合は、RADIUS サーバー上にユーザ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、アクセスデバイスにローカルユーザ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

### 制約事項とガイドライン

802.1X をポートで有効にするには、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。

PVID が Voice VLAN の場合、802.1X 機能はポートで有効になりません。Voice VLAN の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

### 手順

1. システムビューを開始します。  
**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. インターフェイスビューを開始します。

**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終了のイネーブル化

### EAP モードの選択について

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 クライアントおよび RADIUS サーバーでサポートされる認証方式。

### 制約事項とガイドライン

- 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、クライアントからの認証データを変更せずにサーバーに送信します。**user-name-format** コマンドの詳細については、「セキュリティコマンドリファレンス」を参照してください。
- 次のいずれかの状況では、EAP 終端と EAP リレーの両方を使用できます。
  - クライアントは MD 5 チャレンジ EAP 認証だけを使用しています。EAP 終端が使用されている場合は、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、ユーザー名とパスワードの EAP 認証だけを開始します。EAP 終端が使用される場合、アクセスデバイスで PAP または CHAP 認証のいずれかをイネーブルにできます。ただし、セキュリティのために、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 認証方式を使用するには、EAP リレーを使用する必要があります。決定する場合は、「EAP リレーと EAP ターミネーションの比較」を参照してください。

### 手順

1. システムビューを開始します。

#### System-view

2. EAP リレーまたは EAP 終端を設定します。

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

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

## ポート許可状態の設定

### ポートの許可ステートについて

ポートの許可ステートは、クライアントがネットワークへのアクセスを許可されるかどうかを決定します。ポートの次の許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、ポート上のユーザ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:** ポートが無許可状態にして、ポート上のユーザーからのアクセス要求を拒否します。
- **Auto:** ポートを最初は無許可状態にして、EAPOL パケットだけが通過できるようにします。ユーザーが認証を通過した後、ポートを許可状態に設定して、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. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

3. ポートの許可状態を設定します。

**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

## アクセス制御方式について

デバイスは、ポートベースおよび MAC ベースのアクセスコントロール方式をサポートしています。

## 手順

1. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

**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

## 必須認証ドメインについて

ポートでの認証、認可、およびアカウントिंगのために、すべての 802.1X ユーザーを必須認証ドメインに配置できます。どのユーザーも、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。必須認証ドメインの実装により、802.1X アクセスコントロール展開の柔軟性が向上します。

## 手順

1. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

**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

## 802.1X 認証タイムアウトタイマーについて

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すると開始されます。このタイマーの期限が切れたときに応答が受信されない場合、アクセスデバイスは要求をクライアントに再送信します。
- **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すると開始されます。このタイマーの期限が切れたときに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。ネットワークの状況に応じて、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. システムビューを開始します。

### 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

## 制約事項とガイドライン

デバイスは、次の順序で 802.1X 再認証の定期再認証タイマーを選択します。

1. サーバーによって割り当てられた再認証タイマー。
2. ポート固有の再認証タイマー。
3. グローバル再認証タイマー。
4. デフォルトの再認証タイマー。

手動再認証を実行すると、サーバーによって割り当てられた再認証アトリビュートおよびポートの定期的な再認証機能に関係なく、デバイスはポート上のすべてのオンライン 802.1X ユーザーを再認証します。

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

## 手順

1. システムビューを開始します。

### System-view

2. 定期的な再認証タイマーを設定します。
  - グローバル定期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。
  - ポート固有の定期再認証タイマーを設定するには、次のコマンドを順番に実行します。  
**interface interface-type interface-number**  
**dot1x timer reauth-period reauth-period-value**  
**quit**  
 デフォルトでは、定期的な再認証タイマーはポートに設定されていません。ポートはグローバルな 802.1X 定期的再認証タイマーを使用します。
3. インターフェイスビューを開始します。  
**interface interface-type interface-number**
4. 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-authentication**  
 デフォルトでは、この機能はディセーブルです。
5. (任意)ポート上のすべてのオンライン 802.1X ユーザーを手動で再認証します。  
**dot1x re-authentication manual**
6. (任意)802.1X ユーザーの keep-online 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の 802.1X ユーザーをログオフします。  
 実際のネットワークの状態に応じて、keep-online 機能を使用します。高速リカバリネットワークでは、keep-online 機能を使用して、802.1X ユーザーが頻りにオンラインになったりオフライン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

### 待機タイマーについて

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。

### 制約事項とガイドライン

ネットワークの状況に応じて、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。
- 認証応答が迅速なハイパフォーマンスネットワークでは、待機タイマーを低い値に設定します。

### 手順

1. システムビューを開始します。  
**System-view**
2. クワイエット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

### 制約事項とガイドライン

- 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。異なるポートの 802.1X ゲスト VLAN は異なる場合があります。
- ポート上のポート VLAN、Voice VLAN、および 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 VLAN タグ付きの着信トラフィックを正しく処理できるようになります。
- 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 の注意事項に従ってください。

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	関係の説明	参考
スーパーVLAN	VLANをスーパーVLANと802.1XゲストVLANの両方として指定することはできません。	『レイヤー2-LANスイッチングコンフィギュレーションガイド』を参照してください。
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は、802.1XゲストVLANよりもプライオリティが高くなります。	「802.1x操作」を参照してください。
MACベースのアクセス制御を実行するポートでのポート侵入保護アクション	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ポートシャットダウンアクションよりも低くなっています。	「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、次の作業を実行します。

- 802.1X ゲスト VLAN として指定する VLAN を作成します。
- 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は、ポートに対して次の操作を実行します。
  - ポートをハイブリッドポートとして設定します。
  - ポートで MAC ベース VLAN をイネーブルにします。MAC ベース VLAN の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。
  - ポートをタグ無メンバーとして 802.1X ゲスト VLAN に割り当てます。

### 手順

1. システムビューを開始します。  
**system-view**
2. インターフェイスビューを開始します。  
**interface interface-type interface-number**
3. ポートに 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ゲストVLAN割り当て遅延のイネーブル化

## 802.1X ゲスト VLAN 割り当て遅延の概要

この機能は、ポートで 802.1X 認証がトリガーされたときに、802.1X 対応ポートを 802.1X ゲスト VLAN に割り当ててのを遅らせます。

この機能は、802.1X クライアントからの EAPOL-Start パケットまたは未知の MAC アドレスからのパケットによって 802.1X 認証がトリガーされる状況にだけ適用されます。

この機能を使用するには、802.1X 対応ポートで MAC ベースのアクセスコントロールを実行する必要があります。新しい MAC トリガー802.1X ゲスト VLAN 割り当て遅延を使用するには、ポートで 802.1X ユニキャストトリガーも設定する必要があります。

ポートで 802.1X 認証がトリガーされると、デバイスは次の動作を実行します。

1. 認証をトリガーする MAC アドレスにユニキャスト EAP-Request/Identity パケットを送信します。
2. `dot1x timer tx-period` コマンドを使用して設定されたユーザー名要求タイムアウト間隔内に応答が受信されない場合、パケットを再送信します。
3. `dot1x retry` コマンドを使用して設定された要求の最大試行回数に達した後、ポートを 802.1X ゲスト VLAN に割り当てます。

## 手順

1. システムビューを開始します。

**system-view**

2. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

3. ポートで 802.1X ゲスト VLAN 割り当て遅延をイネーブルにします。

**dot1x guest-vlan-delay** { *eapol* | *new-mac* }

デフォルトでは、802.1X ゲスト VLAN 割り当て遅延はポート上でディセーブルです。

# 802.1X認証失敗VLANの設定

## 制約事項とガイドライン

- ポート上のポート VLAN、Voice VLAN、および 802.1X 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 認証失敗 VLAN は 1 つだけです。異なるポートの 802.1X 認証失敗 VLAN は異なる場合があります。
- ポートに複数のセキュリティ機能を設定する場合は、表 5 の注意事項に従ってください。

表 5 802.1X 認証失敗 VLAN とその他の機能との関係

機能	関係の説明	参考
スーパーVLAN	VLANをスーパーVLANと802.1X 認証失敗VLANの両方として指定することはできません。	『レイヤー2-LANスイッチングコンフィギュレーションガイド』を参照してください。
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MAC認証ゲストVLAN	802.1X認証失敗VLANのプライオリティは高くなっています。	「MAC認証の設定」を参照してください。
MACベースのアクセス制御を実	802.1X認証失敗VLAN機能は、	「ポートセキュリティの設定」を参

機能	関係の説明	参考
行するポートでのポート侵入保護アクション	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ポートシャットダウンアクションよりも低くなっています。	照してください。

## 前提条件

802.1X 認証失敗 VLAN を設定する前に、次の作業を実行します。

- 802.1X 認証失敗 VLAN として指定する VLAN を作成します。
- 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は、ポートに対して次の操作を実行します。
  - ポートをハイブリッドポートとして設定します。
  - ポートで MAC ベース VLAN をイネーブルにします。MAC ベース VLAN の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。
  - ポートをタグ無メンバーとして Auth-fail VLAN(認証失敗 VLAN)に割り当てます。

## 手順

1. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

**interface** *interface-type* *interface-number*

3. ポートに 802.1X 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、ポート上に 802.1X 認証失敗 VLAN は存在しません。

# 802.1XクリティカルVLANの設定

## ポートでの 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注意事項

- ポート上の PVID、Voice VLAN、および 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。異なるポートの 802.1X クリティカル VLAN は異なる場合があります。
- VLAN をスーパーVLANと 802.1X クリティカル VLAN の両方として指定することはできません。スーパーVLAN の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

## 前提条件

802.1X クリティカル VLAN を設定する前に、次の作業を実行します。

- クリティカル VLAN として指定する VLAN を作成します。
- 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は、ポートに対して次の操作を実行します。
  - ポートをハイブリッドポートとして設定します。

- ポートで MAC ベース VLAN をイネーブルにします。MAC ベース VLAN の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。
- ポートをタグ無メンバーとして 802.1X クリティカル VLAN に割り当てます。

## 手順

1. システムビューを開始します。  
**system-view**
2. インターフェイスビューを開始します。  
**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、ポート上に 802.1X クリティカル VLAN は存在しません。

# 802.1X クリティカル VLAN 内のユーザーへの EAP-Success パケットの送信

## 802.1X クリティカル VLAN 内のユーザーへの EAP-Success パケット送信について

通常、クライアントユーザーが 802.1X クリティカル VLAN に割り当てられると、デバイスは 802.1X クライアントに EAP-Failure パケットを送信します。Windows 組み込みの 802.1X クライアントなどの一部の 802.1X クライアントは、EAP-Failure パケットを受信した場合、デバイスの EAP-Request/Identity パケットに回答できません。その結果、認証サーバーが到達可能な場合、これらのクライアントの再認証は失敗します。

この機能を使用すると、クライアントユーザーが 802.1X クリティカル VLAN に割り当てられている場合に、EAP-Failure パケットではなく EAP-Success パケットを 802.1X クライアントに送信できます。この操作により、すべての 802.1X クライアントが再認証を実行できるようになります。

## 手順

1. システムビューを開始します。  
**System-view**
2. インターフェイスビューを開始します。  
**interface** *interface-type interface-number*
3. クライアントユーザーがポート上のクリティカル VLAN に割り当てられたときに、EAP-Success パケットを 802.1X クライアントに送信するようにデバイスを設定します。  
**dot1x critical EAPOL**  
デフォルトでは、クライアントユーザーがポート上のクリティカル VLAN に割り当てられると、デバイスは EAP-Failure パケットを 802.1X クライアントに送信します。

# 802.1XクリティカルVoice VLAN機能のイネーブル化

## 制約事項とガイドライン

音声ユーザーが 802.1X 認証失敗 VLAN に属していた場合、この機能は有効になりません。

## 前提条件

ポートで 802.1X クリティカル Voice VLAN 機能をイネーブルにする前に、次の作業を実行します。

- グローバルおよびポートの両方で LLDP をイネーブルにします。  
デバイスは LLDP を使用して音声ユーザーを識別します。LLDP の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。
- ポート上で Voice VLAN をイネーブルにします。  
Voice VLAN の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

## 手順

1. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

3. ポート上で 802.1X クリティカル Voice VLAN 機能をイネーブルにします。

### dot1x critical-voice-vlan

デフォルトでは、802.1X クリティカル Voice VLAN 機能はポート上でディセーブルになっています。

# 802.1X ゲスト VSI の設定

## 制約事項とガイドライン

1 つのポートに設定できる 802.1X ゲスト VSI は 1 つだけです。異なるポート上の 802.1X ゲスト VSI は異なる場合があります。

## 前提条件

802.1X 対応ポートで 802.1X ゲスト VSI を設定する前に、次の作業を実行します。

- L2VPN をイネーブルにします。
- 802.1X ゲスト VSI として指定する VSI を作成し、VSI 用の VXLAN を作成します。
- MAC ベースのアクセスコントロールを実行し、ポート上のダイナミックイーサネットサービスインスタンスの MAC ベースのトラフィックマッチングをイネーブルにするようにポートを設定します。

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

## 手順

1. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

3. ポートに 802.1X ゲスト VSI を設定します。

### dot1x guest-vsi guest-vsi-name

デフォルトでは、ポート上に 802.1X ゲスト VSI は存在しません。



# 802.1XゲストVSI割り当て遅延のイネーブル化

## 802.1X ゲスト VSI 割り当て遅延の概要

この機能は、ポートで 802.1X 認証がトリガーされたときに、802.1X ゲスト VSI への 802.1X 対応ポートの割り当てを遅らせます。

この機能は、802.1X クライアントからの EAPOL-Start パケットまたは未知の MAC アドレスからのパケットによって 802.1X 認証がトリガーされる状況にだけ適用されます。

この機能を使用するには、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必要があります。

ポートで 802.1X 認証がトリガーされると、デバイスは次の動作を実行します。

1. 認証をトリガーする MAC アドレスにユニキャスト EAP-Request/Identity パケットを送信します。
2. `dot1x timer tx-period` コマンドを使用して設定されたユーザー名要求タイムアウト間隔内に応答が受信されない場合、パケットを再送信します。
3. `dot1x retry` コマンドを使用して設定された要求の最大試行回数に達した後、ポートを 802.1X ゲスト VSI に割り当てます。

この機能は、ポートが 802.1X 認証と MAC 認証の組み合わせを実行する場合に、MAC 認証と 802.1X 認証の並列処理機能と連携して動作します。この連携により、ポートは 802.1X ゲスト VSI に割り当てられる前に MAC 認証を実行できます。MAC 認証と 802.1X 認証の並列処理機能の詳細については、「MAC 認証の設定」を参照してください。

## 手順

1. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

`interface interface-type interface-number`

3. ポート上で 802.1X ゲスト VSI 割り当て遅延をイネーブルにします。

`dot1x guest-vsi-delay { eapol | new-mac }`

デフォルトでは、802.1X ゲスト VSI 割り当て遅延はポート上でディセーブルです。

# 802.1X認証失敗VSIの設定

## 制約事項とガイドライン

1つのポートに設定できる 802.1X Auth-Fail VSI は 1つだけです。異なるポートの 802.1X Auth-Fail VSI は異なる場合があります。

## 前提条件

802.1X 対応ポートで 802.1X Auth-Fail VSI を設定する前に、次の作業を実行します。

- L2VPN をイネーブルにします。
- 802.1X 認証失敗 VSI として指定される VSI を作成し、VSI の VXLAN を作成します。
- MAC ベースのアクセスコントロールを実行し、ポート上のダイナミックイーサネットサービスインスタンスの MAC ベースのトラフィックマッチングをイネーブルにするようにポートを設定します。

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

## 手順

1. システムビューを開始します。  
**system-view**
2. インターフェイスビューを開始します。  
**interface** *interface-type interface-number*
3. ポート上で 802.1X 認証失敗 VSI を設定します。  
**dot1x auth-fail vsi** *authfail-vsi-name*  
デフォルトでは、ポート上に 802.1X 認証失敗 VSI は存在しません。

# 802.1XクリティカルVSIの設定

## 制約事項とガイドライン

1 つのポートに設定できる 802.1X クリティカル VSI は 1 つだけです。異なるポートの 802.1X クリティカル VSI は異なる場合があります。

## 前提条件

802.1X 対応ポートで 802.1X クリティカル VSI を設定する前に、次の作業を実行します。

- L2VPN をイネーブルにします。
- 802.1X クリティカル VSI として指定される VSI を作成し、VSI の VXLAN を作成します。
- MAC ベースのアクセスコントロールを実行し、ポート上のダイナミックイーサネットサービスインスタンスの MAC ベースのトラフィックマッチングをイネーブルにするようにポートを設定します。

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

## 手順

1. システムビューを開始します。  
**System-view**
2. インターフェイスビューを開始します。  
**interface** *interface-type interface-number*)
3. ポートに 802.1X クリティカル VSI を設定します。  
**dot1x critical vsi** *critical-vsi-name*  
デフォルトでは、ポート上に 802.1X クリティカル VSI は存在しません。

# 認証トリガー機能の設定

## 認証トリガーについて

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および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)。

## 制約事項とガイドライン

- ポートに接続されたクライアントが 802.1X 認証を開始するための EAPOL-Start パケットを送信できない場合に、ポート上でマルチキャストトリガーをイネーブルにします。

- 少数の 802.1X クライアントだけがポートに接続され、これらのクライアントが認証を開始できない場合は、ポート上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、1つのポート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. システムビューを開始します。

### System-view

2. (任意)ユーザ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. インターフェイスビューを開始します。

**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ユーザーの最大数の設定

## ポート上の同時 802.1X ユーザーの最大数の設定について

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. システムビューを開始します。

### system-view

2. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

3. ポート上の同時 802.1X ユーザーの最大数を設定します。

**dot1x max-user** *max-number*

デフォルトは 4294967295 です。

# 認証要求の最大試行回数設定

## 認証要求の再送信について

アクセスデバイスは、一定期間内にクライアントからの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試行を行っても応答を受信しない場合、要求の再送信を停止します。

## 手順

1. システムビューを開始します。

### system-view

2. 認証要求の送信を試行する最大回数を設定します。

**dot1x retry** *retries*

デフォルト設定は 2 です。

# オンラインユーザーハンドシェイクの設定

## オンラインユーザーハンドシェイクについて

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 ユーザ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、オンラインユーザ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ユーザーから EAP-Response/Identity パケットを受信しない場合、デバイスはユーザ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 EAP-Success パケットを使用して 802.1X クライアントの EAP-Response/Identity パケットに返信しません。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場合、オフラインになります。この問題を回避するには、オンラインユーザーハンドシェイク応答機能をイネーブルにします。

iNode クライアントが展開されている場合は、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。この機能を使用すると、不正なクライアントソフトウェアを使用する 802.1X ユーザーが、デュアルネットワークインターフェイスカード(NIC)検出などの iNode セキュリティチェックをバイパスするのを防ぐことができます。ユーザ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、デバイスはそのユーザーをオフライン状態に設定します。

## 制約事項とガイドライン

- 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、オンラインユーザーハンドシェイク機能を無効にします。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。
- 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、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上でのみ有効です。
- 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、オンラインユーザ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. システムビューを開始します。

### System-view

2. (任意)ハンドシェイクタイマーを設定します。

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

デフォルトは 15 秒です。

3. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

4. 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**

デフォルトでは、この機能はイネーブルになっています。

5. (任意)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**

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 オンラインユーザ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 パケットに返信しません。

## サポートされているドメイン名デリミタの指定

### サポートされているドメイン名デリミタについて

デフォルトでは、アクセスデバイスはデリミタとしてアットマーク(@)をサポートしています。他のドメイン名デリミタを使用する 802.1X ユーザ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。設定可能なデリミタには、アットマーク(@)、バックスラッシュ(\)、ドット(.)、およびスラッシュ(/)が含まれます。ドメイン名を含むユーザー名では、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 ユーザー名文字列に複数の区切り記号が設定されている場合、右端の区切り記号がドメイン名の区切り記号になります。たとえば、円記号(\)、ドット(.)、およびスラッシュ(/)を区切り記号として設定した場合、ユーザー名文字列 121.123/22\@abc のドメイン名の区切り記号は円記号(\)になります。ユーザー名は @abc で、ドメイン名は 121.123/22 です。

### 制約事項とガイドライン

ユーザー名文字列にデリミタ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 ドメインでユーザーを認証します。

ユーザー名とドメイン名を 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。ユーザー名形式の設定については、『セキュリティコマンドリファレンス』の **user-name-format** コマンドを参照してください。

### 手順

1. システムビューを開始します。

#### System-view

2. 802.1X ユーザーのドメイン名デリミタ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(@)デリミタだけがサポートされています。

## ポートから送信された802.1Xプロトコルパケットの VLAN タグの削除

### ポートから送信された 802.1X プロトコルパケットの VLAN タグの削除について

この機能は、ポートが VLAN のタグ付きメンバーであるかタグなしメンバーであるかに関係なく、VLAN タグが削除された 802.1X プロトコルパケットを送信するように、ハイブリッドポートで動作します。

802.1X 対応ハイブリッドポートがその PVID のタグ付きメンバーであり、接続された 802.1X クライアントが VLAN タグ付き 802.1X プロトコルパケットを認識できない場合は、この機能を使用します。

### 制約事項とガイドライン

この機能は、ポートから 802.1X クライアントに送信されるすべての 802.1X プロトコルパケットの VLAN タグを削除します。VLAN 対応の 802.1X クライアントがポートに接続されている場合は、この機能を使用しないでください。

## 前提条件

802.1X 対応ポートのリンクタイプをハイブリッドに設定します。詳細については、『レイヤー2 LAN スイッチングコンフィギュレーションガイド』の「VLAN 設定」を参照してください。

## 手順

1. システムビューを開始します。

**System-view**

2. インターフェイスビューを開始します。

**interface** *interface-type* *interface-number*

3. ポートから 802.1X クライアントに送信されるすべての 802.1X プロトコルパケットの VLAN タグを削除します。

**dot1x eapol untag**

デフォルトでは、ポートから 802.1X クライアントに送信されるすべての 802.1X プロトコルパケットの VLAN タグをデバイスが削除するかどうかは、VLAN モジュールの設定によって決まります。

# MAC 認証ユーザーに対する 802.1X 認証の最大試行回数の設定

## MAC 認証済みユーザーの認証試行について

ポートが 802.1X 認証と MAC 認証の両方を使用する場合、デバイスは MAC 認証されたユーザーからの 802.1X 認証要求を受け入れます。MAC 認証されたユーザーが 802.1X 認証にパスした場合、そのユーザーは 802.1X ユーザーとしてオンラインになります。802.1X 認証に失敗した場合、ユーザーはクライアント設定に応じて 802.1X 認証の試行を続行します。

MAC 認証ユーザーによる 802.1X 認証の試行回数を制限するには、次の作業を実行します。

## 手順

1. システムビューを開始します。

**System-view**

2. インターフェイスビューを開始します。

**interface** *interface-type* *interface-number*

3. ポート上の MAC 認証ユーザーに対する 802.1X 認証の最大試行回数を設定します。

**dot1x after-mac-auth max-attempt** *max-attempts*

デフォルトでは、MAC 認証ユーザーの 802.1X 認証試行回数は、ポート上で制限されません。

# 802.1X ユーザー IP フリーズのイネーブル化

## 802.1X ユーザー IP の凍結について

この機能は、IP ソースガード機能と連動します。802.1X ベースの IP ソースガードでは、802.1X クライアントがアクセスデバイスへのユーザー IP アドレスの送信をサポートしている必要があります。デバイスは、ユーザー MAC アドレスや 802.1X 経由で取得された IP アドレスなどの情報を使用して IPSG バインディングを生成し、認証されていない 802.1X ユーザーからの IPv4 パケットをフィルタリングします。IP ソースガードの詳細については、「IP ソースガードの設定」を参照してください。

この機能により、ポート上の認証済み 802.1X ユーザーは IP アドレスを変更できなくなります。この機能をイネーブルにすると、ポートは 802.1X ユーザーのダイナミック IPSG バインディング内の IP アドレスを更新

しません。802.1X ユーザーが IPSPG バインディングエントリ内の IP アドレスとは異なる IP アドレスを使用する場合、ポートはユーザーアクセスを拒否します。

## 手順

1. システムビューを開始します。  
**System-view**
2. インターフェイスビューを開始します。  
**interface interface-type interface-number**
3. 802.1X ユーザーIP フリーズをイネーブルにします。  
**dot1x user-ip freeze**  
デフォルトでは、802.1X ユーザーIP の凍結はディセーブルです。

# 802.1X MAC アドレスバインディングの設定

## 802.1X MAC アドレスバインディングについて

この機能では、認証された 802.1X ユーザーの MAC アドレスをユーザーのアクセスポートに自動的にバインドし、802.1X MAC アドレスバインディングエントリを生成できます。また、**dot1x mac-binding mac-address** コマンドを使用して、802.1X MAC アドレスバインディングエントリを手動で追加することもできます。

802.1X MAC アドレスバインディングエントリが期限切れになることはありません。これらのエントリは、ユーザーのログオフまたはデバイスのリブート後も存続できます。802.1X MAC アドレスバインディングエントリのユーザーが別のポートで 802.1X 認証を実行する場合、認証を通過できません。

## 制約事項とガイドライン

802.1X MAC アドレスバインディング機能が有効になるのは、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だけです。

802.1X MAC アドレスバインディングエントリを削除するには、**undo dot1x mac-binding mac-address** コマンドを使用する必要があります。エントリ内のユーザーがオンラインの場合、802.1X MAC アドレスバインディングエントリは削除できません。

802.1X MAC アドレスバインディングエントリの数が、同時 802.1X ユーザーの上限(**dot1x max-user** コマンドを使用して設定)に達した後は、次の制限が存在します。

- バインディングエントリ内のユーザーがオフラインになった後でも、バインディングエントリ内にはないユーザーは認証に失敗します。
- 新しい 802.1X MAC アドレスバインディングエントリは許可されません。

## 手順

1. システムビューを開始します。  
**system-view**
2. インターフェイスビューを開始します。  
**interface interface-type interface-number**
3. 802.1X MAC アドレスバインディング機能をイネーブルにします。  
**dot1x mac-binding enable**  
デフォルトでは、この機能はディセーブルです。
4. (任意)802.1X MAC アドレスバインディングエントリを手動で追加します。  
**dot1x mac-binding mac-address**

デフォルトでは、ポート上に 802.1X MAC アドレスバインディングエントリは存在しません。

## EAD Assistant機能の設定

### 制約事項とガイドライン

- EAD Assistant 機能をイネーブルにする前に、MAC 認証および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 VSI またはゲスト VLAN 機能が正しく動作するためには、802.1X ゲスト VSI またはゲスト VLAN 機能とともに EAD アシスタントをイネーブルにしないでください。
- フリーIP 機能と Auth-fail VLAN(認証失敗 VLAN)機能を一緒に使用する場合は、Auth-fail VLAN(認証失敗 VLAN)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。
- リダイレクト URL を提供するサーバーは、非認証ユーザ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. システムビューを開始します。  
**system-view**
2. EAD Assistant 機能をイネーブルにします。  
**dot1x ead-assistant enable**  
デフォルトでは、この機能は無効になっています。
3. 空き IP を設定します。  
**dot1x ead-assistant free-ip ip-address { mask-length | mask-address }**  
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. (任意)ユーザーが 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。  
802.1X ユーザーの HTTPS 要求をリダイレクトするには、デバイス上の HTTPS リダイレクトリスニングポートを指定します。詳細については、『レイヤー3 IP サービスコンフィギュレーションガイド』の「HTTP リダイレクト」を参照してください。
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 ユーザーが存在する場合に ACL リソースの消費を回避するには、EAD ルールタイマーを短くします。

## 802.1Xユーザーのロギングのイネーブル化

### 802.1X ユーザーのロギングについて

この機能を使用すると、デバイスで 802.1X ユーザーのログを生成し、そのログをインフォメーションセンターに送信できます。ログを正しく出力するには、デバイスにインフォメーションセンターを構成する必要もあり



ます。インフォメーションセンターの構成の詳細は、「ネットワーク管理および監視構成ガイド」を参照してください。

## 制約事項とガイドライン

802.1X ユーザーのログが過剰に出力されないように、この機能を無効にすることをお勧めします。

## 手順

1. システムビューを開始します。

**system-view**

2. 802.1X ユーザーのロギングをイネーブルにします。

**dot1x access-user log enable [ abnormal-logoff | failed-login | normal-logoff | successful-login ] \***

デフォルトでは、802.1X ユーザーのすべてのタイプのロギングがディセーブルになっています。

パラメーターを指定しない場合、このコマンドは 802.1X ユーザーのすべてのタイプのロギングをイネーブルにします。

## 802.1X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、ユーザービューでリセットコマンドを実行します。

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。	<b>display dot1x [ session   statistics ] [ interface <i>interface-type interface-number</i> ]</b>
オンライン802.1Xユーザー情報を表示します。	<b>display dot1x connection [ open ] [ interface <i>interface-type interface-number</i>   slot <i>slot-number</i>   user-mac <i>mac-address</i>   user-name <i>name-string</i> ]</b>
特定タイプの802.1X VLANまたはVSI内の802.1XユーザーのMACアドレス情報を表示します。	<b>display dot1x mac-address { auth-fail-vlan   auth-fail-vsi   critical-vlan   critical-vsi   guest-vlan   guest-vsi } [ interface <i>interface-type interface-number</i> ]</b>
ポート上の802.1XゲストVLANからユーザーを削除します。	<b>reset dot1x guest-vlan interface <i>interface-type interface-number</i> [ mac-address <i>mac-address</i> ]</b>
ポート上の802.1XゲストVSIからユーザーを削除します。	<b>reset dot1x guest-vsi interface <i>interface-type interface-number</i> [ mac-address <i>mac-address</i> ]</b>
802.1X統計情報をクリアします。	<b>reset dot1x statistics [ interface <i>interface-type interface-number</i> ]</b>

# 802.1X認証の設定例

## 例:基本 802.1X 認証の設定

### ネットワーク構成

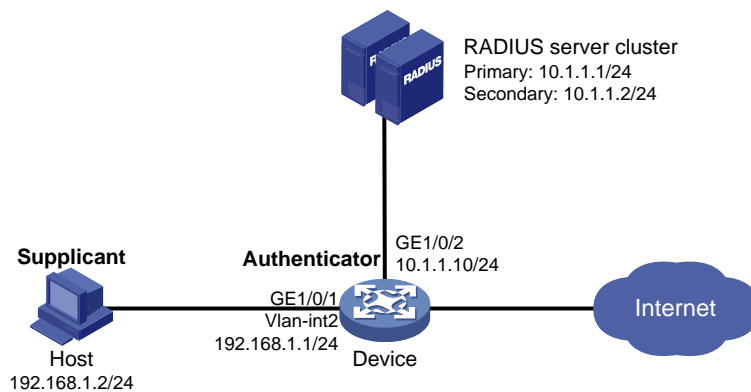
図 30 に示すように、アクセスデバイスは、GigabitEthernet 1/0/1 に接続するユーザーに対して 802.1X 認証を実行します。1 人のユーザーのログオフが他のオンライン 802.1X ユーザーに影響を与えないように、ポートに MAC ベースのアクセスコントロールを実装します。

RADIUS サーバーを使用して、802.1X ユーザーの認証、認可、およびアカウントングを実行します。RADIUS 認証が失敗した場合は、アクセスデバイスでローカル認証を実行します。

10.1.1.1/24 の RADIUS サーバーをプライマリ認証およびアカウントングサーバーとして設定し、10.1.1.2/24 の RADIUS サーバーをセカンダリ認証およびアカウントングサーバーとして設定します。すべてのユーザーを ISP ドメイン **bbb** に割り当てます。

アクセスデバイスと認証サーバーの間のパケットの共有キーを **name** に設定します。アクセスデバイスとアカウントングサーバーの間のパケットの共有キーを **money** に設定します。

図 30 ネットワークダイアグラム



### 手順

1. 802.1X クライアントを構成します。iNode クライアントを使用する場合は、クライアント構成で **carry version info** オプションを選択しないでください(詳細は省略)。
2. RADIUS サーバーを設定し、802.1X ユーザーのユーザーカウントを追加します(詳細は省略)。この例のアクセスデバイスで使用される RADIUS コマンドの詳細については、『Security Command Reference』を参照してください。
3. アクセスデバイスの各インターフェースに IP アドレスを割り当てます(詳細は省略)。
4. アクセスデバイスで 802.1X ユーザーのユーザーカウントを設定します。

#プレーンテキストのユーザー名 **localuser** とパスワード **localpass** を持つローカルネットワークアクセスユーザーを追加します。(ユーザー名とパスワードは、RADIUS サーバーで設定されているものと同じであることを確認してください。)

```
<Device> system-view
[Device] local-user localuser class network
[Device-luser-network-localuser] password simple localpass
#サービスタイプを lan-access に設定します。
[Device-luser-network-localuser] service-type lan-access
[Device-luser-network-localuser] quit
```

5. 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 スキームビューを開始します。
[Device] radius scheme radius1
#プライマリ認証およびアカウントリング RADIUS サーバーの IP アドレスを指定します。
[Device-radius-radius1] primary authentication 10.1.1.1
[Device-radius-radius1] primary accounting 10.1.1.1
#セカンダリ認証およびアカウントリング RADIUS サーバーの IP アドレスを設定します。
[Device-radius-radius1] secondary authentication 10.1.1.2
[Device-radius-radius1] secondary accounting 10.1.1.2
#アクセスデバイスと認証サーバー間の共有キーを指定します。
[Device-radius-radius1] key authentication simple name
#アクセスデバイスとアカウントリングサーバー間の共有キーを指定します。
[Device-radius-radius1] key accounting simple money
#RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。
[Device-radius-radius1] user-name-format without-domain
[Device-radius-radius1] quit
```

---

**注:**

アクセスデバイスは、RADIUS サーバーと同じユーザー名形式を使用する必要があります。RADIUS サーバーのユーザー名に ISP ドメイン名が含まれている場合は、アクセスデバイスも同じ形式を使用する必要があります。

---

6. 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。
[Device] domain bbb
#RADIUS スキーム radius1 を ISP ドメインに適用し、セカンダリ認証方式としてローカル認証を指定
します。
[Device-isp-bbb] authentication lan-access radius-scheme radius1 local
[Device-isp-bbb] authorization lan-access radius-scheme radius1 local
[Device-isp-bbb] accounting lan-access radius-scheme radius1 local
[Device-isp-bbb] quit
```

7. 802.1X の設定:

```
# GigabitEthernet 1/0/1 で 802.1X を有効にします。
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet 1/0/1] dot1x
#ポートで MAC ベースのアクセス制御を有効にします。デフォルトでは、ポートは MAC ベースのアク
セス制御を使用します。
[Device-GigabitEthernet1/0/1] dot1x port-method macbased
#ISP ドメイン bbb を必須ドメインとして指定します。
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain bbb
[Device-GigabitEthernet1/0/1] quit
#802.1X をグローバルにイネーブルにします。
[Device] dot1x
```

**設定の確認**

```
# GigabitEthernet 1/0/1 で 802.1X の設定を確認します。
[Device] display dot1x interface gigabitethernet 1/0/1
```

#802.1X ユーザーが認証に成功した後、ユーザー接続情報を表示します。

```
[Device] display dot1x connection
```

## 例:802.1X ゲスト VLAN および認証 VLAN の設定

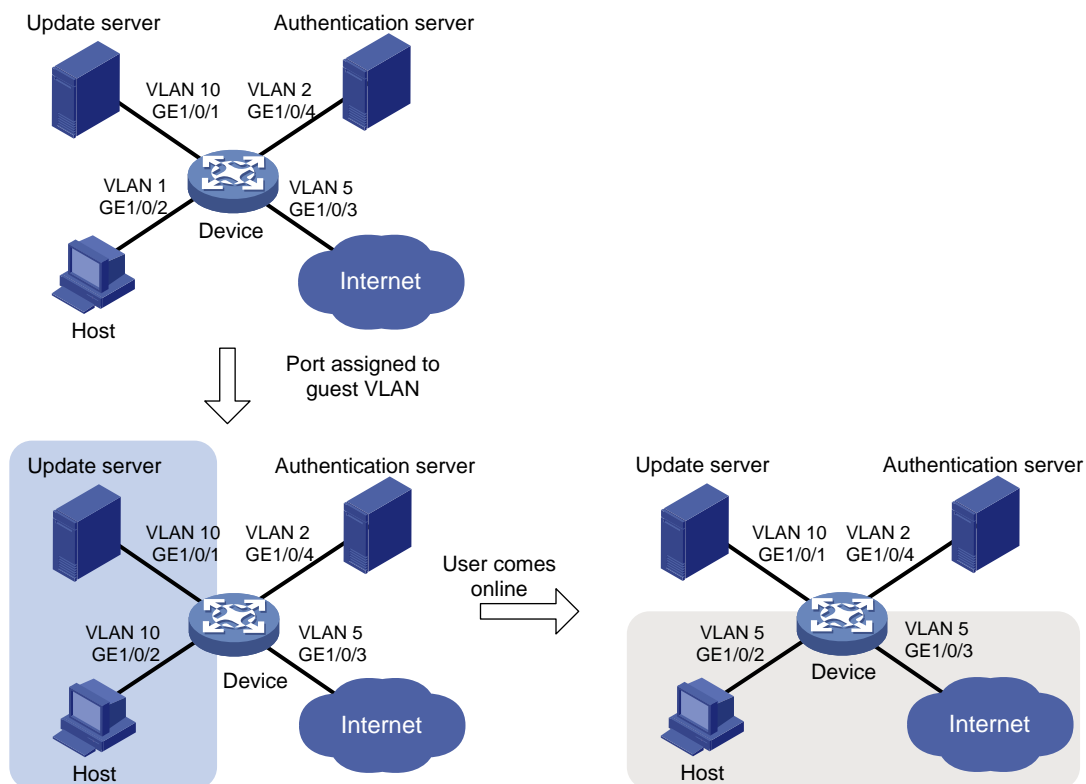
### ネットワーク構成

図 31 に示すように、RADIUS サーバーを使用して、GigabitEthernet 1/0/2 に接続する 802.1X ユーザーの認証、認可、およびアカウントングを実行します。ポートにポートベースのアクセスコントロールを実装します。

GigabitEthernet 1/0/2 で VLAN 10 を 802.1X ゲスト VLAN として設定します。ホストとアップデートサーバーは両方とも VLAN 10 にあり、ホストはアップデートサーバーにアクセスして 802.1X クライアントソフトウェアをダウンロードできます。

ホストが 802.1X 認証に合格すると、アクセスデバイスはホストを GigabitEthernet 1/0/3 の VLAN 5 に割り当てます。ホストはインターネットにアクセスできます。

図 31 ネットワークダイアグラム



### 手順

1. 802.1X クライアントを設定します。アクセスポートがゲスト VLAN または認証 VLAN に割り当てられた後、802.1X クライアントがその IP アドレスを更新できることを確認します(詳細は省略)。
2. 認証、認可、およびアカウントングサービスを提供するように RADIUS サーバーを設定します。ユーザーのユーザーカウントと認証 VLAN(この例では VLAN 5)を設定します(詳細は省略)。
3. VLAN を作成し、アクセスデバイス上の VLAN にポートを割り当てます。

```
<Device> system-view  
[Device] vlan 1  
[Device-vlan1] port gigabitethernet 1/0/2
```

```
[Device-vlan1] quit
[Device] vlan 10
[Device-vlan10] port gigabitethernet 1/0/1
[Device-vlan10] quit
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/4
[Device-vlan2] quit
[Device] vlan 5
[Device-vlan5] port gigabitethernet 1/0/3
[Device-vlan5] quit
```

4. アクセスデバイスで RADIUS スキームを設定します。

#RADIUS スキーム 2000 を作成し、RADIUS スキームビューを開始します。

```
[Device] radius scheme 2000
```

#10.11.1.1 のサーバーをプライマリ認証サーバーとして指定し、認証ポートを 1812 に設定します。

```
[Device-radius-2000] primary authentication 10.11.1.1 1812
```

#10.11.1.1 のサーバーをプライマリアカウンティングサーバーとして指定し、アカウンティングポートを 1813 に設定します。

```
[Device-radius-2000] primary accounting 10.11.1.1 1813
```

#認証サーバーとデバイス間のセキュアな通信のために、プレーンテキストで共有キーを abc に設定します。

```
[Device-radius-2000] key authentication simple abc
```

#アカウンティングサーバーとデバイス間のセキュアな通信のために、共有キーをプレーンテキストの abc に設定します。

```
[Device-radius-2000] key accounting simple abc
```

#RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。

```
[Device-radius-2000] user-name-format without-domain
```

```
[Device-radius-2000] quit
```

5. ISP ドメインを設定します。

#ISP ドメイン bbb を作成し、ISP ドメインビューに入ります。

```
[Device] domain bbb
```

#認証、認可、およびアカウンティングのために、RADIUS スキーム 2000 を ISP ドメインに適用します。

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
```

```
[Device-isp-bbb] authorization lan-access radius-scheme 2000
```

```
[Device-isp-bbb] accounting lan-access radius-scheme 2000
```

```
[Device-isp-bbb] quit
```

6. アクセスデバイスで 802.1X を設定します。

# GigabitEthernet 1/0/2 で 802.1X を有効にします。

```
[Device] interface GigabitEthernet 1/0/2
```

```
[Device-GigabitEthernet 1/0/2] dot1x
```

#ポートにポートベースのアクセス制御を実装します。

```
[Device-GigabitEthernet1/0/2] dot1x port-method portbased
```

#ポート認証モードを **auto** に設定します。デフォルトでは、ポートは auto モードを使用します。

```
[Device-GigabitEthernet1/0/2] dot1x port-control auto
```

# GigabitEthernet 1/0/2 で VLAN 10 を 802.1X ゲスト VLAN として指定します。

```
[Device-GigabitEthernet 1/0/2] dot1x guest-vlan 10
```

```
[Device-GigabitEthernet1/0/2] quit
```

```
#802.1X をグローバルにイネーブルにします。  
[Device] dot1x
```

## 設定の確認

# GigabitEthernet 1/0/2 で 802.1X ゲスト VLAN の設定を確認します。

```
[Device] display dot1x interface gigabitethernet 1/0/2
```

#ユーザーがポートで認証を渡す前に、GigabitEthernet 1/0/2 が VLAN 10 に割り当てられていることを確認します。

```
[Device] display vlan 10
```

#ユーザーが認証に合格すると、GigabitEthernet 1/0/2 の情報が表示されます。GigabitEthernet 1/0/2 が VLAN 5 に割り当てられていることを確認します。

```
[Device] display interface gigabitethernet 1/0/2
```

## 例:ACL 割り当てを使用した 802.1X の設定

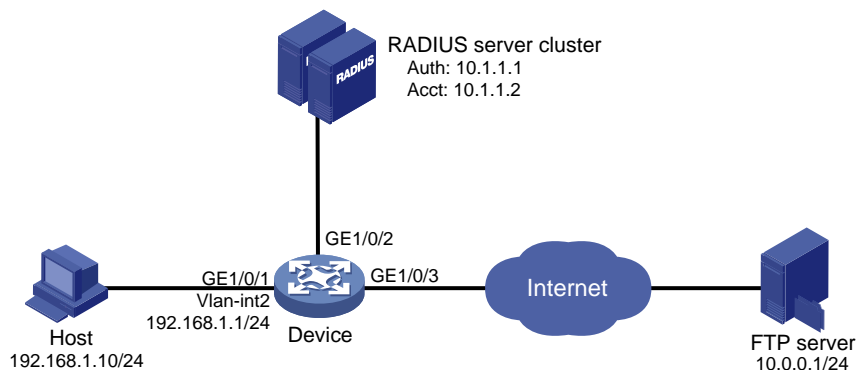
### ネットワーク構成

図 32 に示すように、GigabitEthernet 1/0/1 に接続するホストがインターネットにアクセスするには、802.1X 認証を通過する必要があります。

GigabitEthernet 1/0/1 で 802.1X 認証を実行します。10.1.1.1 の RADIUS サーバーを認証および認可サーバーとして使用し、10.1.1.2 の RADIUS サーバーをアカウントングサーバーとして使用します。

802.1X ユーザーの FTP サーバーへのアクセスを平日の 8:00~18:00 に拒否するには、GigabitEthernet 1/0/1 で ACL 割り当てを設定します。

図 32 ネットワークダイアグラム



### 手順

1. 802.1X クライアントを設定します。アクセスポートが 802.1X ゲスト VLAN または認証 VLAN に割り当てられた後、クライアントが IP アドレスを更新できることを確認します(詳細は省略)。
2. 認証、認可、およびアカウントングサービスを提供するように RADIUS サーバーを設定します。ユーザーカウントを追加し、ユーザーの ACL(この例では ACL 3000)を指定します。詳細は省略)。
3. 図 32 に示すように、各インターフェースに IP アドレスを割り当てます(詳細は省略)。
4. RADIUS スキームを設定します。

```
#RADIUS スキーム 2000 を作成し、RADIUS スキームビューを開始します。
```

```
<Device> system-view
```

```
[Device] radius scheme 2000
```

```
#10.1.1.1 のサーバーをプライマリ認証サーバーとして指定し、認証ポートを 1812 に設定します。
```

```
[Device-radius-2000] primary authentication 10.1.1.1 1812
```

#10.1.1.2 のサーバーをプライマリアカунティングサーバーとして指定し、アカウントングポートを 1813 に設定します。

```
[Device-radius-2000] primary accounting 10.1.1.2 1813
```

#認証サーバーとデバイス間のセキュアな通信のために、プレーンテキストで共有キーを **abc** に設定します。

```
[Device-radius-2000] key authentication simple abc
```

#アカウントングサーバーとデバイス間のセキュアな通信のために、共有キーをプレーンテキストの **abc** に設定します。

```
[Device-radius-2000] key accounting simple abc
```

#RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。

```
[Device-radius-2000] user-name-format without-domain
```

```
[Device-radius-2000] quit
```

5. ISP ドメインを設定します。

#ISP ドメイン bbb を作成し、ISP ドメインビューに入ります。

```
[Device] domain bbb
```

#認証、認可、およびアカウントングのために、RADIUS スキーム 2000 を ISP ドメインに適用します。

```
[Device-isp-bbb] authentication lan-access radius-scheme 2000
```

```
[Device-isp-bbb] authorization lan-access radius-scheme 2000
```

```
[Device-isp-bbb] accounting lan-access radius-scheme 2000
```

```
[Device-isp-bbb] quit
```

6. ftp という名前の時間範囲を平日の 8:00~18:00 に設定します。

```
[Device] time-range ftp 8:00 to 18:00 working-day
```

7. 指定された時間範囲内に 10.0.0.1 の FTP サーバー宛てのパケットを拒否するように ACL 3000 を設定します。

```
[Device] acl advanced 3000
```

```
[Device-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0 time-range ftp
```

```
[Device-acl-ipv4-adv-3000] quit
```

8. 802.1X の設定:

# GigabitEthernet 1/0/1 で 802.1X を有効にします。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] dot1x
```

```
[Device-GigabitEthernet1/0/1] quit
```

#802.1X をグローバルにイネーブルにします。

```
[Device] dot1x
```

## 設定の確認

#ユーザーアカウントを使用して認証を渡します(詳細は省略)。

#ユーザーが平日の 8:00~18:00 の間は FTP サーバーに ping を送信できないことを確認します。

```
C:\>ping 10.0.0.1
```

```
Pinging 10.0.0.1 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Request timed out.
```

```
Ping statistics for 10.0.0.1:
```

Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),  
The output shows that ACL 3000 is active on the user, and the user cannot

この出力は、ユーザーの ACL 3000 がアクティブであり、ユーザーが FTP サーバーにアクセスできないことを示しています。

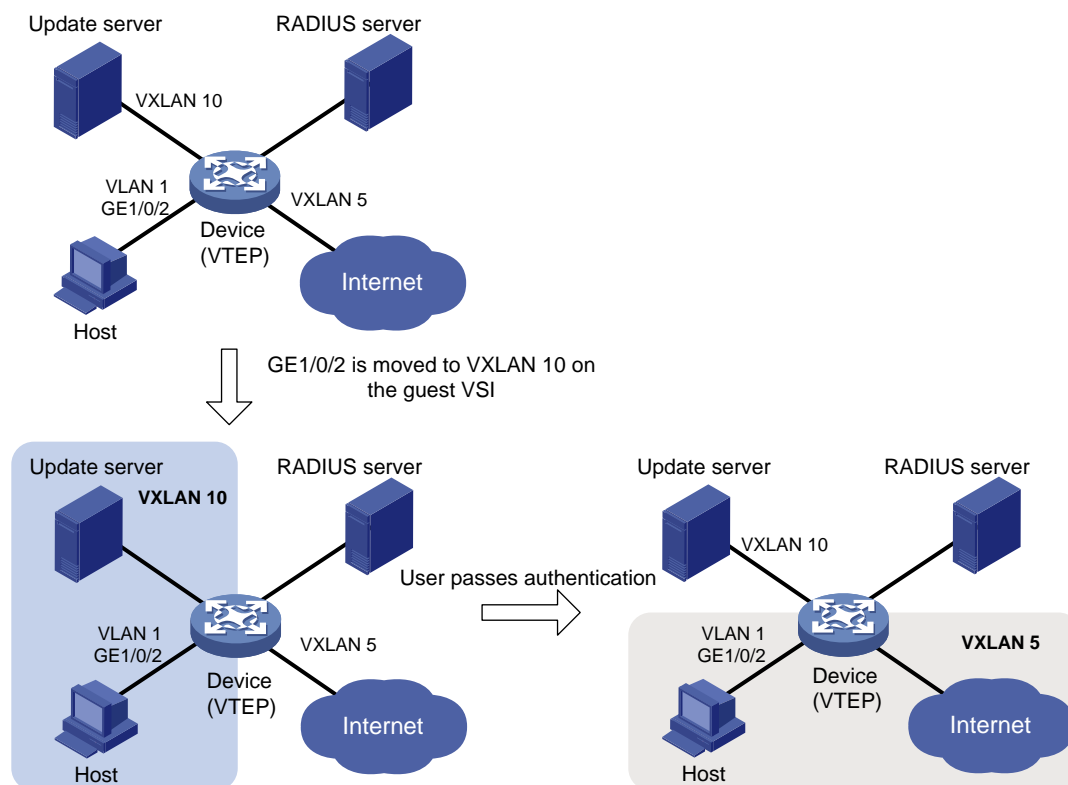
## 例:802.1X ゲスト VSI および認可 VSI の設定

### ネットワーク構成

図 33 に示すように、次のようになります。

- このデバイスは、VXLAN VTEP とネットワークアクセスデバイスの両方として動作します。RADIUS サーバーを使用して、GigabitEthernet 1/0/2 に接続する 802.1X ユーザーの認証、認可、およびアカウントリングを実行します。
- GigabitEthernet 1/0/2 は MAC ベースのアクセスコントロールを使用し、802.1X ゲスト VSI で設定されます。VXLAN 10 はゲスト VSI 上に作成されます。ゲスト VSI のユーザーは、VXLAN 10 のアップデートサーバーにアクセスし、802.1X クライアントソフトウェアをダウンロードできます。
- RADIUS サーバーは、ホストに認可 VSI を割り当てます。VSI は、デバイス上の VXLAN 5 に関連付けられます。認証に合格すると、ホストはインターネットにアクセスできます。

図 33 ネットワークダイアグラム



### 802.1X クライアントの設定

#802.1X クライアントを設定します。アクセスポートがゲスト VSI または認可 VSI に割り当てられた後に、802.1X クライアントが IP アドレスを更新できることを確認します(詳細は省略)。



## RADIUS サーバーの設定

#認証、認可、およびアカウントングサービスを提供するように RADIUS サーバーを設定します。ユーザーのユーザーカウントと認可 VSI(この例では VSI **vpn5**)を設定します(詳細は省略)。

認証および認可に H3C ADCAM サーバーを使用する場合は、サーバーに VSI を設定します。サーバーはこれらの VSI をデバイスに割り当てます。デバイスに VSI を設定する必要はありません。

## デバイスの設定

1. L2VPN をイネーブルにします。  
<Device> system-view  
[Device] l2vpn enable
2. VSI および対応する VXLAN を作成します。  
[Device] vsi vpn10  
[Device-vsi-vpn10] vxlan 10  
[Device-vsi-vpn10-vxlan-10] quit  
[Device-vsi-vpn10] quit  
[Device] vsi vpn5  
[Device-vsi-vpn5] vxlan 5  
[Device-vsi-vpn5-vxlan-5] quit  
[Device-vsi-vpn5] quit
3. RADIUS スキームを設定します。  
#RADIUS スキーム 2000 を作成し、RADIUS スキームビューを開始します。  
[Device] radius scheme 2000  
#10.11.1.1 のサーバーをプライマリ認証サーバーとして指定し、認証ポートを 1812 に設定します。  
[Device-radius-2000] primary authentication 10.11.1.1 1812  
#10.11.1.1 のサーバーをプライマリアccountingサーバーとして指定し、アカウントングポートを 1813 に設定します。  
[Device-radius-2000] primary accounting 10.11.1.1 1813  
#認証サーバーとデバイス間のセキュアな通信のために、プレーンテキストで共有キーを **abc** に設定します。  
[Device-radius-2000] key authentication simple abc  
#アカウントングサーバーとデバイス間のセキュアな通信のために、共有キーをプレーンテキストの **abc** に設定します。  
[Device-radius-2000] key accounting simple abc  
#認証サーバーおよびアカウントングサーバーに送信されるユーザー名から ISP ドメイン名を除外します。  
[Device-radius-2000] user-name-format without-domain  
[Device-radius-2000] quit
4. ISP ドメインを設定します。  
#ISP ドメイン bbb を作成し、ISP ドメインビューに入ります。  
[Device] domain bbb  
#認証、認可、およびアカウントングのために、RADIUS スキーム 2000 を ISP ドメインに適用します。  
[Device-isp-bbb] authentication lan-access radius-scheme 2000  
[Device-isp-bbb] authorization lan-access radius-scheme 2000  
[Device-isp-bbb] accounting lan-access radius-scheme 2000  
[Device-isp-bbb] quit
5. 802.1X の設定:

```

# GigabitEthernet 1/0/2 で 802.1X を有効にします。
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] dot1x
#ポート認証モードを auto に設定します。デフォルトでは、ポートは auto モードを使用します。
[Device-GigabitEthernet1/0/2] dot1x port-control auto
# GigabitEthernet 1/0/2 でダイナミックイーサネットサービスインスタンスの MAC ベーストラフィック
マッピングをイネーブルにします。
[Device-GigabitEthernet1/0/2] mac-based ac
# GigabitEthernet 1/0/2 で 802.1X ユニキャストトリガーをイネーブルにします。
[Device-GigabitEthernet1/0/2] dot1x unicast-trigger
# GigabitEthernet 1/0/2 の 802.1X ゲスト VSI として VSI vpn10 を指定します。
[Device-GigabitEthernet1/0/2] dot1x guest-vsi vpn10
[Device-GigabitEthernet1/0/2] quit
#802.1X をグローバルにイネーブルにします。
[Device] dot1x

```

## 設定の確認

```

# 802.1X 認証がトリガーされた後にクライアントから応答が受信されない場合に、GigabitEthernet 1/0/2
が VSI vpn10 に割り当てられることを確認します。
[Device] display l2vpn forwarding ac verbose
#ユーザーがポートで認証を通過した後、GigabitEthernet 1/0/2 が VSI vpn5 に割り当てられることを確認
します。
[Device] display l2vpn forwarding ac verbose

```

## 例:EAD アシスタントを使用する 802.1X の設定(DHCP リレー エージェントを使用)

### ネットワーク構成

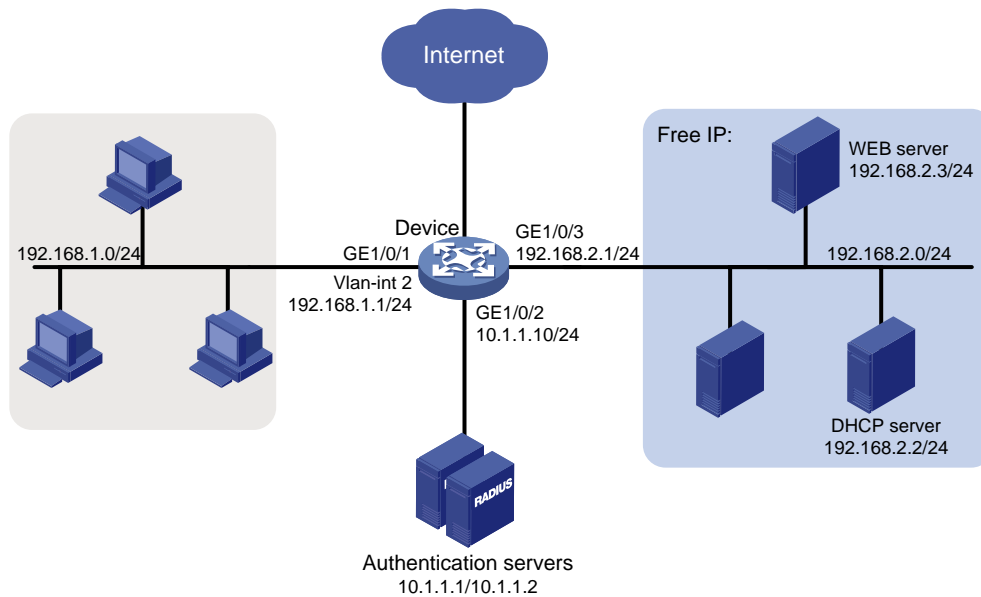
図 34 に示すように、次のようになります。

- イントラネット 192.168.1.0/24 は、アクセスデバイスの GigabitEthernet 1/0/1 に接続されています。
- ホストは DHCP を使用して IP アドレスを取得します。
- DHCP サーバーと Web サーバーは、ユーザーが IP アドレスを取得し、クライアントソフトウェアをダウンロードするために、192.168.2.0/24 サブネットに配置されます。

イントラネット用の EAD ソリューションを導入して、次の要件を満たします。

- 非認証ユーザーおよび 802.1X 認証に失敗したユーザーが 192.168.2.0/24 にアクセスできるようにします。ユーザーは IP アドレスを取得し、ソフトウェアをダウンロードできます。
- これらのユーザーが Web ブラウザーを使用して 192.168.2.0/24 以外のネットワークにアクセスする場合は、802.1X クライアントをダウンロードするために Web サーバーにリダイレクトします。
- 認証された 802.1X ユーザーがネットワークにアクセスできるようにします。

図 34 ネットワークダイアグラム



## 手順

1. DHCP サーバー、Web サーバー、および認証サーバーが正しく設定されていることを確認します(詳細は省略)。
2. 各インターフェースの IP アドレスを設定します(詳細は省略)。
3. DHCP リレーを設定します。  
#DHCP を有効にします。  
<Device> system-view  
[Device] dhcp enable  
#VLAN インターフェース 2 の DHCP リレーエージェントをイネーブルにします。  
[Device] interface vlan-interface 2  
[Device-Vlan-interface2] dhcp select relay  
#リレーエージェントインターフェイス VLAN-interface 2 上の DHCP サーバー192.168.2.2 を指定します。  
[Device-Vlan-interface2] dhcp relay server-address 192.168.2.2  
[Device-Vlan-interface2] quit
4. RADIUS スキームを設定します。  
#RADIUS スキーム 2000 を作成し、RADIUS スキームビューを開始します。  
[Device] radius scheme 2000  
#10.1.1.1 のサーバーをプライマリ認証サーバーとして指定し、認証ポートを 1812 に設定します。  
[Device-radius-2000] primary authentication 10.1.1.1 1812  
#10.1.1.2 のサーバーをプライマリアカウンティングサーバーとして指定し、アカウンティングポートを 1813 に設定します。  
[Device-radius-2000] primary accounting 10.1.1.2 1813  
#認証サーバーとデバイス間のセキュアな通信のために、プレーンテキストで共有キーを **abc** に設定します。  
[Device-radius-2000] key authentication simple abc  
#アカウンティングサーバーとデバイス間のセキュアな通信のために、共有キーをプレーンテキストの **abc** に設定します。

```
[Device-radius-2000] key accounting simple abc
#RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

5. ISP ドメインを設定します。

```
#ISP ドメイン bbb を作成し、ISP ドメインビューに入ります。
[Device] domain bbb
#認証、認可、およびアカウントングのために、RADIUS スキーム 2000 を ISP ドメインに適用します。
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```

6. 802.1X の設定:

```
#空き IP を設定します。
[Device] dot1x ead-assistant free-ip 192.168.2.0 24
#クライアントソフトウェアダウンロード用のリダイレクト URL を設定します。
[Device] dot1x ead-assistant url http://192.168.2.3
#EAD アシスタント機能を有効にします。
[Device] dot1x ead-assistant enable
# GigabitEthernet 1/0/1 で 802.1X を有効にします。
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
[Device-GigabitEthernet1/0/1] quit
#802.1X をグローバルにイネーブルにします。
[Device] dot1x
```

## 設定の確認

#802.1X の設定を確認します。

```
[Device] display dot1x
```

#ホストから空き IP サブネット上の IP アドレスに対して ping を実行できることを確認します。

```
C:\>ping 192.168.2.3
```

```
Pinging 192.168.2.3 with 32 bytes of data:
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 192.168.2.3:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

この出力は、802.1X 認証を通過する前に、空き IP サブネットにアクセスできることを示しています。

#フリー IP がない IP アドレスを Web ブラウザーに入力したときに、Web サーバーにリダイレクトされることを確認します(詳細は省略)。

## 例:EAD アシスタントを使用した 802.1X の設定(DHCP サーバーを使用)

### ネットワーク構成

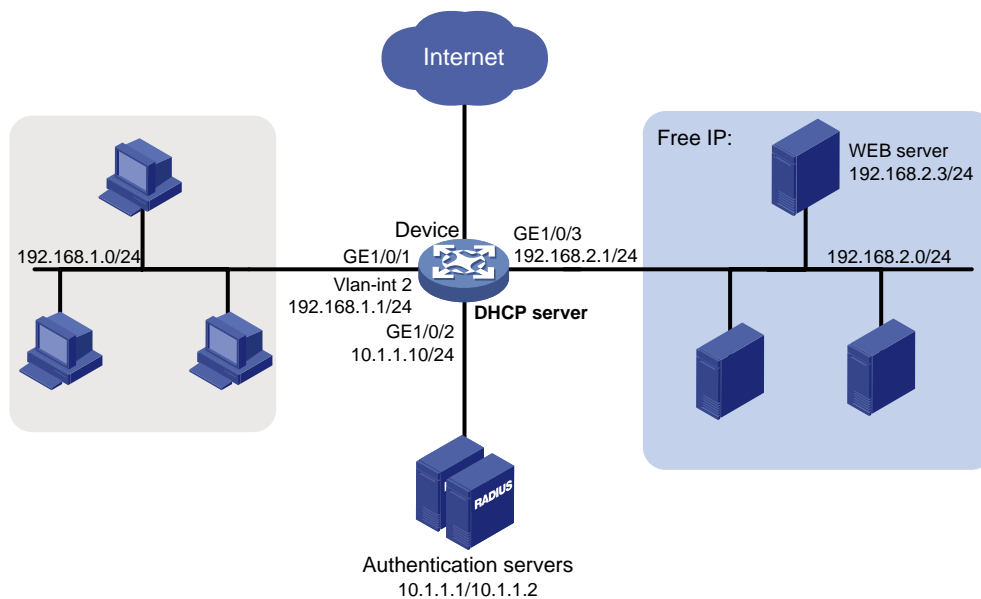
図 35 に示すように、次のようになります。

- イントラネット 192.168.1.0/24 は、アクセスデバイスの GigabitEthernet 1/0/1 に接続されています。
- ホストは DHCP を使用して IP アドレスを取得します。
- Web サーバーは、ユーザーがクライアントソフトウェアをダウンロードするために、192.168.2.0/24 サブネットに配置されます。

イントラネット用の EAD ソリューションを導入して、次の要件を満たします。

- 非認証ユーザーおよび 802.1X 認証に失敗したユーザーが 192.168.2.0/24 にアクセスできるようにします。ユーザーはソフトウェアをダウンロードできます。
- これらのユーザーが Web ブラウザーを使用して 192.168.2.0/24 以外のネットワークにアクセスする場合は、802.1X クライアントをダウンロードするために Web サーバーにリダイレクトします。
- 認証された 802.1X ユーザーがネットワークにアクセスできるようにします。

図 35 ネットワークダイアグラム



### 手順

1. Web サーバーと認証サーバーが正しく構成されていることを確認してください(詳細は省略)。
2. 各インターフェースの IP アドレスを設定します(詳細は省略)。
3. DHCP サーバーを設定します。

#DHCP を有効にします。

```
<Device> system-view  
[Device] dhcp enable
```

#VLAN-interface 2 で DHCP サーバーをイネーブルにします。

```
[Device] interface vlan-interface 2  
[Device-Vlan-interface2] dhcp select server  
[Device-Vlan-interface2] quit
```

#DHCP アドレスプール 0 を作成します。

- ```
[Device] dhcp server ip-pool 0
#DHCP アドレスプール 0 のサブネット 192.168.1.0/24 を指定します。
[Device-dhcp-pool-0] network 192.168.1.0 mask 255.255.255.0
#DHCP アドレスプール 0 のゲートウェイアドレス 192.168.1.1 を指定します。
[Device-dhcp-pool-0] gateway-list 192.168.1.1
[Device-dhcp-pool-0] quit
```
4. RADIUS スキームを設定します。
- ```
#RADIUS スキーム 2000 を作成し、RADIUS スキームビューを開始します。
[Device] radius scheme 2000
#10.1.1.1 のサーバーをプライマリ認証サーバーとして指定し、認証ポートを 1812 に設定します。
[Device-radius-2000] primary authentication 10.1.1.1 1812
#10.1.1.2 のサーバーをプライマリアカウンティングサーバーとして指定し、アカウンティングポートを
1813 に設定します。
[Device-radius-2000] primary accounting 10.1.1.2 1813
#認証サーバーとデバイス間のセキュアな通信のために、プレーンテキストで共有キーを abc に設定
します。
[Device-radius-2000] key authentication simple abc
#アカウンティングサーバーとデバイス間のセキュアな通信のために、共有キーをプレーンテキストの
abc に設定します。
[Device-radius-2000] key accounting simple abc
#RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```
5. ISP ドメインを設定します。
- ```
#ISP ドメイン bbb を作成し、ISP ドメインビューに入ります。
[Device] domain bbb
#認証、認可、およびアカウンティングのために、RADIUS スキーム 2000 を ISP ドメインに適用しま
す。
[Device-isp-bbb] authentication lan-access radius-scheme 2000
[Device-isp-bbb] authorization lan-access radius-scheme 2000
[Device-isp-bbb] accounting lan-access radius-scheme 2000
[Device-isp-bbb] quit
```
6. 802.1X の設定:
- ```
#空き IP を設定します。
[Device] dot1x ead-assistant free-ip 192.168.2.0 24
#クライアントソフトウェアダウンロード用のリダイレクト URL を設定します。
[Device] dot1x ead-assistant url http://192.168.2.3
#EAD アシスタント機能を有効にします。
[Device] dot1x ead-assistant enable
# GigabitEthernet 1/0/1 で 802.1X を有効にします。
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x
[Device-GigabitEthernet1/0/1] quit
#802.1X をグローバルにイネーブルにします。
[Device] dot1x
```

## 設定の確認

#802.1X の設定を確認します。

```
[Device] display dot1x
```

#ホストから空き IP サブネット上の IP アドレスに対して ping を実行できることを確認します。

```
C:\>ping 192.168.2.3
```

```
Pinging 192.168.2.3 with 32 bytes of data:
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Reply from 192.168.2.3: bytes=32 time<1ms TTL=128
```

```
Ping statistics for 192.168.2.3:
```

```
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

この出力は、802.1X 認証を通過する前に、空き IP サブネットにアクセスできることを示しています。

#フリー IP がない IP アドレスを Web ブラウザーに入力したときに、Web サーバーにリダイレクトされることを確認します(詳細は省略)。

# 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

非認証ユーザーは、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

次のいずれかの理由により、リダイレクトは行われません。

- アドレスは文字列形式です。ホストのオペレーティングシステムは文字列を Web サイト名と見なし、文字列を解決しようとします。解決に失敗した場合、オペレーティングシステムは 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、この種類の 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。アドレスを持つ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 が空き 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、その URL を持つサーバーが Web サービスを提供していません。

### 解決策

この問題を解決するには、次の手順に従います

1. 空き IP セグメントにないドット付き 10 進数の 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。

# MAC 認証の設定

## MAC認証について

MAC 認証は、ポート上の送信元 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。この機能はクライアントソフトウェアを必要とせず、ユーザーはネットワークアクセスのためにユーザー名とパスワードを入力する必要がありません。デバイスは、MAC 認証対応ポート上で未知の送信元 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、ユーザー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、デバイスは MAC アドレスをサイレント MAC アドレスとしてマークし、パケットをドロップして、待機タイマーを開始します。デバイスは、待機時間内に MAC アドレスからの後続のすべてのパケットをドロップします。待機メカニズムは、短時間の間に認証が繰り返されることを回避します。

## ユーザーカウントポリシー

MAC 認証は、次のユーザーカウントポリシーをサポートしています。

- ユーザーごとに1つのMACベースのユーザーカウント。図1に示すように、アクセスデバイスはパケット内の送信元MACアドレスをMAC認証用のユーザーのユーザー名およびパスワードとして使用します。このポリシーは、セキュリティ保護されていない環境に適しています。
- すべてのユーザーに対して1つの共有ユーザーカウント。図2に示すように、アクセスデバイス上のすべてのMAC認証ユーザーに対して、1つのユーザー名とパスワード(MACアドレスである必要はありません)を指定します。このポリシーは、セキュアな環境に適しています。

図1 MACベースのユーザーカウントポリシー

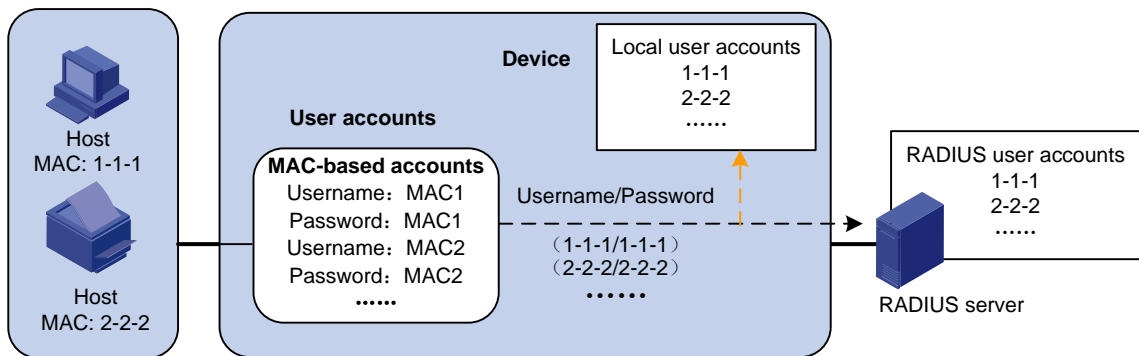
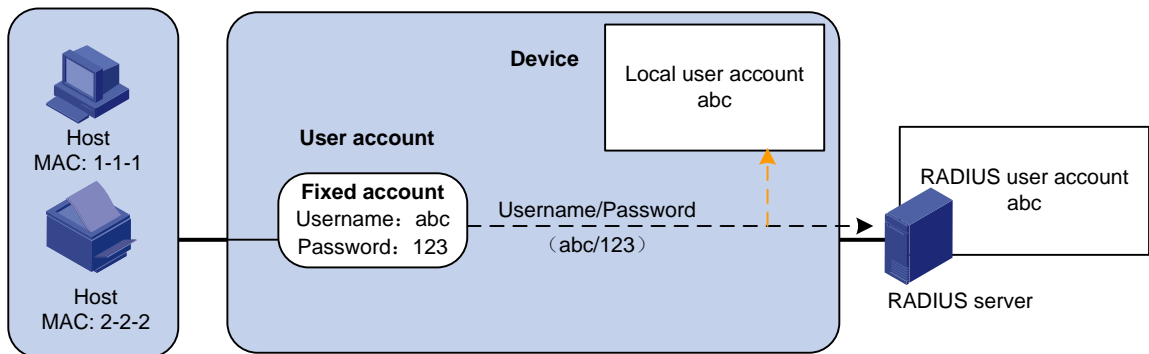


図2 共有ユーザーカウントポリシー





# 認証方式

MAC 認証は、アクセスデバイス上(ローカル認証)または RADIUS サーバーを介して実行できます。

ローカル認証と RADIUS 認証の設定の詳細については、「AAA の設定」を参照してください。

## RADIUS 認証

MAC ベースのアカウントが使用されている場合、アクセスデバイス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認証のために RADIUS サーバーに送信します。

共有アカウントが使用されている場合、アクセスデバイス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が使用されている場合、アクセスデバイス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、ローカルアカウントデータベースで一致するものを検索します。

共有アカウントが使用されている場合、アクセスデバイス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。

# VLAN 割り当て

## 認証 VLAN

認証 VLAN は、許可されたネットワークリソースへの MAC 認証ユーザ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証 VLAN をサポートします。

### ❗ 重要:

リモートサーバーだけが、タグ付き認可 VLAN を割り当てることができます。

## リモート VLAN 認証

リモート VLAN 認可では、リモートサーバー上のユーザーの認可 VLAN を設定する必要があります。ユーザ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、デバイスはユーザーア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証 VLAN 情報の割り当てをサポートします。

- 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 および VLAN 名の文字列。  
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、『Layer 2 LAN Switching Configuration Guide』を参照してください。
- サフィックス t または u を持つ VLAN ID。
- t および u サフィックスを使用すると、デバイスはアクセスポートを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 割り当ての前にその情報を 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、デバイス上に VLAN が作成されていることを確認する必要があります。

サフィックスを使用して VLAN ID を割り当てるには、アクセスポートが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。

❗ **重要:**

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る認可 VLAN は、次のいずれのタイプにもできません。

- ダイナミックに学習された VLAN。
- 予約済み VLAN。
- スーパーVLAN。
- プライベート VLAN。

サーバーが VLAN のグループを割り当てると、アクセスデバイスは VLAN を選択します(表 1 を参照)。

表 1 VLAN グループからの認証 VLAN の選択

VLAN 情報	認証 VLAN の選択
IDによるVLAN 名前によるVLAN VLANグループ名	<p>デバイスは、次の規則に従って、ユーザーのVLANグループから認証VLANを選択します。</p> <ul style="list-style-type: none"><li>• MAC ベース VLAN が有効なハイブリッドポートでは、次のようになります。<ul style="list-style-type: none"><li>○ ポートにオンラインユーザーがいない場合、デバイスは最も小さい ID を持つ VLAN を選択します。</li><li>○ ポートにオンラインユーザーが存在する場合、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 つの VLAN に同数のオンライン 802.1X ユーザーが存在する場合、デバイスは ID が小さい VLAN を選択します。</li></ul></li><li>• アクセス、トランク、または MAC ベース VLAN がディセーブルにされたハイブリッドポートでは、次のようになります。<ul style="list-style-type: none"><li>○ ポートにオンラインユーザーがいない場合、デバイスは最も小さい ID を持つ VLAN を選択します。</li><li>○ ポートにオンラインユーザーが存在する場合、デバイスは VLAN グループでオンラインユーザーの VLAN を調べます。VLAN が検出されると、VLAN は認可 VLAN としてユーザーに割り当てられます。VLAN が検出されない場合、VLAN 認証は失敗します。</li></ul></li></ul>
サフィックスを持つVLAN ID	<ol style="list-style-type: none"><li>1. デバイスは、サフィックスが付いていない左端の VLAN ID、または u が付いた左端の VLAN ID のうち、最も左にあるものをタグなし VLAN として選択します。</li><li>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。</li></ol> <p>たとえば、認証サーバーは文字列 1u 2t 3 をユーザ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 が PVID になります。</p>

## ローカル VLAN 認証

ユーザーに対してローカル VLAN 認証を実行するには、そのユーザーのローカルユーザーカウントの認証アトリビュートリストで VLAN ID を指定します。ローカルユーザーごとに指定できる認証 VLAN ID は 1 つだけです。ユーザーがデバイスにアクセスするポートは、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 認証では、タグ付き VLAN の割り当てはサポートされません。

ローカルユーザー設定の詳細については、「AAA の設定」を参照してください。

## MAC 認証が有効なポートの認証 VLAN 操作

表 2 に、ネットワークアクセスデバイスが MAC 認証ユーザーの認可 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 2 VLAN 操作

ポートの種類	VLAN 操作
<ul style="list-style-type: none"><li>アクセスポート</li><li>トランクポート</li><li>MAC ベース VLAN が無効なハイブリッドポート</li></ul>	<ul style="list-style-type: none"><li>デバイスは最初に認証されたユーザーの認可 VLAN にポートを割り当て、その認証 VLAN にタグなし属性がある場合は、VLAN を PVID として設定します。</li><li>認証 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証 VLAN に割り当てます。</li></ul>
MAC ベース VLAN が有効なハイブリッドポート	デバイスは、ポートがタグ付きメンバーであるかどうかに関係なく、各ユーザーの MAC アドレスを独自の認可 VLAN にマッピングします。ポートの PVID は変更されません。

### ❗ 重要:

- アクセスポートに接続されているユーザーの場合、サーバーによって割り当てられた認証 VLAN にタグなしアトリビュートがあることを確認します。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。
- トランクまたは MAC ベース VLAN がディセーブルのハイブリッドポートに接続されたユーザーに VLAN を割り当てる場合は、タグなし VLAN が 1 つだけ存在することを確認してください。別のタグなし VLAN が後続のユーザーに割り当てられた場合、そのユーザ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認証 VLAN にタグ付きメンバーとして割り当てないでください。

認証 VLAN がユーザーに割り当てられていない場合に、MAC 認証ユーザ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実行します。

- ポートが VLAN 内のユーザ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 内のユーザ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 MAC 認証ゲスト VLAN は、サーバー到達不能以外の理由で MAC 認証に失敗したユーザーに対応します。たとえば、VLAN は、無効なパスワードが入力されたユーザーに対応します。

MAC 認証ゲスト VLAN には、限られたネットワークリソースセットを展開できます。たとえば、ソフトウェアおよびシステムパッチをダウンロードするためのソフトウェアサーバーなどです。

ハイブリッドポートは、常にタグなしメンバーとして MAC 認証ゲスト VLAN に割り当てられます。割り当て後は、ポートを VLAN のタグ付きメンバーとして再設定しないでください。

デバイスは、特定の間隔で MAC 認証ゲスト VLAN 内のユーザーを再認証します。表 3 に、ネットワークアクセスデバイスが MAC 認証ユーザーのゲスト VLAN を処理する方法を示します。

表 3 VLAN 操作

認証ステータス	VLAN 操作
MAC認証ゲストVLAN内のユーザーが、サーバー到達不能以外の理由でMAC認証に失敗した場合。	ユーザーはまだMAC認証ゲストVLAN内にいます。
MAC認証ゲストVLANのユーザーは、MAC認証を通過します。	デバイスは、ユーザーのMACアドレスを、認証サーバーによって割り当てられた認可VLANに再マッピングします。 認証サーバー上のユーザーに認可VLANが設定されていない場合、デバイスはユーザーのMACアドレスをポートのPVIDに再マッピングします。

### クリティカル VLAN

ポート上の MAC 認証クリティカル VLAN は、RADIUS 認証サーバーに到達できないために MAC 認証に失敗したユーザーに対応します。MAC 認証クリティカル VLAN 内のユーザーは、クリティカル VLAN 内のネットワークリソースだけにアクセスできます。

クリティカル VLAN 機能は、MAC 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。MAC 認証ユーザーが RADIUS 認証後にローカル認証に失敗すると、そのユーザーはクリティカル 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。

表 4 に、ネットワークアクセスデバイスが MAC 認証ユーザーの重要な VLAN を処理する方法を示します。

表 4 VLAN 操作

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、ユーザーはMAC認証に失敗します。	デバイスは、ユーザーのMACアドレスをMAC認証クリティカルVLANにマッピングします。 すべてのRADIUSサーバーが到達不能であるためにユーザーがMAC再認証に失敗した場合でも、ユーザーはMAC認証クリティカルVLANに残ります。 MAC認証に不可欠なVLANが設定されていない場合、デバイスはユーザーのMACアドレスをポートのPVIDにマッピングします。
MAC認証に不可欠なVLAN内のユーザーが、サーバーに到達できない以外の理由でMAC認証に失敗した場合。	ゲストVLANが設定されている場合、デバイスはユーザーのMACアドレスをゲストVLANにマッピングします。 ゲストVLANが設定されていない場合、デバイスはユーザーのMACアドレスをポートのPVIDにマッピングします。
MAC認証クリティカルVLAN内のユーザーは、MAC認証を通過します。	デバイスは、ユーザーのMACアドレスを、認証サーバーによって割り当てられた認可VLANに再マッピングします。 認証サーバー上のユーザーに認可VLANが設定されていない場合、デバイスはユーザーのMACアドレスをアクセスポートのPVIDに再マッピングします。

### クリティカルな音声 VLAN

ポート上の MAC 認証クリティカル音声 VLAN は、ISPドメイン内のどの RADIUS サーバーも到達不能であるために認証に失敗した MAC 認証音声ユーザーに対応します。

クリティカル音声 VLAN 機能は、MAC 認証が RADIUS サーバーを介してだけ実行される場合に有効になります。MAC 認証音声ユーザーが RADIUS 認証後にローカル認証に失敗すると、そのユーザーはクリティカル音声 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。

表 5 に、ネットワークアクセスデバイスが MAC 認証音声ユーザーの重要な音声 VLAN を処理する方法を示します。

表 5 VLAN 操作

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、音声ユーザーは MAC 認証に失敗します。	<p>デバイスは、音声ユーザーの MAC アドレスを MAC 認証クリティカル音声 VLAN にマッピングします。</p> <p>すべての RADIUS サーバーが到達不能であるために音声ユーザーが MAC 再認証に失敗した場合でも、音声ユーザーは MAC 認証に不可欠な音声 VLAN に残ります。</p> <p>MAC 認証に不可欠な音声 VLAN が設定されていない場合、デバイスは音声ユーザーの MAC アドレスをポートの PVID にマッピングします。</p>
MAC 認証に不可欠な音声 VLAN 内の音声ユーザーが、サーバーに到達できない以外の理由で MAC 認証に失敗した場合。	<p>ゲスト VLAN が設定されている場合、デバイスは音声ユーザーの MAC アドレスをゲスト VLAN にマッピングします。</p> <p>ゲスト VLAN が設定されていない場合、デバイスは音声ユーザーの MAC アドレスをポートの PVID にマッピングします。</p>
MAC 認証クリティカル音声 VLAN 内の音声ユーザーは、MAC 認証を通過します。	<p>デバイスは、音声ユーザーの MAC アドレスを、認証サーバーによって割り当てられた認可 VLAN に再マッピングします。</p> <p>認証サーバー上で音声ユーザーに認可 VLAN が設定されていない場合、デバイスは音声ユーザーの MAC アドレスをアクセスポートの PVID に再マッピングします。</p>

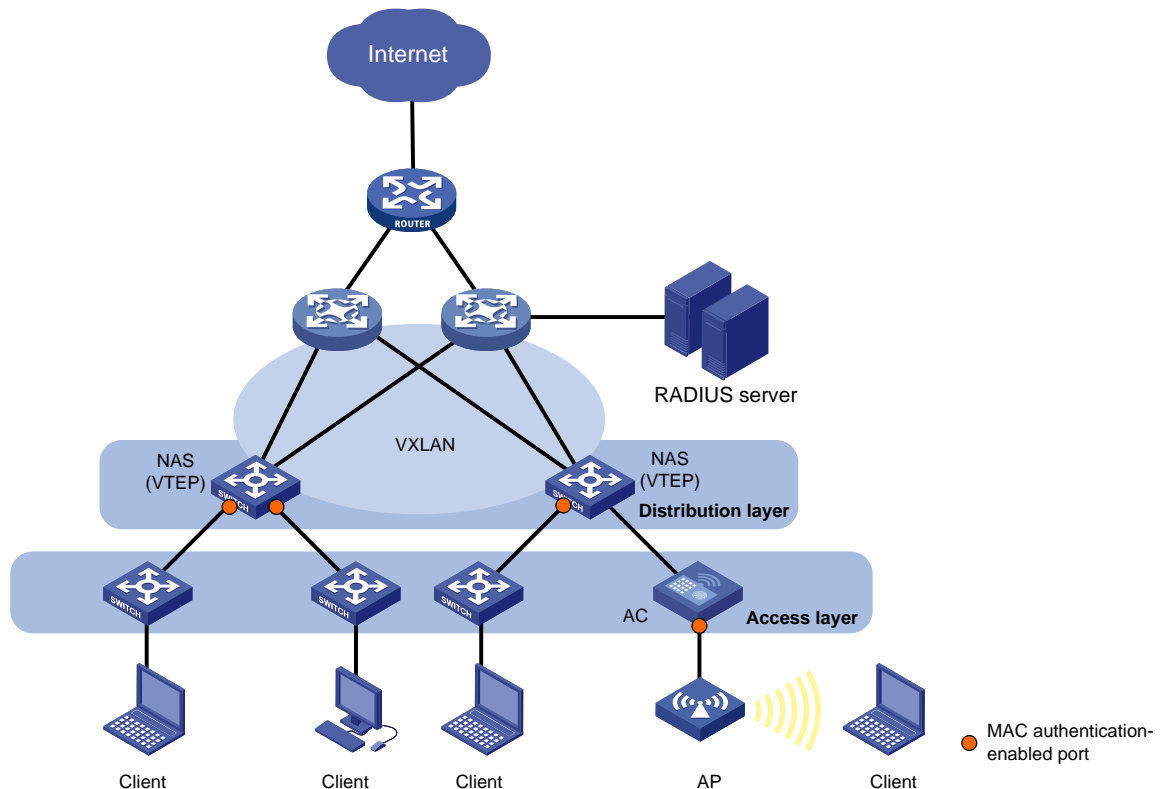
## VSI 操作

### VXLAN の MAC 認証サポート

図 3 示すように、デバイスが VXLAN VTEP と NAS の両方として動作する場合、ユーザーのサービス情報は VLAN によって識別できません。この問題を解決するには、MAC 認証ユーザーに VSI を割り当てるように RADIUS サーバーを設定する必要があります。NAS は、ユーザーのトラフィックを、ユーザーの認可 VSI に関連付けられた VXLAN にマッピングします。マッピング基準には、ユーザーのアクセス VLAN、アクセスポート、および MAC アドレスが含まれます。

VSA および VXLAN の詳細については、『VXLAN Configuration Guide』を参照してください。

図 3 MAC 認証用の VXLAN ネットワーク図



## 認証 VSI

認証 VSI は、非認証ユーザーがアクセスできないネットワークリソースを持つ VXLAN に関連付けられます。

MAC 認証はリモート VSI 認可をサポートします。VTEP が MAC 認証ユーザーの認可 VSI 情報をリモートサーバーから受信しない場合、ユーザーは認証を通過した後に VXLAN 内のリソースにアクセスできません。VTEP がユーザーの認可 VSI 情報をリモートサーバーから受信する場合、VTEP は次の操作を実行します。

- ユーザーのアクセスポート、VLAN、および MAC アドレスに従って、イーサネットサービスインスタンスを動的に作成します。
- イーサネットサービスインスタンスを認可 VSI にマッピングします。

これにより、ユーザーは認可 VSI に関連付けられた VXLAN 内のリソースにアクセスできます。

イーサネットサービスインスタンスの動的作成については、『VXLAN Configuration Guide』を参照してください。

## ゲスト VSI

ポート上の MAC 認証ゲスト VSI は、サーバーに到達できない以外の理由で MAC 認証に失敗したユーザーに対応します。たとえば、VSI は無効なパスワードが入力されたユーザーに対応します。

MAC 認証ゲスト VSI に関連付けられている VXLAN には、ネットワークリソースの限られたセットを展開できます。たとえば、ソフトウェアおよびシステムパッチをダウンロードするためのソフトウェアサーバーなどです。

表 6 に、VTEP が MAC 認証ユーザーのゲスト VSA を処理する方法を示します。

表 6 VSI 操作

認証ステータス	VSI 操作
ユーザーが、サーバー到達不能以外の理由でMAC認証に失敗した場合。	VTEPは、ユーザーのMACアドレスとアクセスVLANをMAC認証ゲストVSIにマッピングします。
MAC認証ゲストVSI内のユーザーが、サーバー到達不能以外の理由でMAC認証に失敗した。	ユーザーはまだMAC認証ゲストVSIにいます。
MAC認証ゲストVSI内のユーザーがMAC認証を通過します。	VTEPは、ユーザーのMACアドレスとアクセスVLANを、認証サーバーによって割り当てられた認可VSIに再マッピングします。

## クリティカル VSI

ポート上の MAC 認証クリティカル VSI は、RADIUS 認証サーバーに到達できないために MAC 認証に失敗したユーザーを受け入れます。MAC 認証クリティカル VSI 内のユーザーは、この VSI に関連付けられた VXLAN 内のネットワークリソースだけにアクセスできます。

重要な VSI 機能は、MAC 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。MAC 認証ユーザーが RADIUS 認証後にローカル認証に失敗すると、そのユーザーは重要な VSI 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。

表 7 に、VTEP が MAC 認証ユーザーの重要な VSA を処理する方法を示します。

表 7 VSI 操作

認証ステータス	VSI 操作
すべてのRADIUSサーバーが到達不能であるため、ユーザーはMAC認証に失敗します。	VTEPは、ユーザーのMACアドレスとアクセスVLANをMAC認証に重要なVSIにマッピングします。 すべてのRADIUSサーバーが到達不能であるためにユーザーがMAC再認証に失敗した場合、ユーザーは引き続きMAC認証クリティカルVSIになります。 MAC認証に不可欠なVSIが設定されていない場合、デバイスはユーザーをログオフします。
MAC認証に重要なVSIのユーザーが、サーバーに到達できないこと以外の理由でMAC認証に失敗した。	ゲストVSIが設定されている場合、VTEPはユーザーのMACアドレスとアクセスVLANをゲストVSIにマッピングします。 ゲストVSIが設定されていない場合、VTEPはユーザーをログオフします。
MAC認証クリティカルVSIのユーザーは、MAC認証を通過します。	VTEPは、ユーザーのMACアドレスとアクセスVLANを、認証サーバーによって割り当てられた認可VSIに再マッピングします。

## ACL 割り当て

認証サーバー上の MAC 認証ユーザーのユーザーカウントに認可 ACL を指定して、ユーザーのネットワークリソースへのアクセスを制御できます。ユーザーが MAC 認証を通過すると、認証サーバー(ローカルまたはリモート)は認可 ACL をユーザーのアクセスポートに割り当てます。ACL はこのユーザーのトラフィックをフィルタリングします。ACL の拒否ルールに一致するトラフィックだけが拒否されます。ACL 割り当て機能を使用するには、アクセスデバイス上で認可 ACL の ACL ルールを設定する必要があります。

ユーザ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認可 ACL を指定します。

サポートされている認可 ACL には、次のタイプがあります。

- 2000～2999 の範囲で番号付けされた基本 ACL。
- 3000～3999 の範囲で番号付けされた拡張 ACL。

認証 ACL を有効にするには、ACL が存在し、counting、established、fragment、または logging キーワードで設定されたルールを除く ACL ルールがあることを確認します。

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

認証サーバー上の MAC 認証ユーザーのユーザーアカウントにユーザープロファイルを指定して、ユーザーのネットワークリソースへのアクセスを制御できます。ユーザーが MAC 認証を通過すると、認証サーバーはユーザープロファイルをユーザーに割り当てて、このユーザーのトラフィックをフィルタリングします。認証サーバーは、ローカルアクセスデバイスまたは RADIUS サーバーです。いずれの場合も、アクセスデバイス上でユーザープロファイルを構成する必要があります。

ユーザーのアクセス認証を変更するには、次のいずれかの方法を使用します。

- アクセスデバイスのユーザープロファイル設定を変更します。
- 認証サーバー上のユーザー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については、「ユーザープロファイルの設定」を参照してください。

## リダイレクト URL の割り当て

デバイスは、RADIUS サーバーによって割り当てられた URL 属性をサポートします。MAC 認証中に、ユーザーの HTTP または HTTPS 要求は、サーバーによって割り当てられた URL 属性によって指定された Web インターフェースにリダイレクトされます。ユーザーが Web 認証に合格すると、RADIUS サーバーはユーザーの MAC アドレスを記録し、DM(接続解除メッセージ)を使用してユーザーをログオフします。ユーザーが MAC 認証を再度開始すると、認証に合格し、正常にオンラインになります。

MAC 認証ユーザーの HTTPS 要求をリダイレクトするには、デバイスの HTTPS リダイレクトリスニングポートを指定します。詳細については、『Layer 3 IP Services Configuration Guide』の「HTTP redirect」を参照してください。

## CAR アトリビュートの割り当て

デバイスは、RADIUS 拡張属性によって割り当てられた CAR 属性を使用して、オンライン MAC 認証ユーザーのアクセスレートを制御できます。拡張 RADIUS 属性については、「AAA の設定」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-Peak-Rate: インバウンドトラフィックのピークレート(bps 単位)。
- Input-Average-Rate: 着信トラフィックの平均レート(bps 単位)。
- Output-Peak-Rate: アウトバウンドトラフィックのピークレート(bps 単位)。
- Output-Average-Rate: アウトバウンドトラフィックの平均レート(bps 単位)。

サーバーがピークレートと平均レートの両方を制御するために CAR アトリビュートを割り当てる場合、デバイスはユーザートラフィックに対してダブルレートトラフィックポリシングを実装します。サーバーが Input-Peak-Rate または Output-Peak-Rate アトリビュートを割り当てない場合、デバイスはユーザートラフィックに対してシングルレートトラフィックポリシングを実装します。トラフィックポリシングの詳細については、『ACL and QoS Configuration Guide』の「QoS configuration」を参照してください。



## Blackhole MAC 属性の割り当て

デバイスは、MAC 認証を通過したユーザーの CoA メッセージを介して RADIUS 認証サーバーによって割り当てられたブラックホール MAC アトリビュートをサポートします。MAC 認証を通過したユーザーのブラックホール MAC アトリビュートを含む CoA メッセージを受信すると、デバイスは次の動作を実行します。

1. ユーザーをログオフします。
2. ユーザーの MAC アドレスをサイレント MAC アドレスとしてマークし、その MAC アドレスの待機タイマーを開始します。

待機タイマーは 10 分で、ユーザーは設定できません。待機タイマーが開始されると、デバイスは MAC アドレスからのすべてのパケットをドロップし、待機タイマーが期限切れになるまで MAC アドレスを認証しません。

サイレント MAC アドレスを表示するには、`display mac-authentication` コマンドを使用します。

## 定期的な MAC 再認証

定期的な MAC 再認証では、オンラインユーザーの接続ステータスが追跡され、RADIUS サーバーによって割り当てられた認可アトリビュートが更新されます。アトリビュートには、ACL および VLAN が含まれます。

定期的な MAC 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 MAC 認証ユーザーを再認証します。この間隔はタイマーによって制御され、タイマーはユーザーが設定できます。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、MAC 認証ユーザーが認証を通過した後にだけ、オンライン MAC 認証ユーザーに適用されます。

サーバーによって割り当てられた RADIUS Session-Timeout(アトリビュート 27)および Termination-Action(アトリビュート 29)アトリビュートは、ともに定期的な MAC 再認証機能に影響を与える可能性があります。サーバーによって割り当てられた Session-Timeout および Termination-Action アトリビュートを表示するには、`display mac-authentication connection` コマンドを使用します。

- 終了アクションがユーザーのログオフである場合、定期的な MAC 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も短い場合にだけ有効になります。セッションタイムアウトタイマーが短い場合、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ると、オンラインで認証されたユーザーをログオフします。
- 終了アクションがユーザーの再認証である場合、デバイスの定期的な MAC 再認証設定は有効になりません。デバイスは、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の期限が切れると、オンライン MAC 認証ユーザーを再認証します。

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 MAC 再認証を実行するかどうかは、デバイスの定期的な MAC 再認証設定によって決まります。Session-Timeout および Termination-Action 属性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。

RADIUS DAS 機能を有効にすると、デバイスは、RADIUS 認証サーバーから再認証アトリビュートを含む CoA メッセージを受信すると、ただちにユーザーを再認証します。この場合、デバイスで定期的な MAC 再認証が有効になっているかどうかに関係なく、再認証が実行されます。RADIUS DAS 設定の詳細については、「AAA の設定」を参照してください。

デフォルトでは、MAC 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 MAC 認証ユーザーをログオフします。オンライン維持機能は、MAC 再認証のために到達可能なサーバーがない場合に、認証された MAC 認証ユーザ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ユーザーに割り当てられる VLAN は、同じであっても異なってもかまいません。

# 制約事項および注意事項:MAC認証の設定

認証サーバーが認証 VSI と認証 VLAN の両方をユーザーに割り当てる場合、デバイスは認証 VLAN だけを使用します。

ポート上では、ゲスト VLAN およびクリティカル VLAN 設定は、ゲスト VSI およびクリティカル VSI 設定と相互に排他的です。

認証 VLAN または認証 VSA を正常に割り当てるには、次の注意事項に従ってください。

- MAC 認証対応ポートがゲスト VLAN およびクリティカル VLAN で設定されている場合は、認証 VLAN を MAC 認証ユーザーに割り当てるように認証サーバーを設定します。
- MAC 認証対応ポートがゲスト VSI およびクリティカル VSI で設定されている場合は、認証 VSI を MAC 認証ユーザーに割り当てるように認証サーバーを設定します。

ポート上の MAC 認証ゲスト VLAN またはクリティカル VLAN にユーザ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。

MAC 認証設定は、レイヤー2 イーサネットインターフェースおよびレイヤー2 集約インターフェースだけでサポートされます。

レイヤー2 イーサネットインターフェースが集約グループに追加された後、インターフェースの MAC 認証設定は有効になりません。

インターフェースにオンライン MAC 認証ユーザーが存在する場合は、レイヤー2 集約インターフェースを削除しないでください。

認証に失敗した MAC アドレスがスタティック MAC アドレスまたはセキュリティ認証に合格した MAC アドレスである場合、デバイスはその MAC アドレスをサイレントアドレスとしてマークしません。

## MAC認証タスクの概要

MAC 認証を設定するには、次の作業を実行します。

1. MAC 認証の有効化
2. 基本的な MAC 認証機能の設定
  - MAC 認証方式の指定
  - MAC 認証ドメインの指定
  - ユーザー アカウント ポリシーの構成
  - (オプション)MAC 認証タイマーの設定
  - (オプション)定期的な MAC 再認証の設定
3. (任意)MAC 認証 VLAN 割り当ての設定
  - MAC 認証ゲスト VLAN の構成
  - MAC 認証クリティカル VLAN の構成
  - MAC 認証クリティカル音声 VLAN 機能の有効化
4. (任意)MAC 認証 VSI 割り当ての設定
  - MAC 認証ゲスト VSI の構成
  - MAC 認証クリティカル VSI の構成
5. (任意)その他の MAC 認証機能の設定
  - 認証されていない MAC 認証ユーザー エージングの構成
  - MAC 認証オフライン検出の構成

- MAC 認証のオンライン ユーザー同期の有効化
- ポートでの同時 MAC 認証ユーザーの最大数の設定
- ポートでの MAC 認証マルチ VLAN モードの有効化  
ポートで VLAN の変更が発生したときにオンラインユーザーを再認証しないようにするには、次の作業を実行します。
- MAC 認証遅延の構成
- MAC 認証要求にユーザー IP アドレスを含める
- 並列 MAC 認証と 802.1X 認証の有効化
- RESTful サーバー支援 MAC 認証ユーザー回復の構成
- MAC 認証での URL リダイレクト用の Web プロキシ ポートの構成 MAC 認証ユーザーのログオフ
- MAC 認証ユーザー ロギングの有効化

## MAC認証の前提条件

MAC 認証を設定する前に、次の作業を実行します。

1. ポートセキュリティ機能が無効になっていることを確認します。ポートセキュリティの詳細については、「ポートセキュリティの設定」を参照してください。
2. 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、「AAA の設定」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 サーバーが相互にアクセスし、RADIUS サーバー上にユーザーカウントを作成できることを確認します。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 認証ユーザーの MAC アドレスと同じであることを確認します。

## MAC認証のイネーブル化

### 制約事項とガイドライン

MAC 認証をポートで有効にするには、この機能をグローバルおよびポートでイネーブルにする必要があります。

### 操作方法

1. system view に入ります。

#### **System-view**

2. MAC 認証をグローバルにイネーブルにします。

#### **mac-authentication**

デフォルトでは、MAC 認証はグローバルにディセーブルです。

3. interface view に入ります。

#### **interface interface-type interface-number**

4. ポート上で MAC 認証をイネーブルにします。

#### **mac-authentication**

デフォルトでは、MAC 認証はポート上でディセーブルです。

# MAC認証ドメインの指定

## MAC 認証用の認証ドメインについて

デフォルトでは、MAC 認証ユーザーはシステムのデフォルト認証ドメイン内にあります。ユーザーに異なるアクセスポリシーを実装するには、次のいずれかの方法を使用して、MAC 認証ユーザーの認証ドメインを指定します。

- System-view でグローバル認証ドメインを指定します。このドメイン設定は、MAC 認証がイネーブルになっているすべてのポートに適用されます。
- インターフェースビューで個々のポートの認証ドメインを指定します。

MAC 認証は、ポート上のユーザーの認証ドメインをポート固有ドメイン、グローバルドメイン、デフォルトドメインの順に選択します。認証ドメインの詳細については、「AAA の設定」を参照してください。

## 操作方法

1. system view に入ります。

### System-view

2. MAC 認証ユーザーの認証ドメインを指定します。

- System-view で、次の操作を行います。  
**mac-authentication domain domain-name**
- インターフェースビュー:  
**interface interface-type interface-number**  
**mac-authentication domain domain-name**

デフォルトでは、システムのデフォルト認証ドメインが MAC 認証ユーザーに使用されます。

# ユーザーアカウントフォーマットの構成

1. system view に入ります。

### System-view

2. MAC 認証ユーザーアカウントの形式を設定します。

- ユーザーごとに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 | without-hyphen } [ lowercase | uppercase ] ] [ password { cipher | simple } string ]**
- すべてのユーザーに対して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 } string ]**

デフォルトでは、デバイスはユーザーのMACアドレスをMAC認証ユーザーのMACアドレスを使用します。MACアドレスはハイフンなしの16進表記で、文字は小文字です。

# MAC認証タイマーの設定

## MAC 認証タイマーについて

MAC 認証では、次のタイマーが使用されます。

- Offline detect timer: ユーザーがアイドル状態であるとデバイスが判断する前に、ユーザーからのトラフィックをデバイスが待機する間隔を設定します。タイマーの期限が切れ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、アカウントिंगサーバーにそのユーザーのアカウントिंगを停止するよう要求します。このタイマーは、MAC 認証オフライン検出機能がイネーブルになっている場合にだけ有効です。  
ベストプラクティスとして、MAC アドレスエージングタイマーをオフライン検出タイマーと同じ値に設定します。この操作により、MAC アドレスエントリの有効期限が切れるために、MAC 認証済みユーザーがオフライン検出時間内にログオフされないようにします。
- Quiet 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、認証の繰り返しによるシステムパフォーマンスへの影響を回避できます。
- Server timeout timer: 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。

## 操作方法

1. system view 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。

# MAC認証ゲストVLANの設定

## 制約事項とガイドライン

ポートに MAC 認証ゲスト VLAN を設定する場合は、表 8 の注意事項に従ってください。

表 8 MAC 認証ゲスト VLAN と他のセキュリティ機能との関係

機能	関係の説明	参照
MAC認証のQuiet機能	MAC認証ゲストVLAN機能の方がプライオリティが高くなります。 ユーザーがMAC認証に失敗すると、ユーザーはゲストVLAN内のリソースにアクセスできません。ユーザーのMACアドレスは、サイレントMACアドレスとしてマークされません。	「Configuring MAC authentication timers.」を参照してください。
スーパーVLAN	VLANをスーパーVLANとMAC認証ゲストVLANの両方として指定することはできません。	『Layer 2-LAN Switching Configuration Guide』を参照してください。
ポート侵入保護	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が、ポート侵入保護機能のシャットダウンポートアクションよりも低いプライオリティを持ちます。	「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

ポート上で MAC 認証ゲスト VLAN を設定する前に、次の作業を実行します。

- MAC 認証ゲスト VLAN として指定する VLAN を作成します。
- ポートをハイブリッドポートとして設定し、VLAN をポート上のタグ無メンバーとして設定します。
- ポート上で MAC ベース VLAN をイネーブルにします。

VLAN 設定の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

## 操作方法

1. system view に入ります。

### System-view

2. interface view に入ります。

**interface** *interface-type interface-number*

3. ポート上で MAC 認証ゲスト VLAN を指定します。

**mac-authentication guest-vlan** *guest-vlan-id*

デフォルトでは、ポート上で MAC 認証ゲスト VLAN は指定されません。

1 つのポートに設定できる MAC 認証ゲスト VLAN は 1 つだけです。異なるポート上の MAC 認証ゲスト VLAN は異なる場合があります。

4. MAC 認証ゲスト VLAN 内のユーザーの認証間隔を設定します。

**mac-authentication guest-vlan auth-period** *period-value*

デフォルト設定は 30 秒です。

# MAC 認証クリティカル VLAN の設定

## 制約事項とガイドライン

ポートに MAC 認証クリティカル VLAN を設定する場合は、表 9 の注意事項に従ってください。

表 9 MAC 認証に不可欠な VLAN と他のセキュリティ機能との関係

機能	関係の説明	参照
MAC 認証の Quiet 機能	MAC 認証クリティカル VLAN 機能のプライオリティが高くなっています。 RADIUS 認証サーバーに到達できないためにユーザーが MAC 認証に失敗した場合、ユーザーはクリティカル VLAN 内のリソースにアクセスできます。ユーザーの MAC アドレスは、サイレント MAC アドレスとしてマークされません。	「MAC 認証タイマーの設定」を参照してください。
スーパー VLAN	VLAN をスーパー VLAN と MAC 認証クリティカル VLAN の両方として指定することはできません。	『Layer 2-LAN Switching Configuration Guide』を参照してください。
ポート侵入保護	クリティカル 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が、ポート侵入保護機能のシャットダウンポートアクションよりも低いプライオリティを持ちます。	「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

ポートに MAC 認証クリティカル VLAN を設定する前に、次の作業を実行します。

- MAC 認証クリティカル VLAN として指定する VLAN を作成します。
- ポートをハイブリッドポートとして設定し、VLAN をポート上のタグ無メンバーとして設定します。

- ポート上で MAC ベース VLAN をイネーブルにします。

VLAN 設定の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

## 操作方法

1. system view に入ります。

### System-view

2. interface view に入ります。

**interface** *interface-type interface-number*

3. ポート上で MAC 認証クリティカル VLAN を指定します。

**mac-authentication critical vlan** *critical-vlan-id*

デフォルトでは、MAC 認証 mac 認証クリティカル VLAN は指定されていません。

1 つのポートに設定できる MAC 認証クリティカル VLAN は 1 つだけです。異なるポート上の MAC 認証クリティカル VLAN は異なる場合があります。

# MAC認証クリティカル音声VLAN機能のイネーブル化

## 前提条件

ポート上で MAC 認証クリティカル音声 VLAN 機能をイネーブルにする前に、次の作業を実行します。

- グローバルとポートの両方で LLDP を有効にします。

デバイスは LLDP を使用して音声ユーザーを識別します。LLDP の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

- ポート上で音声 VLAN をイネーブルにします。

音声 VLAN の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

## 操作方法

1. system view に入ります。

### System-view

2. interface view に入ります。

**interface** *interface-type interface-number*

3. ポート上で MAC 認証クリティカル音声 VLAN 機能をイネーブルにします。

**mac-authentication critical-voice-vlan**

デフォルトでは、MAC 認証クリティカル音声 VLAN 機能はポート上でディセーブルです。

# MAC認証ゲストVSIの設定

## 制約事項とガイドライン

MAC 認証ゲスト VSI 機能は、MAC 認証の待機機能よりも優先されます。ユーザーが MAC 認証に失敗すると、そのユーザーはゲスト VSI 内のリソースにアクセスできます。ユーザーの MAC アドレスは、サイレント MAC アドレスとしてマークされません。

1 つのポートに設定できる MAC 認証ゲスト VSI は 1 つだけです。異なるポート上の MAC 認証ゲスト VSI は異なる場合があります。

## 前提条件

ポート上で MAC 認証ゲスト VSI を設定する前に、次の作業を実行します。

- L2VPN をイネーブルにします。
- MAC 認証ゲスト VSI として指定する VSI を作成し、VSI 用の VXLAN を作成します。
- ダイナミックイーサネットサービスインスタンスの MAC ベースのトラフィックマッチングがポートでイネーブルになっていることを確認します。

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

## 操作方法

1. system view に入ります。

### System-view

2. interface view に入ります。

**interface** *interface-type interface-number*

3. ポート上で MAC 認証ゲスト VSI を指定します。

**mac-authentication guest-vsi** *guest-vsi-name*

デフォルトでは、ポート上に MAC 認証ゲスト VSI は存在しません。

4. (任意)MAC 認証ゲスト VSI のユーザーの認証間隔を設定します。

**mac-authentication guest-vsi auth-period** *period-value*

デフォルト設定は 30 秒です。

# MAC 認証クリティカル VSI の設定

## 制約事項とガイドライン

MAC 認証の重要な VSI 機能は、MAC 認証の待機機能よりも優先されます。ユーザーが MAC 認証に失敗すると、そのユーザーは重要な VSI 内のリソースにアクセスできます。ユーザーの MAC アドレスは、サイレント MAC アドレスとしてマークされません。

1 つのポートに設定できる MAC 認証クリティカル VSI は 1 つだけです。異なるポート上の MAC 認証クリティカル VSI は異なる場合があります。

## 前提条件

MAC 認証に不可欠な VSI をポートに設定する前に、次の作業を実行します。

- L2VPN をイネーブルにします。
- MAC 認証に重要な VSI として指定する VSI を作成し、VSI の VXLAN を作成します。
- ダイナミックイーサネットサービスインスタンスの MAC ベースのトラフィックマッチングがポートでイネーブルになっていることを確認します。

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

## 操作方法

1. system view に入ります。

### System-view

2. interface view に入ります。

**interface** *interface-type interface-number*

3. ポート上で MAC 認証クリティカル VSI を指定します。

**mac-authentication critical vsi** *critical-vsi-name* [ **url-user-logoff** ]



デフォルトでは、MAC 認証に重要な VSI はポート上に存在しません。

`url-user-logout` キーワードを使用すると、最初のユーザーが重要な VSI に割り当てられたときに、ポート上で認可 URL が割り当てられた MAC 認証ユーザーをデバイスがログオフできます。

## MAC認証オフライン検出のイネーブル化

### MAC 認証オフライン検出について

この機能は、オフライン検出時間内にデバイスがユーザーからパケットを受信しなかった場合に、ユーザーをデバイスからログアウトさせます。また、デバイスはアカウントिंगサーバーに対して、そのユーザーのアカウントINGを停止するように要求します。オフライン検出タイマーの詳細については、「MAC 認証タイマーの設定」を参照してください。

この機能をディセーブルにすると、デバイスがオンラインユーザーステータスを検査できなくなります。

### 操作方法

1. system view に入ります。

**System-view**

2. interface view に入ります。

**interface** *interface-type interface-number*

3. MAC 認証オフライン検出をイネーブルにします。

**mac-authentication offline-detect enable**

デフォルトでは、MAC 認証オフライン検出はポート上でイネーブルです。

## ポート上の同時MAC認証ユーザーの最大数の設定

### ポート上の同時 MAC 認証ユーザー数の制限について

システムリソースが過剰使用されないようにするには、次の作業を実行します。

### 操作方法

1. system view に入ります。

**System-view**

2. interface view に入ります。

**interface** *interface-type interface-number*

3. ポート上の同時 MAC 認証ユーザーの最大数を設定します。

**mac-authentication max-user** *max-number*

デフォルト設定は 4294967295 です。

## ポート上でのMAC認証マルチVLANモードの有効化

### MAC 認証マルチ VLAN モードについて

MAC 認証マルチ VLAN モードでは、認証されたオンラインユーザーは、ポート上での VLAN 変更によるサービス中断を回避できます。ポートが、既存の MAC-VLAN マッピングと一致しない VLAN 内のユーザーから送信されたパケットを受信した場合、デバイスはユーザーをログオフせず、再認証も行いません。デバイスはユーザーの新しい MAC-VLAN マッピングを作成し、トラフィック送信は中断されません。ユーザーの元

の MAC-VLAN マッピングは、動的に期限切れになるまでデバイス上に残ります。ベストプラクティスとして、この機能をハイブリッドポートまたはトランクポートに設定します。

この機能により、遅延や干渉の影響を受けやすいデータの伝送が改善されます。通常、この機能は IP 電話ユーザーに適用されます。

## 操作方法

1. system view に入ります。

### System-view

2. interface view に入ります。

**interface** *interface-type interface-number*

3. MAC 認証マルチ VLAN モードをイネーブルにします。

**mac-authentication host-mode multi-vlan**

デフォルトでは、この機能はポート上でディセーブルです。ポートが、既存の MAC-VLAN マッピングと一致しない VLAN 内の認証済みユーザーから送信されたパケットを受信すると、デバイスはログオフしてユーザーを再認証します。

# MAC認証遅延の設定

## MAC 認証遅延について

802.1X 認証と MAC 認証の両方がポートでイネーブルになっている場合は、802.1X 認証が優先的にトリガーされるように、MAC 認証を遅延できます。

802.1X 認証がトリガーされない場合、または遅延期間内に 802.1X 認証が失敗した場合、ポートは MAC 認証の処理を続行します。

## 制約事項とガイドライン

MAC 認証遅延を使用する場合は、ポートセキュリティモードを **mac-else-userlogin-secure** または **mac-else-userlogin-secure-ext** に設定しないでください。遅延は、2 つのモードのいずれかのポートでは有効になりません。ポートセキュリティモードの詳細については、「ポートセキュリティの設定」を参照してください。

## 操作方法

1. system view に入ります。

### System-view

2. interface view に入ります。

**interface** *interface-type interface-number*

3. MAC 認証遅延をイネーブルにし、遅延タイマーを設定します。

**mac-authentication timer auth-delay** *time*

デフォルトでは、MAC 認証遅延はディセーブルになっています。

# 定期的なMAC再認証の設定

## 制約事項とガイドライン

デバイスは、次の順序で MAC 再認証用の定期再認証タイマーを選択します。

1. サーバーによって割り当てられた再認証タイマー。
2. ポート固有の再認証タイマー。
3. グローバル再認証タイマー。

#### 4. デフォルトの再認証タイマー。

MAC 認証ドメインまたはユーザーカウントの形式の設定を変更しても、オンライン MAC 認証ユーザ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 MAC 認証ユーザーにのみ有効です。

### 操作方法

1. system view に入ります。

#### System-view

2. 定期的な MAC 再認証タイマーを設定します。

- グローバルな定期的再認証タイマーを設定します。

```
mac-authentication timer reauth-period reauth-period-value
```

デフォルト設定は 3600 秒です。

- 次のコマンドを順番に実行して、ポート固有の定期的な再認証タイマーを設定します。

```
interface interface-type interface-number
```

```
mac-authentication timer reauth-period reauth-period-value quit
```

デフォルトでは、定期的な MAC 再認証タイマーはポートに設定されていません。ポートはグローバルな定期的 MAC 再認証タイマーを使用します。

3. interface view に入ります。

```
interface interface-type interface-number
```

4. 定期的な MAC 再認証をイネーブルにします。

```
mac-authentication re-authenticate
```

デフォルトでは、定期的な MAC 再認証はポート上でディセーブルです。

5. (任意)ポート上の認証された MAC 認証ユーザーに対して、オンライン維持機能をイネーブルにします。

```
mac-authentication reauthenticate server-unreachable keep-online
```

デフォルトでは、keep-online 機能はディセーブルです。MAC 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 MAC 認証ユーザーをログオフします。

高速リカバリネットワークでは、keep-online 機能を使用して、MAC 認証ユーザーが頻繁にオンラインになったりオフラインになったりしないようにすることができます。

## MAC認証要求へのユーザーIPアドレスの追加

### MAC 認証要求にユーザーIP アドレスを含める機能について

#### ❗ 重要:

この機能は、IMC サーバーとの組み合わせでのみ動作します。

スタティック IP アドレスへの変更によって発生する IP 競合を回避するには、スタティック IP アドレスを使用する MAC 認証ユーザーが存在するポートでこの機能を使用します。

この機能は、認証サーバーに送信される MAC 認証要求にユーザーIP アドレスを追加します。ユーザーに対して MAC 認証がトリガーされると、デバイスはユーザーの IP アドレスが無効であるかどうかをチェックします。

- IP アドレスが有効な場合、デバイスは IP アドレスを含む MAC 認証要求を送信します。
- IP アドレスが有効なホスト IP アドレスでない場合、またはトリガーパケットに IP アドレスが含まれていない場合、デバイスは MAC 認証を開始しません。

- パケットの送信元 IP アドレスが 0.0.0.0 の DHCP パケットである場合、デバイスは IP アドレスを含まない MAC 認証要求を送信します。この場合、IMC サーバーは認証時にユーザー IP アドレスを検査しません。

ユーザーの IP アドレスを含む認証要求を受信すると、IMC サーバーはユーザーの IP アドレスと MAC アドレスを IP-MAC マッピングと比較します。

- 完全一致が見つかった場合、または一致が見つからなかった場合、ユーザーは MAC 認証を通過します。後者の場合、サーバーはユーザーの IP-MAC マッピングを作成します。
- MAC アドレスのマッピングが検出されても IP アドレスが一致しない場合、ユーザーは MAC 認証に失敗します。

### 制約事項とガイドライン

この機能は、ポート上で MAC 認証ゲスト VLAN またはゲスト VSI と併用しないでください。これらの機能を併用すると、ユーザーが MAC 認証ゲスト VLAN またはゲスト VSI に追加されると、デバイスはそのユーザーに対して MAC 認証を実行できなくなります。

### 操作方法

1. system view に入ります。

#### System-view

2. interface view に入ります。

**interface** *interface-type* *interface-number*

3. MAC 認証要求にユーザー IP アドレスを含める。

**mac-authentication carry user-ip**

デフォルトでは、MAC 認証要求にはユーザー IP アドレスは含まれません。

## MAC 認証と 802.1X 認証の並列処理の有効化

### MAC 認証と 802.1X 認証の並列処理について

この機能により、802.1X 認証の完了後に MAC 認証を処理するポートが、802.1X 認証と並行して MAC 認証を処理できるようになります。

ポートが次の要件を満たしていることを確認します。

- ポートは 802.1X 認証と MAC 認証の両方を使用して設定され、802.1X 認証用の MAC ベースのアクセスコントロールを実行します。
- ポートは 802.1X ユニキャストトリガーでイネーブルになっています。

ポートが未知の MAC アドレスからパケットを受信すると、ユニキャスト EAP-Request/Identity パケットをその MAC アドレスに送信します。その後、ポートは 802.1X 認証結果を待たずに、ただちに MAC 認証を処理します。

MAC 認証が成功すると、ポートは MAC 認証許可 VLAN に割り当てられます。

- 802.1X 認証が失敗した場合、MAC 認証結果が有効になります。
- 802.1X 認証が成功すると、デバイスは 802.1X 認証の結果に基づいてポートと MAC アドレスを処理します。

802.1X 認証と MAC 認証のプロセスシーケンスは、別の方法で設定できます。ポートが 802.1X ゲスト VLAN またはゲスト VSI に割り当てられる前に MAC 認証を実行するには、新しい MAC トリガー 802.1X ゲスト VLAN または VSI 割り当て遅延をイネーブルにします。新しい MAC トリガー 802.1X ゲスト VLAN または VSI 割り当て遅延については、を参照してください。

## 制約事項とガイドライン

ポートで 802.1X 認証と MAC 認証の両方を設定するには、次のいずれかの方法を使用します。

- ポート上で 802.1X および MAC 認証機能を個別にイネーブルにします。
- ポートでポートセキュリティをイネーブルにします。ポートセキュリティモードは、**userlogin-secure-or-mac** または **userlogin-secure-or-mac-ext** である必要があります。

ポートセキュリティモードの設定については、「ポートセキュリティの設定」を参照してください。

並列処理機能を正しく動作させるには、ポート上で MAC 認証遅延をイネーブルにしないでください。この操作により、802.1X 認証がトリガーされた後に MAC 認証が遅延されます。

## 操作方法

1. system view に入ります。

### System-view

2. interface view に入ります。

**interface** *interface-type* *interface-number*

3. ポート上で MAC 認証と 802.1X 認証の並列処理をイネーブルにします。

**mac-authentication parallel-with-dot1x**

デフォルトでは、この機能はディセーブルです。

# MAC認証ユーザーのロギングのイネーブル化

## MAC 認証ユーザーのロギングについて

この機能を使用すると、デバイスは MAC 認証ユーザーのログを生成し、そのログをインフォメーションセンターに送信できます。ログを正しく出力するには、デバイス上でインフォメーションセンターも構成する必要があります。インフォメーションセンターの構成の詳細は、ネットワーク管理と監視構成ガイドを参照してください。

## 制約事項とガイドライン

ベストプラクティスとして、この機能をディセーブルにして、MAC 認証ユーザーのログが過剰に出力されないようにします。

## 操作方法

1. system view に入ります。

### System-view

2. MAC 認証ユーザーのロギングをイネーブルにします。

**mac-authentication access-user log enable [ failed-login | logoff | successful-login ]**  
\*

デフォルトでは、すべてのタイプのロギングが MAC 認証ユーザーに対してディセーブルです。

パラメーターを指定しない場合、このコマンドは MAC 認証ユーザーのすべてのタイプのロギングをイネーブルにします。

# MAC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
MAC認証情報を表示します。	<b>display mac-authentication</b> [ <b>interface</b> <i>interface-type interface-number</i> ]
MAC認証接続を表示します。	<b>display mac-authentication connection</b> [ <b>open</b> ] [ <b>interface</b> <i>interface-type interface-number</i>   <b>slot</b> <i>slot-number</i>   <b>user-mac</b> <i>mac-address</i>   <b>user-name</b> <i>user-name</i> ]
特定のMAC認証VLANまたは特定のタイプのVSA内のMAC認証ユーザーのMACアドレス情報を表示します。	<b>display mac-authentication mac-address</b> { <b>critical-vlan</b>   <b>critical-vsi</b>   <b>guest-vlan</b>   <b>guest-vsi</b> } [ <b>interface</b> <i>interface-type interface-number</i> ]
MAC認証統計情報をクリアします。	<b>reset mac-authentication statistics</b> [ <b>interface</b> <i>interface-type interface-number</i> ]
ポート上のMAC認証クリティカルVLANからユーザーを削除します。	<b>reset mac-authentication critical vlan</b> <b>interface</b> <i>interface-type interface-number</i> [ <b>mac-address</b> <i>mac-address</i> ]
ポート上のMAC認証クリティカルな音声VLANからユーザーを削除します。	<b>reset mac-authentication critical-voice-vlan</b> <b>interface</b> <i>interface-type interface-number</i> [ <b>mac-address</b> <i>mac-address</i> ]
ポート上のMAC認証ゲストVLANからユーザーを削除します。	<b>reset mac-authentication guest-vlan interface</b> <i>interface-type interface-number</i> [ <b>mac-address</b> <i>mac-address</i> ]
ポート上のMAC認証クリティカルVSIからユーザーを削除します。	<b>reset mac-authentication critical vsi interface</b> <i>interface-type interface-number</i> [ <b>mac-address</b> <i>mac-address</i> ]
ポート上のMAC認証ゲストVSIからユーザーを削除します。	<b>reset mac-authentication guest-vsi interface</b> <i>interface-type interface-number</i> [ <b>mac-address</b> <i>mac-address</i> ]

## MAC認証の設定例

### 例:ローカル MAC 認証の設定

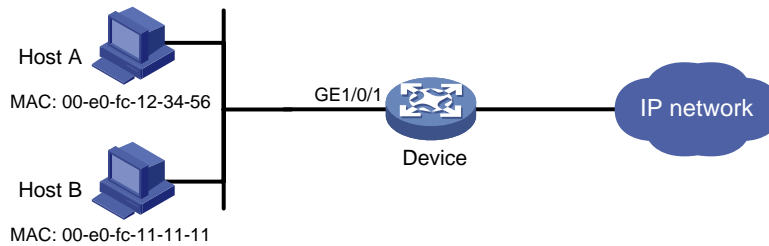
#### ネットワーク構成

図 4 に示すように、デバイスはローカル MAC 認証を実行して、ユーザーのインターネットアクセスを制御します。

次の要件を満たすようにデバイスを設定します。

- ユーザーが 180 秒ごとにオフラインになったかどうかを検出します。
- ユーザーが MAC 認証に失敗した場合に、そのユーザーを 180 秒間拒否します。
- ISP ドメイン bbb のすべてのユーザーを認証します。
- 各ユーザーの MAC アドレスを認証用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、ハイフン付きの 16 進表記で、文字は小文字です。

図 4 ネットワーク図



## 操作方法

#ネットワークアクセスローカルユーザーを追加します。この例では、ユーザー名とパスワードの両方をホスト A の MAC アドレス 00-e0-fc-12-34-56 として設定します。

```
<Device>System-view
```

```
[Device] local-user 00-e0-fc-12-34-56 class network
```

```
[Device-luser-network-00-e0-fc-12-34-56] password simple 00-e0-fc-12-34-56
```

#ユーザーの LAN アクセスサービスを指定します。

```
[Device-luser-network-00-e0-fc-12-34-56] service-type lan-access
```

```
[Device-luser-network-00-e0-fc-12-34-56] quit
```

#LAN ユーザーのローカル認証を実行するように ISP ドメイン **bbb** を構成します。

```
[Device] domain bbb
```

```
[Device-isp-bbb] authentication lan-access local
```

```
[Device-isp-bbb] quit
```

# GigabitEthernet 1/0/1 で MAC 認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] mac-authentication
```

```
[Device-GigabitEthernet1/0/1] quit
```

#MAC 認証ドメインとして ISP ドメイン **bbb** を指定します。

```
[Device] mac-authentication domain bbb
```

#MAC 認証タイマーを設定します。

```
[Device] mac-authentication timer offline-detect 180
```

```
[Device] mac-authentication timer quiet 180
```

#MAC ベースのアカウントを使用するように MAC 認証を設定します。各 MAC アドレスは、ハイフンを含む 16 進数表記で、文字は小文字です。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

#MAC 認証をグローバルにイネーブルにします。

```
[Device] mac-authentication
```

## 設定の確認

#MAC 認証設定と統計情報を表示して、設定を確認します。

```
[Device] display mac-authentication
```

```
Global MAC authentication parameters:
```

```
MAC authentication      : Enabled
```

```
User name format       : MAC address in lowercase(xx-xx-xx-xx-xx-xx)
```

```
Username               : mac
```

```
Password               : Not configured
```

```
Offline detect period  : 180 s
```

```
Quiet period           : 180 s
```

```
Server timeout      : 100 s
Reauth period      : 3600 s
Authentication domain : bbb
Online MAC-auth users : 1
```

Silent MAC users:

MAC address	VLAN ID	From port	Port index
00e0-fc11-1111	8	GE1/0/1	1

GigabitEthernet 1/0/1 is link-up

```
MAC authentication      : Enabled
Carry User-IP          : Disabled
Authentication domain   : Not configured
Auth-delay timer       : Disabled
Periodic reauth        : Disabled
Re-auth server-unreachable : Logoff
Guest VLAN              : Not configured
Guest VLAN auth-period : 30 s
Critical VLAN           : Not configured
Critical voice VLAN     : Disabled
Host mode               : Single VLAN
Offline detection       : Enabled
Authentication order    : Default
Guest VSI               : Not configured
Guest VSI auth-period  : 30 s
Critical VSI            : Not configured
Auto-tag feature        : Disabled
VLAN tag configuration ignoring : Disabled
Max online users        : 4294967295
Authentication attempts : successful 1, failed 0
Current online users    : 1
  MAC address  Auth state
  00e0-fc12-3456  Authenticated
```

出力には、ホスト A が MAC 認証に合格し、オンラインになったことが示されています。ホスト B は MAC 認証に失敗し、その MAC アドレスはサイレント MAC アドレスとしてマークされています。

## 例:RADIUS ベースの MAC 認証の設定

### ネットワーク構成

図 5 に示すように、デバイスは RADIUS サーバーを使用して、ユーザーの認証、認可、アカウントングを実行します。

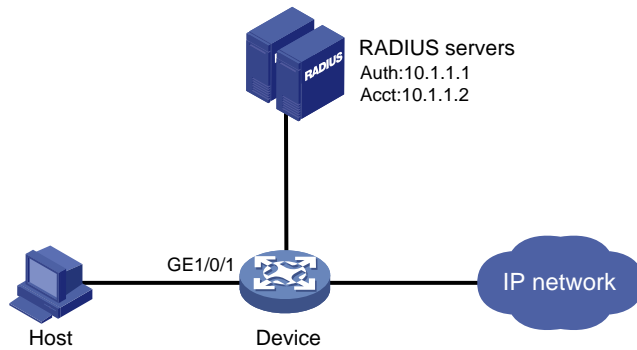
MAC 認証によってインターネットへのユーザーアクセスを制御するには、次の作業を実行します。

- MAC 認証をグローバルにイネーブルにし、GigabitEthernet 1/0/1 で有効にします。
- ユーザーが 180 秒ごとにオフラインになったかどうかを検出するようにデバイスを設定します。
- ユーザーが MAC 認証に失敗した場合に、そのユーザーを 180 秒間拒否するようにデバイスを設定します。
- すべてのユーザーが ISP ドメイン **bbb** に属するように設定します。



- すべてのユーザーに対して共有ユーザーアカウントを使用します。ユーザー名は **aaa**、パスワードは **123456** です。

図 5 ネットワーク図



## 操作方法

1. RADIUS サーバーとアクセスデバイスが相互にアクセスできることを確認します(詳細は省略)。
2. RADIUS サーバーを設定します。  
#MAC 認証ユーザー用の共有アカウントを作成します(詳細は省略)。  
#アカウントのユーザー名 **aaa** とパスワード **123456** を設定します(詳細は省略)。
3. デバイスに RADIUS ベースの MAC 認証を設定します。  
#RADIUS スキームを設定します。  

```
<Device> system-view
[Device] radius scheme 2000
[Device-radius-2000] primary authentication 10.1.1.1 1812
[Device-radius-2000] primary accounting 10.1.1.2 1813
[Device-radius-2000] key authentication simple abc
[Device-radius-2000] key accounting simple abc
[Device-radius-2000] user-name-format without-domain
[Device-radius-2000] quit
```

#RADIUS スキームを ISP ドメイン **bbb** に適用して、認証、認可、アカウントिंगを行います。

```
[Device] domain bbb
[Device-isp-bbb] authentication default radius-scheme 2000
[Device-isp-bbb] authorization default radius-scheme 2000
[Device-isp-bbb] accounting default radius-scheme 2000
[Device-isp-bbb] quit
```

# GigabitEthernet 1/0/1 で MAC 認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
[Device-GigabitEthernet1/0/1] quit
```

#MAC 認証ドメインを ISP ドメイン **bbb** として指定します。

```
[Device] mac-authentication domain bbb
```

#MAC 認証タイマーを設定します。

```
[Device] mac-authentication timer offline-detect 180
[Device] mac-authentication timer quiet 180
```

#MAC 認証ユーザーが共有するアカウントのユーザー名 **aaa** とパスワード **123456** をプレーンテキストで指定します。

```
[Device] mac-authentication user-name-format fixed account aaa password simple
123456
```

#MAC 認証をグローバルにイネーブルにします。

[Device]mac-authentication

## 設定の確認

#MAC 認証の設定を確認します。

[Device] display mac-authentication

Global MAC authentication parameters:

MAC authentication : Enabled

Username format : Fixed account

Username : aaa

Password : \*\*\*\*\*

Offline detect period : 180 s

Quiet period : 180 s

Server timeout : 100 s

Reauth period : 3600 s

Authentication domain : bbb

Online MAC-auth users : 1

Silent MAC users:

MAC address	VLAN ID	From port	Port index
-------------	---------	-----------	------------

GigabitEthernet 1/0/1 is link-up

MAC authentication : Enabled

Carry User-IP : Disabled

Authentication domain : Not configured

Auth-delay timer : Disabled

Periodic reauth : Disabled

Re-auth server-unreachable : Logoff

Guest VLAN : Not configured

Guest VLAN auth-period : 30 s

Critical VLAN : Not configured

Critical voice VLAN : Disabled

Host mode : Single VLAN

Offline detection : Enabled

Authentication order : Default

Guest VSI : Not configured

Guest VSI auth-period : 30 s

Critical VSI : Not configured

Auto-tag feature : Disabled

VLAN tag configuration ignoring : Disabled

Max online users : 4294967295

Authentication attempts : successful 1, failed 0

Current online users : 1

MAC address	Auth state
-------------	------------

00e0-fc12-3456	Authenticated
----------------	---------------

# 例: サーバー割り当て MAC ベース VLAN

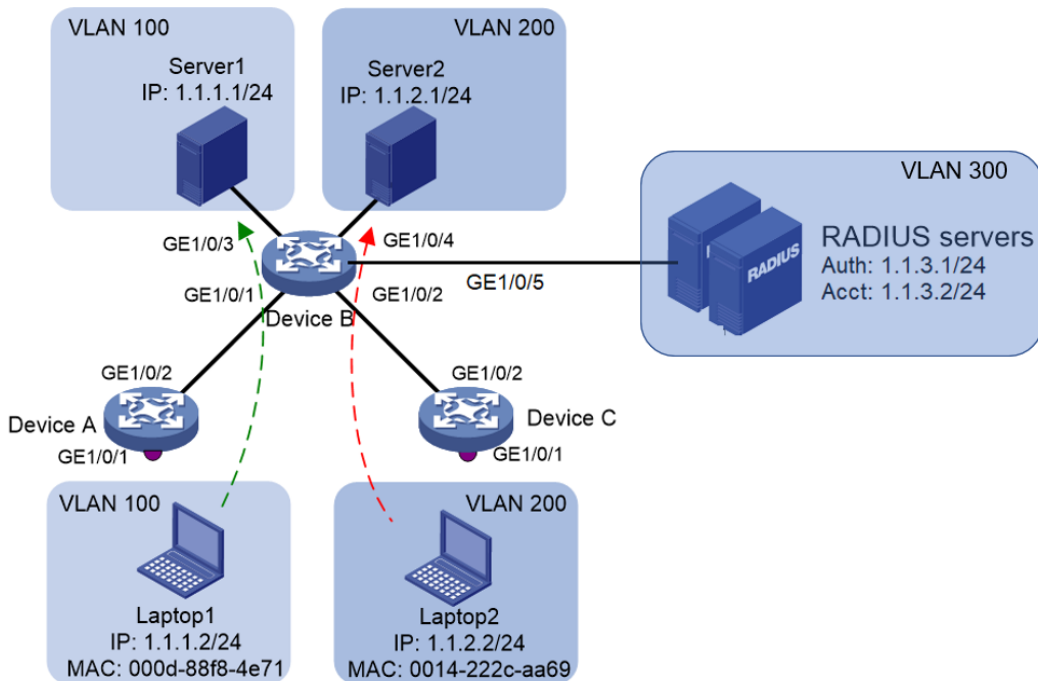
## ネットワーク構成

図 6 に示すように:

- GigabitEthernet 1/0/1 のデバイス A と GigabitEthernet 1/0/2 のデバイス C はそれぞれ会議室に接続されています。Laptop 1 と Laptop 2 は会議室で使用され、2つの会議室のいずれかで使用される可能性があります。
- 一方の部門は VLAN 100 を使用し、Laptop 1 を所有しています。もう一方の部門は VLAN 200 を使用し、Laptop 2 を所有しています。

Laptop 1 と Laptop 2 がどちらの会議室で使用されていても、それぞれ Server 1 と Server 2 にアクセスできるように、MAC ベース VLAN を設定します。MAC アドレスとその MAC アドレスが所属する VLAN の情報は RADIUS サーバーに設定しておきます。MAC アドレスが RADIUS に登録されていない場合、Laptop は認証に失敗してデバイス B のポートへのアクセスが禁止されます。

図 6 ネットワーク図



## 手順

1. デバイス B を設定します。

# VLAN 100 を作成し、GigabitEthernet 1/0/3 を VLAN 100 に割り当てます。

```
<DeviceB>system-view
```

```
[DeviceB] vlan 100
```

```
[DeviceB-vlan100] port GigabitEthernet 1/0/3
```

```
[DeviceB-vlan100] quit
```

# VLAN 200 を作成し、GigabitEthernet 1/0/4 を VLAN 200 に割り当てます。

```
[DeviceB] vlan 200
```

```
[DeviceB-vlan200] port GigabitEthernet 1/0/4
```

```
[DeviceB-vlan200] quit
```

# VLAN 300 を作成し、GigabitEthernet 1/0/5 を VLAN 300 に割り当てます。

```
[DeviceB] vlan 300
```

```
[DeviceB-vlan300] port GigabitEthernet 1/0/5
```

```
[DeviceB-vlan300] quit
```

# GigabitEthernet 1/0/1, GigabitEthernet 1/0/2 を hybrid ポートと設定し、タグなし VLAN メンバーとして VLAN 100 及び 200 を割り当てます。

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] port link-type hybrid
```

```
[DeviceB-GigabitEthernet1/0/1] port hybrid vlan 1 100 200 untagged
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] port link-type hybrid
```

```
[DeviceB-GigabitEthernet1/0/2] port hybrid vlan 1 100 200 untagged
```

```
[DeviceB-GigabitEthernet1/0/2] quit
```

2. RADIUS サーバーとアクセスデバイスが相互にアクセスできることを確認します(詳細は省略)。

# VLAN 300 に RADIUS サーバーとアクセスするために IP アドレスを割り当てます。

```
[DeviceB] interface vlan 300
```

```
[DeviceB-Vlan-interface300] ip address 1.1.3.10 24
```

```
[DeviceB-Vlan-interface300] quit
```

3. RADIUS サーバー / クライアントを設定します。

# RADIUS に MAC 認証ユーザー用の共有アカウントを作成します(詳細は省略)。

# RADIUS にアクセスのためのパスワード **abc** を設定します(詳細は省略)。

デバイス B に RADIUS ベースの MAC 認証を設定します。

# RADIUS スキームを設定します。

```
[DeviceB] radius scheme 2000
```

```
[DeviceB-radius-2000] primary authentication 1.1.3.1 1812
```

```
[DeviceB-radius-2000] primary accounting 1.1.3.2 1813
```

```
[DeviceB-radius-2000] key authentication simple abc
```

```
[DeviceB-radius-2000] key accounting simple abc
```

```
[DeviceB-radius-2000] user-name-format without-domain
```

```
[DeviceB-radius-2000] quit
```

# RADIUS スキームを ISP ドメイン **bbb** に適用して、認証、認可、アカウントिंगを行います。

```
[DeviceB] domain bbb
```

```
[DeviceB-isp-bbb] authentication default radius-scheme 2000
```

```
[DeviceB-isp-bbb] authorization default radius-scheme 2000
```

```
[DeviceB-isp-bbb] accounting default radius-scheme 2000
```

```
[DeviceB-isp-bbb] quit
```

```

# MAC 認証ドメインを ISP ドメイン bbb として指定します。
[DeviceB]mac-authentication domain bbb
# MAC 認証タイマーを設定します。
[DeviceB] mac-authentication timer offline-detect 180
[DeviceB] mac-authentication timer quiet 180
# MAC 認証方法に chap を設定します。
[DeviceB] mac-authentication authentication-method chap
# MAC 認証の結果の記録します
[DeviceB] mac-authentication access-user log enable failed-login logoff successful-login
# GigabitEthernet 1/0/1, GigabitEthernet 1/0/2 で MAC 認証機能及び MAC ベース VLAN 機能
# をイネーブルにします。
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] mac-vlan enable
[DeviceB-GigabitEthernet1/0/1] mac-authentication
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] mac-vlan enable
[DeviceB-GigabitEthernet1/0/2] mac-authentication
# MAC 認証をグローバルにイネーブルにします。
[DeviceB]mac-authentication

```

4. デバイス A 及びデバイス C は特別な設定は必要ありません。

## 設定の確認

#Laptop 1 が Server 1 のみにアクセスでき、Laptop 2 が Server 2 のみにアクセスできることを確認します (詳細は省略)。

#デバイス A およびデバイス C(たとえば、デバイス A)の MAC-to-VLAN エントリを確認します。

```

[DeviceA] display mac-vlan all
The following MAC VLAN addresses exist:
S:Static D:Dynamic
MAC address      Mask          VLAN ID      Priority  State
-----
000d-88f8-4e71   ffff-ffff-fff 100          0        S
0014-222c-aa69   ffff-ffff-fff 200          0        S

```

Total MAC VLAN address count: 2

## 設定ファイル

```

#
mac-authentication
mac-authentication timer offline-detect 180
mac-authentication timer quiet 180
mac-authentication domain bbb
mac-authentication access-user log enable failed-login logoff successful-login

```

```
mac-authentication authentication-method chap
#
vlan 1
#
vlan 100
#
vlan 200
#
vlan 300
#
interface Vlan-interface1
#
interface Vlan-interface100
#
interface Vlan-interface200
#
interface Vlan-interface300
ip address 1.1.3.10 255.255.255.0
#
interface GigabitEthernet1/0/1
port link-type hybrid
port hybrid vlan 1 100 200 untagged
mac-vlan enable
mac-authentication
#
interface GigabitEthernet1/0/2
port link-type hybrid
port hybrid vlan 1 100 200 untagged
mac-vlan enable
mac-authentication
#
interface GigabitEthernet1/0/3
port access vlan 100
#
interface GigabitEthernet1/0/4
port access vlan 200
#
interface GigabitEthernet1/0/5
```

```
port access vlan 300
#
radius scheme 2000
primary authentication 1.1.3.1 1812
primary accounting 1.1.3.2 1813
key authentication simple abc
key accounting simple abc
user-name-format without-domain
#
domain bbb
authentication default radius-scheme 2000
authorization default radius-scheme 2000
accounting default radius-scheme 2000
#
domain system
#
domain default enable bbb
#
```

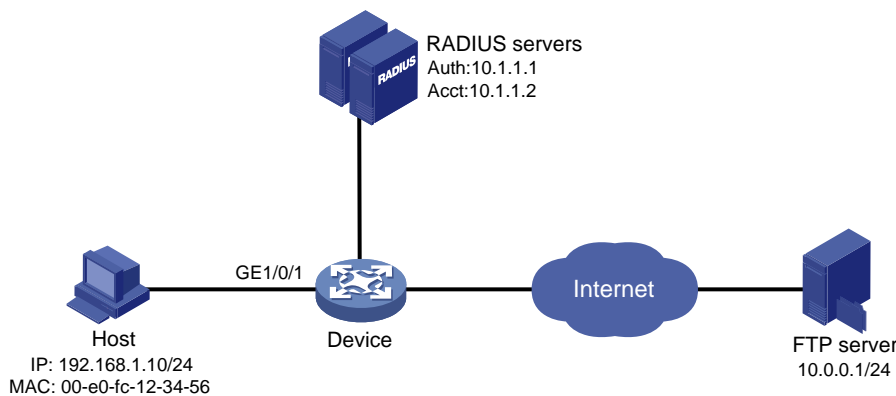
# 例:MAC 認証用の ACL 割り当ての設定

## ネットワーク構成

図 7 に示すように、次の要件を満たすようにデバイスを設定します。

- RADIUS サーバーを使用して、ユーザーの認証、認可、アカウンティングを実行します。
- GigabitEthernet 1/0/1 で MAC 認証を実行して、インターネットアクセスを制御します。
- MAC 認証ユーザーには MAC ベースのユーザーカウントを使用します。各 MAC アドレスは、ハイフン付きの 16 進数表記で、文字は小文字です。
- ACL を使用して、認証済みユーザーが 10.0.0.1 の FTP サーバーにアクセスすることを拒否します。

図 7 ネットワーク図



## 操作方法

RADIUS サーバーとアクセスデバイスが相互に到達できることを確認します。

1. 10.0.0.1 宛てのパケットを拒否するように ACL 3000 を設定します。  
<Device>System-view  
[Device]acl advanced 3000  
[Device-acl-ipv4-adv-3000] rule 0 deny ip destination 10.0.0.1 0  
[Device-acl-ipv4-adv-3000] quit
2. デバイスに RADIUS ベースの MAC 認証を設定します。  
#RADIUS スキームを設定します。  
[Device] radius scheme 2000  
[Device-radius-2000] primary authentication 10.1.1.1 1812  
[Device-radius-2000] primary accounting 10.1.1.2 1813  
[Device-radius-2000] key authentication simple abc  
[Device-radius-2000] key accounting simple abc  
[Device-radius-2000] user-name-format without-domain  
[Device-radius-2000] quit  
#RADIUS スキームを ISP ドメインに適用して、認証、認可、およびアカウンティングを行います。  
[Device] domain bbb  
[Device-isp-bbb] authentication default radius-scheme 2000  
[Device-isp-bbb] authorization default radius-scheme 2000  
[Device-isp-bbb] accounting default radius-scheme 2000  
[Device-isp-bbb] quit  
#MAC 認証用の ISP ドメインを指定します。  
[Device]mac-authentication domain bbb



#MAC ベースのユーザーカウントを使用するようにデバイスを設定します。各 MAC アドレスは、ハイフンを含む 16 進表記で、文字は小文字です。

```
[Device]mac-authentication user-name-format mac-address with-hyphen lowercase
```

# GigabitEthernet 1/0/1 で MAC 認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] mac-authentication
```

```
[Device-GigabitEthernet1/0/1] quit
```

#MAC 認証をグローバルにイネーブルにします。

```
[Device]mac-authentication
```

### 3. RADIUS サーバーを設定します。

#00-e0-fc-12-34-56 のユーザーカウントを、ユーザー名とパスワードの両方として各 RADIUS サーバーに追加します(詳細は省略)。

#ユーザーカウントの認可 ACLとして ACL 3000 を指定します(詳細は省略します)。

## 設定の確認

#MAC 認証の設定を確認します。

```
[Device] display mac-authentication
```

Global MAC authentication parameters:

MAC authentication : Enabled

Username format : MAC address in lowercase(xx-xx-xx-xx-xx-xx)

Username : mac

Password : Not configured

Offline detect period : 300 s

Quiet period : 60 s

Server timeout : 100 s

Reauth period : 3600 s

Authentication domain : bbb

Online MAC-auth users : 1

Silent MAC users:

MAC address	VLAN ID	From port	Port index
-------------	---------	-----------	------------

GigabitEthernet 1/0/1 is link-up

MAC authentication : Enabled

Carry User-IP : Disabled

Authentication domain : Not configured

Auth-delay timer : Disabled

Periodic reauth : Disabled

Re-auth server-unreachable : Logoff

Guest VLAN : Not configured

Guest VLAN auth-period : 30 s

Critical VLAN : Not configured

Critical voice VLAN : Disabled

Host mode : Single VLAN

Offline detection : Enabled

Authentication order : Default

Guest VSI : Not configured

Guest VSI auth-period : 30 s

Critical VSI : Not configured

```

Auto-tag feature      : Disabled
VLAN tag configuration ignoring : Disabled
Max online users      : 4294967295
Authentication attempts : successful 1, failed 0
Current online users  : 1
  MAC address   Auth state
  00e0-fc12-3456  Authenticated

```

#ホストから FTP サーバーに ping を実行できないことを確認します。

```
C:\>ping 10.0.0.1
```

Pinging 10.0.0.1 with 32 bytes of data:

```

Request timed out.
Request timed out.
Request timed out.
Request timed out.

```

Ping statistics for 10.0.0.1:

```
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

GigabitEthernet 1/0/1 出力には、FTP サーバーへのアクセスを拒否するために ACL 3000 が割り当てられていることが示されています。

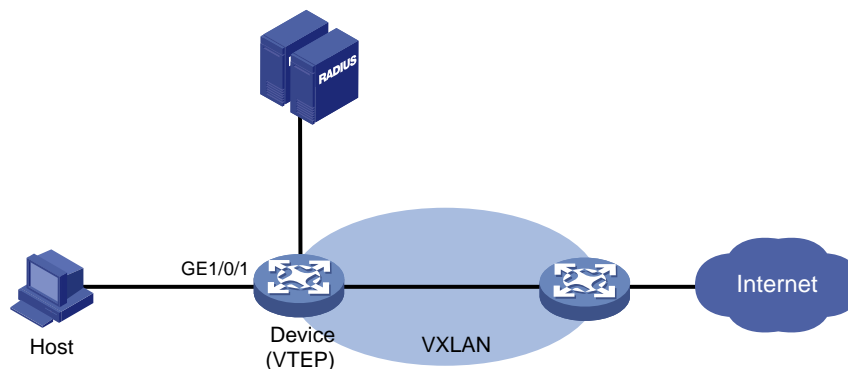
## 例:MAC 認証認可 VSI 割り当ての設定

### ネットワーク構成

図 8 に示すように、次の要件を満たすようにデバイスを設定します。

- RADIUS サーバーを使用して、ユーザーの認証、認可、アカウントングを実行します。
- GigabitEthernet 1/0/1 で MAC 認証を実行して、インターネットアクセスを制御します。
- ホストが MAC 認証を通過したときに VSI BBB をホストに割り当てるように RADIUS サーバーを設定します。
- ISP ドメイン 2000 内のすべてのユーザーを認証します。
- MAC 認証ユーザーには MAC ベースのユーザーカウントを使用します。各 MAC アドレスは、ハイフン付きの 16 進数表記で、文字は小文字です。

図 8 ネットワーク図



## 操作方法

RADIUS サーバーとアクセスデバイスが相互に到達できることを確認します。

### 1. RADIUS サーバーを設定します。

#認証、許可、およびアカウントサービスを提供するように RADIUS サーバーを設定します(詳細は省略)。

#RADIUS サーバーにユーザー名とパスワードに **d4-85-64-be-c6-3e** を使用してユーザーカウントを追加します(詳細は省略)。

#ユーザーアカウントの認証 VSI として VSI bbb を指定します。(詳細は省略。)

---

#### 注:

認証および認可に H3C ADCAM サーバーを使用する場合は、サーバー上で VSA を設定します。サーバーはこれらの VSA をデバイスに割り当てます。デバイス上で VSA を設定する必要はありません。

---

### 2. デバイスに RADIUS ベースの MAC 認証を設定します。

#RADIUS スキームを設定します。

```
<Device> system-view
[Device] radius scheme bbb
[Device-radius-bbb] primary authentication 10.1.1.1
[Device-radius-bbb] primary accounting 10.1.1.2
[Device-radius-bbb] key authentication simple bbb
[Device-radius-bbb] key accounting simple bbb
[Device-radius-bbb] user-name-format without-domain
[Device-radius-bbb] quit
```

#認証、許可、およびアカウントのために、RADIUS スキームを ISP ドメイン 2000 に適用します。

```
[Device] domain 2000
[Device-isp-2000] authentication lan-access radius-scheme bbb
[Device-isp-2000] authorization lan-access radius-scheme bbb
[Device-isp-2000] accounting lan-access radius-scheme bbb
[Device-isp-2000] quit
```

# GigabitEthernet 1/0/1 で MAC 認証を有効にします。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication
```

#GigabitEthernet 1/0/1 でダイナミックイーサネットサービスインスタンスの MAC 一致モードをイネーブルにします。

```
[Device-GigabitEthernet1/0/1] mac-based ac
[Device-GigabitEthernet1/0/1] quit
```

#L2VPN をイネーブルにします。

```
[Device] l2vpn enable
```

#bbb という名前の VSI と、関連する VXLAN を作成します。

```
[Device] vsi bbb
[Device-vsi-bbb] vxlan 5
[Device-vsi-bbb-vxlan-5] quit
```

#MAC 認証用の ISP ドメインを指定します。

```
[Device] mac-authentication domain 2000
```

#MAC ベースのユーザーカウントを使用するようにデバイスを設定します。各 MAC アドレスは、ハイフンを含む 16 進表記で、文字は小文字です。

```
[Device] mac-authentication user-name-format mac-address with-hyphen lowercase
```

#MAC 認証をグローバルにイネーブルにします。

[Device] mac-authentication

## 設定の確認

#ユーザーが認証に合格した後に、VSI **bbb** が MAC 認証ユーザーに割り当てられることを確認します。

[Device] display mac-authentication connection

Total connections: 1

Slot ID: 1

User MAC address: d485-64be-c63e

Access interface: GigabitEthernet 1/0/1

Username: d4-85-64-be-c6-3e

User access state: Successful

Authentication domain: 2000

IPv4 address: 192.168.1.1

IPv6 address: 2000:0:0:0:1:2345:6789:abcd

Initial VLAN: 1

Authorization untagged VLAN: N/A

Authorization tagged VLAN: N/A

Authorization VSI: bbb

Authorization ACL ID: N/A

Authorization user profile: N/A

Authorization CAR: N/A

Authorization URL: N/A

Termination action: N/A

Session timeout period: N/A

Online from: 2016/06/13 09:06:37

Online duration: 0h 0m 35s

# MAC アドレス d485-64be-c63e に対して動的 AC が作成されていることを確認します。。

[Device] display l2vpn forwarding ac verbose

VSI Name: bbb

Interface: GE1/0/1 Service Instance: 1

Link ID : 0

Access Mode : VLAN

Encapsulation: untagged

Type : Dynamic (MAC-based)

MAC address : d485-64be-c63e

# ポータル認証の設定

## ポータル認証について

ポータル認証は、ネットワークへのユーザーアクセスを制御します。ポータルは、ユーザーがポータル認証ページで入力したユーザー名とパスワードによってユーザーを認証します。通常、ポータル認証はアクセスレイヤーと重要なデータエントリに配置されます。

ポータル対応のネットワークでは、ユーザーはポータル Web サーバーによって提供される認証 Web サイトにアクセスすることによって、ポータル認証をアクティブに開始できます。または、他の Web サイトにアクセスすると、認証のためにポータル認証ページにリダイレクトされます。

ポータル認証は、レイヤー3 インターフェースだけでサポートされます。

このデバイスは、Portal 1.0、Portal 2.0、および Portal 3.0をサポートします。

## ポータル認証の利点

ポータル認証には、次の利点があります。

- クライアントソフトウェアをインストールせずに、ユーザーが Web ブラウザを使用して認証を実行できるようにします。
- ISP に多様な管理オプションと拡張機能を提供します。たとえば、ISP は、認証ページに広告を掲載したり、コミュニティサービスを提供したり、情報を公開したりできます。
- 複数の認証モードをサポートします。たとえば、再 DHCP 認証は柔軟なアドレス割り当て方式を実装し、パブリック IP アドレスを保存します。クロスサブネット認証は、アクセスデバイスとは異なるサブネットに存在するユーザーを認証できます。

## 拡張ポータル機能

パッチ適用およびウイルス対策ポリシーを強制することにより、拡張ポータル機能は、ホストがウイルスから保護するのに役立ちます。ポータルは、次の拡張機能をサポートしています：

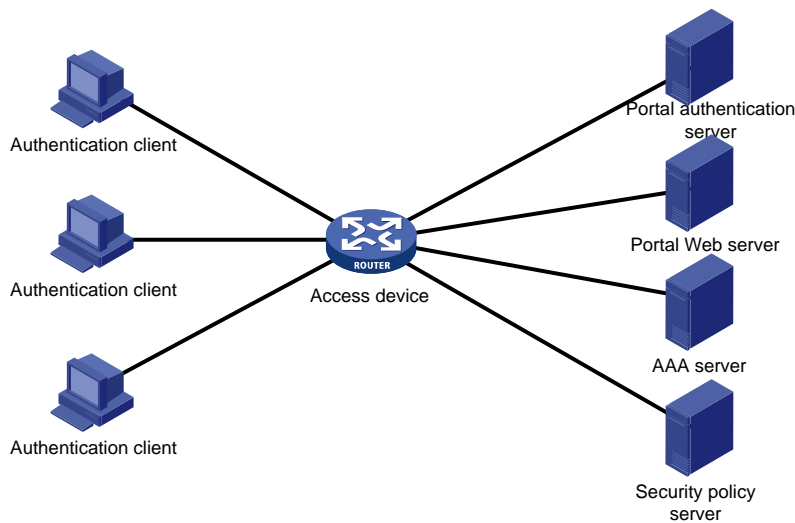
- **セキュリティチェック:** 認証後に、ユーザーホストがアンチウイルスソフトウェア、ウイルス定義ファイル、不正なソフトウェア、およびオペレーティングシステムのパッチをインストールしているかどうかを検出します。
- **リソースアクセス制限:** 認証されたユーザーが、ウイルスサーバーやパッチサーバーなどの特定のネットワークリソースにアクセスできるようにします。ユーザーは、セキュリティチェックに合格すると、より多くのネットワークリソースにアクセスできます。

セキュリティチェックは、H3C IMC セキュリティポリシーサーバーおよび iNode クライアントと連携する必要があります。

## ポータルシステム

一般的なポータルシステムは、認証クライアント、アクセスデバイス、ポータル認証サーバー、ポータル Web サーバー、AAA サーバー、およびセキュリティポリシーサーバーの基本コンポーネントで構成されます。

図 1 ポータルシステム



## 認証クライアント

認証クライアントは、HTTP/HTTPS を実行する Web ブラウザ、またはポータルクライアントを実行するユーザーホストです。ユーザーホストのセキュリティチェックは、ポータルクライアントとセキュリティポリシーサーバー間の対話によって実装されます。サポートされるのは H3C iNode クライアントのみです。

## アクセスデバイス

アクセスデバイスは、アクセスサービスを提供します。アクセスデバイスには、次の機能があります。

- 非認証ユーザーのすべての HTTP 要求または HTTPS 要求をポータル Web サーバーにリダイレクトします。
- ポータル認証サーバーおよび AAA サーバーと対話して、認証、認可、アカウンティングを完了します。
- ポータル認証に合格したユーザーが、許可されたネットワークリソースにアクセスできるようにします。

## ポータルサーバー

ポータルサーバーとは、ポータル認証サーバーとポータル Web サーバーの総称です。

ポータル Web サーバーは、Web 認証ページを認証クライアントにプッシュし、ユーザー認証情報(ユーザー名とパスワード)をポータル認証サーバーに転送します。ポータル認証サーバーは、認証クライアントから認証要求を受信し、アクセスデバイスと対話してユーザーを認証します。ポータル Web サーバーは通常、ポータル認証サーバーと統合され、独立したサーバーにすることもできます。

## AAA サーバー

AAA サーバーはアクセスデバイスと対話して、ポータルユーザーの認証、認可、アカウンティングを実装します。ポータルシステムでは、RADIUS サーバーはポータルユーザーの認証、認可、アカウンティングを実行でき、LDAP サーバーはポータルユーザーの認証を実行できます。

## セキュリティポリシーサーバー

セキュリティポリシーサーバーは、ユーザーのセキュリティチェックおよび認可のために、ポータルクライアントおよびアクセスデバイスと対話します。ポータルクライアントを実行するホストのみが、セキュリティポリシーサーバーと対話します。

## リモートポータルサーバーを使用したポータル認証

ポータルシステムのコンポーネントは、次のように相互作用します。

1. 認証されていないユーザーは、Web ブラウザを介してインターネット Web サイトにアクセスすることによって認証を開始します。HTTP または HTTPS 要求を受信すると、アクセスデバイスはそれをポータル Web サーバーによって提供される Web 認証ページにリダイレクトします。ユーザーは、認証 Web サイトにアクセスしてログインすることもできます。ユーザーは、拡張ポータル機能のために H3C iNode クライアントを介してログインする必要があります。
2. ユーザーは、認証ページダイアログボックスに認証情報を入力し、その情報を送信します。ポータル Web サーバーは、その情報をポータル認証サーバーに転送します。ポータル認証サーバーは、その情報を処理してアクセスデバイスに転送します。
3. アクセスデバイスは AAA サーバーと対話して、ユーザーの認証、認可、アカウントリングを実装します。
4. セキュリティポリシーがユーザーに適用されていない場合、アクセスデバイスは認証されたユーザーがネットワークにアクセスすることを許可します。

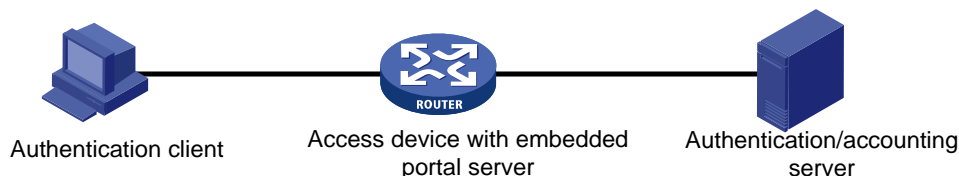
セキュリティポリシーがユーザーに適用されている場合、ポータルクライアント、アクセスデバイスおよびセキュリティポリシーサーバーは相互作用してユーザーホストをチェックします。ユーザーがセキュリティチェックに合格すると、セキュリティポリシーサーバーは、チェック結果に基づいてユーザーがリソースにアクセスすることを許可します。

## ローカルポータルサービス

### システムコンポーネント

図 2 に示すように、ローカルポータルシステムは、認証クライアント、アクセスデバイス、および AAA サーバーで構成されます。アクセスデバイスは、ポータル Web サーバーおよびポータル認証サーバーの両方として機能し、認証クライアントにローカルポータル Web サービスを提供します。認証クライアントには Web ブラウザだけを使用でき、ポータルクライアントを実行するユーザーホストは使用できません。したがって、拡張ポータル機能はサポートされず、セキュリティポリシーサーバーは必要ありません。

図 2 システムコンポーネント



### ポータルページのカスタマイズ

ローカルポータル Web サービスを提供するには、デバイスがユーザーにプッシュする認証ページのセットをカスタマイズする必要があります。複数の認証ページのセットをカスタマイズし、ページの各セットを.zip ファイルに圧縮し、圧縮されたファイルをデバイスのストレージメディアにアップロードできます。デバイスでは、**default-logon-page** コマンドを使用して、いずれかのファイルをデフォルトの認証ページファイルとして指定する必要があります。

認証ページのカスタマイズの詳細については、「認証ページのカスタマイズ」を参照してください。

## ポータル認証モード

ポータル認証には、直接認証、再 DHCP 認証、およびクロスサブネット認証の 3 つのモードがあります。直接認証および再 DHCP 認証では、認証クライアントとアクセスデバイスの間にレイヤー 3 転送デバイスは存在しません。クロスサブネット認証では、認証クライアントとアクセスデバイスの間にレイヤー 3 転送デバイスが存在できます。

## 直接認証

ユーザーは、パブリック IP アドレスを手動で構成するか、DHCP を介してパブリック IP アドレスを取得します。認証の前に、ユーザーはポータル Web サーバーおよび事前定義された認証不要の Web サイトにのみアクセスできます。認証に合格すると、ユーザーは他のネットワークリソースにアクセスできます。直接認証のプロセスは、再 DHCP 認証のプロセスよりも単純です。

## Re-DHCP 認証

ユーザーが認証を通過する前に、DHCP は IP アドレス(プライベート IP アドレス)をユーザーに割り当てます。ユーザーは、ポータル Web サーバーおよび事前定義された認証不要の Web サイトにのみアクセスできます。ユーザーが認証を通過すると、DHCP は IP アドレス(パブリック IP アドレス)をユーザーに再割り当てします。これにより、ユーザーは他のネットワークリソースにアクセスできるようになります。認証に失敗したユーザーには、パブリック IP アドレスは割り当てられません。DHCP の再認証では、パブリック IP アドレスが保存されます。たとえば、ISP は、ブロードバンドユーザーが住宅用コミュニティネットワークを越えてネットワークにアクセスする場合にのみ、パブリック IP アドレスをブロードバンドユーザーに割り当てることができます。

再 DHCP 認証をサポートしているのは、H3C iNode クライアントだけです。IPv6 ポータル認証は、再 DHCP 認証モードをサポートしていません。

## サブネット間認証

クロスサブネット認証は直接認証と似ていますが、認証クライアントとアクセスデバイスの間にレイヤー3 転送デバイスが存在できる点が異なります。

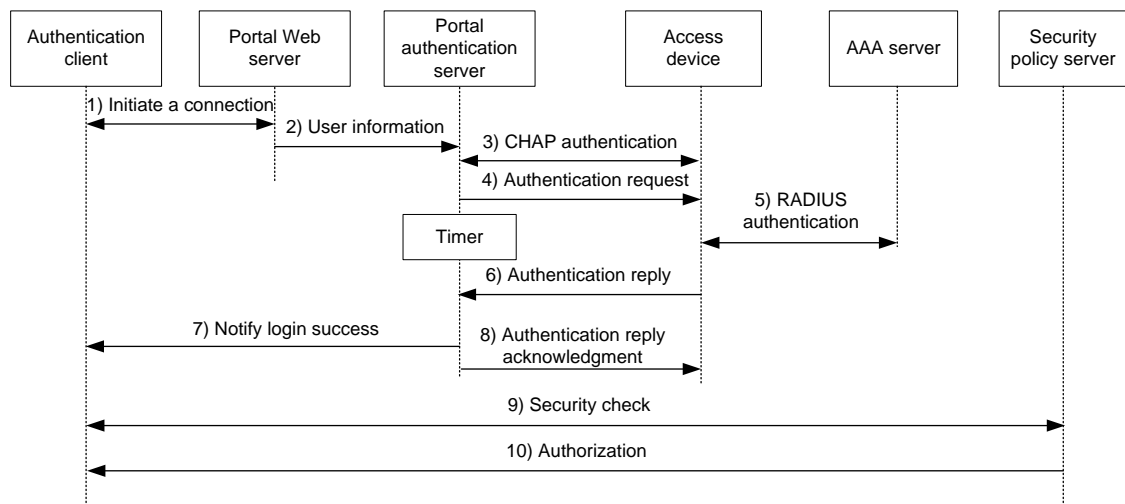
直接認証、再 DHCP 認証、およびサブネット間認証では、ユーザーの IP アドレスによってユーザーが独自に識別されます。ユーザーが認証を通過すると、アクセスデバイスはユーザーの IP アドレスに基づいてユーザーの ACL を生成し、ユーザーからのパケットの転送を制御します。直接認証および再 DHCP 認証では、認証クライアントとアクセスデバイスの間にレイヤー3 転送デバイスが存在しないため、アクセスデバイスはユーザーの MAC アドレスを学習できます。アクセスデバイスは、学習した MAC アドレスを使用して、パケット転送を制御する機能を強化できます。

# ポータル認証プロセス

直接認証とサブネット間認証は同じ認証プロセスを共有します。再 DHCP 認証には 2 つのアドレス割り当て手順があるため、異なるプロセスがあります。

## 直接認証/サブネット間認証プロセス(CHAP/PAP 認証を使用)

図 3 直接認証/サブネット間認証プロセス





直接/サブネット間認証プロセスは次のとおりです。

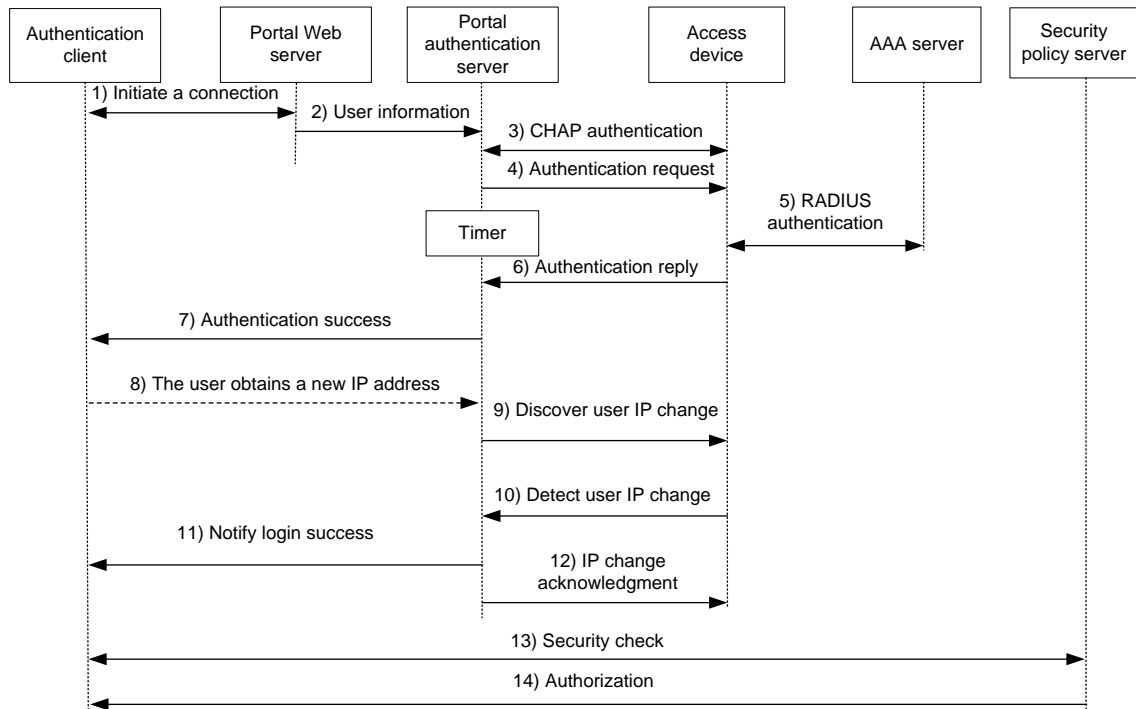
1. ポータルユーザーが HTTP または HTTPS を使用してインターネットにアクセスし、HTTP または HTTPS パケットがアクセスデバイスに到達します。
  - パケットがポータルフリールールに一致する場合、アクセスデバイスはパケットの通過を許可します。
  - パケットがどのポータルフリー規則にも一致しない場合、アクセスデバイスはパケットをポータル Web サーバーにリダイレクトします。ポータル Web サーバーは、ユーザーがユーザー名とパスワードを入力できるように、Web 認証ページをユーザーにプッシュします。
2. ポータル Web サーバーは、ユーザー認証情報をポータル認証サーバーに送信します。
3. ポータル認証サーバーとアクセスデバイスは CHAP メッセージを交換します。PAP 認証の場合、この手順はスキップされます。ポータル認証サーバーは、使用する方式(CHAP または PAP)を決定します。
4. ポータル認証サーバーは、ユーザー名とパスワードを認証要求パケットに追加して、アクセスデバイスに送信します。一方、ポータル認証サーバーは、認証応答パケットを待機するタイマーを開始します。
5. アクセスデバイスと RADIUS サーバーは、RADIUS パケットを交換します。
6. アクセスデバイスは、認証応答パケットをポータル認証サーバーに送信して、認証の成功または失敗を通知します。
7. ポータル認証サーバーは、認証の成功または失敗のパケットをクライアントに送信します。
8. 認証が成功した場合、ポータル認証サーバーは認証応答確認パケットをアクセスデバイスに送信します。

クライアントが iNode クライアントの場合、認証プロセスには拡張ポータル機能のステップ 9 とステップ 10 が含まれます。それ以外の場合、認証プロセスは完了します。

9. クライアントとセキュリティポリシーサーバーは、セキュリティチェック情報を交換します。セキュリティポリシーサーバーは、ユーザーホストがアンチウイルスソフトウェア、ウイルス定義ファイル、不正なソフトウェア、およびオペレーティングシステムのパッチをインストールしているかどうかを検出します。
10. セキュリティポリシーサーバーは、チェック結果に基づいて、ユーザーが特定のネットワークリソースにアクセスすることを許可します。アクセスデバイスは、許可情報を保存し、それを使用してユーザーのアクセスを制御します。

## 再 DHCP 認証プロセス(CHAP/PAP 認証を使用)

図 4 Re-DHCP 認証プロセス



DHCP 再認証プロセスは次のとおりです。

ステップ 1～7 は、直接認証/サブネット間認証プロセスのステップと同じです。

8. 認証成功パケットを受信した後、クライアントは DHCP を介してパブリック IP アドレスを取得します。次に、クライアントはポータル認証サーバーにパブリック IP アドレスがあることを通知します。
9. ポータル認証サーバーは、クライアントがパブリック IP アドレスを取得したことをアクセスデバイスに通知します。
10. アクセスデバイスは DHCP を介してクライアントの IP 変更を検出し、クライアント IP の IP 変更を検出したことをポータル認証サーバーに通知します。
11. クライアントおよびアクセスデバイスによって送信された IP 変更通知パケットを受信した後、ポータル認証サーバーはログインの成功をクライアントに通知します。
12. ポータル認証サーバーは、IP 変更確認応答パケットをアクセスデバイスに送信します。

ステップ 13 とステップ 14 は、拡張ポータル機能用です。

13. クライアントとセキュリティポリシーサーバーは、セキュリティチェック情報を交換します。セキュリティポリシーサーバーは、ユーザーホストがアンチウイルスソフトウェア、ウイルス定義ファイル、不正なソフトウェア、およびオペレーティングシステムのパッチをインストールしているかどうかを検出します。
14. セキュリティポリシーサーバーは、チェック結果に基づいて、ユーザーが特定のネットワークリソースにアクセスすることを許可します。アクセスデバイスは、許可情報を保存し、それを使用してユーザーのアクセスを制御します。

## EAP のポータルサポート

EAP をサポートするポータル認証を使用するには、ポータル認証サーバーおよびクライアントが H3C IMC ポータルサーバーおよび H3C iNode ポータルクライアントである必要があります。ローカルポータル認証は EAP 認証をサポートしていません。

ユーザー名およびパスワードベースの認証と比較して、デジタル証明書ベースの認証はより高いセキュリティを保證します。

Extensible Authentication Protocol(EAP;拡張認証プロトコル)は、EAP-TLS など、いくつかのデジタル証明書ベースの認証方式をサポートしています。ポータル認証は、EAP と連携して、デジタル証明書ベースのユーザー認証を実装できます。

図 5 EAP のポータルサポート作業フロー図

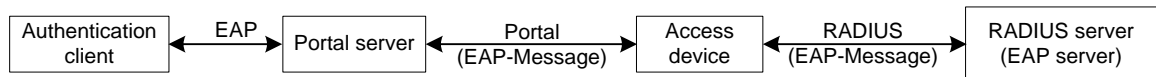


図 5 示すように、認証クライアントとポータル認証サーバーは EAP 認証パケットを交換します。ポータル認証サーバーとアクセスデバイスは、EAP-Message アトリビュートを伝送するポータル認証パケットを交換します。アクセスデバイスと RADIUS サーバーは、EAP-Message アトリビュートを伝送する RADIUS パケットを交換します。EAP サーバー機能をサポートする RADIUS サーバーは、EAP-Message アトリビュートにカプセル化された EAP パケットを処理し、EAP 認証結果を提供します。

アクセスデバイスは、ポータル認証サーバーと RADIUS サーバーの間で EAP-Message アトリビュートを処理せず、転送するだけです。そのため、アクセスデバイスでは、EAP 認証をサポートするための追加設定は必要ありません。

## ポータルフィルタルール

アクセスデバイスは、ポータルフィルタリングルールを使用して、ユーザートラフィック転送を制御します。

ポータルユーザーの設定および認証ステータスに基づいて、デバイスは次のカテゴリのポータルフィルタリングルールを生成します。

- 第 1 カテゴリ:このルールでは、ポータル Web サーバー宛てのユーザーパケットと、ポータルフリールールに一致するパケットの通過が許可されます。
- 2 番目のカテゴリ:ACL が許可されていない認証済みユーザーの場合、ルールにより、ユーザーは任意の宛先ネットワークリソースにアクセスできます。ACL が許可されている認証済みユーザーの場合、ルールにより、ユーザーは ACL で許可されたリソースにアクセスできます。デバイスは、ユーザーがオンラインになったときにルールを追加し、ユーザーがオフラインになったときにルールを削除します。

デバイスは、基本 ACL(ACL 2000~ACL 2999)および拡張 ACL(ACL 3000~ACL 3999)をサポートします。ポータルユーザーが認証に合格した後にオンラインになるようにするには、ユーザーに割り当てられた認可 ACL のルールに送信元 IP アドレスまたは送信元 MAC アドレスが含まれていないことを確認します。

- 3 番目のカテゴリ:このルールは、認証されていないユーザーからのすべての HTTP または HTTPS 要求をポータル Web サーバーにリダイレクトします。
- 4 番目のカテゴリ:直接認証およびサブネット間認証の場合、ルールはすべてのユーザーパケットの通過を禁止します。再 DHCP 認証の場合、デバイスはプライベート送信元アドレスを持つユーザーパケットの通過を禁止します。

ユーザーパケットを受信した後、デバイスはパケットを第 1 カテゴリから第 4 カテゴリまでのフィルタリングルールと比較します。パケットがルールと一致すると、一致プロセスが完了します。

## 制約事項および注意事項:ポータル設定

ポータル認証は、レイヤー3 インターフェースだけでサポートされます。

Web 経由のポータル認証では、ユーザーのセキュリティチェックはサポートされていません。セキュリティチェックを実装するには、クライアントが H3C iNode クライアントである必要があります。

ポータル認証は、Web クライアントまたは H3C iNode クライアントによって開始された NAT トラバーサルをサポートします。ポータルクライアントがプライベートネットワーク上にあり、ポータルサーバーがパブリックネットワーク上にある場合は、NAT トラバーサルを構成する必要があります。

ポータル認証に合格した後にポータルユーザーがオンラインになるようにするには、ポータルユーザーに割り当てられた authorization ACL に、送信元 IP または MAC アドレスで指定されたルールがないことを確認します。

## ポータル認証タスクの概要

ポータル認証を設定するには、次の作業を実行します。

1. 必要に応じてリモートまたはローカルのポータルサービスを構成する
  - リモートポータルサービスを構成する
    - リモートポータル認証サーバーの構成
    - ポータル Web サーバーの構成
  - ローカルポータルサービスを構成する
    - ローカルポータルサービス機能の構成
    - ポータル Web サーバーの構成
2. ポータル認証の使用可能化およびポータル Web サーバーの指定
  - インターフェースでのポータル認証の有効化
  - インターフェースでのポータル Web サーバーの指定
3. (省略可能) 事前認証 IP アドレスプールの指定
4. (省略可能) ポータル認証ドメインの指定
5. (省略可能) ポータルユーザーアクセスの制御
  - ポータルフリールールの構成
  - 認証元サブネットの構成
  - 認証先サブネットの設定
  - ポータルユーザーの最大数の設定
  - ポータル認証情報の厳密なチェックを有効にする
  - DHCP によって割り当てられた IP アドレスを持つユーザーのみがポータル認証を通過できるようにする
  - ポータル認証のための Web プロキシのサポートの構成
  - ポータルのローミングを有効にする
  - ポータルのフェイル許可機能の構成
6. (省略可能) ポータル検出機能の構成
  - ポータル ユーザーのオンライン検出の構成
  - ポータル認証サーバー検出の構成
  - ポータル Web サーバー検出の構成
  - ポータルユーザー同期の構成
7. (任意) ポータルパケットおよび RADIUS パケットのアトリビュートの設定
  - ポータルパケット属性の構成

- ポータルパケットの BAS-IP または BAS-IPv6 アトリビュートを設定し、デバイス ID を指定できます。
- RADIUS パケットの属性の構成  
NAS-Port-Id アトリビュートフォーマットを設定し、NAS-ID プロファイルをインターフェースに適用できます。
8. (省略可能) ポータルクライアントのルール ARP または ND エントリ機能の無効化
  9. (省略可能)ポータルユーザーのオンラインおよびオフライン関連機能の構成
    - オンラインポータルユーザーのログアウト
    - ポータルユーザーのログイン/ログアウトログの有効化
  10. (省略可能) Web リダイレクトの構成

## ポータル認証の前提条件

ポータル機能は、ユーザーID 認証とセキュリティチェックのためのソリューションを提供します。ユーザーID 認証を完了するには、ポータルが RADIUS と連携する必要があります。

ポータルを構成する前に、次のタスクを完了する必要があります。

- ポータル認証サーバー、ポータル Web サーバー、および RADIUS サーバーが正しくインストールされ、構成されている。
- re-DHCP ポータル認証モードを使用するには、アクセスデバイスで DHCP リレーエージェントがイネーブルになっていて、DHCP サーバーが正しくインストールおよび設定されていることを確認します。
- ポータルクライアント、アクセスデバイス、およびサーバーは相互に到達できます。
- リモート RADIUS サーバーを使用するには、RADIUS サーバーでユーザー名とパスワードを設定し、アクセスデバイスで RADIUS クライアントを設定します。RADIUS クライアント設定の詳細については、「AAA の設定」を参照してください。
- 拡張ポータル機能を実装するには、CAMS EAD または IMC EAD をインストールして設定します。アクセスデバイスに設定されている ACL が、セキュリティポリシーサーバーの隔離 ACL およびセキュリティ ACL に対応していることを確認します。アクセスデバイスのセキュリティポリシー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。セキュリティポリシーサーバーのインストールおよび設定については、『CAMS EAD Security Policy Component User Manual』または IMC EAD Security Policy Help を参照してください。

## リモートポータル認証サーバーの設定

### リモートポータル認証サーバーの設定について

ポータル認証がイネーブルの場合、デバイスは、パケットの送信元 IP アドレスおよび VPN 情報に従って、受信したポータル要求パケットのポータル認証サーバーを検索します。

- 一致するポータル認証サーバーが見つかり、デバイスはパケットを有効と見なし、認証応答パケットをポータル認証サーバーに送信します。ユーザーがデバイスにログインすると、ユーザーは必要に応じてポータル認証サーバーと対話します。
- 一致するポータル認証サーバーが見つからない場合、デバイスはパケットをドロップします。

### 制約事項とガイドライン

使用中のポータル認証サーバーを削除しないでください。削除しないと、そのサーバーによって認証されたユーザーは正しくログアウトできません。

## 手順

1. システムビューを開始します。  
**system-view**
2. ポータル認証サーバーを作成し、そのビューを入力します。  
**portal server server-name**  
複数のポータル認証サーバーを作成できます。
3. ポータル認証サーバーの IP アドレスを指定します。  
IPv4 の場合:  
**ip ipv4-address [ vpn-instance ipv4-vpn-instance-name ] [ key { cipher | simple } string ]**  
IPv6 の場合:  
**ipv6 ipv6-address [ vpn-instance ipv6-vpn-instance-name ] [ key { cipher | simple } string ]**
4. (任意)要求されていないポータルパケットをポータル認証サーバーに送信するためにデバイスが使用する宛先 UDP ポート番号を設定します。  
**port port-number**  
デフォルトでは、UDP ポート番号は 50100 です。  
このポート番号は、ポータル認証サーバーで指定されたリスニングポート番号と同じである必要があります。
5. (任意)ポータル認証サーバータイプを指定します。  
**server-type { cmcc | imc }**  
デフォルトでは、ポータル認証サーバータイプは IMC です。  
指定されたサーバータイプは、実際に使用されるポータル認証サーバーのタイプと同じでなければなりません。
6. (任意)ポータル認証サーバーに定期的に登録するようにデバイスを設定します。  
**server-register [ interval interval-value ]**  
デフォルトでは、デバイスはポータル認証サーバーに登録されません。

# ポータルWebサーバーを構成する

## ポータル Web サーバータスクの概要

ポータル Web サーバーを構成するには、次のタスクを実行します。

1. ポータル Web サーバーの基本パラメーターを構成する
2. (省略可能) キャプティブ バイパス機能を有効にする
3. (省略可能) URL リダイレクトの一致ルールの構成

## ポータル Web サーバーの基本パラメーターを構成する

1. システムビューを開始します。  
**system-view**
2. ポータル Web サーバーを作成し、そのビューを入力します。  
**portal web-server server-name**  
複数のポータル Web サーバーを作成できます。

3. ポータル Web サーバーが属する VPN インスタンスを指定します。

**vpn-instance** *vpn-instance-name*

既定では、ポータル Web サーバーはパブリックネットワークに属しています。

4. ポータル Web サーバーの URL を指定します。

**url** *url-string*

デフォルトでは、ポータル Web サーバーの URL は指定されていません。

ユーザーの HTTPS 要求をポータル Web サーバーの URL にリダイレクトするには、HTTPS リダイレクトのリスニングポート番号を指定する必要があります。HTTPS リダイレクトのリスニングポート番号の指定の詳細は、『Layer 3 IP Services Configuration Guide』の「HTTP redirect」を参照してください。

5. デバイスが URL をユーザーにリダイレクトするときに URL で伝送されるパラメーターを設定します。

**url-parameter** *param-name* { **original-url** | **source-address** | **source-mac** [ **encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string* ] | **value** *expression* }

デフォルトでは、リダイレクション URL パラメーターは設定されていません。

6. (省略可能)ポータル Web サーバーの種類を指定します。

**server-type** { **cmcc** | **imc** }

既定では、ポータル Web サーバーの種類は IMC です。

この設定は、リモートポータルサービスだけに適用されます。

指定されたサーバータイプは、実際に使用されるポータル Web サーバーのタイプと同じでなければなりません。

## キャプティブバイパス機能のイネーブル化

### キャプティブバイパス機能について

デフォルトでは、iOS デバイスおよび一部の Android デバイスがネットワークに接続されると、デバイスによってポータル認証ページが自動的にプッシュされます。キャプティブバイパス機能を使用すると、iOS デバイスおよび一部の Android デバイスがブラウザを使用してインターネットにアクセスする場合にのみ、デバイスによってポータル認証ページがプッシュされます。

### 手順

1. システムビューを開始します。

**system-view**

2. ポータル Web サーバービューを入力してください。

**portal web-server** *server-name*

3. キャプティブパス機能をイネーブルにします。

**captive-bypass** **enable**

デフォルトでは、キャプティブバイパス機能はディセーブルになっています。

## URL リダイレクションの一致ルールの設定

### URL リダイレクトの一致ルールについて

URL リダイレクション一致ルールは、ユーザーが要求した URL またはユーザーエージェント情報に基づいて HTTP または HTTPS 要求を照合し、一致する HTTP または HTTPS 要求を指定されたリダイレクション URL にリダイレクトします。

ポータル Web サーバーの場合、url コマンドおよび if-match コマンドを URL リダイレクト用に構成できます。url コマンドは、認証されていないユーザーからのすべての HTTP または HTTPS 要求を、認証のためにポータル Web サーバーにリダイレクトします。if-match コマンドを使用すると、特定の HTTP または HTTPS 要求を特定のリダイレクト URL にリダイレクトすることにより、柔軟な URL リダイレクトが可能になります。

## 制約事項とガイドライン

ユーザーがリダイレクション URL に正常にアクセスできるようにするには、リダイレクション URL 宛での HTTP または HTTPS 要求の通過を許可するポータルフリールールを設定します。ポータルフリールールの設定の詳細については、portal free-rule コマンドを参照してください。

url コマンドと if-match コマンドの両方が実行された場合、if-match コマンドが優先されて URL リダイレクションが実行されます。

## 手順

1. システムビューを開始します。

**system-view**

2. ポータル Web サーバービューを入力してください。

**portal web-server server-name**

3. URL リダイレクションの一致ルールを設定します。

```
if-match { original-url url-string redirect-url url-string [ url-param-encryption { aes | des } key { cipher | simple } string ] | user-agent string redirect-url url-string }
```

# ローカルポータルサービス機能を構成する

## ローカルポータルサービスについて

ローカルポータルサービスが構成されると、デバイスはポータル Web サーバーおよびポータル認証サーバーとして機能し、ユーザーに対してポータル認証を実行します。ポータル認証ページファイルは、デバイスのルートディレクトリに保存されます。

## ローカルポータルサービス機能を設定するための制約事項とガイドライン

インターフェースでローカルポータルサービスを使用するには、インターフェースに指定されたポータル Web サーバーの URL が次の要件を満たしている必要があります。

- URL 内の IP アドレスは、デバイス上のレイヤー3 インターフェース(127.0.0.1 を除く)の IP アドレスである必要があります。また、IP アドレスはポータルクライアントに到達可能である必要があります。
- URL は、/portal/ で終わる必要があります。例: **http://1.1.1.1/portal/**

デバイスは、デフォルトの認証ページファイルを提供します。カスタマイズされた認証ページを使用するには、認証ページを編集し、ファイルに圧縮してから、ファイルをデバイスにアップロードする必要があります。デバイス上で、ファイルをデフォルトの認証ページファイルとして指定します。

## 認証ページのカスタマイズ

### 認証ページのカスタマイズについて

認証ページは HTML ファイルです。ローカルポータル認証には、次の認証ページが必要です。

- ログオンページ



- ログオン成功ページ
- ログオンの失敗ページ
- オンラインページ
- システムビジーページ
- ログオフの成功ページ

認証ページが使用するページ要素(認証ページ **Logon.htm** の **back.jpg** など)を含めて、認証ページをカスタマイズする必要があります。

認証ページファイルを編集するときは、認証ページのカスタマイズ規則に従ってください。

## ファイル名の規則

メイン認証ページファイルの名前は固定されています(表 1 を参照)。メイン認証ページファイル以外のファイル名を定義できます。ファイル名およびディレクトリ名では、大文字と小文字は区別されません。

表 1 メイン認証ページのファイル名

メイン認証ページ	ファイル名
ログオンページ	logon.htm
ログオン成功ページ	logonSuccess.htm
ログオンの失敗ページ	logonFail.htm
オンラインページ ユーザーがオンラインになった後、オンライン通知のためにプッシュされます。	online.htm
システムビジーページ システムがビジー状態のとき、またはユーザーがログインプロセス中のときにプッシュされます。	busy.htm
ログオフの成功ページ	logoffSuccess.htm

## ページ要求ルール

ローカルポータル Web サーバーは、Get 要求と Post 要求のみをサポートします。

- **Get requests:** 認証ページのスタティックファイルを取得し、再帰を許可しない場合に使用します。たとえば、**Logon.htm** ファイルに **ca.htm** ファイルに対して Get アクションを実行するコンテンツが含まれている場合、**ca.htm** ファイルには **Logon.htm** ファイルへの参照を含めることはできません。
- **Post requests:** ユーザーがユーザー名とパスワードのペアを送信し、ログインおよびログアウトするときに使用されます。

## POST 要求の属性ルール

1. 認証ページのフォームを編集する場合は、次の要件に従ってください。
  - 認証ページには複数のフォームを含めることができますが、アクションが **logon.cgi** であるフォームは 1 つだけである必要があります。そうしないと、ユーザー情報をアクセスデバイスに送信できません。
  - **username** アトリビュートは **PtUser** に固定されています。**password** アトリビュートは **PtPwd** に固定されています。
  - **PtButton** 属性の値は、**Logon** または **Logoff** のいずれかで、ユーザーが要求するアクションを示します。
  - ログオン POST 要求には、**PtUser**、**PtPwd**、および **PtButton** 属性が含まれている必要があります。
  - ログオフ Post 要求には、**PtButton** 属性が含まれている必要があります。

2. 認証ページ **logon.htm** および **logonFail.htm** には、ログオン POST 要求を含める必要があります。

次の例は、page logon.htm のスクリプトの一部を示しています。

```
<form action=logon.cgi method = post >
<p>User name:<input type="text" name = "PtUser" style="width:160px;height:22px"
maxlength=64>
<p>Password :<input type="password" name = "PtPwd" style="width:160px;height:22px"
maxlength=32>
<p><input type=SUBMIT value="Logon" name = "PtButton" style="width:60px;"
onclick="form.action=form.action+location.search;">
</form>
```

3. 認証ページ **logonSuccess.htm** および **online.htm** には、ログオフ POST 要求が含まれている必要があります。

次の例は、online.htm ページのスクリプトの一部を示しています。

```
<form action=logon.cgi method = post >
<p><input type=SUBMIT value="Logoff" name="PtButton" style="width:60px;">
</form>
```

### ページファイルの圧縮と保存のルール

認証ページとそのページ要素を標準の zip ファイルに圧縮する必要があります。

- zip ファイルの名前に使用できるのは、文字、数字、および下線だけです。
- 認証ページは、zip ファイルのルートディレクトリに配置する必要があります。
- Zip ファイルは、FTP または TFTP を使用してデバイスに転送でき、デバイスのルートディレクトリに保存する必要があります。

デバイス上の zip ファイルの例:

```
<Sysname> dir
```

```
Directory of flash:
```

```
 1  -rw-   1405 Feb 28 2008 15:53:20  ssid1.zip
 0  -rw-   1405 Feb 28 2008 15:53:31  ssid2.zip
 2  -rw-   1405 Feb 28 2008 15:53:39  ssid3.zip
 3  -rw-   1405 Feb 28 2008 15:53:44  ssid4.zip
```

```
2540 KB total (1319 KB free)
```

### 認証されたユーザーを特定の Web ページにリダイレクトする

認証されたユーザーを特定の Web ページに自動的にリダイレクトするようにデバイスを設定するには、logon.htm および logonSuccess.htm で次の操作を行います。

1. logon.htm で、Form のターゲット属性を **\_blank** に設定します。

内容は灰色で表示されています。

```
<form method=post action=logon.cgi target="_blank">
```

2. pt\_init()をロードするための関数を logonSuccess.htm に追加します。

内容は灰色で表示されています。

```
<html>
```

```
<head>
```

```
<title>LogonSucceeded</title>
```

```
<script type="text/javascript" language="javascript" src="pt_private.js"></script>
```

```
</head>
```

```
<body onload="pt_init();" onbeforeunload="return pt_unload();">
```

```
... ..
```

```
</body>
</html>
```

## ローカルポータル Web サービスを構成する

### 前提条件

HTTPS ベースのローカルポータル Web サービスを構成する前に、次のタスクを完了する必要があります。

- PKI ポリシーを設定し、CA 証明書を取得して、ローカル証明書を要求します。詳細については、「PKI の構成」を参照してください。
- SSL サーバーポリシーを設定し、PKI ポリシーで設定された PKI ドメインを指定します。

SSL 接続の確立中に、サーバーID を証明書で確認できないことを示すメッセージがユーザーブラウザに表示される場合があります。このようなメッセージを確認せずにポータル認証を実行するユーザーには、クライアントが信頼する証明書をデバイスで要求するように SSL サーバーポリシーを設定します。ポリシーの名前は **https\_redirect** である必要があります。SSL サーバーポリシー設定の詳細については、「SSL の設定」を参照してください。

### 手順

1. システムビューを開始します。

**system-view**

2. HTTP または HTTPS ベースのローカルポータル Web サービスを作成し、そのビューを入力します。

```
portal local-web-server { http | https ssl-server-policy policy-name [ tcp-port port-number ] }
```

3. ローカルポータル Web サービスの既定の認証ページファイルを指定します。

**default-logon-page filename**

デフォルトでは、ローカルポータル Web サービスのデフォルト認証ページファイルは指定されていません。

ユーザーにローカルポータル Web サービスを提供するには、このコマンドを使用して、カスタマイズされた認証ページファイルをデフォルトの認証ページファイルとして指定する必要があります。

4. (省略可能)ローカルポータル Web サービスのリスニング TCP ポートを構成します。

**tcp-port port-number**

デフォルトでは、HTTP サービスリスニングポート番号は 80 で、HTTPS サービスリスニングポート番号は **portal local-web-server** コマンドで設定された TCP ポート番号です。

## インターフェースでのポータル認証のイネーブル化

### 制約事項とガイドライン

インターフェースでポータル認証をイネーブルにする場合は、次の制約事項および注意事項に従ってください。

- クロスサブネット認証モード(レイヤー3)では、アクセスデバイスとポータル認証クライアントの間にレイヤー3 転送デバイスは必要ありません。ただし、認証クライアントとアクセスデバイスの間にレイヤー3 転送デバイスが存在する場合は、クロスサブネットポータル認証モードを使用する必要があります。
- インターフェースでは、IPv4 ポータル認証と IPv6 ポータル認証の両方をイネーブルにできます。

インターフェースに re-DHCP ポータル認証を設定する場合は、次の制約事項および注意事項に従ってください。

- インターフェースで再 DHCP ポータル認証をイネーブルにする前に、インターフェースに有効な IP アドレスが設定されていることを確認します。
- 再 DHCP ポータル認証を使用して、有効なユーザーだけがネットワークにアクセスできるようにするためのベストプラクティスとして、インターフェースに認可 ARP を設定します。認可 ARP がインターフェースに設定されている場合、インターフェースは、DHCP からパブリックアドレスを取得したユーザーからのみ ARP エントリを学習します。
- DHCP ポータルの再認証を成功させるには、BAS-IP または bas-ipv6 アトリビュート値が、ポータル認証サーバーで指定されたデバイス IP アドレスと同じであることを確認します。アトリビュートを設定するには、**portal { bas-ip | bas-ipv6 }** コマンドを使用します。
- IPv6 ポータルサーバーは、再 DHCP ポータル認証をサポートしていません。

## 手順

1. システムビューを開始します。  
**system-view**
2. レイヤー3 インターフェースビューを開始します。  
**interface interface-type interface-number**
3. ポータル認証をイネーブルにします。  
IPv4 の場合:  
**portal enable method { direct | layer3 | redhcp }**  
IPv6 の場合:  
**portal ipv6 enable method { direct | layer3 }**  
デフォルトでは、ポータル認証はディセーブルです。

# インターフェース上のポータルWebサーバーの指定

## インターフェースでのポータル Web サーバーの指定について

インターフェース上でポータル Web サーバーを指定すると、デバイスはインターフェース上のポータルユーザーの HTTP 要求をポータル Web サーバーにリダイレクトします。

インターフェースには、IPv4 ポータル Web サーバーと IPv6 ポータル Web サーバーの両方を指定できます。

## 手順

1. システムビューを開始します。  
**system-view**
2. レイヤー3 インターフェースビューを開始します。  
**interface interface-type interface-number**
3. インターフェース上のポータル Web サーバーを指定します。  
**portal [ ipv6 ] apply web-server server-name [ fail-permit ]**  
デフォルトでは、インターフェースにポータル Web サーバーは指定されていません。

# 事前認証IPアドレスプールの指定

## 事前認証 IP アドレスプールについて

次の状況では、ポータル対応インターフェースで事前認証 IP アドレスプールを指定する必要があります。

- ポータルユーザーは、ポータル対応インターフェースのサブインターフェースを介してネットワークにアクセスします。
- サブインターフェースに IP アドレスがありません。
- ポータルユーザーは、DHCP を介して IP アドレスを取得する必要があります。

ポータル対応のインターフェースに接続したユーザーは、次の規則に従って、ポータル認証に IP アドレスを使用します。

- 事前認証 IP アドレスプールを使用してインターフェースを設定した場合、ユーザーは次の IP アドレスを使用します。
  - DHCP を介して IP アドレスを自動的に取得するようにクライアントが設定されている場合、ユーザーは指定された IP アドレスプールからアドレスを取得します。
  - クライアントに静的 IP アドレスが設定されている場合、ユーザーはその静的 IP アドレスを使用します。ただし、インターフェースに IP アドレスが設定されていない場合、静的 IP アドレスを使用するユーザーは認証を通過できません。
- インターフェースに IP アドレスが設定されているが、事前認証 IP プールが指定されていない場合、ユーザーはスタティック IP アドレスまたは DHCP サーバーから取得した IP アドレスを使用します。
- インターフェースに IP アドレスまたは事前認証 IP プールが指定されていない場合、ユーザーはポータル認証を実行できません。

ユーザーがポータル認証に合格すると、AAA サーバーは、ユーザーに IP アドレスを再割り当てするための IP アドレスプールを許可します。許可された IP アドレスプールが展開されていない場合、ユーザーは以前の IP アドレスを引き続き使用します。

## 制約事項とガイドライン

この設定が有効になるのは、インターフェースで直接 IPv4 ポータル認証がイネーブルになっている場合だけです。

指定された IP アドレスプールが存在し、完全であることを確認してください。存在しない場合、ユーザーは IP アドレスを取得できず、ポータル認証を実行できません。

ポータルユーザーが認証を実行しない場合、または認証に失敗した場合でも、割り当てられた IP アドレスは保持されます。

## 手順

1. システムビューを開始します。
2. レイヤー3 インターフェースビューを開始します。
3. インターフェースの事前認証 IP アドレスプールを指定します。

```
system-view
```

```
interface interface-type interface-number
```

```
portal [ ipv6 ] pre-auth ip-pool pool-name
```

デフォルトでは、インターフェースに事前認証 IP アドレスプールは指定されていません。

# ポータル認証ドメインの指定

## ポータル認証ドメインについて

認証ドメインは、一連の認証、認可、およびアカウントポリシーを定義します。各ポータルユーザーは認証ドメインに属し、ドメイン内で認証、認可、およびアカウントポリシーされます。

インターフェースで認証ドメインが指定されている場合、デバイスはポータルユーザーの AAA に認証ドメインを使用します。これにより、柔軟なポータルアクセスコントロールが可能になります。

## ポータル認証ドメインを指定するための制限およびガイドライン

デバイスは、次の順序でポータルユーザーの認証ドメインを選択します。

1. インターフェースに指定された ISP ドメイン。
2. ユーザー名で伝送される ISP ドメイン。
3. システムのデフォルト ISP ドメイン。

選択されたドメインがデバイスに存在しない場合、デバイスは、存在しないドメインに割り当てられたユーザーに対応するように設定された ISP ドメインを検索します。このような ISP ドメインが設定されていない場合、ユーザー認証は失敗します。ISP ドメインの詳細については、「AAA の構成」を参照してください。

## インターフェース上のポータル認証ドメインの指定

1. システムビューを開始します。  
**system-view**
2. レイヤー3 インターフェースビューを開始します。  
**interface interface-type interface-number**
3. インターフェース上のポータル認証ドメインを指定します。

**portal [ ipv6 ] domain domain-name**

デフォルトでは、インターフェースにポータル認証ドメインは指定されていません。

インターフェースには、IPv4 ポータル認証ドメインと IPv6 ポータル認証ドメインの両方を指定できます。

## ポータルユーザーアクセスの制御

### ポータルフリー規則の設定

#### ポータルフリー規則について

ポータルフリー規則を使用すると、指定したユーザーは、ポータル認証なしで指定した外部 Web サイトにアクセスできます。

ポータルフリー規則の一致項目には、ホスト名、送信元/宛先 IP アドレス、TCP/UDP ポート番号、送信元 MAC アドレス、アクセスインターフェース、および VLAN が含まれます。ポータルフリー規則に一致するパケットはポータル認証をトリガーしないため、パケットを送信するユーザーは、指定された外部 Web サイトに直接アクセスできます。

#### ポータルフリー規則を設定する場合の制約事項とガイドライン

VLAN とインターフェースの両方を指定する場合、インターフェースは VLAN に属している必要があります。インターフェースが VLAN に属していない場合、ポータルフリー規則は有効になりません。

同じフィルタリング基準を使用して 2 つ以上のポータルフリー規則を設定することはできません。設定しない場合は、規則がすでに存在することを示すプロンプトが表示されます。

ポータル認証が有効かどうかにかかわらず、追加または削除できるのはポータルフリールールのみです。変更はできません。

## IP ベースのポータルフリー規則の設定

1. システムビューを開始します。

**system-view**

2. IP ベースのポータルフリー規則を設定します。

IPv4 の場合:

```
portal free-rule rule-number { destination ip { ipv4-address { mask-length | mask } | any }  
[ tcp tcp-port-number | udp udp-port-number ] | source ip { ipv4-address { mask-length |  
mask } | any } [ tcp tcp-port-number | udp udp-port-number ] } * [ interface interface-type  
interface-number ]
```

IPv6 の場合:

```
portal free-rule rule-number { destination ipv6 { ipv6-address prefix-length | any } [ tcp  
tcp-port-number | udp udp-port-number ] | source ipv6 { ipv6-address prefix-length | any }  
[ tcp tcp-port-number | udp udp-port-number ] } * [ interface interface-type interface-  
number ]
```

## ソースベースのポータルフリー規則の設定

1. システムビューを開始します。

**system-view**

2. ソースベースのポータルフリー規則を設定します。

```
portal free-rule rule-number source { interface interface-type interface-number | mac  
mac-address | vlan vlan-id } *
```

**vlan** *vlan-id* オプションは、VLAN インターフェースを介してネットワークにアクセスするポータルユーザーに対してだけ有効です。

## x宛先ベースのポータルフリー規則の設定

1. システムビューを開始します。

**system-view**

2. 宛先ベースのポータルフリー規則を設定します。

```
portal free-rule rule-number destination host-name
```

# 認証送信元サブネットの設定

## 認証送信元サブネットについて

認証ソースサブネットを構成することにより、認証ソースサブネット上のユーザーからの HTTP または HTTPS パケットのみがポータル認証をトリガーできるように指定します。認証されていないユーザーが認証ソースサブネット上にいない場合、アクセスデバイスは、ポータルフリールールに一致しないユーザーの HTTP または HTTPS パケットをすべて廃棄します。

## 制約事項とガイドライン

認証ソースサブネットは、クロスサブネットポータル認証にのみ適用されます。

直接または再 DHCP ポータル認証モードでは、ポータルユーザーとそのアクセスインターフェース(ポータル対応)は同じサブネット上にあります。認証ソースサブネットとしてサブネットを指定する必要はありません。

- 直接モードでは、アクセスデバイスは認証送信元サブネットを任意の送信元 IP アドレスと見なします。
- re-DHCP モードでは、アクセスデバイスはインターフェース上の認証送信元サブネットを、インターフェースのプライベート IP アドレスが属するサブネットと見なします。

認証送信元サブネットと宛先サブネットの両方がインターフェースに設定されている場合は、認証宛先サブネットだけが有効になります。

複数の認証ソースサブネットを構成できます。ソースサブネットが重複している場合は、最大のアドレス範囲(最小のマスクまたは接頭辞)を持つサブネットが有効になります。

## 手順

1. システムビューを開始します。

**system-view**

2. レイヤー3 インターフェースビューを開始します。

**interface** *interface-type interface-number*

3. ポータル認証送信元サブネットを設定します。

IPv4 の場合:

**portal layer3 source** *ipv4-network-address { mask-length | mask }*

デフォルトでは、すべてのサブネットのユーザーがポータル認証を通過する必要があります。

IPv6 の場合:

**portal ipv6 layer3 source** *ipv6-network-address prefix-length*

デフォルトでは、すべてのサブネットのユーザーがポータル認証を通過する必要があります。

## 認証先サブネットの設定

### 認証先サブネットについて

認証宛先サブネットを構成することにより、ユーザーが指定されたサブネット(ポータルフリールールで指定された宛先 IP アドレスおよびサブネットを除く)にアクセスする場合にのみポータル認証をトリガーするように指定します。ユーザーは、ポータル認証なしで他のサブネットにアクセスできます。

### 制約事項とガイドライン

認証送信元サブネットと宛先サブネットの両方がインターフェースに設定されている場合は、認証宛先サブネットだけが有効になります。

複数の認証宛先サブネットを設定できます。宛先サブネットが重複している場合は、最大のアドレススコープ(最小のマスクまたはプレフィクス)を持つサブネットが有効になります。

## 手順

1. システムビューを開始します。

**system-view**

2. レイヤー3 インターフェースビューを開始します。

**interface** *interface-type interface-number*

3. ポータル認証の宛先サブネットを設定します。

IPv4 の場合:

**portal free-all except destination** *ipv4-network-address { mask-length | mask }*

IPv6 の場合:

**portal ipv6 free-all except destination** *ipv6-network-address prefix-length*

デフォルトでは、任意のサブネットにアクセスするユーザーはポータル認証を通過する必要があります。



# ポータルユーザーの最大数の設定

## ポータルユーザーの最大数の設定について

システム内のポータルユーザーの総数、およびインターフェース上の IPv4 または IPv6 ポータルユーザーの最大数を制御するには、次の作業を実行します。

## ポータルユーザーの最大数を設定するための制限とガイドライン

すべてのインターフェースで指定された IPv4 および IPv6 ポータルユーザーの最大合計数が、システムで許可された最大数を超えないようにしてください。そうしないと、超えた数のポータルユーザーがデバイスにログインできなくなります。

## ポータルユーザーのグローバル最大数の設定

1. システムビューを開始します。

**system-view**

2. ポータルユーザーのグローバル最大数を設定します。

**portal max-user max-number**

デフォルトでは、ポータルユーザーのグローバル数に制限は設定されていません。

グローバル最大数をデバイス上の現在のオンラインポータルユーザー数よりも小さく設定した場合でも、この設定は有効です。オンラインユーザーは影響を受けませんが、システムは新しいポータルユーザーのログインを禁止します。

## インターフェース上のポータルユーザーの最大数の設定

1. システムビューを開始します。

**system-view**

2. レイヤー3 インターフェースビューを開始します。

**interface interface-type interface-number**

3. ポータルユーザーの最大数を設定します。

**portal { ipv4-max-user | ipv6-max-user } max-number**

デフォルトでは、インターフェース上のポータルユーザー数に制限は設定されていません。

インターフェース上のポータルユーザーの現在の数よりも小さい最大数を設定した場合でも、この設定は有効です。オンラインユーザーは影響を受けませんが、システムは新しいポータルユーザーがインターフェースからログインすることを禁止します。

# ポータル許可情報の厳密な検査の使用可能化

## ポータル許可情報の厳密な検査について

厳密なチェック機能を使用すると、ユーザーの認可情報が正常に展開された場合に限り、ポータルユーザーはオンライン状態を維持できます。認可された ACL またはユーザープロファイルがデバイスに存在しない場合、またはデバイスが認可された ACL またはユーザープロファイルの展開に失敗した場合、厳密なチェックは失敗します。

許可された ACL、許可されたユーザープロファイル、またはその両方に対する厳密なチェックを有効にできます。ACL チェックとユーザープロファイルチェックの両方を有効にした場合、いずれかのチェックが失敗すると、ユーザーはログアウトされます。

## インターフェース上のポータル認証情報の厳密なチェックのイネーブル化

1. システムビューを開始します。

**system-view**

- レイヤー3 インターフェースビューを開始します。

**interface** *interface-type interface-number*

- ポータル認可情報の厳密なチェックをイネーブルにします。

**portal authorization { acl | user-profile } strict-checking**

デフォルトでは、インターフェース上でのポータル認可情報の厳密なチェックはディセーブルになっています。ポータルユーザーは、認可された ACL またはユーザープロファイルが存在しない場合や、デバイスが認可された ACL またはユーザープロファイルの展開に失敗した場合でも、オンライン状態を維持します。

## DHC P で割り当てられた IP アドレスを持つユーザーだけがポータル認証を通過できるようにする

DHC P で割り当てられた IP アドレスを持つユーザーだけがポータル認証を通過できるようにすることについて

この機能を使用すると、DHCP で割り当てられた IP アドレスを持つユーザーのみがポータル認証を通過できます。静的 IP アドレスを持つユーザーは、ポータル認証を通過してオンラインになることはできません。この機能を使用して、有効な IP アドレスを持つユーザーのみがネットワークにアクセスできるようにします。

### 制約事項とガイドライン

DHC P で割り当てられた IP アドレスを持つユーザーだけがポータル認証を通過するときに、IPv6 ユーザーがポータル認証を通過できるようにするには、端末デバイスで一時 IPv6 アドレス機能を無効にします。無効にしないと、IPv6 ユーザーは一時 IPv6 アドレスを使用して IPv6 ネットワークにアクセスし、ポータル認証に失敗します。

この設定は、オンラインポータルのユーザーには影響しません。

DHC P で割り当てられた IP アドレスを持つユーザーだけがインターフェース上でポータル認証を通過できるようにする

- システムビューを開始します。

**system-view**

- レイヤー3 インターフェースビューを開始します。

**interface** *interface-type interface-number*

- DHC P で割り当てられた IP アドレスを持つユーザーだけがポータル認証を通過できるようにします。

**portal [ ipv6 ] user-dhcp-only**

デフォルトでは、DHCP を通じて取得された IP アドレスを持つユーザーと、静的 IP アドレスを持つユーザーの両方が、認証を通過してオンラインになることができます。

## ポータル認証のための Web プロキシのサポートの構成

ポータル認証のための Web プロキシのサポートについて

Web プロキシサーバーによってプロキシ処理される HTTP 要求がポータル認証をトリガーできるようにするには、デバイス上の Web プロキシサーバーのポート番号を指定します。Web プロキシサーバーポートがデバイス上で指定されていない場合、Web プロキシサーバーによってプロキシ処理される HTTP 要求はドロップされ、ポータル認証はトリガーできません。

### 制約事項とガイドライン

ユーザーのブラウザが Web Proxy Auto-Discovery(WPAD)プロトコルを使用して Web プロキシサーバーを検出する場合は、デバイスで次のタスクを実行する必要があります。

- Web プロキシサーバーのポート番号を指定します。
- WPAD サーバー宛てのユーザーパケットが認証なしで通過できるように、ポータルフリー規則を設定します。

ポータルユーザーがブラウザで Web プロキシを有効にする場合、ユーザーはポータル認証サーバーの IP アドレスをプロキシ例外としてブラウザに追加する必要があります。したがって、ユーザーがポータル認証サーバーに送信する HTTP パケットは、Web プロキシサーバーには送信されません。

デバイス上の Web プロキシサーバーポート 443 は指定できません。

このコマンドを複数回実行して、Web プロキシサーバーの複数のポート番号を指定することができます。

## 手順

1. システムビューを開始します。

**system-view**

2. Web プロキシサーバーのポート番号を指定します。

**portal web-proxy port *port-number***

デフォルトでは、Web プロキシサーバーのポート番号は指定されていません。プロキシされた HTTP 要求はドロップされます。

## ポータルローミングを有効にする

### ポータルローミングについて

ポータルローミングが VLAN インターフェイスでイネーブルになっている場合、オンラインポータルユーザーは、再認証なしで VLAN 内の任意のレイヤー2 ポートからリソースにアクセスできます。

ポータルローミングがディセーブルの場合、VLAN の現在のアクセスポートとは異なるレイヤー2 ポートから外部ネットワークリソースにアクセスするには、ユーザーは次の手順を実行する必要があります。

1. 現在のポートからログアウトします。
2. 新しいレイヤー2 ポートで再認証します。

### 制約事項とガイドライン

ポータルローミングは、VLAN インターフェイスからログインするポータルユーザーに対してのみ有効です。共通レイヤー3 インターフェイスからログインするポータルユーザーには有効ではありません。

オンラインポータルユーザーがデバイスに存在する場合は、ポータルローミングをイネーブルにできません。

ポータルローミングを有効にするには、**undo portal refresh { arp | nd } enable** コマンドを使用して、ルール ARP または ND エントリ機能をディセーブルにする必要があります。

## 手順

1. システムビューを開始します。

**system-view**

2. ポータルローミングを有効にします。

**portal roaming enable**

デフォルトでは、ポータルローミングは無効になっています。

# ポータルの失敗許容機能の設定

## ポータルの Fail-Permit 機能について

インターフェース上でポータルフェール許可機能を設定するには、次の作業を実行します。アクセスデバイスは、ポータル認証サーバーまたはポータル Web サーバーが到達不能であることを検出すると、インターフェース上のユーザーがポータル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。

インターフェース上のポータル認証サーバーとポータル Web サーバーの両方で fail-permit をイネーブルにした場合、インターフェースは次の処理を実行します。

- いずれかのサーバーが到達不能な場合に、ポータル認証をディセーブルにします。
- 両方のサーバーが到達可能になると、ポータル認証を再開します。

ポータル認証が再開された後、認証されていないユーザーがネットワークにアクセスするには、ポータル認証を通過する必要があります。失敗許可イベントの前にポータル認証を通過したユーザーは、ネットワークへのアクセスを続行できます。

## 手順

1. システムビューを開始します。

**system-view**

2. レイヤー3 インターフェースビューを開始します。

**interface** *interface-type* *interface-number*

3. ポータル認証サーバーの portal fail-permit をイネーブルにします。

**portal** [ **ipv6** ] **fail-permit server** *server-name*

デフォルトでは、ポータル認証サーバーの portal fail-permit はディセーブルです。

4. ポータル Web サーバーの portal fail-permit を有効にします。

**portal** [ **ipv6** ] **apply web-server** *server-name* [ **fail-permit** ]

デフォルトでは、portal fail-permit はポータル Web サーバーに対して無効になっています。

# ポータル検出機能の設定

## ポータルユーザーのオンライン検出の設定

### ポータルユーザーのオンライン検出について

オンライン検出機能を使用して、ポータルユーザーの異常なログアウトを迅速に検出します。IPv4 ポータルユーザーの ARP または ICMP 検出を設定します。IPv6 ポータルユーザーの ND または ICMPv6 検出を設定します。

デバイスがアイドル時間内にポータルユーザーからパケットを受信しない場合、デバイスは次のようにユーザーのオンラインステータスを検出します。

- **ICMP または ICMPv6 検出:** ユーザーの状態を検出するために、設定可能な間隔で ICMP または ICMPv6 要求をユーザーに送信します。
  - デバイスは、最大検出試行回数以内に応答を受信すると、ユーザーがオンラインであると見なし、検出パケットの送信を停止します。その後、デバイスはアイドルタイマーをリセットし、タイマーが期限切れになったときに検出プロセスを繰り返します。
  - 最大回数の検出試行後にデバイスが応答を受信しない場合、デバイスはユーザーをログアウトします。

- **ARP または ND 検出:** ARP または ND 要求をユーザーに送信し、設定可能な間隔でユーザーの ARP または ND エントリステータスを検出します。
  - ユーザーの ARP または ND エントリが最大検出試行回数以内にリフレッシュされた場合、デバイスはユーザーがオンラインであると見なし、検出を停止します。その後、デバイスはアイドルタイマーをリセットし、タイマーが期限切れになったときに検出プロセスを繰り返します。
  - 最大検出試行回数を超えてもユーザーの ARP または ND エントリがリフレッシュされない場合、デバイスはユーザーをログアウトします。

## 制約事項とガイドライン

ARP 検出および ND 検出は、直接および再 DHCP ポータル認証にのみ適用されます。ICMP 検出は、すべてのポータル認証モードに適用されます。

## 手順

1. システムビューを開始します。
2. レイヤー3 インターフェースビューを開始します。
3. ポータルユーザーのオンライン検出を設定します。

IPv4 の場合:

```
portal user-detect type { arp | icmp } [ retry retries ] [ interval interval ] [ idle time ]
```

IPv6 の場合:

```
portal ipv6 user-detect type { icmpv6 | nd } [ retry retries ] [ interval interval ] [ idle time ]
```

デフォルトでは、インターフェース上のポータルユーザーのオンライン検出はディセーブルです。

# ポータル認証サーバー検出の設定

## ポータル認証サーバーの検出について

ポータル認証中に、アクセスデバイスとポータル認証サーバー間の通信が切断された場合、新しいポータルユーザーはログインできません。オンラインポータルユーザーは正常にログアウトできません。

この問題に対処するには、アクセスデバイスがポータルサーバーの到達可能性の変更を迅速に検出し、その変更に対応するアクションを実行できる必要があります。

ポータル認証サーバー検出機能を使用すると、デバイスは、ポータル認証サーバーから送信されたポータルパケットを定期的に検出して、サーバーの到達可能性を判断できます。デバイスが検出タイムアウト (timeout timeout) 内にポータルパケットを受信し、ポータルパケットが有効な場合、デバイスはポータル認証サーバーが到達可能であると見なします。それ以外の場合、デバイスはポータル認証サーバーが到達不能であると見なします。

ポータルパケットには、ユーザーログインパケット、ユーザーログアウトパケットおよびハートビートパケットが含まれます。ハートビートパケットは、サーバーによって定期的送信されます。ハートビートパケットを検出することにより、デバイスは、他のポータルパケットを検出するよりも迅速にサーバーの実際のステータスを検出できます。

## 制約事項とガイドライン

ポータル認証サーバー検出機能は、デバイスにポータル対応のインターフェースがある場合にだけ有効です。

ハートビートパケットの送信をサポートしているのは、IMC ポータル認証サーバーだけです。ハートビートパケットを検出してサーバーの到達可能性をテストするには、IMC ポータル認証サーバーでサーバーハートビート機能をイネーブルにする必要があります。

サーバー到達可能性ステータスが変更されたときに、次の 1 つまたは複数のアクションを実行するようにデバイスを設定できます。

- ログメッセージの送信。このメッセージには、ポータル認証サーバーの名前、現在の状態、および元の状態が含まれます。
- ポータル失敗許容の有効化。ポータル認証サーバーに到達できない場合、インターフェース上のポータル失敗許容機能により、インターフェース上のユーザーがネットワークにアクセスできるようになります。サーバーが回復すると、インターフェース上のポータル認証が再開されます。詳細については、「ポータルのフェイル許可機能の構成」を参照してください。
- デバイ스에設定されている検出タイムアウトが、ポータル認証サーバーに設定されているサーバーハートビート間隔よりも大きいことを確認します。

## 手順

1. システムビューを開始します。

**system-view**

2. ポータル認証サーバービューを開始します。

**portal server server-name**

3. ポータル認証サーバー検出を設定します。

**server-detect [ timeout timeout ] log**

デフォルトでは、ポータル認証サーバー検出はディセーブルになっています。

## ポータル Web サーバーの検出の構成

### ポータル Web サーバーの検出について

アクセスデバイスとポータル Web サーバー間の通信が切断されている場合、ポータル認証プロセスを完了できません。この問題に対処するには、アクセスデバイスでポータル Web サーバーの検出を有効にします。

ポータル Web サーバー検出機能を使用すると、アクセスデバイスは Web アクセスプロセスをシミュレートして、ポータル Web サーバーへの TCP 接続を開始します。TCP 接続が正常に確立された場合、アクセスデバイスは検出が成功したと見なし、ポータル Web サーバーは到達可能であると見なします。それ以外の場合は、検出が失敗したと見なします。アクセスデバイスのインターフェース上のポータル認証ステータスは、ポータル Web サーバー検出機能には影響しません。

次の検出パラメーターを設定できます。

- **検出間隔:** デバイスがサーバーの到達可能性を検出する間隔。
- **連続した失敗の最大数:** 連続した検出失敗の数がこの値に達すると、アクセスデバイスはポータル Web サーバーが到達不能であると見なします。

サーバー到達可能性ステータスが変更されたときに、次の 1 つまたは複数のアクションを実行するようにデバイスを設定できます。

- ログメッセージの送信。ログメッセージには、ポータル Web サーバーの名前、現在の状態、および元の状態が含まれます。
- ポータル失敗の許可を有効にします。ポータル Web サーバーに到達できない場合、インターフェース上のポータル失敗の許可機能によって、インターフェース上のユーザーがネットワークにアクセスできるようになります。サーバーが回復すると、インターフェース上のポータル認証が再開されます。詳細については、「ポータルのフェイル許可機能の構成」を参照してください。

## 制約事項とガイドライン

ポータル Web サーバー検出機能が有効になるのは、ポータル Web サーバーの URL が指定されていて、デバイスにポータル対応のインターフェースがある場合だけです。

### 手順

1. システムビューを開始します。  
**system-view**
2. ポータル Web サーバービューを入力してください。  
**portal web-server server-name**
3. ポータル Web サーバーの検出を構成します。  
**server-detect [ interval interval ] [ retry retries ] log**  
デフォルトでは、ポータル Web サーバーの検出は無効になっています。

## ポータルユーザー同期の構成

### ポータルユーザーの同期について

アクセスデバイスがポータル認証サーバーとの通信を失うと、通信が再開された後に、アクセスデバイスとポータル認証サーバーのポータルユーザー情報が一致しなくなる可能性があります。この問題に対処するために、デバイスにはポータルユーザー同期機能が用意されています。この機能は、次のようにポータル同期パケットを送信および検出することによって実装されます。

1. ポータル認証サーバーは、ユーザーハートビート間隔の同期パケットで、オンラインユーザー情報をアクセスデバイスに送信します。  
ユーザーのハートビート間隔は、ポータル認証サーバーで設定されます。
2. 同期パケットを受信すると、アクセスデバイスはパケットで伝送されたユーザーを自身のユーザーリストと比較し、次の操作を実行します。
  - パケットに含まれるユーザーがアクセスデバイスに存在しない場合、アクセスデバイスはポータル認証サーバーにユーザーを削除するように通知します。アクセスデバイスは、ユーザーがログインするとすぐに同期検出タイマー(**timeout timeout**)を開始します。
  - 同期検出間隔内のどの同期パケットにもユーザーが表示されない場合、アクセスデバイスはそのユーザーがポータル認証サーバーに存在しないと見なし、ユーザーをログアウトします。

## 制約事項とガイドライン

ポータルユーザーの同期には、ポータルユーザーハートビート機能をサポートするポータル認証サーバーが必要です。ポータルユーザーハートビート機能をサポートしているのは、IMC ポータル認証サーバーだけです。ポータルユーザー同期機能を実装するには、ポータル認証サーバーでユーザーハートビート機能を構成する必要もあります。ポータル認証サーバーで構成されたユーザーハートビート間隔が、アクセスデバイスで構成された同期検出タイムアウトより大きくないことを確認してください。

アクセスデバイス上のポータル認証サーバーを削除すると、ポータル認証サーバーのユーザー同期設定も削除されます。

### 手順

1. システムビューを開始します。  
**system-view**
2. ポータル認証サーバービューを開始します。  
**portal server server-name**
3. ポータルユーザーの同期を設定します。

**user-sync timeout timeout**

デフォルトでは、ポータルユーザーの同期は無効になっています。

## ポータルパケット属性の設定

### BAS-IP または BAS-IPv6 アトリビュートの設定

#### ポータルパケットの BAS-IP アトリビュートおよび BAS-IPv6 アトリビュートについて

デバイスが Portal 2.0 を実行している場合、ポータル認証サーバーに送信される非送信請求パケットは、BAS-IP アトリビュートを伝送する必要があります。デバイスが Portal 3.0 を実行している場合、ポータル認証サーバーに送信される非送信請求パケットは、BAS-IP アトリビュートまたは BAS-IPv6 アトリビュートを伝送する必要があります。

このアトリビュートを設定すると、デバイスがポータル認証サーバーに送信する非送信請求通知ポータルパケットの送信元 IP アドレスは、設定された BAS-IP または BAS-IPv6 アドレスになります。アトリビュートが設定されていない場合、ポータルパケットの送信元 IP アドレスは、パケット出力インターフェースの IP アドレスになります。

#### 制約事項とガイドライン

再 DHCP ポータル認証または必須ユーザーログアウトプロセス中に、デバイスはポータル認証サーバーにポータル通知パケットを送信します。認証またはログアウトプロセスを完了するには、BAS-IP/BAS-IPv6 アトリビュートがポータル認証サーバーで指定されたデバイス IP アドレスと同じであることを確認します。

次の条件が満たされる場合は、ポータル認証がイネーブルになっているインターフェースで BAS-IP または BAS-IPv6 アトリビュートを設定する必要があります。

- ポータル認証サーバーは、H3C IMC サーバーです。
- ポータル認証サーバーで指定されたポータルデバイスの IP アドレスが、ポータルパケット出力インターフェースの IP アドレスではありません。

#### インターフェースでの BAS-IP または BAS-IPv6 アトリビュートの設定

1. システムビューを開始します。

**system-view**

2. レイヤー3 インターフェースビューを開始します。

**interface interface-type interface-number**

3. BAS-IP または BAS-IPv6 アトリビュートを設定します。

IPv4 の場合:

**portal bas-ip ipv4-address**

デフォルトでは、IPv4 ポータル応答パケットの BAS-IP アトリビュートは、パケットの送信元 IPv4 アドレスです。IPv4 ポータル通知パケットの BAS-IP アトリビュートは、パケットの出力インターフェースの IPv4 アドレスです。

IPv6 の場合:

**portal bas-ipv6 ipv6-address**

デフォルトでは、IPv6 ポータル応答パケットの BAS-IPv6 属性は、パケットの送信元 IPv6 アドレスです。IPv6 ポータル通知パケットの BAS-IPv6 属性は、パケットの出力インターフェースの IPv6 アドレスです。



# デバイス ID の指定

## デバイス ID の指定について

ポータル認証サーバーは、デバイス ID を使用して、プロトコルパケットをポータルサーバーに送信するデバイスを識別します。

## 制約事項とガイドライン

設定されたデバイス ID が、同じポータル認証サーバーと通信している他のアクセスデバイスと異なることを確認します。

## 手順

1. システムビューを開始します。

**system-view**

2. デバイス ID を指定します。

**portal device-id device-id**

デフォルトでは、デバイスにはデバイス ID が設定されていません。

# RADIUSパケットの属性の設定

## NAS-Port-Id 属性のフォーマットの指定

### NAS-Port-Id 属性のフォーマットの指定について

異なるベンダーの RADIUS サーバーでは、RADIUS パケット内の NAS-Port-Id 属性の形式が異なる場合があります。必要に応じて、NAS-Port-Id 属性の形式を指定できます。

デバイスは定義済みの形式(形式 1、2、3、および 4)をサポートしています。形式の詳細については、「セキュリティコマンドリファレンス」のポータルコマンドを参照してください。

## 手順

1. システムビューを開始します。

**system-view**

2. NAS-Port-Id 属性の形式を指定します。

**portal nas-port-id format { 1 | 2 | 3 | 4 }**

デフォルトでは、NAS-Port-Id 属性の形式は format 2 です。

# インターフェースへの NAS-ID プロファイルの適用

## インターフェースへの NAS-ID プロファイルの適用について

デフォルトでは、デバイスはすべての RADIUS 要求の NAS-Identifier アトリビュートでデバイス名を送信します。

NAS-ID プロファイルを使用すると、異なる VLAN からの RADIUS 要求で異なる NAS-Identifier 属性文字列を送信できます。文字列は、管理要件に応じて、組織名、サービス名、または任意のユーザー分類基準になります。

たとえば、NAS-ID **companyA** を会社 A のすべての VLAN にマッピングします。デバイスは、RADIUS サーバーの NAS-Identifier アトリビュートで **companyA** を送信して、会社 A のユーザーからの要求を識別します。

## 制約事項とガイドライン

NAS-ID プロファイルは、ポータル対応のインターフェースに適用できます。インターフェースに NAS-ID プロファイルが指定されていない場合、または指定されたプロファイルに一致する NAS-ID が見つからない場合、デバイスはインターフェースの NAS-ID としてデバイス名を使用します。

### 手順

1. システムビューを開始します。

**system-view**

2. NAS-ID プロファイルを作成し、NAS-ID プロファイルビューを開始します。

**aaa nas-id profile profile-name**

このコマンドの詳細については、「セキュリティコマンドリファレンス」を参照してください。

3. プロファイルで NAS ID および VLAN バインディングを設定します。

**nas-id nas-identifier bind vlan vlan-id**

このコマンドの詳細については、『Security Command Reference』を参照してください。ポータルアクセスは、QinQ パケットの内部 VLAN ID だけを照合します。QinQ の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

4. インターフェースの NAS-ID プロファイルを指定します。

- a. システムビューに戻ります。

**quit**

- b. レイヤー3 インターフェースビューを開始します。

**interface interface-type interface-number**

- c. インターフェースの NAS-ID プロファイルを指定します。

**portal nas-id-profile profile-name**

## ポータルクライアントのルールARPまたはNDエントリ機能の無効化

### ポータルクライアントのルール ARP または ND エントリ機能について

ポータルクライアントに対してルール ARP または ND エントリ機能が有効になっている場合、ポータルクライアントの ARP または ND エントリは、クライアントがオンラインになった後のルールエントリです。ルールエントリは期限切れにならず、ポータルクライアントがオフラインになった直後に削除されます。ポータルクライアントがオフラインになり、クライアントの ARP または ND エントリが再学習される前にオンラインになろうとすると、クライアントは認証に失敗します。このような認証の失敗を回避するには、この機能を無効にします。その後、ポータルクライアントの ARP または ND エントリは、クライアントがオンラインになった後の動的エントリであり、期限切れになった場合にのみ削除されます。

### 制約事項とガイドライン

この機能をイネーブルまたはディセーブルにしても、既存のルール/ダイナミック ARP または ND エントリには影響しません。

### 手順

1. システムビューを開始します。

**system-view**

2. ポータルクライアントのルール ARP または ND エントリ機能を無効にします。

**undo portal refresh { arp | nd } enable**

デフォルトでは、ポータルクライアントの Rule ARP または ND エントリ機能はイネーブルになっています。

## オンラインポータルユーザーのログアウト

### オンラインポータルユーザーのログアウトについて

この機能は、ポータル認証に合格したユーザーを削除し、進行中のポータル認証を終了します。

### 制約事項とガイドライン

オンラインユーザーの数が 2000 を超える場合、portal delete-user コマンドの実行には数分かかります。

オンラインユーザーのログアウトを成功させるには、コマンドの実行中にポータル対応インターフェースでポータル認証をディセーブルにしないでください。

### 手順

1. システムビューを開始します。

**system-view**

2. オンラインポータルユーザーをログアウトします。

```
portal delete-user { ipv4-address | all | interface interface-type interface-number | ipv6  
ipv6-address }
```

## ポータルユーザーのログイン/ログアウトロギングの使用可能化

### ポータルユーザーのログイン/ログアウトロギングの使用可能化について

この機能は、ユーザーのログインおよびログアウトイベントに関する情報を記録します。情報には、ユーザー名、ユーザーの IP アドレスと MAC アドレス、ユーザーアクセスインターフェース、VLAN、およびログイン結果が含まれます。ログは、デバイスのインフォメーションセンターに送信されます。ログを正しく出力するには、デバイスにインフォメーションセンターを設定する必要があります。インフォメーションセンターの設定の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

### 手順

1. システムビューを開始します。

**system-view**

2. ポータルユーザーのログイン/ログアウトロギングをイネーブルにします。

**portal log enable**

デフォルトでは、ポータルユーザーのログイン/ログアウトロギングは無効になっています。

## Webリダイレクトの構成

### Web リダイレクトについて

Web リダイレクトは、簡素化されたポータル機能です。Web リダイレクトを使用すると、ユーザーはポータル認証を実行しませんが、ブラウザでの最初の Web アクセス試行時に指定された URL に直接リダイレクトされます。指定されたリダイレクト間隔の後、ユーザーは Web サイトから指定された URL に再度リダイレクトされます。

Web リダイレクトは、ISP に拡張サービスを提供できます。たとえば、ISP は、リダイレクトされた Web ページに広告を掲載し、情報を公開できます。

## 制約事項とガイドライン

Web リダイレクト機能は、デフォルトのポート番号 80 を使用する HTTP パケットに対してのみ有効です。Web リダイレクトとポータル認証の両方が有効になっている場合、Web リダイレクトは機能しません。

## 手順

1. システムビューを開始します。  
**system-view**
2. レイヤー3 インターフェイスビューを開始します。  
**interface** *interface-type* *interface-number*
3. Web リダイレクトを設定します。  
**web-redirect** [ **ipv6** ] **url** *url-string* [ **interval** *interval* ]  
デフォルトでは、Web リダイレクトは無効になっています。

# ポータルの表示および保守コマンド

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

タスク	コマンド
ポータル構成とポータルの実行状態を表示します。	<b>display portal interface</b> <i>interface-type</i> <i>interface-number</i>
ポータル認証サーバーのパケット統計情報を表示します。	<b>display portal packet statistics</b> [ <b>server</b> <i>server-name</i> ]
ポータルルールを表示します。	<b>display portal rule</b> { <b>all</b>   <b>dynamic</b>   <b>static</b> } <b>interface</b> <i>interface-type</i> <i>interface-number</i> [ <b>slot</b> <i>slot-number</i> ]
ポータル認証サーバー情報を表示します。	<b>display portal server</b> [ <i>server-name</i> ]
ポータルユーザー情報を表示します。	<b>display portal user</b> { <b>all</b>   <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>ip</b> <i>ipv4-address</i>   <b>ipv6</b> <i>ipv6-address</i> } [ <b>verbose</b> ]
ポータルWebサーバー情報を表示します。	<b>display portal web-server</b> [ <i>server-name</i> ]
Webリダイレクトルール情報を表示します。	<b>display web-redirect rule interface</b> <i>interface-type</i> <i>interface-number</i> [ <b>slot</b> <i>slot-number</i> ]
ポータル認証サーバーのパケット統計情報をクリアします。	<b>reset portal packet statistics</b> [ <b>server</b> <i>server-name</i> ]

# ポータル構成の例

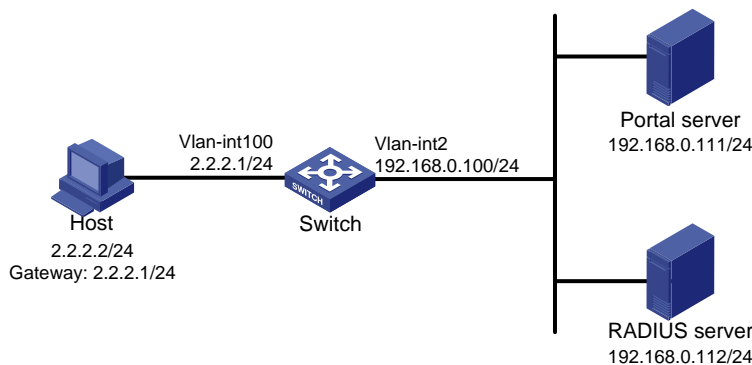
## 例:ダイレクトポータル認証の設定

### ネットワーク構成

図 6 に示すように、ホストはスイッチ(アクセスデバイス)に直接接続されています。ホストには、手動または DHCP を介してパブリック IP アドレスが割り当てられます。ポータルサーバーは、ポータル認証サーバーとポータル Web サーバーの両方として機能します。RADIUS サーバーは、認証/アカウントサーバーとして機能します。

ホストが認証を渡す前にポータルサーバーだけにアクセスし、認証を渡した後に他のネットワークリソースにアクセスできるように、ダイレクトポータル認証を設定します。

図 6 ネットワークダイアグラム



### 前提条件

- 図 6 に示すように、ホスト、スイッチ、およびサーバーの IP アドレスを設定し、それらが相互に到達できることを確認します。
- RADIUS サーバーを正しく設定して、認証およびアカウント機能を提供します。

### IMC PLAT 3.20 でのポータル認証サーバーの設定

この例では、ポータルサーバーは IMC PLAT 3.20-R2602P13 および IMC UAM 3.60-E6301 上で動作します。

1. ポータル認証サーバーを設定します。
  - a. IMC にログインし、**Service** タブをクリックします。
  - b. ナビゲーションツリーから **Access Service > Portal Service Management > Server** を選択して、ポータルサーバー設定ページを開きます(図 7 を参照)。
  - c. 必要に応じて、ポータルサーバーのパラメーターを構成します。  
この例では、デフォルト値を使用します。
  - d. **OK** をクリックします。

図 7 ポータル認証サーバーの構成

Service >> Access Service >> Portal Service Management >> Server

**Portal Server Configuration**

**Basic Information**

\* Log Level: Info

\* Server Heartbeat Interval: 20 Seconds

\* Request Timeout: 5 Seconds

\* User Heartbeat Interval: 5 Minutes

**Advanced Information**

**Service Type List**

Add

Total Items: 0.

Service Type ID	Service Type	Delete
-----------------	--------------	--------

OK Refresh

2. IP アドレスグループを設定します。
  - a. ナビゲーションツリーから **Access Service > Portal Service Management > IP Group** を選択して、ポータル IP アドレスグループ設定ページを開きます。
  - b. **Add** をクリックしてページを開きます(図 8 を参照)。
  - c. IP グループ名を入力します。
  - d. IP グループの開始 IP アドレスと終了 IP アドレスを入力します。  
ホスト IP アドレス(2.2.2.2)が IP グループに含まれていることを確認します。
  - e. サービスグループを選択します。  
この例では、既定のグループ **Ungrouped** を使用します。
  - f. **Normal** アクションを選択します。
  - g. **OK** をクリックします。

図 8 IP アドレスグループの追加

Service >> Access Service >> Portal Service Management >> Portal IP Group Configuration >> Add IP Group

**Add IP Group**

\* IP Group Name: Portal\_user

\* Start IP: 2.2.2.1

\* End IP: 2.2.2.255

\* Service Group: Ungrouped

\* Action: Normal

OK Cancel

3. ポータルデバイスを追加します。
  - a. ナビゲーションツリーから[Access Service]>[Portal Service Management]>[Device]を選択して、ポータルデバイス設定ページを開きます。
  - b. **Add** をクリックしてページを開きます(図 9 を参照)。
  - c. デバイス名 **NAS** を入力します。
  - d. ホストに接続されているスイッチのインターフェースの IP アドレスを入力します。
  - e. キーを入力します。このキーは、スイッチに設定されているキーと同じでなければなりません。
  - f. IP アドレスの再割り当てを有効にするかどうかを設定します。

この例では、直接ポータル認証を使用します。そのため、**Reallocate IP** リストから **No** を選択します。

- g. ポータルサーバーハートビートおよびユーザーハートビート機能をサポートするかどうかを設定します。

この例では、**Support Server Heartbeat** と **Support User Heartbeat** の両方で **No** を選択します。

- h. **OK** をクリックします。

図 9 ポータルデバイスを追加する

Service >> Access Service >> Portal Service Management >> Portal Device Configuration >> Add Device

**Add Device**

**Device Information**

- \* Device Name:
- \* Version:
- \* Listening Port:
- \* Authentication Retries:
- \* Reallocate IP:
- \* Support Server Heartbeat:
- \* Service Group:
- \* Device Description:
- \* IP Address:
- \* Key:
- \* Local Challenge:
- \* Logout Retries:
- \* Support User Heartbeat:

OK Cancel

- 4. ポータルデバイスを IP アドレスグループに関連付けます。

- a. 図 10 に示すように、デバイス **NAS** の **Port Group Information Management** カラムのアイコンをクリックして、ポートグループ設定ページを開きます。

図 10 デバイスリスト

Device Information List							
Add							
1-1 of 1. Page 1 of 1.							Items per Page: 8 15 <b>50</b> 100 200
Device Name	Version	Service Group	IP Address	Details	Modify	Delete	Port Group Information Management
NAS	Portal 2.0	Ungrouped	2.2.2.1				

- b. **Add** をクリックしてページを開きます(図 11 を参照)。

図 11 ポートグループ設定

Service >> Access Service >> Portal Service Management >> Portal Device Configuration >> Port Group Info Config >> Add Port Group Info

**Add Port Group Info**

**Port Group Information**

- \* Port Group Name:
- \* Start Port:
- \* Protocol:
- \* NAT or Not:
- \* Authentication Type:
- \* Heartbeat Interval:  Minutes
- User Domain:
- User Attribute Type:
- Default Authentication Type:
- \* Language:
- \* End Port:
- \* Quick Authentication:
- \* Error Transparent Transmission:
- \* IP Group:
- \* Heartbeat Timeout:  Minutes
- Port Group Description:
- Default Authentication Page:

OK Cancel

- c. ポートグループ名を入力します。
  - d. 設定済みの IP アドレスグループを選択します。  
ユーザーがネットワークにアクセスするために使用する IP アドレスは、この IP アドレスグループ内にある必要があります。
  - e. OK をクリックします。
5. ナビゲーションツリーから **Access Service > Service Parameters > Validate System Configuration** を選択して、設定を検証します。

## IMC PLAT 5.0 でのポータル認証サーバーの設定

この例では、ポータルサーバーは IMC PLAT 5.0(E0101)および IMC UAM 5.0(E0101)上で動作します。

1. ポータル認証サーバーを設定します。
  - a. IMC にログインし、**Service** タブをクリックします。
  - b. ナビゲーションツリーから **User Access Manager > Portal Service Management > Server** を選択して、ポータルサーバー設定ページを開きます(図 12 を参照)。
  - c. 必要に応じて、ポータルサーバーのパラメーターを構成します。  
この例では、既定の設定を使用します。
  - d. OK をクリックします。

図 12 ポータルサーバーの設定

The screenshot shows the 'Portal Server Configuration' page. The breadcrumb path is 'Service >> User Access Manager >> Portal Service Management >> Server'. The page is divided into 'Basic Information' and 'Advanced Information' sections.

**Basic Information:**

- Log Level: Info (dropdown)
- Request Timeout: 5 Seconds
- Server Heartbeat Interval: 20 Seconds
- User Heartbeat Interval: 5 Minutes
- Portal Page: http://192.168.0.111:8080/portal

**Advanced Information:**

Service Type List

Add

Total Items: 0.

Service Type ID	Service Type	Delete
-----------------	--------------	--------

OK

2. IP アドレスグループを設定します。
  - a. ナビゲーションツリーから **User Access Manager > Portal Service Management > IP Group** を選択して、ポータル IP アドレスグループ設定ページを開きます。
  - b. **Add** をクリックしてページを開きます(図 13 を参照)。
  - c. IP グループ名を入力します。
  - d. IP グループの開始 IP アドレスと終了 IP アドレスを入力します。  
ホスト IP アドレスが IP グループに含まれていることを確認します。
  - e. サービスグループを選択します。



この例では、既定のグループ **Ungrouped** を使用します。

- f. **Normal** アクションを選択します。
- g. **OK** をクリックします。

図 13 IP アドレスグループの追加

Service >> User Access Manager >> Portal Service Management >> Portal IP Group Configuration >> Add IP Group

**Add IP Group**

* IP Group Name	Portal_user
* Start IP	2.2.2.1
* End IP	2.2.2.255
Service Group	Ungrouped
* Action	Normal

OK Cancel

- 3. ポータルデバイスを追加します。
  - a. ナビゲーションツリーから **User Access Manager > Portal Service Management > Device** を選択して、ポータルデバイス設定ページを開きます。
  - b. **Add** をクリックしてページを開きます(図 14 を参照)。
  - c. デバイス名 **NAS** を入力します。
  - d. ホストに接続されているスイッチのインターフェースの IP アドレスを入力します。
  - e. キーを入力します。このキーは、スイッチに設定されているキーと同じでなければなりません。
  - f. IP アドレスの再割り当てを有効にするかどうかを設定します。

この例では、直接ポータル認証を使用するため、**Reallocate IP** リストから **No** を選択します。
  - g. サーバーハートビート機能とユーザーハートビート機能をサポートするかどうかを選択します。

この例では、**Support Server Heartbeat** と **Support User Heartbeat** の両方で **No** を選択します。
  - h. **OK** をクリックします。

図 14 ポータルデバイスを追加する

Service >> User Access Manager >> Portal Service Management >> Portal Device Configuration >> Add Device

**Add Device**

* Device Name	NAS	* IP Address	2.2.2.1
* Version	Portal 2.0	* Key	portal
* Listening Port	2000	* Local Challenge	No
* Authentication Retries	2	* Logout Retries	4
* Reallocate IP	No	* Support Server Heartbeat	No
* Support Server Heartbeat	No	* Support User Heartbeat	No
* Service Group	Ungrouped		
Device Description			

OK Cancel

4. ポータルデバイスを IP アドレスグループに関連付けます。
  - a. 図 15 に示すように、デバイス NAS の **Port Group Information Management** カラムのアイコンをクリックして、ポートグループ設定ページを開きます。
  - b. **Add** をクリックしてページを開きます(図 16 を参照)。
  - c. ポートグループ名を入力します。
  - d. 設定済みの IP アドレスグループを選択します。  
ユーザーがネットワークにアクセスするために使用する IP アドレスは、この IP アドレスグループ内にある必要があります。
  - e. その他のパラメーターには既定の設定を使用します。
  - f. **OK** をクリックします。

図 15 デバイスリスト





Device Information List							
Add							
1-2 of 2. Page 1 of 1.						Items per Page: 8 15 [50] 100 200	
Device Name	Version	Service Group	IP Address	Port Group Information Management	Details	Modify	Delete
NAS	Portal 2.0	Ungrouped	2.2.2.1				

図 16 ポートグループの追加

Service >> User Access Manager >> Portal Service Management >> Portal Device Configuration >> Port Group Info Config >> Add Help

**Port Group Info**

**Add Port Group Info**

<p>* Port Group Name: <input type="text" value="group"/></p> <p>* Start Port: <input type="text" value="0"/></p> <p>* Protocol: <input type="text" value="HTTP"/></p> <p>* NAT or Not: <input type="text" value="No"/></p> <p>* Authentication Type: <input type="text" value="CHAP"/></p> <p>* Heartbeat Interval: <input type="text" value="10"/> Minutes</p> <p>User Domain: <input type="text"/></p> <p>User Attribute Type: <input type="text"/></p> <p>Default Authentication Type: <input type="text" value="Web Identity AuthN"/></p>	<p>* Language: <input type="text" value="Dynamic Detection"/></p> <p>* End Port: <input type="text" value="zzzzz"/></p> <p>* Quick Authentication: <input type="text" value="No"/></p> <p>* Error Transparent Transmission: <input type="text" value="Yes"/></p> <p>* IP Group: <input type="text" value="Portal_user"/></p> <p>* Heartbeat Timeout: <input type="text" value="30"/> Minutes</p> <p>Port Group Description: <input type="text"/></p> <p>Default Authentication Page: <input type="text" value="index_default.jsp"/></p>
---	---

5. ナビゲーションツリーから **User Access Manager > Service Parameters > Validate System Configuration** を選択して、設定を検証します。

## スイッチの設定

1. RADIUS スキームを設定します。  
# rs1 という名前の RADIUS スキームを作成し、そのビューを入力します。  
<Switch> system-view  
[Switch] radius scheme rs1  
# プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。  
[Switch-radius-rs1] primary authentication 192.168.0.112  
[Switch-radius-rs1] primary accounting 192.168.0.112

```

[Switch-radius-rs1] key authentication simple radius
[Switch-radius-rs1] key accounting simple radius
# RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。
[Switch-radius-rs1] user-name-format without-domain
[Switch-radius-rs1] quit
# RADIUS セッション制御を有効にします。
[Switch] radius session-control enable
2. 認証ドメインを構成します。
# dm1 という名前の ISP ドメインを作成し、そのビューを入力します。
[Switch] domain dm1
# ISP ドメインの AAA 方式を設定します。
[Switch-isp-dm1] authentication portal radius-scheme rs1
[Switch-isp-dm1] authorization portal radius-scheme rs1
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
# ドメイン dm1 をデフォルトの ISP ドメインとして設定します。ユーザーがログイン時に ISP ドメイン名
なしでユーザー名を入力した場合、そのユーザーにはデフォルトドメインの認証およびアカウントイン
グ方式が使用されます。
[Switch] domain default enable dm1
3. ポータル認証を構成します。
# ポータル認証サーバーを構成します。
[Switch] portal server newpt
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
[Switch-portal-server-newpt] port 50100
[Switch-portal-server-newpt] quit
# ポータル Web サーバーを構成します。
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Switch-portal-websvr-newpt] quit
# VLAN インターフェース 100 でダイレクトポータル認証をイネーブルにします。
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] portal enable method direct
# VLAN インターフェース 100 上のポータル Web サーバーnewpt を指定します。
[Switch-Vlan-interface100] portal apply web-server newpt
# VLAN インターフェース 100 からポータル認証サーバーに送信されるポータルパケットの BAS-IP
を 2.2.2.1 に設定します。
[Switch-Vlan-interface100] portal bas-ip 2.2.2.1
[Switch-Vlan-interface100] quit

```

## 設定の確認

```

#ポータル構成が有効になっていることを確認します。
[Switch] display portal interface vlan-interface 100
Portal information of Vlan-interface100
NAS-ID profile: Not configured
Authorization : Strict checking
ACL          : Disabled
User profile  : Disabled

```

IPv4:

Portal status: Enabled  
Portal authentication method: Direct  
Portal web server: newpt  
Portal mac-trigger-server: Not configured  
Authentication domain: Not configured  
User-dhcp-only: Disabled  
Pre-auth IP pool: Not configured  
Max Portal users: Not configured  
Bas-ip: 2.2.2.1  
User detection: Not configured  
Action for server detection:  
    Server type  Server name                    Action  
    --          --                    --  
Layer3 source network:  
    IP address          Mask  
  
Destination authenticate subnet:  
    IP address          Mask

IPv6:

Portal status: Disabled  
Portal authentication method: Disabled  
Portal web server: Not configured  
Portal mac-trigger-server: Not configured  
Authentication domain: Not configured  
User-dhcp-only: Disabled  
Pre-auth IP pool: Not configured  
Max Portal users: Not configured  
Bas-ipv6: Not configured  
User detection: Not configured  
Action for server detection:  
    Server type  Server name                    Action  
    --          --                    --  
Layer3 source network:  
    IP address                            Prefix length  
  
Destination authenticate subnet:  
    IP address                            Prefix length

ユーザーは、H3C iNode クライアントまたは Web ブラウザを使用してポータル認証を実行できます。認証にパスする前に、ユーザーは <http://192.168.0.111:8080/portal> の認証ページにのみアクセスできます。ユーザーからのすべての Web 要求は、認証ページにリダイレクトされます。認証にパスした後、ユーザーは他のネットワークリソースにアクセスできます。

# ユーザーが認証に合格したら、次のコマンドを使用してポータルユーザーに関する情報を表示します。

[Switch] display portal user interface vlan-interface 100

Total portal users: 1  
Username: abc  
Portal server: newpt  
State: Online  
VPN instance: N/A

```

MAC          IP          VLAN Interface
0015-e9a6-7cfe 2.2.2.2      100 Vlan-interface100
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL: N/A
  Inbound CAR: N/A
  Outbound CAR: N/A

```

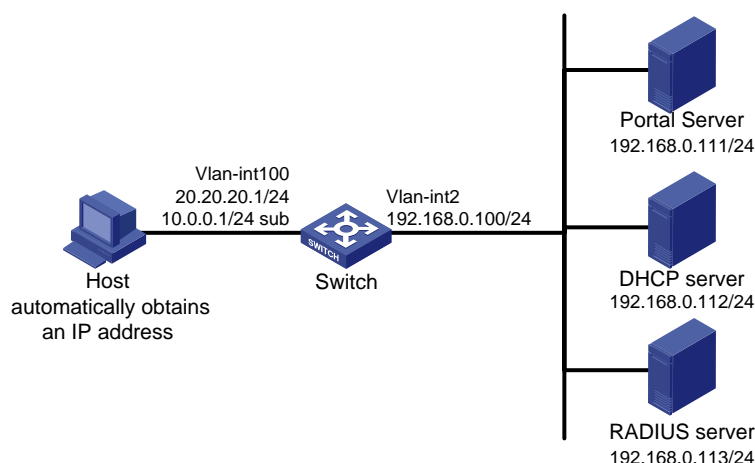
## 例:再 DHCP ポータル認証の設定

### ネットワーク構成

図 17 に示すように、ホストはスイッチ(アクセスデバイス)に直接接続されています。ホストは DHCP サーバーを介して IP アドレスを取得します。ポータルサーバーは、ポータル認証サーバーとポータル Web サーバーの両方として機能します。RADIUS サーバーは、認証/アカウントングサーバーとして機能します。

再 DHCP ポータル認証を構成します。認証にパスする前に、ホストにプライベート IP アドレスが割り当てられます。認証にパスした後、ホストはパブリック IP アドレスを取得し、ネットワークリソースにアクセスできます。

図 17 ネットワークダイアグラム



### 前提条件

- 図 18 に示すように、スイッチおよびサーバーの IP アドレスを設定し、ホスト、スイッチ、およびサーバーが相互に到達できることを確認します。
- RADIUS サーバーを正しく設定して、認証およびアカウントング機能を提供します。

### 制約事項とガイドライン

- DHCP ポータル再認証の場合は、DHCP サーバーにパブリックアドレスプール(20.20.20.0/24)とプライベートアドレスプール(10.0.0.0/24)を設定します(詳細は表示されません)。
- DHCP ポータル再認証の場合:
  - スイッチは DHCP リレーエージェントとして設定する必要があります。
  - ポータル対応インターフェースには、プライマリ IP アドレス(パブリック IP アドレス)とセカンダリ IP アドレス(プライベート IP アドレス)を設定する必要があります。

DHCP リレーエージェント設定の詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。

- ポータルサーバーに追加されたポータルデバイスの IP アドレスが、ホストに接続するスイッチのインターフェースのパブリック IP アドレス(20.20.20.1)であることを確認します。ポータルデバイスに関連付けられた IP アドレスグループのプライベート IP アドレス範囲は、ホストが存在するプライベートサブネットワーク 10.0.0.0/24 です。IP アドレスグループのパブリック IP アドレス範囲は、パブリックサブネットワーク 20.20.20.0/24 です。

## 手順

1. RADIUS スキームを設定します。

# **rs1** という名前の RADIUS スキームを作成し、そのビューを入力します。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

# プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。

```
[Switch-radius-rs1] primary authentication 192.168.0.113
```

```
[Switch-radius-rs1] primary accounting 192.168.0.113
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-radius-rs1] key accounting simple radius
```

# RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。

```
[Switch-radius-rs1] user-name-format without-domain
```

```
[Switch-radius-rs1] quit
```

# RADIUS セッション制御を有効にします。

```
[Switch] radius session-control enable
```

2. 認証ドメインを構成します。

# **dm1** という名前の ISP ドメインを作成し、そのビューを入力します。

```
[Switch] domain dm1
```

# ISP ドメインの AAA 方式を設定します。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-isp-dm1] quit
```

# ドメイン **dm1** をデフォルトの ISP ドメインとして設定します。ユーザーがログイン時に ISP ドメイン名なしでユーザー名を入力した場合、そのユーザーにはデフォルトドメインの認証およびアカウントिंग方式が使用されます。

```
[Switch] domain default enable dm1
```

3. DHCP リレーおよび許可 ARP を設定します。

# DHCP リレーを設定します。

```
[Switch] dhcp enable
```

```
[Switch] dhcp relay client-information record
```

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] ip address 20.20.20.1 255.255.255.0
```

```
[Switch-Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
```

```
[Switch-Vlan-interface100] dhcp select relay
```

```
[Switch-Vlan-interface100] dhcp relay server-address 192.168.0.112
```

# 許可された ARP を有効にします。

```
[Switch-Vlan-interface100] arp authorized enable
```

```
[Switch-Vlan-interface100] quit
```

4. ポータル認証を構成します。
- ```
# ポータル認証サーバーを構成します。
[Switch] portal server newpt
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
[Switch-portal-server-newpt] port 50100
[Switch-portal-server-newpt] quit

# ポータル Web サーバーを構成します。
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Switch-portal-websvr-newpt] quit

# VLAN インターフェース 100 で再 DHCP ポータル認証をイネーブルにします。
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] portal enable method redhcp

# VLAN インターフェース 100 上のポータル Web サーバーnewpt を指定します。
[Switch-Vlan-interface100] portal apply web-server newpt

# VLAN インターフェース 100 からポータル認証サーバーに送信されるポータルパケットの BAS-IP
を 20.20.20.1 に設定します。
[Switch-Vlan-interface100] portal bas-ip 20.20.20.1
[Switch-Vlan-interface100] quit
```

#### 設定の確認

```
#ポータル構成が有効になっていることを確認します。
[Switch] display portal interface vlan-interface 100
Portal information of Vlan-interface100
  NAS-ID profile: Not configured
  Authorization : Strict checking
  ACL           : Disabled
  User profile  : Disabled
IPv4:
  Portal status: Enabled
  Portal authentication method: Redhcp
  Portal web server: newpt
  Portal mac-trigger-server: Not configured
  Authentication domain: Not configured
  User-dhcp-only: Disabled
  Pre-auth IP pool: Not configured
  Max Portal users: Not configured
  Bas-ip: 20.20.20.1
  User detection: Not configured
  Action for server detection:
    Server type  Server name          Action
    --          --                  --
  Layer3 source network:
    IP address      Mask
  Destination authenticate subnet:
    IP address      Mask
IPv6:
  Portal status: Disabled
```

```

Portal authentication method: Disabled
Portal web server: Not configured
Portal mac-trigger-server: Not configured
Authentication domain: Not configured
User-dhcp-only: Disabled
Pre-auth IP pool: Not configured
Max Portal users: Not configured
Bas-ipv6: Not configured
User detection: Not configured
Action for server detection:
  Server type  Server name          Action
  --          --                  --
Layer3 source network:
  IP address          Prefix length

Destination authenticate subnet:
  IP address          Prefix length

```

認証にパスする前に、H3C iNode クライアントを使用するユーザーは、認証ページ <http://192.168.0.111:8080/portal> にのみアクセスできます。ユーザーからのすべての Web 要求は、認証ページにリダイレクトされます。認証にパスした後、ユーザーは他のネットワークリソースにアクセスできません。

#ユーザーが認証に合格したら、次のコマンドを使用してポータルユーザーに関する情報を表示します。

```

[Switch] display portal user interface vlan-interface 100
Total portal users: 1
Username: abc
Portal server: newpt
State: Online
VPN instance: N/A
MAC          IP          VLAN  Interface
0015-e9a6-7cfe  20.20.20.2  100  Vlan-interface100
Authorization information:
DHCP IP pool: N/A
User profile: N/A
Session group profile: N/A
ACL: N/A
Inbound CAR: N/A
Outbound CAR: N/A

```

## 例:クロスサブネットポータル認証の設定

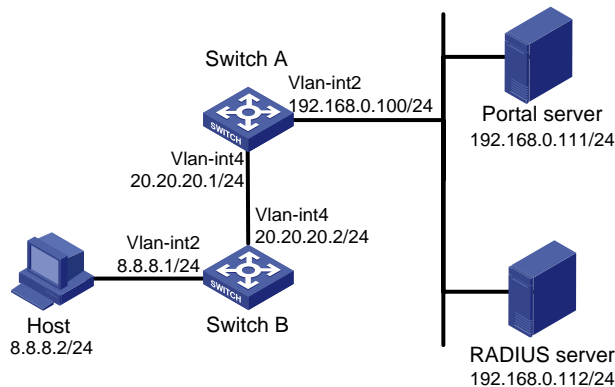
### ネットワーク構成

図 18 に示すように、スイッチ A はポータル認証をサポートしています。ホストはスイッチ B を介してスイッチ A にアクセスします。ポータルサーバーは、ポータル認証サーバーとポータル Web サーバーの両方として機能します。RADIUS サーバーは、認証/アカウンティングサーバーとして機能します。

スイッチ A をクロスサブネットポータル認証用に設定します。認証にパスする前に、ホストはポータル Web サーバーにのみアクセスできます。認証にパスした後、ユーザーは他のネットワークリソースにアクセスできます。



図 18 ネットワークダイアグラム



## 前提条件

- 図 18 に示すように、スイッチおよびサーバーの IP アドレスを設定し、ホスト、スイッチ、およびサーバーが相互に到達できることを確認します。
- RADIUS サーバーを正しく設定して、認証およびアカウントング機能を提供します。

## 制約事項とガイドライン

ポータル認証サーバーに追加されたポータルデバイスの IP アドレスが、ホストに接続しているスイッチのインターフェースの IP アドレス(20.20.20.1)であることを確認します。ポータルデバイスに関連付けられた IP アドレスグループは、ホストのサブネット(8.8.8.0/24)です。

## 手順

1. RADIUS スキームを設定します。

#rs1 という名前の RADIUS スキームを作成し、そのビューを入力します。

```
<SwitchA> system-view
```

```
[SwitchA] radius scheme rs1
```

# プライマリ認証サーバーおよびプライマリアccountingサーバーを指定し、サーバーと通信するためのキーを設定します。

```
[SwitchA-radius-rs1] primary authentication 192.168.0.112
```

```
[SwitchA-radius-rs1] primary accounting 192.168.0.112
```

```
[SwitchA-radius-rs1] key authentication simple radius
```

```
[SwitchA-radius-rs1] key accounting simple radius
```

#RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。

```
[SwitchA-radius-rs1] user-name-format without-domain
```

```
[SwitchA-radius-rs1] quit
```

#RADIUS セッション制御を有効にします。

```
[SwitchA] radius session-control enable
```

2. 認証ドメインを構成します。

# dm1 という名前の ISP ドメインを作成し、そのビューを入力します。

```
[SwitchA] domain dm1
```

#ISP ドメインの AAA 方式を設定します。

```
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
```

```
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
```

```
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
```

```
[SwitchA-isp-dm1] quit
```

#ドメイン dm1 をデフォルトの ISPドメインとして設定します。ユーザーがログイン時に ISPドメイン名なしでユーザー名を入力した場合、そのユーザーにはデフォルトドメインの認証およびアカウントインテグレーション方式が使用されます。

```
[SwitchA] domain default enable dm1
```

### 3. ポータル認証を構成します。

# ポータル認証サーバーを構成します。

```
[SwitchA] portal server newpt
```

```
[SwitchA-portal-server-newpt] ip 192.168.0.111 key simple portal
```

```
[SwitchA-portal-server-newpt] port 50100
```

```
[SwitchA-portal-server-newpt] quit
```

# ポータル Web サーバーを構成します。

```
[SwitchA] portal web-server newpt
```

```
[SwitchA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

```
[SwitchA-portal-websvr-newpt] quit
```

# VLAN インターフェース 4 でクロスサブネットポータル認証を有効にします。

```
[SwitchA] interface vlan-interface 4
```

```
[SwitchA-Vlan-interface4] portal enable method layer3
```

# VLAN-interface 4 のポータル Web サーバーnewpt を指定します。

```
[SwitchA-Vlan-interface4] portal apply web-server newpt
```

# VLAN インターフェース 4 からポータル認証サーバーに送信されるポータルパケットの BAS-IP を 20.20.20.1 に設定します。

```
[SwitchA-Vlan-interface4] portal bas-ip 20.20.20.1
```

```
[SwitchA-Vlan-interface4] quit
```

## 設定の確認

#ポータル構成が有効になっていることを確認します。

```
[SwitchA] display portal interface vlan-interface 4
```

```
Portal information of Vlan-interface4
```

```
  NAS-ID profile: Not configured
```

```
  Authorization : Strict checking
```

```
  ACL           : Disabled
```

```
  User profile  : Disabled
```

```
IPv4:
```

```
  Portal status: Enabled
```

```
  Portal authentication method: Layer3
```

```
  Portal web server: newpt
```

```
  Portal mac-trigger-server: Not configured
```

```
  Authentication domain: Not configured
```

```
  User-dhcp-only: Disabled
```

```
  Pre-auth IP pool: Not configured
```

```
  Max Portal users: Not configured
```

```
  Bas-ip: 20.20.20.1
```

```
  User detection: Not configured
```

```
  Action for server detection:
```

```
    Server type  Server name          Action
```

```
    --          --                  --
```

```
  Layer3 source network:
```

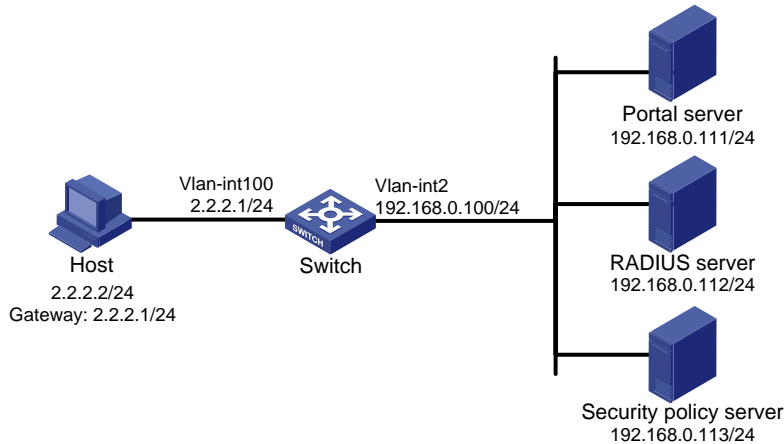
```
    IP address      Mask
```



ポータル Web サーバーの両方として機能します。RADIUS サーバーは、認証/アカウントングサーバーとして機能します。

拡張ダイレクトポータル認証を構成します。ホストが ID 認証に合格した後にセキュリティチェックに失敗した場合、サブネット 192.168.0.0/24 にのみアクセスできます。セキュリティチェックに合格した後、ホストは他のネットワークリソースにアクセスできます。

図 19 ネットワークダイアグラム



## 前提条件

- 図 19 に示すように、ホスト、スイッチ、およびサーバーの IP アドレスを設定し、それらが相互に到達できることを確認します。
- RADIUS サーバーを正しく設定して、認証およびアカウントング機能を提供します。

## 手順

1. RADIUS スキームを設定します。

#rs1 という名前の RADIUS スキームを作成し、そのビューを入力します。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

#プライマリ認証サーバーおよびプライマリアカウントングサーバーを指定し、サーバーと通信するためのキーを設定します。

```
[Switch-radius-rs1] primary authentication 192.168.0.112
```

```
[Switch-radius-rs1] primary accounting 192.168.0.112
```

```
[Switch-radius-rs1] key accounting simple radius
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-radius-rs1] user-name-format without-domain
```

#RADIUS セッション制御を有効にします。

```
[Switch] radius session-control enable
```

# プレーンテキスト形式で、IP アドレスが 192.168.0.112、共有キーが 12345 のセッション制御クライアントを指定します。

```
[Switch] radius session-control client ip 192.168.0.112 key simple 12345
```

2. 認証ドメインを構成します。

# dm1 という名前の ISP ドメインを作成し、そのビューを入力します。

```
[Switch] domain dm1
```

# ISP ドメインの AAA 方式を設定します。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
[Switch-isp-dm1] quit
```

#ドメイン **dm1** をデフォルトの ISPドメインとして設定します。ユーザーがログイン時に ISPドメイン名なしでユーザー名を入力した場合、そのユーザーにはデフォルトドメインの認証およびアカウントイング方式が使用されます。

```
[Switch] domain default enable dm1
```

3. ACL 3000 を隔離 ACL として設定し、ACL 3001 をセキュリティ ACL として設定します。

```
[Switch] acl advanced 3000
[Switch-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
[Switch-acl-ipv4-adv-3000] rule deny ip
[Switch-acl-ipv4-adv-3000] quit
[Switch] acl advanced 3001
[Switch-acl-ipv4-adv-3001] rule permit ip
[Switch-acl-ipv4-adv-3001] quit
```

---

#### 注:

セキュリティポリシーサーバーで、隔離 ACL として ACL 3000 を指定し、セキュリティ ACL として ACL 3001 を指定していることを確認します。

---

4. ポータル認証を構成します。

# ポータル認証サーバーを構成します。

```
[Switch] portal server newpt
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
[Switch-portal-server-newpt] port 50100
[Switch-portal-server-newpt] quit
```

# ポータル Web サーバーを構成します。

```
[Switch] portal web-server newpt
[Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[Switch-portal-websvr-newpt] quit
```

# VLAN インターフェース 100 でダイレクトポータル認証をイネーブルにします。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] portal enable method direct
```

# VLAN インターフェース 100 上のポータル Web サーバーnewpt を指定します。

```
[Switch-Vlan-interface100] portal apply web-server newpt
```

# VLAN インターフェース 100 からポータル認証サーバーに送信されるポータルパケットの BAS-IP を 2.2.2.1 に設定します。

```
[Switch-Vlan-interface100] portal bas-ip 2.2.2.1
[Switch-Vlan-interface100] quit
```

#### 設定の確認

# ポータル構成が有効になっていることを確認します。

```
[Switch] display portal interface vlan-interface 100
Portal information of Vlan-interface100
NAS-ID profile: Not configured
Authorization : Strict checking
ACL          : Disabled
User profile  : Disabled
IPv4:
```

Portal status: Enabled  
 Portal authentication method: Direct  
 Portal web server: newpt  
 Portal mac-trigger-server: Not configured  
 Authentication domain: Not configured  
 User-dhcp-only: Disabled  
 Pre-auth IP pool: Not configured  
 Max Portal users: Not configured  
 Bas-ip: 2.2.2.1  
 User detection: Not configured  
 Action for server detection:

| Server type | Server name | Action |
|-------------|-------------|--------|
| --          | --          | --     |

Layer3 source network:

| IP address | Mask |
|------------|------|
|            |      |

Destination authenticate subnet:

| IP address | Mask |
|------------|------|
|            |      |

IPv6:

Portal status: Disabled  
 Portal authentication method: Disabled  
 Portal web server: Not configured  
 Portal mac-trigger-server: Not configured  
 Authentication domain: Not configured  
 User-dhcp-only: Disabled  
 Pre-auth IP pool: Not configured  
 Max Portal users: Not configured  
 Bas-ipv6: Not configured  
 User detection: Not configured  
 Action for server detection:

| Server type | Server name | Action |
|-------------|-------------|--------|
| --          | --          | --     |

Layer3 source network:

| IP address | Prefix length |
|------------|---------------|
|            |               |

Destination authenticate subnet:

| IP address | Prefix length |
|------------|---------------|
|            |               |

ポータル認証を通過する前に、H3C iNode クライアントを使用するユーザーは、**http://192.168.0.111:8080/portal** の認証ページにのみアクセスできます。ユーザーからのすべての Web 要求は、認証ページにリダイレクトされます。

- ユーザーは、ID 認証だけを通過した後、ACL 3000 によって許可されたリソースにアクセスできます。
- ユーザーは、ID 認証とセキュリティチェックの両方に合格すると、ACL 3001 によって許可されたネットワークリソースにアクセスできます。

#ユーザーが ID 認証とセキュリティチェックに合格したら、次のコマンドを使用してポータルユーザーに関する情報を表示します。

```

[Switch] display portal user interface vlan-interface 100
Total portal users: 1
Username: abc
Portal server: newpt
  
```

```

State: Online
VPN instance: N/A
MAC      IP      VLAN Interface
0015-e9a6-7cfe  2.2.2.2    100  Vlan-interface100
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL: 3001
  Inbound CAR: N/A
  Outbound CAR: N/A

```

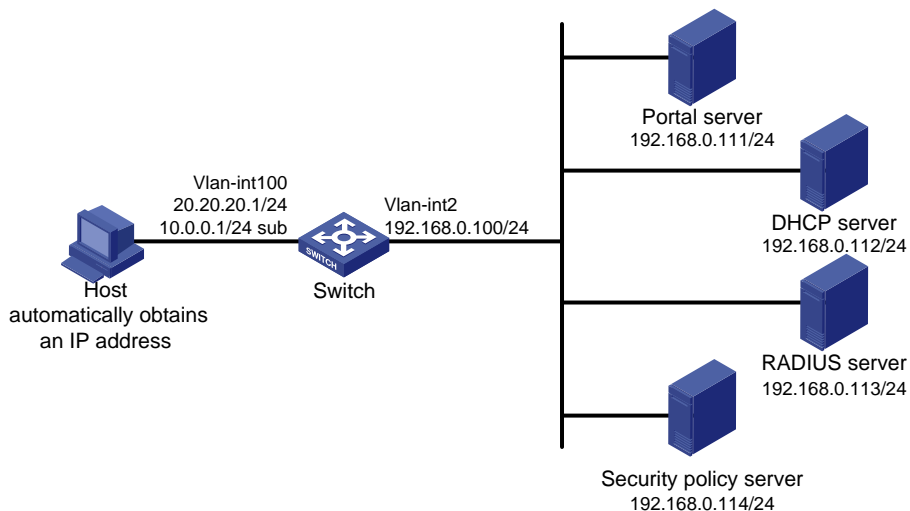
## 例:拡張 re-DHCP ポータル認証の設定

### ネットワーク構成

図 20 に示すように、ホストはスイッチ(アクセスデバイス)に直接接続されています。ホストは DHCP サーバーを介して IP アドレスを取得します。ポータルサーバーは、ポータル認証サーバーとポータル Web サーバーの両方として機能します。RADIUS サーバーは、認証/アカウントサーバーとして機能します。

拡張再 DHCP ポータル認証を構成します。ポータル認証を通過する前に、ホストにプライベート IP アドレスが割り当てられます。ポータル ID 認証を通過した後、ホストはパブリック IP アドレスを取得し、セキュリティチェックを受け入れます。ホストがセキュリティチェックに失敗した場合、サブネット 192.168.0.0/24 にのみアクセスできます。セキュリティチェックに合格した後、ホストは他のネットワークリソースにアクセスできます。

図 20 ネットワークダイアグラム



### 前提条件

- 図 20 に示すように、スイッチおよびサーバーの IP アドレスを設定し、ホスト、スイッチ、およびサーバーが相互に到達できることを確認します。
- RADIUS サーバーを正しく設定して、認証およびアカウント機能を提供します。

### 制約事項とガイドライン

- DHCP ポータル再認証の場合は、DHCP サーバーにパブリックアドレスプール(20.20.20.0/24)とプライベートアドレスプール(10.0.0.0/24)を設定します(詳細は表示されません)。
- DHCP ポータル再認証の場合:

- スイッチは DHCP リレーエージェントとして設定する必要があります。
- ポータル対応インターフェースには、プライマリ IP アドレス(パブリック IP アドレス)とセカンダリ IP アドレス(プライベート IP アドレス)を設定する必要があります。

DHCP リレーエージェント設定の詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。

- ポータルサーバーに追加されたポータルデバイスの IP アドレスが、ホストに接続するスイッチのインターフェースのパブリック IP アドレス(20.20.20.1)であることを確認します。ポータルデバイスに関連付けられた IP アドレスグループのプライベート IP アドレス範囲は、ホストが存在するプライベートサブネット 10.0.0.0/24 です。IP アドレスグループのパブリック IP アドレス範囲は、パブリックサブネット 20.20.20.0/24 です。

## 手順

1. RADIUS スキームを設定します。

# rs1 という名前の RADIUS スキームを作成し、そのビューを入力します。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

# プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。

```
[Switch-radius-rs1] primary authentication 192.168.0.113
```

```
[Switch-radius-rs1] primary accounting 192.168.0.113
```

```
[Switch-radius-rs1] key accounting simple radius
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-radius-rs1] user-name-format without-domain
```

# RADIUS セッション制御を有効にします。

```
[Switch] radius session-control enable
```

# プレーンテキスト形式で、IP アドレスが 192.168.0.113、共有キーが 12345 のセッション制御クライアントを指定します。

```
[Switch] radius session-control client ip 192.168.0.113 key simple 12345
```

2. 認証ドメインを構成します。

# dm1 という名前の ISP ドメインを作成し、そのビューを入力します。

```
[Switch] domain dm1
```

# ISP ドメインの AAA 方式を設定します。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-isp-dm1] quit
```

# ドメイン dm1 をデフォルトの ISP ドメインとして設定します。ユーザーがログイン時に ISP ドメイン名なしでユーザー名を入力した場合、そのユーザーにはデフォルトドメインの認証およびアカウンティング方式が使用されます。

```
[Switch] domain default enable dm1
```

3. ACL 3000 を隔離 ACL として設定し、ACL 3001 をセキュリティ ACL として設定します。

```
[Switch] acl advanced 3000
```

```
[Switch-acl-ipv4-adv-3000] rule permit ip destination 192.168.0.0 0.0.0.255
```

```
[Switch-acl-ipv4-adv-3000] rule deny ip
```

```
[Switch-acl-ipv4-adv-3000] quit
```

```
[Switch] acl advanced 3001
```

```
[Switch-acl-ipv4-adv-3001] rule permit ip
```

```
[Switch-acl-ipv4-adv-3001] quit
```



---

**注:**

セキュリティポリシーサーバーで、隔離 ACL として ACL 3000 を指定し、セキュリティ ACL として ACL 3001 を指定していることを確認します。

---

**4. DHCP リレーおよび許可 ARP を設定します。**

# DHCP リレーを設定します。

```
[Switch] dhcp enable
```

```
[Switch] dhcp relay client-information record
```

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] ip address 20.20.20.1 255.255.255.0
```

```
[Switch-Vlan-interface100] ip address 10.0.0.1 255.255.255.0 sub
```

```
[Switch-Vlan-interface100] dhcp select relay
```

```
[Switch-Vlan-interface100] dhcp relay server-address 192.168.0.112
```

# 許可された ARP を有効にします。

```
[Switch-Vlan-interface100] arp authorized enable
```

```
[Switch-Vlan-interface100] quit
```

**5. ポータル認証を構成します。**

# ポータル認証サーバーを構成します。

```
[Switch] portal server newpt
```

```
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal
```

```
[Switch-portal-server-newpt] port 50100
```

```
[Switch-portal-server-newpt] quit
```

# ポータル Web サーバーを構成します。

```
[Switch] portal web-server newpt
```

```
[Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal
```

```
[Switch-portal-websvr-newpt] quit
```

# VLAN インターフェース 100 で再 DHCP ポータル認証をイネーブルにします。

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] portal enable method redhcp
```

# VLAN インターフェース 100 上のポータル Web サーバー newpt を指定します。

```
[Switch-Vlan-interface100] portal apply web-server newpt
```

# VLAN インターフェース 100 からポータル認証サーバーに送信されるポータルパケットの BAS-IP を 20.20.20.1 に設定します。

```
[Switch-Vlan-interface100] portal bas-ip 20.20.20.1
```

```
[Switch-Vlan-interface100] quit
```

**設定の確認**

#ポータル構成が有効になっていることを確認します。

```
[Switch] display portal interface vlan-interface 100
```

```
Portal information of Vlan-interface100
```

```
NAS-ID profile: Not configured
```

```
Authorization : Strict checking
```

```
ACL          : Disabled
```

```
User profile  : Disabled
```

```
IPv4:
```

```
Portal status: Enabled
```

```
Portal authentication method: Redhcp
```

Portal web server: newpt  
 Portal mac-trigger-server: Not configured  
 Authentication domain: Not configured  
 User-dhcp-only: Disabled  
 Pre-auth IP pool: Not configured  
 Max Portal users: Not configured  
 Bas-ip: 20.20.20.1  
 User detection: Not configured  
 Action for server detection:  

| Server type | Server name | Action |
|-------------|-------------|--------|
| --          | --          | --     |

Layer3 source network:  

| IP address | Mask |
|------------|------|
|            |      |

Destination authenticate subnet:  

| IP address | Mask |
|------------|------|
|            |      |

#### IPv6:

Portal status: Disabled  
 Portal authentication method: Disabled  
 Portal web server: Not configured  
 Portal mac-trigger-server: Not configured  
 Authentication domain: Not configured  
 User-dhcp-only: Disabled  
 Pre-auth IP pool: Not configured  
 Max Portal users: Not configured  
 Bas-ipv6: Not configured  
 User detection: Not configured  
 Action for server detection:  

| Server type | Server name | Action |
|-------------|-------------|--------|
| --          | --          | --     |

Layer3 source network:  

| IP address | Prefix length |
|------------|---------------|
|            |               |

Destination authenticate subnet:  

| IP address | Prefix length |
|------------|---------------|
|            |               |

ポータル認証を通過する前に、H3C iNode クライアントを使用するユーザーは、<http://192.168.0.111:8080/portal> の認証ページにのみアクセスできます。ユーザーからのすべての Web 要求は、認証ページにリダイレクトされます。

- ユーザーは、ID 認証だけを通過した後、ACL 3000 によって許可されたリソースにアクセスできます。
- ユーザーは、ID 認証とセキュリティチェックの両方に合格すると、ACL 3001 によって許可されたネットワークリソースにアクセスできます。

#ユーザーが ID 認証とセキュリティチェックに合格したら、次のコマンドを使用してポータルユーザーに関する情報を表示します。

```
[Switch] display portal user interface vlan-interface 100
```

Total portal users: 1

Username: abc

Portal server: newpt

State: Online

VPN instance: N/A

```

MAC          IP          VLAN Interface
0015-e9a6-7cfe 20.20.20.2 100 Vlan-interface100
Authorization information:
  DHCP IP pool: N/A
  User profile: N/A
  Session group profile: N/A
  ACL: 3001
  Inbound CAR: N/A
  Outbound CAR: N/A

```

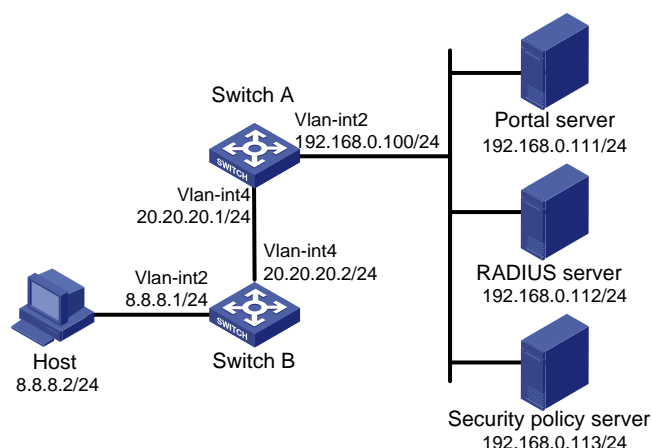
## 例:拡張クロスサブネットポータル認証の設定

### ネットワーク構成

図 21 に示すように、スイッチ A はポータル認証をサポートしています。ホストはスイッチ B を介してスイッチ A にアクセスします。ポータルサーバーは、ポータル認証サーバーとポータル Web サーバーの両方として機能します。RADIUS サーバーは、認証/アカウントサーバーとして機能します。

拡張クロスサブネットポータル認証用にスイッチ A を設定します。ポータル認証にパスする前に、ホストはポータルサーバーにのみアクセスできます。ポータル ID 認証にパスした後、ホストはセキュリティチェックを受け入れます。ホストがセキュリティチェックに失敗した場合、サブネット 192.168.0.0/24 にのみアクセスできます。セキュリティチェックにパスした後、ホストは他のネットワークリソースにアクセスできます。

図 21 ネットワークダイアグラム



### 前提条件

- 図 21 に示すように、スイッチおよびサーバーの IP アドレスを設定し、ホスト、スイッチ、およびサーバーが相互に到達できることを確認します。
- RADIUS サーバーを正しく設定して、認証およびアカウント機能を提供します。

### 制約事項とガイドライン

ポータルサーバーに追加されたポータルデバイスの IP アドレスが、ホストに接続しているスイッチのインターフェースの IP アドレス(20.20.20.1)であることを確認します。ポータルデバイスに関連付けられた IP アドレスグループは、ホストのサブネット(8.8.8.0/24)です。

### 手順

1. RADIUS スキームを設定します。  
# rs1 という名前の RADIUS スキームを作成し、そのビューを入力します。

```
<SwitchA> system-view
[SwitchA] radius scheme rs1
# プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信する
ためのキーを設定します。
[SwitchA-radius-rs1] primary authentication 192.168.0.112
[SwitchA-radius-rs1] primary accounting 192.168.0.112
[SwitchA-radius-rs1] key accounting simple radius
[SwitchA-radius-rs1] key authentication simple radius
[SwitchA-radius-rs1] user-name-format without-domain
# RADIUS セッション制御を有効にします。
[SwitchA] radius session-control enable
# プレーンテキスト形式で、IP アドレスが 192.168.0.112、共有キーが 12345 のセッション制御クライ
アントを指定します。
[SwitchA] radius session-control client ip 192.168.0.112 key simple 12345
```

2. 認証ドメインを構成します。

```
# dm1 という名前の ISP ドメインを作成し、そのビューを入力します。
[SwitchA] domain dm1
# ISP ドメインの AAA 方式を設定します。
[SwitchA-isp-dm1]認証ポータル radius-scheme rs1
[SwitchA-isp-dm1]許可ポータル radius-scheme rs1
[SwitchA-isp-dm1]アカウントポータル radius-scheme rs1
[SwitchA-isp-dm1]終了
# ドメイン dm1 をデフォルトの ISP ドメインとして設定します。ユーザーがログイン時に ISP ドメイン名
なしでユーザー名を入力した場合、そのユーザーにはデフォルトドメインの認証およびアカウント
ング方式が使用されます。
[SwitchA]ドメインデフォルトで dm1 を有効にする
```

3. ACL 3000 を隔離 ACL として設定し、ACL 3001 をセキュリティ ACL として設定します。

```
[SwitchA-isp-dm1] authentication portal radius-scheme rs1
[SwitchA-isp-dm1] authorization portal radius-scheme rs1
[SwitchA-isp-dm1] accounting portal radius-scheme rs1
[SwitchA-isp-dm1] quit
```

---

**注:**

セキュリティポリシーサーバーで、隔離 ACL として ACL 3000 を指定し、セキュリティ ACL として ACL 3001 を指定していることを確認します。

---

4. ポータル認証を構成します。

```
# ポータル認証サーバーを構成します。
[SwitchA] portal server newpt
[SwitchA-portal-server-newpt] ip 192.168.0.111 key simple portal
[SwitchA-portal-server-newpt] port 50100
[SwitchA-portal-server-newpt] quit
# ポータル Web サーバーを構成します。
[SwitchA] portal web-server newpt
[SwitchA-portal-websvr-newpt] url http://192.168.0.111:8080/portal
[SwitchA-portal-websvr-newpt] quit
# VLAN インターフェース 4 でクロスサブネットポータル認証を有効にします。
```

```
[SwitchA] interface vlan-interface 4
[SwitchA-Vlan-interface4] portal enable method layer3
# VLAN-interface 4 のポータル Web サーバーnewpt を指定します。
[SwitchA-Vlan-interface4] portal apply web-server newpt
# VLAN インターフェース 4 からポータル認証サーバーに送信されるポータルパケットの BAS-IP を
20.20.20.1 に設定します。
[SwitchA-Vlan-interface4] portal bas-ip 20.20.20.1
[SwitchA-Vlan-interface4] quit
```

## 設定の確認

# ポータル構成が有効になっていることを確認します。

```
[SwitchA] display portal interface vlan-interface 4
```

```
Portal information of Vlan-interface4
```

```
NAS-ID profile: Not configured
```

```
Authorization : Strict checking
```

```
ACL          : Disabled
```

```
User profile : Disabled
```

```
IPv4:
```

```
Portal status: Enabled
```

```
Portal authentication method: Layer3
```

```
Portal web server: newpt
```

```
Portal mac-trigger-server: Not configured
```

```
Authentication domain: Not configured
```

```
User-dhcp-only: Disabled
```

```
Pre-auth IP pool: Not configured
```

```
Max Portal users: Not configured
```

```
Bas-ip: 20.20.20.1
```

```
User detection: Not configured
```

```
Action for server detection:
```

| Server type | Server name | Action |
|-------------|-------------|--------|
| --          | --          | --     |

```
Layer3 source network:
```

| IP address | Mask |
|------------|------|
|            |      |

```
Destination authenticate subnet:
```

| IP address | Mask |
|------------|------|
|            |      |

```
IPv6:
```

```
Portal status: Disabled
```

```
Portal authentication method: Disabled
```

```
Portal web server: Not configured
```

```
Portal mac-trigger-server: Not configured
```

```
Authentication domain: Not configured
```

```
User-dhcp-only: Disabled
```

```
Pre-auth IP pool: Not configured
```

```
Max Portal users: Not configured
```

```
Bas-ip: Not configured
```

```
User detection: Not configured
```

```
Action for server detection:
```

| Server type | Server name | Action |
|-------------|-------------|--------|
|             |             |        |

-- -- --  
Layer3 source network:

IP address

Prefix length

Destination authenticate subnet:

IP address

Prefix length

ポータル認証を通過する前に、H3C iNode クライアントを使用するユーザーは、<http://192.168.0.111:8080/portal> の認証ページにのみアクセスできます。ユーザーからのすべての Web 要求は、認証ページにリダイレクトされます。

- ユーザーは、ID 認証だけを通過した後、ACL 3000 によって許可されたリソースにアクセスできます。
- ユーザーは、ID 認証とセキュリティチェックの両方に合格すると、ACL 3001 によって許可されたネットワークリソースにアクセスできます。

#ユーザーが ID 認証とセキュリティチェックに合格したら、次のコマンドを使用してポータルユーザーに関する情報を表示します。

```
[SwitchA] display portal user interface vlan-interface 4
```

```
Total portal users: 1
```

```
Username: abc
```

```
Portal server: newpt
```

```
State: Online
```

```
VPN instance: N/A
```

```
MAC          IP          VLAN  Interface
```

```
0015-e9a6-7cfe 8.8.8.2    4    Vlan-interface4
```

```
Authorization information:
```

```
DHCP IP pool: N/A
```

```
User profile: N/A
```

```
Session group profile: N/A
```

```
ACL: 3001
```

```
Inbound CAR: N/A
```

```
Outbound CAR: N/A
```

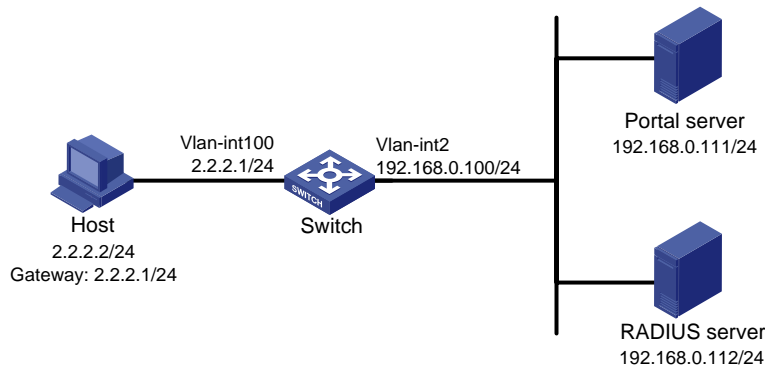
## 例:ポータルサーバーの検出とポータルユーザーの同期化の構成

### ネットワーク構成

図 22 に示すように、ホストはスイッチ(アクセスデバイス)に直接接続されています。ホストには、手動または DHCP を介してパブリック IP アドレスが割り当てられます。ポータルサーバーは、ポータル認証サーバーとポータル Web サーバーの両方として機能します。RADIUS サーバーは、認証/アカウンティングサーバーとして機能します。

- スイッチに直接ポータル認証を設定して、ホストが認証を渡す前にポータルサーバーだけにアクセスし、認証を渡した後、他のネットワークリソースにアクセスできるようにします。
- ポータル認証サーバーの到達可能性ステータスを検出し、ステータス変更時にログメッセージを送信し、認証サーバーが到達不能な場合にポータル認証をディセーブルにするようにスイッチを設定します。
- ポータルユーザー情報をポータルサーバーと定期的に同期するようにスイッチを設定します。

図 22 ネットワークダイアグラム



## 前提条件

- 図 22 に示すように、スイッチおよびサーバーの IP アドレスを設定し、ホスト、スイッチ、およびサーバーが相互に到達できることを確認します。
- RADIUS サーバーを正しく設定して、認証およびアカウントング機能を提供します。

## IMC PLAT 3.20 でのポータル認証サーバーの設定

この例では、ポータルサーバーは IMC PLAT 3.20-R2602P13 および IMC UAM 3.60-E6301 上で動作します。

1. ポータル認証サーバーを設定します。
  - a. IMC にログインし、**Service** タブをクリックします。
  - b. ナビゲーションツリーから **Access Service > Portal Service Management > Server** を選択して、ポータルサーバー設定ページを開きます(図 23 を参照)。
  - c. ポータルサーバーのハートビート間隔とユーザーのハートビート間隔を構成します。
  - d. その他のパラメーターには既定の設定を使用します。
  - e. **OK** をクリックします。

図 23 ポータル認証サーバーの構成

Service >> Access Service >> Portal Service Management >> Server

Portal Server Configuration

**Basic Information**

\* Log Level: Info

\* Server Heartbeat Interval: 20 Seconds

\* Request Timeout: 5 Seconds

\* User Heartbeat Interval: 5 Minutes

**Advanced Information**

Service Type List

Add

Total Items: 0.

| Service Type ID | Service Type | Delete |
|-----------------|--------------|--------|
|-----------------|--------------|--------|

OK Refresh

2. IP アドレスグループを設定します。
  - a. ナビゲーションツリーから **Access Service > Portal Service Management > IP Group** を選択して、ポータル IP アドレスグループ設定ページを開きます。
  - b. **Add** をクリックしてページを開きます(図 24 を参照)。
  - c. IP グループ名を入力します。

- d. IP グループの開始 IP アドレスと終了 IP アドレスを入力します。  
ホスト IP アドレス(2.2.2.2)が IP グループに含まれていることを確認します。
- e. サービスグループを選択します。  
この例では、既定のグループ **Ungrouped** を使用します。
- f. **Normal** アクションを選択します。
- g. **OK** をクリックします。

図 24 IP アドレスグループの追加

3. ポータルデバイスを追加します。
  - a. ナビゲーションツリーから **Access Service > Portal Service Management > Device** を選択して、ポータルデバイス設定ページを開きます。
  - b. **Add** をクリックしてページを開きます(図 25 を参照)。
  - c. デバイス名 **NAS** を入力します。
  - d. ホストに接続されているスイッチのインターフェースの IP アドレスを入力します。
  - e. キーを入力します。このキーは、スイッチに設定されているキーと同じでなければなりません。
  - f. IP アドレスの再割り当てを有効にするかどうかを設定します。  
この例では、直接ポータル認証を使用するため、**Reallocate IP** リストから **No** を選択します。
  - g. ポータルサーバーハートビートおよびユーザーハートビート機能をサポートするかどうかを設定します。  
この例では、**Support Server Heartbeat** と **Support User Heartbeat** の両方で **Yes** を選択します。
  - h. **OK** をクリックします。

図 25 ポータルデバイスを追加する



4. ポータルデバイスを IP アドレスグループに関連付けます。
  - a. 図 26 に示すように、デバイス NAS の **Port Group Information Management** カラムのアイコンをクリックして、ポートグループ設定ページを開きます。

図 26 デバイスリスト

| Device Information List |            |               |            |         |        |                                   |                                   |
|-------------------------|------------|---------------|------------|---------|--------|-----------------------------------|-----------------------------------|
| Add                     |            |               |            |         |        |                                   |                                   |
| 1-1 of 1. Page 1 of 1.  |            |               |            |         |        | Items per Page: 8 15 [50] 100 200 |                                   |
| Device Name             | Version    | Service Group | IP Address | Details | Modify | Delete                            | Port Group Information Management |
| NAS                     | Portal 2.0 | Ungrouped     | 2.2.2.1    |         |        |                                   |                                   |

- b. **Add** をクリックしてページを開きます(図 27 を参照)。

図 27 ポートグループ設定

Service >> Access Service >> Portal Service Management >> Portal Device Configuration >> Port Group Info Config >> Add Port Group Info

**Add Port Group Info**

**Port Group Information**

|                             |                                    |                                  |                      |
|-----------------------------|------------------------------------|----------------------------------|----------------------|
| * Port Group Name           | <input type="text" value="group"/> | * Language                       | Dynamic Detection    |
| * Start Port                | <input type="text" value="0"/>     | * End Port                       | zzzzzz               |
| * Protocol                  | HTTP                               | * Quick Authentication           | No                   |
| * NAT or Not                | No                                 | * Error Transparent Transmission | Yes                  |
| * Authentication Type       | CHAP                               | * IP Group                       | Portal_user          |
| * Heartbeat Interval        | 10 Minutes                         | * Heartbeat Timeout              | 30 Minutes           |
| User Domain                 | <input type="text"/>               | Port Group Description           | <input type="text"/> |
| User Attribute Type         | <input type="text"/>               | Default Authentication Page      | index_default.jsp    |
| Default Authentication Type | Web Identity AuthN                 |                                  |                      |

OK Cancel

- c. ポートグループ名を入力します。
  - d. 設定済みの IP アドレスグループを選択します。  
ユーザーがネットワークにアクセスするために使用する IP アドレスは、この IP アドレスグループ内にある必要があります。
  - e. その他のパラメーターのユーザーデフォルト値。
  - f. **OK** をクリックします。
5. ナビゲーションツリーから[Access Service]>[Service Parameters]>[Validate System Configuration]を選択して、設定を検証します。

## IMC PLAT 5.0 でのポータル認証サーバーの設定

この例では、ポータルサーバーは IMC PLAT 5.0(E0101)および IMC UAM 5.0(E0101)上で動作します。

1. ポータル認証サーバーを設定します。
  - a. IMC にログインし、**Service** タブをクリックします。
  - b. ナビゲーションツリーから **User Access Manager > Portal Service Management > Server** を選択して、ポータルサーバー設定ページを開きます(図 28 を参照)。
  - c. ポータルサーバーのハートビート間隔とユーザーのハートビート間隔を構成します。
  - d. その他のパラメーターには既定の設定を使用します。
  - e. **OK** をクリックします。

図 28 ポータル認証サーバーの構成

2. IP アドレスグループを設定します。
  - a. ナビゲーションツリーから **User Access Manager > Portal Service Management > IP Group** を選択して、ポータル IP アドレスグループ設定ページを開きます。
  - b. **Add** をクリックしてページを開きます(図 29 を参照)。
  - c. IP グループ名を入力します。
  - d. IP グループの開始 IP アドレスと終了 IP アドレスを入力します。  
ホスト IP アドレスが IP グループに含まれていることを確認します。
  - e. サービスグループを選択します。  
この例では、既定のグループ **Ungrouped** を使用します。
  - f. **Normal** アクションを選択します。
  - g. **OK** をクリックします。

図 29 IP アドレスグループの追加

3. ポータルデバイスを追加します。

- a. ナビゲーションツリーから **User Access Manager > Portal Service Management > Device** を選択して、ポータルデバイス設定ページを開きます。
- b. **Add** をクリックしてページを開きます(図 30 を参照)。
- c. デバイス名 **NAS** を入力します。
- d. ホストに接続されているスイッチのインターフェースの IP アドレスを入力します。
- e. キーを入力します。このキーは、スイッチに設定されているキーと同じでなければなりません。
- f. IP アドレスの再割り当てを有効にするかどうかを設定します。  
この例では、直接ポータル認証を使用するため、**Reallocate IP** リストから **No** を選択します。
- g. サーバーハートビート機能とユーザーハートビート機能をサポートするかどうかを選択します。  
この例では、**Support Server Heartbeat** と **Support User Heartbeat** の両方で **Yes** を選択します。
- h. **OK** をクリックします。

図 30 ポータルデバイスを追加する

Service>>User Access Manager>>Portal Service Management>>Portal Device Configuration>>Add Device

**Add Device**

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                            |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>* Device Name <input type="text" value="NAS"/></p> <p>* Version <input type="text" value="Portal 2.0"/></p> <p>* Listening Port <input type="text" value="2000"/></p> <p>* Authentication Retries <input type="text" value="2"/></p> <p>* Reallocate IP <input type="text" value="No"/></p> <p>* Support Server Heartbeat <input type="text" value="Yes"/></p> <p>* Service Group <input type="text" value="Ungrouped"/></p> <p>Device Description <input type="text"/></p> | <p>* IP Address <input type="text" value="2.2.2.1"/></p> <p>* Key <input type="text" value="portal"/></p> <p>* Local Challenge <input type="text" value="No"/></p> <p>* Logout Retries <input type="text" value="4"/></p> <p>* Support User Heartbeat <input type="text" value="Yes"/></p> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

4. ポータルデバイスを IP アドレスグループに関連付けます。
  - a. 図 31 に示すように、デバイス **NAS** の **Port Group Information Management** カラムのアイコンをクリックして、ポートグループ設定ページを開きます。
  - b. **Add** をクリックしてページを開きます(図 32 を参照)。
  - c. ポートグループ名を入力します。
  - d. 設定済みの IP アドレスグループを選択します。  
ユーザーがネットワークにアクセスするために使用する IP アドレスは、この IP アドレスグループ内にある必要があります。
  - e. その他のパラメーターには既定の設定を使用します。
  - f. **OK** をクリックします。

図 31 デバイスリスト

| Device Information List |            |               |            |                                   |         |        |        |
|-------------------------|------------|---------------|------------|-----------------------------------|---------|--------|--------|
| Device Name             | Version    | Service Group | IP Address | Port Group Information Management | Details | Modify | Delete |
| NAS                     | Portal 2.0 | Ungrouped     | 2.2.2.1    |                                   |         |        |        |

図 32 ポートグループの追加

| Add Port Group Info              |                    |
|----------------------------------|--------------------|
| * Port Group Name                | group              |
| * Start Port                     | 0                  |
| * Protocol                       | HTTP               |
| * NAT or Not                     | No                 |
| * Authentication Type            | CHAP               |
| * Heartbeat Interval             | 10 Minutes         |
| User Domain                      |                    |
| User Attribute Type              |                    |
| Default Authentication Type      | Web Identity AuthN |
| * Language                       | Dynamic Detection  |
| * End Port                       | zzzzz              |
| * Quick Authentication           | No                 |
| * Error Transparent Transmission | Yes                |
| * IP Group                       | Portal_user        |
| * Heartbeat Timeout              | 30 Minutes         |
| Port Group Description           |                    |
| Default Authentication Page      | index_default.jsp  |

- ナビゲーションツリーから **User Access Manager > Service Parameters > Validate System Configuration** を選択して、設定を検証します。

## スイッチの設定

- RADIUS スキームを設定します。

# rs1 という名前の RADIUS スキームを作成し、そのビューを入力します。

```
<Switch> system-view
```

```
[Switch] radius scheme rs1
```

# プライマリ認証サーバーおよびプライマリアカウンティングサーバーを指定し、サーバーと通信するためのキーを設定します。

```
[Switch-radius-rs1] primary authentication 192.168.0.112
```

```
[Switch-radius-rs1] primary accounting 192.168.0.112
```

```
[Switch-radius-rs1] key authentication simple radius
```

```
[Switch-radius-rs1] key accounting simple radius
```

# RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。

```
[Switch-radius-rs1] user-name-format without-domain
```

```
[Switch-radius-rs1] quit
```

# RADIUS セッション制御を有効にします。

```
[Switch] radius session-control enable
```

- 認証ドメインを構成します。

# dm1 という名前の ISP ドメインを作成し、そのビューを入力します。

```
[Switch] domain dm1
```

# ISP ドメインの AAA 方式を設定します。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-isp-dm1] quit
```

# ドメイン dm1 をデフォルトの ISP ドメインとして設定します。ユーザーがログイン時に ISP ドメイン名なしでユーザー名を入力した場合、そのユーザーにはデフォルトドメインの認証およびアカウンティング方式が使用されます。

```
[Switch] domain default enable dm1
```

3. ポータル認証を構成します。

# ポータル認証サーバーを構成します。

```
[Switch] portal server newpt  
[Switch-portal-server-newpt] ip 192.168.0.111 key simple portal  
[Switch-portal-server-newpt] port 50100
```

# ポータル認証サーバーの到達可能性検出を設定します。サーバー検出間隔を 40 秒に設定し、到達可能性ステータスが変更されたときにログメッセージを送信します。

```
[Switch-portal-server-newpt] server-detect timeout 40 log
```

---

**注:**

タイムアウトの値は、ポータルサーバーのハートビート間隔以上でなければなりません。

---

# ポータル認証サーバーとのポータルユーザー同期を設定し、同期検出間隔を 600 秒に設定します。

```
[[Switch-portal-server-newpt] user-sync timeout 600  
[Switch-portal-server-newpt] quit
```

---

**注:**

タイムアウトの値は、ポータルユーザーのハートビート間隔以上でなければなりません。

---

# ポータル Web サーバーを構成します。

```
[Switch] portal web-server newpt  
[Switch-portal-websvr-newpt] url http://192.168.0.111:8080/portal  
[Switch-portal-websvr-newpt] quit
```

# VLAN インターフェース 100 でダイレクトポータル認証をイネーブルにします。

```
[Switch] interface vlan-interface 100  
[Switch-Vlan-interface100] portal enable method direct
```

# ポータル認証サーバーnewpt のポータル失敗許可を有効にする

```
[Switch-Vlan-interface100] portal fail-permit server newpt
```

# VLAN インターフェース 100 上のポータル Web サーバーnewpt を指定します。

```
[Switch-Vlan-interface100] portal apply web-server newpt
```

# VLAN インターフェース 100 からポータル認証サーバーに送信されるポータルパケットの BAS-IP を 2.2.2.1 に設定します。

```
[Switch-Vlan-interface100] portal bas-ip 2.2.2.1  
[Switch-Vlan-interface100] quit
```

## 設定の確認

#ポータル認証サーバーに関する情報を表示するには、次のコマンドを使用します。

```
[Switch] display portal server newpt  
Portal server: newpt  
Type          : IMC  
IP            : 192.168.0.111  
VPN instance  : Not configured  
Port          : 50100  
Server Detection : Timeout 40s Action: log  
User synchronization : Timeout 600s  
Status        : Up
```

ポータル認証サーバーの Up ステータスは、ポータル認証サーバーが到達可能であることを示します。ポータル認証サーバーが到達不能であることをアクセスデバイスが検出した場合、コマンド出力の Status フィールドには **Down** と表示されます。アクセスデバイスは、サーバー到達不能ログ「Portal server newpnt turns down from up.」を生成し、ホストが認証なしで外部ネットワークにアクセスできるように、アクセスインターフェースでポータル認証をディセーブルにします。

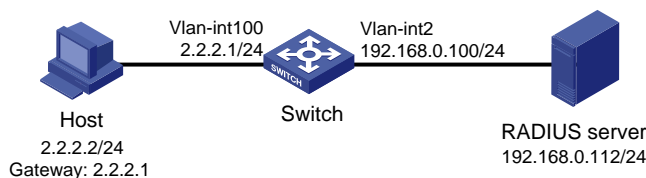
## 例:ローカルポータル Web サービスを使用した直接ポータル認証の構成

### ネットワーク構成

図 33 に示すように、ホストはスイッチ(アクセスデバイス)に直接接続されています。ホストには、手動または DHCP を介してパブリック IP アドレスが割り当てられます。スイッチは、ポータル認証サーバーおよびポータル Web サーバーの両方として機能します。RADIUS サーバーは、認証/アカウントングサーバーとして機能します。

スイッチに直接ポータル認証を設定します。ユーザーがポータル認証を通過する前は、ポータル Web サーバーにのみアクセスできます。ポータル認証を通過した後は、他のネットワークリソースにアクセスできます。

図 33 ネットワークダイアグラム



### 前提条件

- 図 33 に示すように、ホスト、スイッチ、およびサーバーの IP アドレスを設定し、それらが相互に到達できることを確認します。
- RADIUS サーバーを正しく設定して、認証およびアカウントング機能を提供します。
- 認証ページをカスタマイズし、ファイルに圧縮して、スイッチのストレージメディアのルートディレクトリにファイルをアップロードします。

### 手順

1. RADIUS スキームを設定します。  
#rs1 という名前の RADIUS スキームを作成し、そのビューを入力します。  
<Switch> system-view  
[Switch] radius scheme rs1  
#プライマリ認証サーバーおよびプライマリアカウントングサーバーを指定し、サーバーと通信するためのキーを設定します。  
[Switch-radius-rs1] primary authentication 192.168.0.112  
[Switch-radius-rs1] primary accounting 192.168.0.112  
[Switch-radius-rs1] key authentication simple radius  
[Switch-radius-rs1] key accounting simple radius  
#RADIUS サーバーに送信されるユーザー名から ISP ドメイン名を除外します。  
[Switch-radius-rs1] user-name-format without-domain  
[Switch-radius-rs1] quit  
#RADIUS セッション制御を有効にします。  
[Switch] radius session-control enable

2. 認証ドメインを構成します。

# dm1 という名前の ISP ドメインを作成し、そのビューを入力します。

```
[Switch] domain dm1
```

# ISP ドメインの AAA 方式を設定します。

```
[Switch-isp-dm1] authentication portal radius-scheme rs1
```

```
[Switch-isp-dm1] authorization portal radius-scheme rs1
```

```
[Switch-isp-dm1] accounting portal radius-scheme rs1
```

```
[Switch-isp-dm1] quit
```

# ドメイン dm1 をデフォルトの ISP ドメインとして設定します。ユーザーがログイン時に ISP ドメイン名なしでユーザー名を入力した場合、そのユーザーにはデフォルトドメインの認証およびアカウントインテグレーション方式が使用されます。

```
[Switch] domain default enable dm1
```

3. ポータル認証を構成します。

# newpt という名前のポータル Web サーバーを設定し、ポータル Web サーバーの URL として http://2.2.2.1:2331/portal を指定します。URL の IP アドレスは、ポータルクライアントに到達可能なレイヤー3 インターフェース、またはデバイス上のループバックインターフェース(127.0.0.1 を除く)の IP アドレスである必要があります。

```
[Switch] portal web-server newpt
```

```
[Switch-portal-websvr-newpt] url http://2.2.2.1:2331/portal
```

```
[Switch-portal-websvr-newpt] quit
```

# VLAN インターフェース 100 でダイレクトポータル認証をイネーブルにします。

```
[Switch] interface vlan-interface 100
```

```
[Switch-Vlan-interface100] portal enable method direct
```

# VLAN インターフェース 100 上のポータル Web サーバーnewpt を指定します。

```
[Switch-Vlan-interface100] portal apply web-server newpt
```

```
[Switch-Vlan-interface100] quit
```

# HTTP ベースのローカルポータル Web サービスを作成し、そのビューを入力します。

```
[Switch] portal local-web-server http
```

# ローカルポータル Web サービスのデフォルトの認証ページファイルとして、ファイル abc.zip を指定します(ファイルがスイッチのルートディレクトリに存在することを確認してください)。

```
[Switch-portal-local-websvr-http] default-logon-page abc.zip
```

# ローカルポータル Web サービスの HTTP リスニングポート番号を 2331 に設定します。

```
[Switch-portal-local-webserver-http] tcp-port 2331
```

```
[Switch-portal-local-websvr-http] quit
```

## 設定の確認

#ポータル構成が有効になっていることを確認します。

```
[Switch] display portal interface vlan-interface 100
```

```
Portal information of Vlan-interface 100
```

```
Authorization          Strict checking
```

```
ACL                    Disabled
```

```
User profile           Disabled
```

```
IPv4:
```

```
Portal status: Enabled
```

```
Portal authentication method: Direct
```

```
Portal web server: newpt
```

```
Portal mac-trigger-server: Not configured
```

```
Authentication domain: Not configured
```

User-dhcp-only: Disabled  
 Pre-auth IP pool: Not configured  
 Max Portal users: Not configured  
 Bas-ip: Not configured  
 User detection: Not configured  
 Action for server detection:

| Server type | Server name | Action |
|-------------|-------------|--------|
| --          | --          | --     |

Layer3 source network:

| IP address | Mask |
|------------|------|
|            |      |

Destination authenticate subnet:

| IP address | Mask |
|------------|------|
|            |      |

IPv6:

Portal status: Disabled  
 Portal authentication method: Disabled  
 Portal web server: Not configured  
 Portal mac-trigger-server: Not configured  
 Authentication domain: Not configured  
 User-dhcp-only: Disabled  
 Pre-auth IP pool: Not configured  
 Max Portal users: Not configured  
 Bas-ipv6: Not configured  
 User detection: Not configured  
 Action for server detection:

| Server type | Server name | Action |
|-------------|-------------|--------|
| --          | --          | --     |

Layer3 source network:

| IP address | Prefix length |
|------------|---------------|
|            |               |

Destination authenticate subnet:

| IP address | Prefix length |
|------------|---------------|
|            |               |

ユーザーは、Web ページを介してポータル認証を実行できます。認証にパスする前に、ユーザーは **http://2.2.2.1:2331/portal** の認証ページにのみアクセスでき、すべての Web 要求は認証ページにリダイレクトされます。認証にパスした後、ユーザーは他のネットワークリソースにアクセスできます。

#ユーザーが認証に合格したら、次のコマンドを使用してポータルユーザーに関する情報を表示します。

[Switch] display portal user interface vlan-interface 100

Total portal users: 1

Username: abc

Portal server: newpt

State: Online

VPN instance: --

| MAC            | IP      | VLAN | Interface         |
|----------------|---------|------|-------------------|
| 0015-e9a6-7cfe | 2.2.2.2 | 100  | Vlan-interface100 |

Authorization information:

IP pool: N/A

User profile: N/A

Session group profile: N/A

ACL: N/A



Inbound CAR: N/A  
Outbound CAR: N/A

## ポータルトラブルシューティング

### ユーザーのポータル認証ページはプッシュされません。

#### 症状

ユーザーが IMC ポータル認証サーバーにリダイレクトされた場合、ポータル認証ページまたはエラーメッセージは表示されません。ログインページは空白です。

#### 解析

ポータルアクセスデバイスに設定されたキーとポータル認証サーバーに設定されたキーが矛盾しています。その結果、パケットの検証が失敗し、ポータル認証サーバーは認証ページのプッシュを拒否します。

#### 解決策

ポータル認証サーバーにキーが設定されているかどうかを確認するには、アクセスデバイスで **display portal server** コマンドを使用します。

- キーが設定されていない場合は、正しいキーを設定します。
- キーが設定されている場合は、ポータル認証サーバービューで **ip** または **ipv6** コマンドを使用してキーを修正するか、ポータル認証サーバー上のアクセスデバイスに設定されているキーを修正します。

### アクセスデバイスのポータルユーザーをログアウトできません

#### 症状

アクセスデバイスで **portal delete-user** コマンドを使用してポータルユーザーをログアウトすることはできませんが、ポータルユーザーはポータル認証クライアントの **Disconnect** ボタンをクリックすることでログアウトできます。

#### 解析

アクセスデバイスで **portal delete-user** コマンドを実行してユーザーをログアウトするとき、アクセスデバイスは、要求されていないログアウト通知メッセージをポータル認証サーバーに送信します。ログアウト通知の宛先ポート番号は、アクセスデバイスに設定されたポータル認証サーバーのリスニングポート番号です。このリスニングポート番号が、サーバーに設定された実際のリスニングポート番号でない場合、サーバーは通知を受信できません。その結果、サーバーはユーザーをログアウトしません。

ユーザーが認証クライアントの[Disconnect]ボタンを使用してログアウトすると、ポータル認証サーバーは非送信請求のログアウト要求メッセージをアクセスデバイスに送信します。アクセスデバイスは、ログアウト要求の送信元ポートをログアウト ACK メッセージの宛先ポートとして使用します。その結果、ポータル認証サーバーは確実にログアウト ACK メッセージを受信してユーザーをログアウトできます。

#### 解決策

1. アクセスデバイスに設定されているポータル認証サーバーのリスニングポートを表示するには、**display portal server** コマンドを使用します。
2. リスニングポート番号をポータル認証サーバーの実際のリスニングポートに変更するには、システムビューで **portal server** コマンドを使用します。

# RADIUS サーバー上のポータルユーザーをログアウトできない

## 症状

アクセスデバイスは、H3C IMC サーバーを RADIUS サーバーとして使用して、ポータルユーザーの ID 認証を実行します。RADIUS サーバー上のポータルユーザーはログアウトできません。

## 解析

H3C IMC サーバーは、セッション制御パケットを使用して、接続解除要求をアクセスデバイスに送信します。アクセスデバイスでは、セッション制御パケットをリッスンする UDP ポートがデフォルトで無効になっています。そのため、アクセスデバイスは RADIUS サーバーからポータルユーザーのログアウト要求を受信できません。

## 解決策

アクセスデバイスで、システムビューで **radius session-control enable** コマンドを実行して、RADIUS セッション制御機能をイネーブルにします。

# アクセスデバイスによってログアウトされたユーザーは、ポータル認証サーバーにまだ存在しています。

## 症状

アクセスデバイスでポータルユーザーをログアウトした後も、そのユーザーはポータル認証サーバーに存在します。

## 解析

アクセスデバイスで **portal delete-user** コマンドを実行してユーザーをログアウトするとき、アクセスデバイスは、要求されていないログアウト通知をポータル認証サーバーに送信します。ログアウト通知で伝送される BAS-IP または BAS-IPv6 アドレスが、ポータル認証サーバーで指定されたポータルデバイスの IP アドレスと異なる場合、ポータル認証サーバーはログアウト通知を廃棄します。ログアウト通知の送信がタイムアウトになると、アクセスデバイスはユーザーをログアウトします。ただし、ポータル認証サーバーはログアウト通知を正常に受信しないため、ユーザーはまだオンラインであると見なされます。

## 解決策

ポータル認証が有効になっているインターフェースに BAS-IP または BAS-IPv6 属性を設定します。属性値が、ポータル認証サーバーで指定されたポータルデバイスの IP アドレスと同じであることを確認してください。

# Re-DHCP ポータルで認証されたユーザーが正常にログインできない

## 症状

デバイスは、ユーザーに対して再 DHCP ポータル認証を実行します。ユーザーが正しいユーザー名とパスワードを入力すると、クライアントはプライベート IP アドレスとパブリック IP アドレスを正常に取得します。ただし、ユーザーの認証結果は失敗です。

## 解析

アクセスデバイスは、クライアントの IP アドレスが変更されたことを検出すると、IP の変更を通知する非送信請求ポータルパケットをポータル認証サーバーに送信します。ポータル認証サーバーが認証の成功を通知するのは、アクセスデバイスとクライアントの両方から IP 変更通知を受信した後だけです。

ポータル通知パケットで伝送される BAS-IP または BAS-IPv6 アドレスが、ポータル認証サーバーで指定されたポータルデバイスの IP アドレスと異なる場合、ポータル認証サーバーはポータル通知パケットを廃棄します。その結果、ポータル認証サーバーはユーザーが認証に失敗したと見なします。

## 解決策

ポータル認証が有効になっているインターフェースに BAS-IP または BAS-IPv6 属性を設定します。属性値が、ポータル認証サーバーで指定されたポータルデバイスの IP アドレスと同じであることを確認してください。

# Web 認証の設定

## Web 認証について

Web 認証は、アクセス デバイスのレイヤー 2 イーサネット インターフェースに導入され、ネットワークへのユーザー アクセスを制御します。アクセス デバイスは、認証されていないユーザーを指定された Web サイトにリダイレクトします。ユーザーは認証なしで Web サイト上のリソースにアクセスできます。ユーザーが他のネットワーク リソースにアクセスしたい場合は、認証に合格する必要があります。

## Web 認証のメリット

Web 認証には次の利点があります。

- ユーザーはクライアント ソフトウェアをインストールせずに、Web ページを通じて認証を実行できます。
- ISP に多様な管理の選択肢と拡張機能を提供します。たとえば、ISP は広告を掲載したり、コミュニティ サービスを提供したり、認証ページに情報を公開したりできます。

## Web 認証システム

一般的な Web 認証システムは、認証クライアント、アクセス デバイス、ローカル ポータル Web サーバー、および AAA サーバーの 4 つの基本コンポーネントで構成されます。

図 1 ローカルポータルサーバーを利用した Web 認証システム



### 認証クライアント

認証クライアントは、HTTP を実行する Web ブラウザーです。

### アクセスデバイス

アクセスデバイスには次の機能があります。

- 認証フリーのルールに一致しないすべてのユーザーの HTTP リクエストを、認証前に Web 認証ページにリダイレクトします。
- AAA サーバーと通信して、認証、認可、およびアカウントリングを完了します。AAA の詳細については、「AAA の設定」を参照してください。
- 認証に合格したユーザーに、許可されたネットワーク リソースへのアクセスを許可します。

### ローカルポータル Web サーバー

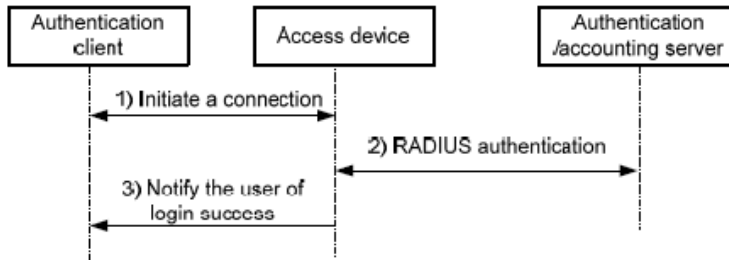
アクセス デバイスは、ローカル ポータル Web サーバーとして機能します。ローカル ポータル Web サーバーは、Web 認証ページを認証クライアントにプッシュし、ユーザー認証情報 (ユーザー名とパスワード) を取得します。

## AAA サーバー

AAA サーバーは、アクセス デバイスと対話して、ユーザーの認証、認可、およびアカウントングを実装します。RADIUS サーバーは、Web 認証ユーザーの認証、認可、アカウントングを実行できます。LDAP サーバーは、Web 認証ユーザーの認証を実行できます。

## Web 認証プロセス

図 2 Web 認証プロセス



Web 認証プロセスは次のとおりです。

1. 認証されていないユーザーが HTTP リクエストを送信します。アクセス デバイスは、Web 認証が有効になっているレイヤー 2 イーサネットインターフェースで HTTP リクエストを受信すると、リクエストを Web 認証ページにリダイレクトします。ユーザーは、Web 認証ページでユーザー名とパスワードを入力します。

ユーザーが Web 認証ページまたは認証フリーの Web リソースを要求すると、アクセス デバイスはその要求を許可します。Web 認証は行われません。

2. アクセス デバイスと AAA サーバーは、RADIUS パケットを交換してユーザーを認証します。
3. ユーザーが RADIUS 認証に合格すると、ローカル ポータル Web サーバーはログイン成功ページを認証クライアントにプッシュします。

ユーザーが RADIUS 認証に失敗した場合、ローカル ポータル Web サーバーはログイン失敗ページを認証クライアントにプッシュします。

## VLAN 割り当ての Web 認証サポート

### 認可 VLAN

Web 認証は、AAA サーバーまたはアクセス デバイスによって許可された VLAN を使用して、認証されたユーザーのネットワークリソースアクセスを制御します。

ユーザーが Web 認証に合格すると、AAA サーバーまたはアクセス デバイスはユーザーに VLAN へのアクセスを許可します。認可 VLAN が存在しない場合、アクセス デバイスは最初に VLAN を作成し、次にユーザー アクセス インターフェースをタグなしメンバーとして VLAN に割り当てます。認可 VLAN がすでに存在する場合、アクセス デバイスは、ユーザー アクセス インターフェースをタグなしメンバーとして VLAN に直接割り当てます。これにより、ユーザーは認可 VLAN 内のリソースにアクセスできるようになります。

表 1 は、アクセス デバイスが Web 認証されたユーザーの認可 VLAN を処理する方法を示しています。

表 1 VLAN の操作

| ポートの種類                                                                                                                 | VLAN の操作                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• アクセスポート</li><li>• トランクポート</li><li>• MAC ベース VLAN が無効になっているハイブリッド ポート</li></ul> | デバイスは、最初に認証されたユーザーの認可 VLAN にポートを割り当てます。認可 VLAN が PVID になります。ポート上のすべての Web 認証ユーザーには、同じ認可 VLAN を割り当てる必要があります。後続のユーザーに異なる認可 VLAN が割り当てられている場合、そのユーザー |

| ポートの種類                           | VLAN の操作                                                                                |
|----------------------------------|-----------------------------------------------------------------------------------------|
|                                  | はWeb認証を通過できません。                                                                         |
| MAC ベース VLAN が有効になっているハイブリッド ポート | デバイスは、ポートがタグ付きメンバーであるかどうかに関係なく、各ユーザーの MAC アドレスを独自の認可 VLAN にマッピングします。ポートの PVID は変更されません。 |

## 認証失敗 VLAN

認証失敗 VLAN は、認証に失敗したユーザーに割り当てられる VLAN です。認証失敗 VLAN は、パッチサーバー、ウイルス定義サーバー、クライアント ソフトウェア サーバー、ウイルス対策ソフトウェア サーバーなどのネットワーク リソースをユーザーに提供します。ユーザーはこれらのリソースを使用して、クライアント ソフトウェアまたは他のプログラムをアップグレードできます。

Web 認証は、MAC ベースのアクセス制御を実行する インターフェースで Auth-Fail VLAN をサポートします。インターフェース上のユーザーが認証に失敗した場合、アクセス デバイスはユーザーの MAC アドレスに基づいて MAC VLAN エントリを作成し、そのユーザーを認証失敗 VLAN に追加します。これにより、ユーザーは認証失敗 VLAN 内のポータルフリー IP リソースにアクセスできるようになります。ポータルフリーでない IP リソースへのすべての HTTP リクエストは、認証ページにリダイレクトされます。それでもユーザーが認証に失敗した場合、インターフェースは認証失敗 VLAN に残ります。ユーザーが認証に合格すると、アクセス デバイスは インターフェースを認証失敗 VLAN から削除し、次のように インターフェースを VLAN に割り当てます。

- 認証サーバーがユーザーに認可 VLAN を割り当てると、アクセス デバイスは インターフェースを認可 VLAN に割り当てます。
- 認証サーバーがユーザーに認可 VLAN を割り当てない場合、アクセス デバイスは インターフェースをデフォルト VLAN に割り当てます。

## 認可 ACL の Web 認証サポート

Web 認証は、AAA サーバーまたはアクセス デバイスによって認可された ACL を使用して、ネットワーク リソースへのユーザー アクセスを制御し、ユーザー アクセス権を制限します。ユーザーが認証に合格すると、AAA サーバーとアクセス デバイスはユーザーのアクセス インターフェースに認可 ACL を割り当てます。アクセス デバイスは、許可された ACL に従って、アクセス インターフェース上のユーザーからのトラフィックをフィルタリングします。

認証サーバーで認可 ACL を指定する場合は、アクセス デバイスで認可 ACL を設定する必要があります。

ユーザーのアクセス制御基準を変更するには、認証サーバーで別の認可 ACL を指定するか、アクセス デバイスの認可 ACL のルールを変更します。

## 制限事項とガイドライン: Web 認証の構成

認可 VLAN または認証失敗 VLAN 内のリソースにアクセスするには、ユーザーは認可 VLAN または認証失敗 VLAN に割り当てられた後、クライアントの IP アドレスを更新する必要があります。

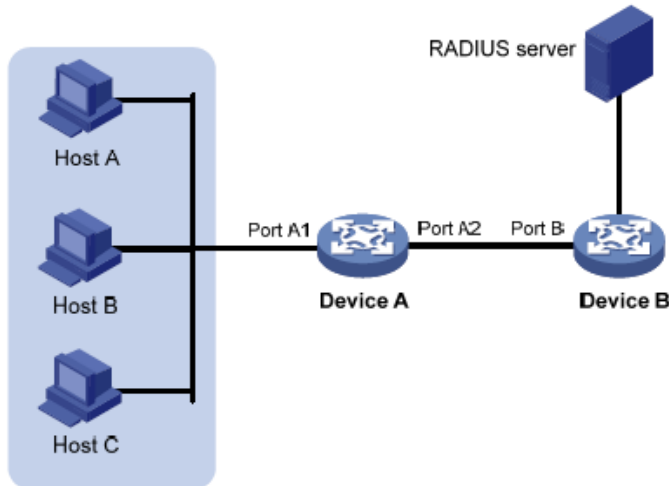
デバイスは次の認可 ACL をサポートしています。

- 基本 ACL (ACL 2000 ~ ACL 2999)。
- 高度な ACL (ACL 3000 ~ ACL 3999)。

ベスト プラクティスとして、デバイスに直接接続しているユーザーに対して Web 認証を実行します。図 87 に示すように、直接接続されていないユーザー (ホスト) を認証するためにポート B で Web 認証を有効にする場合は、次の制限とガイドラインに従う必要があります。

- RADIUS サーバーがユーザーに認可 VLAN を割り当てる場合は、次の条件が満たされていることを確認してください。
  - デバイス A とデバイス B の間のリンクはトランク リンクです。
  - ポート A1 とポート B の PVID は認可 VLAN ID と同じです。
- RADIUS サーバーがユーザーに認可 VLAN を割り当てない場合は、ポート A1 とポート B の PVID が同じであることを確認してください。

図 3 直接接続していないユーザーの Web 認証



## Web 認証タスクの概要

Web 認証を構成するには、次のタスクを実行します。

1. Web 認証サーバーの設定
2. ローカルポータルサービスの構成  
この構成の詳細については、「ポータル認証の構成」を参照してください。
3. Web 認証を有効にする
4. (オプション) Web 認証ドメインの指定
5. (オプション) リダイレクト待ち時間の設定
6. (オプション) Web 認証フリーのサブネットの構成
7. (オプション) Web 認証ユーザーの最大数の設定
8. (オプション) オンライン Web 認証ユーザー検出の構成
9. (オプション) 認証失敗 VLAN の設定
10. (オプション) Web プロキシをサポートするための Web 認証の構成

## Web 認証の前提条件

本装置は、ローカル認証と RADIUS 認証の 2 つの Web 認証方式をサポートしています。

RADIUS 認証方法を使用するには、次のタスクを完了する必要があります。

- RADIUS サーバーをインストールし、RADIUS サーバーを適切に構成します。

- 認証クライアント、アクセス デバイス、および RADIUS サーバーが相互に接続できることを確認してください。
- RADIUS サーバー上でユーザー アカウントを設定し、アクセス デバイス上で RADIUS クライアント情報を設定します。

ローカル認証方法を使用するには、アクセス デバイス上でローカル ユーザーを構成する必要があります。RADIUS クライアントとローカル ユーザーの詳細については、「AAA の設定」を参照してください。

## Web認証サーバーの設定

### 制限事項とガイドライン

Web 認証サーバーのリスニング IP アドレスとして、Web クライアントにルーティング可能なデバイス上のレイヤー 3 インターフェースの IP アドレスを指定します。ベスト プラクティスとして、レイヤー 3 インターフェースの IP アドレスではなく、ループバック インターフェースの IP アドレスを使用します。ループバック インターフェースには次の利点があります。

- ループバック インターフェースのステータスは安定しています。インターフェース障害による認証ページへのアクセス障害は発生しません。
- ループバック インターフェースは、受信したパケットをどのネットワークにも転送しないため、ネットワーク アクセス要求が多数ある場合でもシステム パフォーマンスへの影響が回避されます。

### 手順

1. システムビューに入ります。

**system-view**

2. Web 認証サーバーを作成し、そのビューに入ります。

**web-auth server server-name**

3. Web 認証サーバーの IP アドレスとポート番号を指定します。

**ip ipv4-address port port-number**

Web 認証サーバーのポート番号は、ローカル ポータル Web サービスのリスニング ポートと同じである必要があります。

4. Web 認証サーバーのリダイレクト URL を指定します。

**url url-string**

指定するリダイレクト URL の IP アドレスとポート番号は、Web 認証サーバーの IP アドレスとポート番号と同じである必要があります。

5. (オプション) Web 認証サーバーのリダイレクト URL にパラメーターを追加します。

**url-parameter parameter-name { original-url | source-address | source-mac | value expression }**

デフォルトでは、Web 認証サーバーのリダイレクト URL にはパラメーターは追加されません。

## Web認証を有効にする

### 制限事項とガイドライン

Web 認証が正しく動作するためには、ポート セキュリティを有効にしないでください。また、Web 認証が有効になっているレイヤー 2 イーサネット インターフェースでポート セキュリティ モードを設定しないでください。ポートセキュリティの詳細については、「ポートセキュリティの設定」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. インターフェースビューに入ります。  
**interface** *interface-type interface-number*
3. Web 認証を有効にし、Web 認証サーバーを指定します。  
**web-auth enable apply server** *server-name*  
デフォルトでは、Web 認証は無効になっています。

# Web認証ドメインの指定

## Web 認証ドメインについて

異なる インターフェース上の Web 認証ユーザーに対して異なる認証ドメインを指定できます。インターフェースで Web 認証ドメインを指定すると、デバイスは、インターフェース上のすべての Web 認証ユーザーの AAA の認証ドメインを使用し、ユーザー名に含まれるドメイン名を無視します。

デバイスは、インターフェース上の Web 認証ユーザーの認証ドメインを次の順序で選択します。

1. インターフェースに指定された認証ドメイン。
2. ユーザー名に含まれる認証ドメイン。
3. システムのデフォルトの認証ドメイン。
4. 存在しないドメインに割り当てられたユーザーに対応するように構成された ISP ドメイン。

選択したドメインがデバイス上に存在しない場合、ユーザー認証は失敗します。ISP ドメインの詳細については、「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. インターフェースビューに入ります。  
**interface** *interface-type interface-number*
3. インターフェース上で Web 認証ユーザーの認証ドメインを指定します。  
**web-auth domain** *domain-name*  
デフォルトでは、Web 認証ユーザーに対して認証ドメインは指定されていません。

# リダイレクト待ち時間の設定

## リダイレクト待ち時間について

リダイレクト待機時間は、ユーザーが Web 認証に合格した後、デバイスがユーザーを指定された Web ページにリダイレクトするまで待機する時間の長さを決定します。

一部のシナリオでは、たとえば、ユーザーが Web 認証を通過した後にクライアント IP アドレスを更新する必要がある場合など、リダイレクト待機時間を変更する必要があります。指定した Web ページを確実に開くことができるようにするには、リダイレクト待機時間を、ユーザーがクライアントの IP アドレスを更新するのにかかる時間よりも長く設定します。

## 手順

1. システムビューに入ります。

### **system-view**

2. Web 認証サーバービューに入ります。

**web-auth server** *server-name*

3. リダイレクトの待ち時間を設定します。

**redirect-wait-time** *period*

デフォルトでは、認証されたユーザーのリダイレクト待ち時間は 5 秒です。

## Web 認証フリーのサブネットの構成

### Web 認証フリーサブネットについて

Web 認証フリーのサブネットを構成すると、ユーザーが認証を受けずにサブネット内のネットワーク リソースに自由にアクセスできるようになります。

### 制限事項とガイドライン

ベスト プラクティスとして、Web 認証フリーのサブネットと 802.1X のフリー IP に同じアドレス値を構成しないでください。それ以外の場合、いずれかの構成をキャンセルすると、もう一方の構成も有効になりません。

### 手順

1. システムビューに入ります。

**system-view**

2. Web 認証フリーのサブネットを構成します。

**web-auth free-ip** *ip-address* { *mask-length* | *mask* }

## Web 認証ユーザーの最大数を設定する

### 制限事項とガイドライン

設定したオンライン Web 認証ユーザーの最大数が現在のオンライン Web 認証ユーザーの最大数より少ない場合、制限は正常に設定され、オンライン Web 認証ユーザーには影響しません。ただし、Web 認証ユーザーの数が制限を下回るまで、新しい Web 認証ユーザーのログインは許可されません。

### 手順

1. システムビューに入ります。

**system-view**

2. インターフェイス ビューに入ります。

**interface** *interface-type* *interface-number*

3. インターフェイス上の Web 認証ユーザーの最大数を設定します。

**web-auth max-user** *max-number*

デフォルトでは、Web 認証ユーザーの最大数は 1024 です。

## オンライン Web 認証ユーザー検出の構成

### オンライン Web 認証のユーザー検出について

この機能により、デバイスは指定された検出間隔でオンライン ユーザーのパケットを検出できるようになります。一定期間内にユーザーからのパケットを受信しない場合、デバイスはユーザーをログアウトし、RADIUS サーバーにユーザーのアカウントを停止するように通知します。

## 制限事項とガイドライン

デバイスがユーザーを誤ってログアウトしないようにするには、検出間隔を MAC アドレス エントリのエージング タイムと同じに設定します。

### 手順

1. システムビューに入ります。  
**system-view**
2. インターフェイス ビューに入ります。  
**interface** *interface-type interface-number*
3. オンライン Web 認証ユーザー検出を有効にします。  
**web-auth offline-detect interval** *interval*  
デフォルトでは、オンライン Web 認証のユーザー検出は無効になっています。

## 認証失敗 VLAN の設定

### 制限事項とガイドライン

認証失敗 VLAN を有効にするには、インターフェイス上で MAC ベース VLAN を有効にし、認証失敗 VLAN のサブネットを Web 認証フリーのサブネットとして設定する必要があります。

MAC ベース VLAN はハイブリッド ポートでのみ有効であるため、認証失敗 VLAN もハイブリッド ポートでのみ有効です。

VLAN がスーパー VLAN として指定されている場合、その VLAN を インターフェイスの認証失敗 VLAN として設定しないでください。VLAN が インターフェイスの認証失敗 VLAN として指定されている場合、その VLAN をスーパー VLAN として設定しないでください。

認証失敗 VLAN として設定されている VLAN は削除しないでください。この VLAN を削除するには、まず **undo web-auth auth-fail vlan** を使用して認証失敗 VLAN 設定をキャンセルします。

### 手順

1. システムビューに入ります。  
**system-view**
2. インターフェイス ビューに入ります。  
**interface** *interface-type interface-number*
3. 認証失敗 VLAN を設定します。  
**web-auth auth-fail vlan** *authfail-vlan-id*  
デフォルトでは、インターフェイス上に認証失敗 VLAN は設定されていません。

## Webプロキシをサポートするための Web 認証の構成

### Web 認証における Web プロキシのサポートについて

デフォルトでは、プロキシされた HTTP リクエストは Web 認証をトリガーできませんが、サイレントにドロップされます。このような HTTP 要求が Web 認証をトリガーできるようにするには、デバイス上の Web プロキシ サーバーのポート番号を指定します。

## 制限事項とガイドライン

ユーザーのブラウザが Web プロキシ自動検出 (WPAD) プロトコルを使用して Web プロキシ サーバーを検出する場合は、次のタスクを実行する必要があります。

- デバイス上の Web プロキシ サーバーのポート番号を追加します。
- 認証フリールールを構成して、WPAD サーバーの IP アドレス宛てのユーザー パケットが認証なしで通過できるようにします。

Web プロキシをサポートする Web 認証の場合:

- デバイスに Web プロキシ サーバーのポート番号を追加する必要があります。
- ユーザーは、Web プロキシ サーバーを使用するブラウザが、ローカル ポータル Web サーバーのリスニング IP アドレスにプロキシ サーバーを使用していないことを確認する必要があります。したがって、Web 認証ユーザーがローカル ポータル Web サーバーに送信する HTTP パケットは、Web プロキシ サーバーには送信されません。

## 手順

1. システムビューに入ります。

**system-view**

2. Web プロキシサーバーのポート番号を追加します。

**web-auth proxy port port-number**

このコマンドを複数回実行することで、Web プロキシサーバーのポート番号を複数指定できます。

## Web認証の表示・保守コマンド

任意のビューで **display** コマンドを実行します。

| タスク                       | 指図                                                                                                                               |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------|
| インターフェースのWeb認証設定情報を表示します。 | <b>display web-auth</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i> ]                                       |
| Web認証フリーのサブネットを表示します。     | <b>display web-auth free-ip</b>                                                                                                  |
| Web認証サーバーの情報を表示します。       | <b>display web-auth server</b> [ <i>server-name</i> ]                                                                            |
| Web認証ユーザー情報を表示します。        | <b>display web-auth user</b> [ <b>interface</b> <i>interface-type</i> <i>interface-number</i>   <b>slot</b> <i>slot-number</i> ] |

## Web認証の設定例

### 例: ローカル認証方式を使用した Web 認証の構成

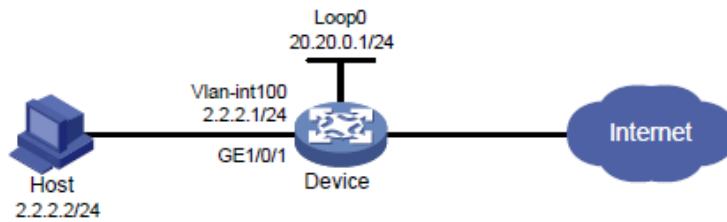
#### ネットワーク設定

図 4 に示すように、ホストは GigabitEthernet1/0/1 を介してデバイスに直接接続されています。

GigabitEthernet1/0/1 で Web 認証を設定し、ユーザに対してローカル認証および許可を使用します。

カスタマイズされた Web 認証ページをユーザにプッシュし、HTTP を使用して認証データを転送するようにデバイスを設定します。

図 4 ネットワークダイアグラム



## 手順

1. 認証ページをカスタマイズし、ファイルに圧縮して、デバイスのストレージメディアのルートディレクトリにファイルをアップロードします。この例では、ファイルは abc.zip です(詳細省略)。
2. 図 4 に示すように、ホストとデバイスに IP アドレスを割り当て、ホストとデバイスが相互に到達できることを確認します。
3. ローカルユーザーを設定します。  
# **localuser** という名前のローカルネットワークアクセスユーザーを作成します。  
<Device>system-view  
[Device] local-user localuser class network  
# ユーザ **localuser** のパスワードをプレーンテキスト形式で **localpass** に設定します。  
[Device-user-network-localuser] password simple localpass  
# LAN アクセスサービスの使用をユーザに許可します。  
[Device-user-network-localuser] service-type lan-access  
[Device-user-network-localuser] quit
4. ISPドメインを設定します。  
# **local** という名前の ISPドメインを作成します。  
[Device] domain local  
# LAN アクセスユーザーのローカル認証、認可、およびアカウントを実行するように ISPドメインを設定します。  
[Device-isp-local] authentication lan-access local  
[Device-isp-local] authorization lan-access local  
[Device-isp-local] accounting lan-access local  
[Device-isp-local] quit
5. ローカルポータル Web サービスを構成します。  
# HTTP ベースのローカルポータル Web サービスを作成し、そのビューを入力します。  
[Device] portal local-web-server http  
# ローカルポータル Web サービスの既定の認証ページファイルとして、**abc.zip** ファイルを指定します(このファイルは、デバイスのルートディレクトリに存在する必要があります)。  
[Device-portal-local-websvr-http] default-logon-page abc.zip  
# ポータル Web サービスの HTTP リスニングポート番号を 80 に指定します。  
[Device-portal-local-websvr-http] tcp-port 80  
[Device-portal-local-websvr-http] quit
6. Web 認証を設定します。  
# **user** という名前の Web 認証サーバーを作成します。  
[Device] web-auth server user  
# Web 認証サーバーのリダイレクト URL を http://20.20.0.1/portal/として構成します。  
[Device-web-auth-server-user] url http://20.20.0.1/portal/

```

# Web 認証サーバの IP アドレスとして 20.20.0.1、ポート番号として 80 を指定します。
[Device-web-auth-server-user] ip 20.20.0.1 port 80
[Device-web-auth-server-user] quit
# Web 認証ドメインとして ISP ドメイン local を指定します。
[Device] interface GigabitEthernet 1/0/1
[Device-GigabitEthernet 1/0/1] web-auth domain local
# Web 認証サーバ user を使用して、Web 認証を有効にします。
[Device-GigabitEthernet 1/0/1] web-auth enable apply server user
[Device-GigabitEthernet 1/0/1] quit

```

## 設定の確認

#ユーザー **localuser** が Web 認証を通過した後、オンライン Web 認証ユーザー情報を表示します。

```

<Device> display web-auth user
Total online web-auth users: 1

```

```

User Name: localuser
MAC address: acf1-df6c-f9ad
Access interface: GigabitEthernet 1/0/1
Initial VLAN: 1
Authorization VLAN: N/A
Authorization ACL ID: N/A
Authorization user profile: N/A

```

## 例:RADIUS 認証方式を使用した Web 認証の設定

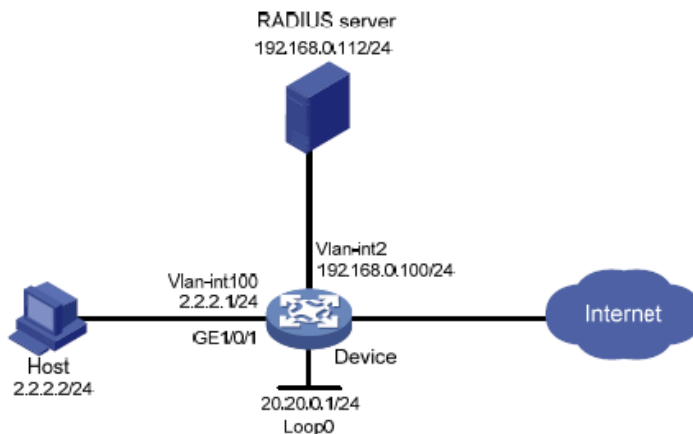
### ネットワーク構成

図 5 に示すように、ホストは GigabitEthernet1/0/1 を介してデバイスに直接接続されています。

GigabitEthernet1/0/1 で Web 認証を設定し、RADIUS サーバを使用してユーザの認証と認可を実行します。

カスタマイズされた Web 認証ページをユーザにプッシュし、HTTP を使用して認証データを転送するようにデバイスを設定します。

図 5 ネットワーク図



## 手順

1. RADIUS サーバを適切に設定して、ユーザに認証およびアカウントング機能を提供します。この例では、ユーザ名は RADIUS サーバで user1 として設定されています(詳細は省略)。
2. 認証ページをカスタマイズし、ファイルに圧縮して、スイッチのストレージメディアのルートディレクトリにファイルをアップロードします。この例では、ファイルは abc.zip です。
3. VLAN を作成し、IP アドレスを VLAN インターフェースに割り当て、インターフェースを VLAN に割り当てます。ホスト、RADIUS サーバ、およびデバイスが相互に到達できることを確認します(詳細は表省略)。
4. RADIUS スキームを構成します。  
# rs1 という名前の RADIUS スキームを作成します。  
<Device> system-view  
[Device] radius scheme rs1  
# プライマリ認証サーバーとプライマリ アカウントングサーバーを指定し、サーバーとの通信用のキーを構成します。  
[Device-radius-rs1] primary authentication 192.168.0.112  
[Device-radius-rs1] primary accounting 192.168.0.112  
[Device-radius-rs1] key authentication simple radius  
[Device-radius-rs1] key accounting simple radius  
# RADIUS サーバに送信されるユーザ名から ISP ドメイン名を除外します。  
[Device-radius-rs1] user-name-format without-domain  
[Device-radius-rs1] quit
5. 認証ドメインを構成します。  
# dm1 という名前の ISP ドメインを作成します。  
[Device] domain dm1  
# ISP ドメインの AAA メソッドを設定する  
[Device-isp-dm1] authentication lan-access radius-scheme rs1  
[Device-isp-dm1] authorization lan-access radius-scheme rs1  
[Device-isp-dm1] accounting lan-access radius-scheme rs1  
[Device-isp-dm1] quit
6. ローカル ポータル Web サービスを構成します。  
# HTTP ベースのローカル ポータル Web サービスを作成します。  
[Device] portal local-web-server http  
# ファイル **abc.zip** をローカル ポータル Web サービスのデフォルトの認証ページ ファイルとして指定します。(このファイルは、記憶媒体の直接のルート ディレクトリに存在する必要があります。)  
[Device-portal-local-websvr-http] default-logon-page abc.zip  
# ローカル ポータル Web サービスがリッスンするポート番号として 80 を指定します。  
[Device-portal-local-websvr-http] tcp-port 80  
[Device-portal-local-websvr-http] quit
7. Web 認証を構成します。  
# user という名前の Web 認証サーバーを作成します。  
[Device] web-auth server user  
# Web 認証サーバーのリダイレクト URL として **http://20.20.0.1/portal/** を指定します。  
[Device-web-auth-server-user] url http://20.20.0.1/portal/  
# Web 認証サーバーの IP アドレスを 20.20.0.1、ポート番号を 80 に指定します。  
[Device-web-auth-server-user] ip 20.20.0.1 port 80  
[Device-web-auth-server-user] quit

```
# Web 認証ドメインとしてドメイン dml を指定します。
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] web-auth domain dm1
# Web 認証サーバーuser を使用して Web 認証を有効にします。
[Device-GigabitEthernet1/0/1] web-auth enable apply server user
[Device-GigabitEthernet1/0/1] quit
```

## 構成の確認

# ユーザー**user1** が Web 認証に合格した後に、Web 認証ユーザー情報を表示します。

```
<Device> display web-auth user
Total online web-auth users: 1
```

```
User Name: user1
MAC address: acf1-df6c-f9ad
Access interface: GigabitEthernet1/0/1
Initial VLAN: 1
Authorization VLAN: N/A
Authorization ACL ID: N/A
Authorization user profile: N/A
```

# Web認証のトラブルシューティング

## オンラインにならない (デフォルトの ISP ドメインを使用するローカル認証 インターフェース)

### 症状

ローカル認証 インターフェースに認証ドメインが指定されていません。ユーザーがオンラインになるための Web 認証に合格できませんでした。

### 分析

Web 認証ドメインが指定されていない場合は、システムのデフォルトの ISP ドメイン (ドメインシステム) が Web 認証に使用されます。システムのデフォルトドメインは、デフォルトでローカル認証方法を使用します。これらのデフォルトのドメイン設定を使用すると、ローカル認証が正しく動作するはずですが、

システムのデフォルトドメインの認証方法が変更されたか、システムのデフォルトドメインが変更されたことが原因で、ローカル認証が失敗する可能性があります。

### 解決

問題を解決するには、次のタスクを実行します。

1. **show domain** コマンドを使用して、システムのデフォルトドメイン内の Web ユーザーの AAA メソッドがローカルであるかどうかを確認します。
2. システムのデフォルトドメイン内の Web ユーザーの AAA メソッドがローカルでない場合は、AAA メソッドをローカルとして再設定します。



# トリプル認証の設定

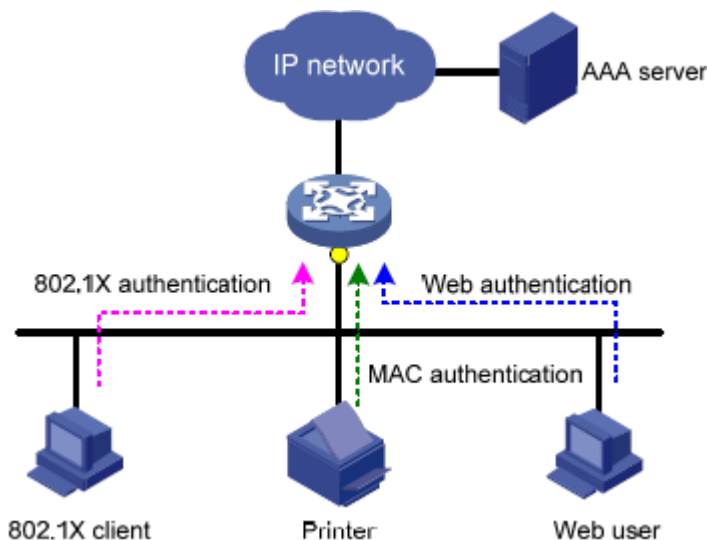
## トリプル認証について

トリプル認証を使用すると、アクセスポートで Web、MAC、および 802.1X 認証を実行できます。端末は、1 つのタイプの認証に合格するとネットワークにアクセスできます。802.1X 認証、MAC 認証、および Web 認証の詳細については、「802.1X 認証の設定」、「MAC 認証の設定」、および「Web 認証の設定」を参照してください。

## トリプル認証の典型的なネットワーク

トリプル認証は、図 1 に示すように、異なる認証サービスを必要とする端末で構成される LAN に適しています。トリプル認証対応のアクセスポートは、プリンタの MAC 認証、802.1X クライアントがインストールされた PC の 802.1X 認証、および Web ユーザーの Web 認証を実行できます。

図 1 トリプル認証ネットワーク図



## トリプル認証メカニズム

3 種類の認証は、異なるパケットによってトリガーされます。

- アクセスポートは、端末から ARP または DHCP ブロードキャストパケットを初めて受信したときに、端末の MAC 認証を実行します。端末が MAC 認証に合格すると、端末はネットワークにアクセスできます。MAC 認証に失敗すると、アクセスポートは 802.1X または Web 認証を実行します。
- アクセスポートは、802.1X クライアントまたはサードパーティクライアントから EAP パケットを受信すると、802.1X 認証を実行します。802.1X のユニキャストトリガー機能がアクセスポートでイネーブルになっている場合、クライアントからのすべてのパケットが 802.1X 認証をトリガーできます。
- アクセスポートは、端末から HTTP パケットを受信すると、Web 認証を実行します。

端末が異なるタイプの認証をトリガーした場合、認証は同時に処理されます。1つのタイプの認証が失敗しても、他のタイプの認証には影響しません。端末が1つのタイプの認証を通過すると、他のタイプの認証は次のように処理されます。

- 端末が最初にMAC認証にパスした場合、Web認証はすぐに終了しますが、802.1X認証は続行されます。端末が802.1X認証にもパスした場合、802.1X認証情報は端末。端末が802.1X認証に失敗した場合、ユーザーはMAC認証ユーザーとしてオンラインのままになり、802.1X認証だけが再度トリガーされます。
- 端末が最初に802.1XまたはWeb認証を通過した場合、他のタイプの認証はすぐに終了し、再度トリガーすることはできません。

## VLAN割り当てのトリプル認証サポート

### 認可 VLAN

ユーザーが認証を通過すると、認証サーバーはユーザーのアクセスポートに認可 VLAN を割り当てます。ユーザーは、認可 VLAN 内のネットワークリソースにアクセスできます。

### 認証失敗 VLAN

アクセスポートは、ユーザーが認証に失敗した後、ポートに設定されている認証失敗 VLAN にユーザーを追加します。

- 802.1X認証ユーザーの場合:802.1X認証用に設定されたAuth-fail VLAN(認証失敗VLAN)にユーザーを追加します。
- Web認証ユーザーの場合:Web認証用に設定されたAuth-fail VLAN(認証失敗VLAN)にユーザーを追加します。
- MAC認証ユーザーの場合:MAC認証用に設定されたゲストVLANにユーザーを追加します。

アクセスポートでは、すべてのタイプの認証失敗 VLAN を同時に設定できます。ユーザーが複数のタイプの認証に失敗した場合、そのユーザーの認証失敗 VLAN は次のように変更されます。

- Web Auth-fail VLAN(Web認証失敗VLAN)のユーザーがMAC認証に失敗した場合、そのユーザーはMAC認証ゲストVLANに移動されます。
- Web認証失敗VLANまたはMAC認証ゲストVLANのユーザーが802.1X認証に失敗した場合、そのユーザーは802.1X認証失敗VLANに移動されます。
- 802.1X認証失敗VLANのユーザーがMAC認証またはWeb認証に失敗しても、そのユーザーは802.1X認証失敗VLANのままです。

### サーバー到達不能 VLAN

到達不能なサーバーが原因でユーザーが認証に失敗した場合、アクセスポートはそのユーザーをサーバー到達不能 VLAN に追加します。

- 802.1X認証ユーザーの場合:802.1X認証用に設定されたクリティカルVLANにユーザーを追加します。
- Web認証ユーザーの場合:Web認証用に設定されたAuth-fail VLAN(認証失敗VLAN)にユーザーを追加します。
- MAC認証ユーザーの場合:MAC認証用に設定されたクリティカルVLANにユーザーを追加

します。

アクセスポートでは、すべてのタイプのサーバー到達不能 VLAN を同時に設定できます。ユーザーは、次のようにサーバー到達不能 VLAN に追加されます。

- ユーザーが802.1X認証を受けない場合、そのユーザーは最後の認証用に設定されたサーバー到達不能VLANに追加されます。
- Web Auth-Fail VLAN(Web認証失敗VLAN)またはMAC認証クリティカルVLANのユーザーが802.1X認証にも失敗した場合、そのユーザーは802.1X認証クリティカルVLANに追加されます。

## ACL許可のトリプル認証サポート

ユーザーが認証を通過すると、認証サーバーはユーザーのアクセスポートに認可 ACL を割り当てます。アクセスポートは ACL を使用して、ユーザーのトラフィックをフィルタリングします。

ACL 認可を使用するには、認証サーバーで認可 ACL を指定し、アクセスデバイスで ACL を設定する必要があります。ユーザーのアクセス認可を変更するには、認証サーバーで認可 ACL を変更するか、アクセスデバイスで認可 ACL のルールを変更します。

## オンラインユーザー検出のためのトリプル認証サポート

ユーザーのオンラインステータスを検出するために、次の機能を設定できます。

- Web認証ユーザーのオンラインユーザー検出をイネーブルにします。
- 802.1Xユーザーのオンラインユーザーハンドシェイクまたは定期的なオンラインユーザー再認証機能をイネーブルにします。
- MAC認証ユーザーのオフライン検出をイネーブルにします。

## 制約事項および注意事項:トリプル認証

トリプル認証では、802.1X 認証は MAC ベースのアクセスコントロール方式を使用する必要があります。

Web 認証がポートでイネーブルになっている場合は、ポートの認証失敗 VLAN およびサーバー到達不能 VLAN のサブネットを Web 認証フリーサブネットとして設定します。これにより、認証失敗ユーザーが認証失敗 VLAN またはサーバー到達不能 VLAN にアクセスできるようになります。

Web 認証フリーIP と 802.1X フリーIP の両方を構成しないでください。構成した場合、802.1X フリーIP のみが有効になります。

## トリプル認証タスクの概要

必要に応じて、次のタスクを選択します。

- 802.1X認証を設定する  
詳細については、「802.1X の設定」を参照してください。

- MAC認証の設定  
詳細については、「MAC認証の設定」を参照してください。
- Web認証を構成する  
詳細については、「Web認証の設定」を参照してください。

## トリプル認証の設定例

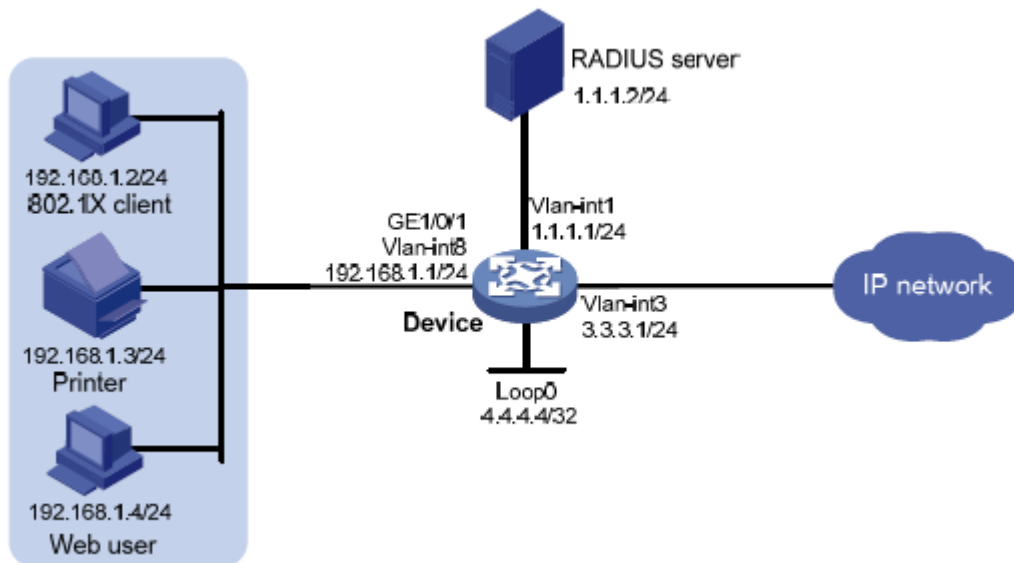
### 例:基本トリプル認証の設定

#### ネットワーク構成

図 2 に示すように、端末は IP ネットワークにアクセスするためにデバイスに接続されます。端末に接続するデバイスのレイヤー2 インターフェースにトリプル認証を設定します。802.1X 認証、Web 認証、および MAC 認証の 3 つの認証方式のいずれかを通過する端末は、IP ネットワークにアクセスできます。

- サブネット192.168.1.0/24のIPアドレスを端末に割り当てます。
- リモートRADIUSサーバーを使用して、認証、認可、およびアカウントングを実行します。ISPドメイン名を持たないユーザー名をRADIUSサーバーに送信するようにデバイスを設定します。
- リスニングIPアドレス4.4.4.4を使用するように、デバイス上のローカルWeb認証サーバーを構成します。デフォルトの認証ページをWebユーザーに送信し、HTTPを使用して認証データを転送するようにデバイスを構成します。

図 2 ネットワークダイアグラム



#### 手順

1. 端末、サーバー、およびデバイスが相互に到達できることを確認します(詳細は省略)。
2. ユーザーに通常の認証、認可、およびアカウントングを提供するようにRADIUSサーバーを設定します。この例では、RADIUSサーバーで次のように設定します。
  - ユーザー名がuserdotの802.1Xユーザー。
  - ユーザー名がuserptのWeb認証ユーザー。
  - ユーザー名とパスワードの両方がプリンタf07d6870725fのMACアドレスであるMAC認証ユーザー。

3. Web認証を設定します。

# VLAN インターフェースの VLAN および IP アドレスを設定し、特定の VLAN にポートを追加します。(詳細は省略)

# 認証ページを編集し、abc という名前の.zip ファイルにページを圧縮し、その.zip ファイルを FTP でデバイスにアップロードします(詳細は省略)。

# HTTP を使用するようにローカル Web サーバーを構成します。ファイル abc.zip をローカル Web サーバーのデフォルトの認証ページファイルとして構成します。

```
<Device> system-view
```

```
[Device] portal local-web-server http
```

```
[Device-portal-local-websvr-http] default-logon-page abc.zip
```

```
[Device-portal-local-websvr-http] quit
```

# インターフェイスループバック 0 の IP アドレスを 4.4.4.4 に設定します。

```
[Device] interface loopback 0
```

```
[Device-LoopBack0] ip address 4.4.4.4
```

```
[Device-LoopBack0] quit
```

# webserver という名前の Web 認証サーバーを作成し、そのビューを入力します。

```
[Device] web-auth server webserver
```

# Web 認証サーバーのリダイレクト URL を http://4.4.4.4/portal/として構成します。

```
[Device-web-auth-server-webserver] url http://4.4.4.4/portal/
```

# Web 認証サーバーの IP アドレスとポート番号を 4.4.4.4 と 80 に設定します。

```
[Device-web-auth-server-webserver] ip 4.4.4.4 port 80
```

```
[Device-web-auth-server-webserver] quit
```

# GigabitEthernet 1/0/1 で Web 認証をイネーブルにし、ポートの Web 認証サーバーWeb サーバーを指定します。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] web-auth enable apply server webserver [Device-GigabitEthernet1/0/1] quit
```

4. 802.1X認証を設定します。

# 802.1X 認証をグローバルにイネーブルにします。

```
[Device] dot1x
```

# GigabitEthernet 1/0/1 で 802.1X 認証をイネーブルにします(MAC ベースのアクセスコントロールが必要)。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] dot1x port-method macbased
```

```
[Device-GigabitEthernet1/0/1] dot1x
```

```
[Device-GigabitEthernet1/0/1] quit
```

5. MAC認証を設定します。

# MAC 認証をグローバルにイネーブルにします。

- ```
[Device] mac-authentication
# GigabitEthernet1/0/1 で MAC 認証をイネーブルにします。

[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] mac-authentication

[Device-GigabitEthernet1/0/1] quit
```
6. RADIUSスキームを設定します。
- ```
# rs1 という名前の RADIUS スキームを作成します。

[Device] radius scheme rs1
# プライマリ認証およびアカウントングサーバーとキーを指定します。

[Device-radius-rs1] primary authentication 1.1.1.2

[Device-radius-rs1] primary accounting 1.1.1.2

[Device-radius-rs1] key authentication simple radius

[Device-radius-rs1] key accounting simple radius

# ドメイン名を持たないように、RADIUS サーバーに送信するユーザー名を指定します。

[Device-radius-rs1] user-name-format without-domain

[Device-radius-rs1] quit
```
7. ISPドメインを設定します。
- ```
# triple という名前の ISP ドメインを作成します。

[Device] domain triple
# LAN アクセスユーザーの認証、認可、およびアカウントングに RADIUS スキーム rs1 を使用するようにドメインを設定します。

[Device-isp-triple] authentication lan-access radius-scheme rs1

[Device-isp-triple] authorization lan-access radius-scheme rs1

[Device-isp-triple] accounting lan-access radius-scheme rs1

[Device-isp-triple] quit

# デフォルトドメインとしてドメイントリプルを設定します。ユーザーが入力したユーザー名に ISP ドメイン名が含まれていない場合は、デフォルトドメインの AAA 方式が使用されます。

[Device] domain default enable triple
```

## 設定の確認

1. WebユーザーがWeb認証を通過できることを確認します。
- ```
# Web ユーザーターミナルで、Web ブラウザーを使用して外部ネットワークにアクセスし、
http://4.4.4.4/portal/logon.html の認証ページで正しいユーザー名とパスワードを入力します(詳細は省略)。
```
- ```
# オンライン Web 認証ユーザーに関する情報を表示します。

[Device] display web-auth user Total

online web-auth users: 1
```

User Name: localuser  
MAC address: acf1-df6c-f9ad  
Access interface: GigabitEthernet1/0/1  
Initial VLAN: 1  
Authorization VLAN: N/A  
Authorization ACL ID: N/A  
Authorization user profile: N/A

2. プリンタがMAC認証をパスできることを確認します。  
# プリンタをネットワークに接続します(詳細は省略)。  
# オンライン MAC 認証ユーザーに関する情報を表示します。

Total connections: 1  
Slot ID: 1  
User MAC address: f07d-6870-725f  
Access interface: GigabitEthernet1/0/1  
Username: f07d6870725f

User access state: Successful  
Authentication domain: triple  
Initial VLAN: 14  
Authorization untagged VLAN: 14  
Authorization tagged VLAN: N/A  
Authorization VSI: N/A  
Authorization ACL ID: N/A  
Authorization user profile: N/A  
Authorization URL: N/A  
Termination action: Default  
Session timeout period: N/A  
Online from: 2015/01/04 18:01:43  
Online duration: 0h 0m 2s

3. 802.1Xクライアントが802.1X認証を通過できることを確認します。  
# 802.1X クライアントで、802.1X 認証を開始し、正しいユーザー名とパスワードを入力します(詳細は省略)。  
# オンライン 802.1X ユーザーに関する情報を表示します。

Total connections: 1  
Slot ID: 1  
User MAC address: 7446-a091-84fe Access  
interface: GigabitEthernet1/0/1  
Username: userdot  
User access state: Successful  
Authentication domain: triple

IPv4 address: 192.168.1.2  
Authentication method: CHAP  
Initial VLAN: 14  
Authorization untagged VLAN: 14  
Authorization tagged VLAN list: N/A  
Authorization VSI: N/A  
Authorization ACL ID: N/A  
Authorization user profile: N/A  
Authorization URL: N/A  
Termination action: Default  
Session timeout period: N/A  
Online from: 2015/01/04 18:13:01  
Online duration: 0h 0m 14s

## 例:許可VLANおよび認証失敗VLANをサポートするためのトリプル認証の設定

### ネットワーク構成

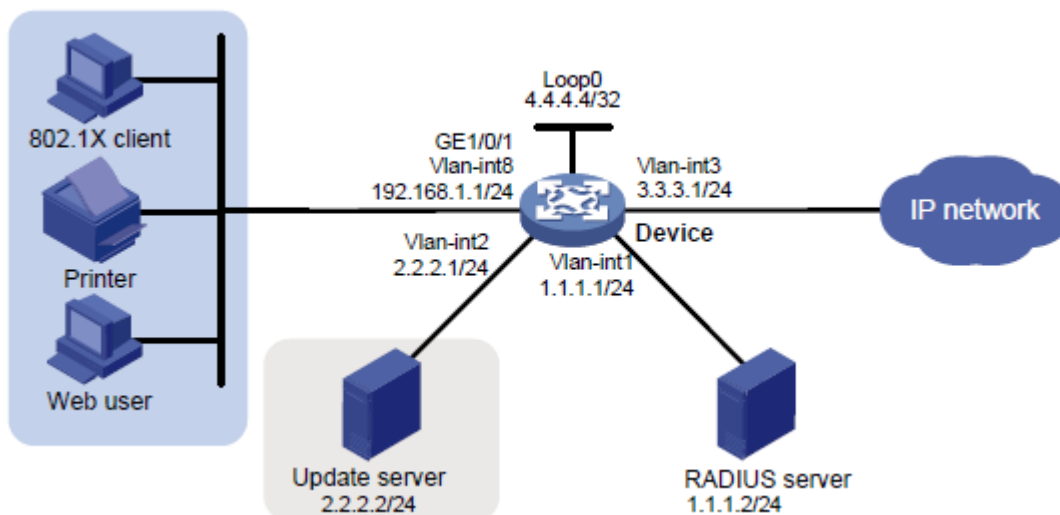
図 3 に示すように、端末は IP ネットワークにアクセスするためにデバイスに接続されます。端末に接続されたデバイスのレイヤー 2 インターフェースにトリプル認証を設定します。802.1X 認証、Web 認証、および MAC 認証の 3 つの認証方式のいずれかを通過する端末は、IP ネットワークにアクセスできます。

- Web認証端末はDHCPを使用して、認証前に192.168.1.0/24のIPアドレスを取得し、認証に合格した後に3.3.3.0/24のIPアドレスを取得します。端末が認証に失敗した場合は、DHCPを介して2.2.2.0/24のIPアドレスを要求します。  
アクセスデバイスまたは接続デバイスを DHCP サーバーとして使用できます。この例では、アクセスデバイス(デバイス)が DHCP サービスを提供します。
- 802.1X端末はDHCPを使用して、認証前に192.168.1.0/24のIPアドレスを取得し、認証に合格した後に3.3.3.0/24のIPアドレスを取得します。端末が認証に失敗した場合は、DHCPを介して2.2.2.0/24のIPアドレスを要求します。
- 認証に合格すると、プリンタはDHCPを介してMACアドレスにバインドされたIPアドレス3.3.3.111/24を取得します。
- リモートRADIUSサーバーを使用して、認証、認可、およびアカウントを実行します。RADIUSサーバーに送信されるユーザー名からISPドメイン名を削除するようにデバイスを設定します。
- リスニングIPアドレス4.4.4.4を使用するように、デバイス上のローカルWeb認証サーバーを構成します。デフォルトの認証ページをWebユーザーに送信し、HTTPを使用して認証データを転送するようにデバイスを構成します。
- VLAN 3を許可VLANとして設定します。認証に合格したユーザーは、このVLANに追加されます。
- VLAN 2を認証失敗VLANとして設定します。認証に失敗したユーザーは、このVLANに追加され



ます。

図 3 ネットワークダイアグラム



## 手順

1. 端末、サーバー、およびデバイスが相互に到達できることを確認します(詳細は省略)。
2. ユーザーに通常の認証、認可、およびアカウントングを提供するようにRADIUSサーバーを設定します。この例では、RADIUSサーバーで次のように設定します。
  - ユーザー名がuserdotの802.1Xユーザー。
  - ユーザー名がuserptのWeb認証ユーザー。
  - ユーザー名とパスワードの両方がプリンタf07d6870725fのMACアドレスであるMAC認証ユーザー。
  - 許可VLAN(VLAN 3)。
3. サーバアップデートのIPアドレスを認証フリーのIPアドレスとして設定します。

```
<Device> system-view
```

```
[Device] web-auth free-ip 2.2.2.2 24
```

4. 認証ページを編集し、defaultfileという名前の.zipファイルにページを圧縮し、その.zipファイルをFTPでデバイスにアップロードします(詳細は省略)。
5. DHCPを設定します。
  - # VLAN インターフェースの VLAN および IP アドレスを設定し、特定の VLAN にポートを追加します。(詳細は省略。)
  - # DHCP を有効にします。

```
[Device] dhcp enable
```

  - # アップデートサーバーの IP アドレスを動的アドレス割り当てから除外します。

```
[Device] dhcp server forbidden-ip 2.2.2.2
```

  - # DHCP アドレスプール 1 を設定して、サブネット 192.168.1.0 上のクライアントに IP アドレスとその他の設定パラメーターを割り当てます。

```
[Device] dhcp server ip-pool 1
```

```
[Device-dhcp-pool-1] network 192.168.1.0 mask 255.255.255.0
```

```
[Device-dhcp-pool-1] expired day 0 hour 0 minute 1
```

```
[Device-dhcp-pool-1] gateway-list 192.168.1.1
```

```
[Device-dhcp-pool-1] quit
```

# DHCP アドレスプール 2 を設定して、IP アドレスおよびその他の設定パラメーターをサブネット 2.2.2.0 上のクライアント

```
[Device] dhcp server ip-pool 2
[Device-dhcp-pool-2] network 2.2.2.0 mask 255.255.255.0
[Device-dhcp-pool-2] expired day 0 hour 0 minute 1
[Device-dhcp-pool-2] gateway-list 2.2.2.1
```

```
[Device-dhcp-pool-2] quit
```

# DHCP アドレスプール 3 を設定して、IP アドレスとその他の設定パラメーターをサブネット 3.3.3.0 上のクライアント

```
[Device] dhcp server ip-pool 3
[Device-dhcp-pool-3] network 3.3.3.0 mask 255.255.255.0
[Device-dhcp-pool-3] expired day 0 hour 0 minute 1
[Device-dhcp-pool-3] gateway-list 3.3.3.1
```

```
[Device-dhcp-pool-3] quit
```

# DHCP アドレスプール 4 を設定し、プリンタの MAC アドレス f07d-6870-725f を IP にバインドします。

このアドレスプール内のアドレス 3.3.3.111/24。

```
[Device] dhcp server ip-pool 4
[Device-dhcp-pool-4] static-bind ip-address 3.3.3.111 mask 255.255.255.0
client-identifier f07d-6870-725f
[Device-dhcp-pool-4] quit
```

## 6. Web認証を設定します。

# HTTP を使用するようにローカル Web サーバーを構成します。ファイル defaultfile.zip をローカル Web サーバーのデフォルトの認証ページファイルとして構成します。

```
[Device] portal local-web-server http
[Device-portal-local-websvr-http] default-logon-page defaultfile.zip
[Device-portal-local-websvr-http] quit
```

# インターフェース Loopback 0 に IP アドレス 4.4.4.4 を割り当てます。

```
[Device] interface loopback 0
[Device-LoopBack0] ip address 4.4.4.4 32
[Device-LoopBack0] quit
```

# webserver という名前の Web 認証サーバーを作成します。

# ローカルポータルサーバーのリスニング IP アドレスを 4.4.4.4 に指定します。

```
[Device] web-auth server webserver
# Web 認証サーバーのリダイレクト URL を http://4.4.4.4/portal/として構成します。
[Device-web-auth-server-webserver] url http://4.4.4.4/portal/
# Web 認証サーバーの IP アドレスとして 4.4.4.4、ポート番号として 80 を指定します。
[Device-web-auth-server-webserver] ip 4.4.4.4 port 80
```

```
[Device-web-auth-server-webserver] quit
```

# アップデートサーバーの IP アドレスを認証フリーの IP アドレスとして設定します。

```
[Device] web-auth free-ip 2.2.2.2 24
# GigabitEthernet 1/0/1 で Web 認証をイネーブルにし、Auth-fail VLAN(認証失敗 VLAN)として
VLAN 2 を指定します。
[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] port link-type hybrid

[Device-GigabitEthernet1/0/1] mac-vlan enable

[Device-GigabitEthernet1/0/1] web-auth enable apply server webserver

[Device-GigabitEthernet1/0/1] web-auth auth-fail vlan 2

[Device-GigabitEthernet1/0/1] quit
```

7. 802.1X認証を設定します。  
# 802.1X 認証をグローバルにイネーブルにします。

```
[Device] dot1x
# GigabitEthernet 1/0/1 で 802.1X 認証(MAC ベースのアクセスコントロールが必要)をイネーブル
にし、VLAN 2 を Auth-fail VLAN(認証失敗 VLAN)として指定します。
[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] dot1x port-method macbased

[Device-GigabitEthernet1/0/1] dot1x

[Device-GigabitEthernet1/0/1] dot1x auth-fail vlan 2

[Device-GigabitEthernet1/0/1] quit
```

8. MAC認証を設定します。  
# MAC 認証をグローバルにイネーブルにします。

```
[Device] mac-authentication
# GigabitEthernet 1/0/1 で MAC 認証をイネーブルにし、VLAN 2 をゲスト VLAN として指定します。
[Device] interface gigabitethernet 1/0/1

[Device-GigabitEthernet1/0/1] mac-authentication

[Device-GigabitEthernet1/0/1] mac-authentication guest-vlan 2

[Device-GigabitEthernet1/0/1] quit
```

9. RADIUSスキームを設定します。  
# rs1 という名前の RADIUS スキームを作成します。

```
[Device] radius scheme rs1
```

# プライマリ認証およびアカウントングサーバーとキーを指定します。

```
[Device-radius-rs1] primary authentication 1.1.1.2
[Device-radius-rs1] primary accounting 1.1.1.2
[Device-radius-rs1] key authentication simple radius
[Device-radius-rs1] key accounting simple radius
```

# ドメイン名を持たないように、RADIUS サーバーに送信するユーザー名を指定します。

```
[Device-radius-rs1] user-name-format without-domain
```

```
[Device-radius-rs1] quit
10. ISPドメインを設定します。
# triple という名前の ISPドメインを作成します。

[Device] domain triple
# LAN アクセスユーザーの認証、認可、およびアカウントリングに RADIUS スキーム rs1 を使用する
ようにドメインを設定します。

[Device-isp-triple] authentication lan-access radius-scheme rs1
[Device-isp-triple] authorization lan-access radius-scheme rs1
[Device-isp-triple] accounting lan-access radius-scheme rs1
[Device-isp-triple] quit

# デフォルトドメインとしてドメイントリプルを設定します。ユーザーが入力したユーザー名に ISP ドメ
イン名が含まれていない場合は、デフォルトドメインの AAA 方式が使用されます。

[Device] domain default enable triple
```

## 設定の確認

1. WebユーザーがWeb認証を通過できることを確認します。
 

```
# Web ユーザーターミナルで、Web ブラウザーを使用して外部ネットワークにアクセスし、
http://4.4.4.4/portal/logon.html の認証ページで正しいユーザー名とパスワードを入力します(詳
細は省略)。

# オンラインユーザーに関する情報を表示するには、display web-auth user コマンドを使用します。
[Device] display web-auth user Total
online web-auth users: 1

User Name: userpt
MAC address: 6805-ca17-4a0b
Access interface: GigabitEthernet1/0/1
Initial VLAN: 14
Authorization VLAN: 3
Authorization ACL ID: N/A
Authorization user profile: N/A
```
2. プリンタがMAC認証をパスできることを確認します。
 

```
# プリンタをネットワークに接続します(詳細は省略)。

# オンライン MAC 認証ユーザーに関する情報を表示します。
[Device] display mac-authentication connection Total
connections: 1

Slot ID: 1
User MAC address: f07d-6870-725f

Access interface: GigabitEthernet1/0/1

Username: f07d6870725f
User access state:Successful
```

Authentication domain: triple  
Initial VLAN: 14  
Authorization untagged VLAN: 3  
Authorization tagged VLAN: N/A  
Authorization VSI: N/A  
Authorization ACL ID: N/A  
Authorization user profile: N/A  
Authorization URL: N/A  
Termination action: Default  
Session timeout period: N/A  
Online from: 2015/01/04 18:01:43  
Online duration: 0h 0m 2s

3. 802.1Xユーザーが802.1X認証を通過できることを確認します。  
# 802.1X クライアントで、802.1X 認証を開始し、正しいユーザー名とパスワードを入力します(詳細は省略)。

# オンライン 802.1X ユーザーに関する情報を表示します。

Total connections: 1  
Slot ID: 1  
User MAC address: 7446-a091-84fe  
Access interface: GigabitEthernet1/0/1  
Username: userdot

User access state: Successful  
Authentication domain: triple IPv4  
address: 3.3.3.2 Authentication  
method: CHAP Initial VLAN: 14

Authorization untagged VLAN: 3  
Authorization tagged VLAN list: N/A  
Authorization VSI: N/A Authorization  
ACL ID: N/A Authorization user  
profile: N/A Authorization URL: N/A

Termination action: Default  
Session timeout period: N/A  
Online from: 2015/01/04 18:13:01  
Online duration: 0h 0m 14s

4. 認証に合格したユーザーに認可VLANが割り当てられていることを確認します。  
# オンラインユーザーの MAC-VLAN エントリを表示します。

[Device] display mac-vlan all

The following MAC VLAN addresses exist:

S:Static D:Dynamic

MAC ADDR	MASK	VLAN ID	PRIO	STATE
6805-ca17-4a0b	ffff-ffff-ffff	3	0	D
f07d-6870-725f	ffff-ffff-ffff	3	0	D
7446-a091-84fe	ffff-ffff-ffff	3	0	D

Total MAC VLAN address count:3

5. オンラインユーザーにIPアドレスが割り当てられていることを確認します。

[Device] display dhcp server ip-in-use

IP address	Client-identifier/ Type Hardware address	Lease	expiration
3.3.3.111	01f0-7d68-7072-5f	Jan 4 18:14:17 2015	Auto:(C)
3.3.3.2	0168-05ca-174a-0b	Jan 4 18:15:01 2015	Auto:(C)
3.3.3.3	0174-46a0-9184-fe	Jan 4 18:15:03 2015	Auto:(C)

6. 認証に失敗した端末は、VLAN 2に追加されます。上記の表示コマンドを使用すると、端末のMAC-VLANエントリおよびIPアドレスを表示できます(詳細は省略)。

# ポートセキュリティの設定

## ポートセキュリティについて

ポートセキュリティは、802.1X 認証と MAC 認証を組み合わせることで拡張し、MAC ベースのネットワークアクセスコントロールを提供します。この機能は、ユーザーに対して異なる認証方式を使用するポートに適用されます。

## 主な機能

ポートセキュリティは、次の機能を提供します。

- 着信トラフィックの送信元MACアドレスをチェックすることにより、ネットワークへの不正アクセスを防止します。
- 発信トラフィックの宛先MACアドレスをチェックすることにより、不正なデバイスやホストへのアクセスを防止します。
- ポートでのMACアドレス学習および認証を制御して、ポートが送信元の信頼できるMACアドレスだけを学習するようにします。

## ポートセキュリティ機能

### NTK

Need to Know(NTK)機能は、アウトバウンドフレーム内の宛先 MAC アドレスをチェックすることによって、トラフィックの傍受を防止します。この機能により、フレームは次のホストにのみ送信されます。

- 認証に合格したホスト。
- アクセスデバイスで学習または設定されたMACアドレスを持つホスト。

### 侵入保護

侵入保護機能は、着信フレーム内の送信元 MAC アドレスに不正なフレームがないかどうかをチェックし、検出された不正なフレームに対して事前に定義されたアクションを実行します。アクションには、ポートを一時的に無効にする、ポートを永続的に無効にする、不正な MAC アドレスからのフレームを 3 分間ブロックする(ユーザーが設定できない)などがあります。

フレームの送信元 MAC アドレスがポートセキュリティモードで学習できない場合、またはフレームが 802.1X または MAC 認証に失敗したクライアントからのものである場合、フレームは不正です。

## ポートセキュリティモード

ポートセキュリティでは、次のカテゴリのセキュリティモードがサポートされます。

- **MAC学習制御:** autoLearnとsecureの2つのモードがあります。MACアドレス学習は、autoLearnモードのポートでは許可されますが、secureモードではディセーブルになります。
- **Authentication:** このカテゴリのセキュリティモードは、MAC認証、802.1X認証、またはこれ

ら2つの認証方式の組み合わせを実装します。

セキュリティモードのポートは、フレームを受信すると、MAC アドレステーブルで送信元 MAC アドレスを検索します。一致が見つかった場合、ポートはフレームを転送します。一致が見つからない場合、ポートは MAC アドレスを学習するか、セキュリティモードに応じて認証を実行します。フレームが不正な場合、ポートは事前定義された NTK または侵入保護アクションを実行するか、SNMP 通知を送信します。発信フレームは、NTK 機能をトリガーしない限り、ポートセキュリティの NTK アクションによって制限されません。

表 1 に、ポートセキュリティモードとセキュリティ機能を示します。

表 1 ポートセキュリティモード

目的	セキュリティモード		トリガー可能な機能
ポートセキュリティ機能をオフにする	noRestrictions(デフォルトモード) このモードでは、ポートセキュリティはポート上でディセーブルになり、ポートへのアクセスは制限されません。		該当なし
MACアドレス学習の制御	autoLearn		NT K/侵入保護
	Secure		
802.1X認証の実行	userLogin		該当なし
	userLoginSecure		NT K/侵入保護
	userLoginSecureExt		
	userLoginWithOUI		
MAC認証の実行	macAddressWithRadius		NT K/侵入保護
MAC認証と802.1X認証の組み合わせの実行	Or	macAddressOrUserLoginSecure	NT K/侵入保護
		macAddressOrUserLoginSecureExt	
	Else	macAddressElseUserLoginSecure	
		macAddressElseUserLoginSecureExt	

モード名を次に示します。

- **userLogin**: 802.1X認証およびポートベースのアクセスコントロールを指定します。**userLogin with Secure**は、802.1X認証およびMACベースのアクセスコントロールを指定します。**Ext**は、複数の802.1Xユーザーが同時に認証され、サービスを受けることを許可することを示します。Extを使用しないセキュリティモードでは、1人のユーザーのみが802.1X認証を通過できます。
- **macAddress**: MAC認証を指定します。
- **Else**: **Else**の前の認証方式が最初に適用されることを指定します。認証が失敗した場合、**Else**の後の認証方式に切り替えるかどうかは、認証要求のプロトコルタイプによって異なります。
- **Or**: **Or**に続く認証方式が最初に適用されることを指定します。認証に失敗した場合は、**Or**の前の認証方式が適用されます。

## MAC アドレス学習の制御

- **autoLearn**。

このモードのポートは、MAC アドレスを学習できます。自動的に学習された MAC アドレスは、ダイナミック MAC アドレスとして MAC アドレステーブルに追加されません。代わりに、これらの MAC アドレスは、



セキュア MAC アドレスとしてセキュア MAC アドレステーブルに追加されます。セキュア MAC アドレスは、**port-security mac-address security** コマンドを使用して設定することもできます。

自動学習モードのポートでは、次の MAC アドレスを送信元とするフレームを通過させることができます。

- セキュア MAC アドレス。
- **mac-address dynamic** および **mac-address static** コマンドを使用して設定された MAC アドレス。

セキュア MAC アドレスの数が上限に達すると、ポートはセキュアモードに移行します。

- セキュア。  
MAC アドレス学習は、セキュアモードのポートではディセーブルです。MAC アドレスを設定するには、**mac-address static** コマンドおよび **mac-address dynamic** コマンドを使用します。MAC アドレステーブルエントリの設定の詳細については、『Layer 2 LAN Switching Configuration Guide』を参照してください。

セキュアモードのポートでは、次の MAC アドレスを送信元とするフレームだけを通過させることができます。

- セキュア MAC アドレス。
- **mac-address dynamic** および **mac-address static** コマンドを使用して設定された MAC アドレス。

## 802.1X 認証の実行

- **userLogin**

このモードのポートは、802.1X 認証を実行し、ポートベースのアクセスコントロールを実装します。ポートは、複数の 802.1X ユーザーにサービスを提供できます。802.1X ユーザーがポートで認証を渡すと、その後の 802.1X ユーザ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。

- **userLoginSecure**

このモードのポートは、802.1X 認証を実行し、MAC ベースのアクセスコントロールを実装します。ポートは、802.1X 認証を通過する 1 人のユーザーだけにサービスを提供します。

- **userLoginSecureExt**

このモードは userLoginSecure モードに似ていますが、複数のオンライン 802.1X ユーザーをサポートする点が異なります。

- **userLoginWithOUI**

このモードは userLoginSecure モードに似ています。違いは、このモードのポートでは、MAC アドレスに特定の OUI が含まれている 1 人のユーザーからのフレームも許可されることです。

このモードでは、ポートは最初に OUI チェックを実行します。OUI チェックが失敗した場合、ポートは 802.1X 認証を実行します。ポートは、OUI チェックまたは 802.1X 認証を通過するフレームを許可します。

---

### 注:

OUI は、ベンダー、製造元、または組織を独自に識別する 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。

---

## MAC 認証の実行

macAddressWithRadius: このモードのポートは、MAC 認証を実行し、複数のユーザーにサービスを提供します。

## MAC 認証と 802.1X 認証の組み合わせの実行

- **macAddressOrUserLoginSecure**

このモードは、macAddressWithRadius モードと userLoginSecure モードを組み合わせたものです。このモードでは、1人の 802.1X 認証ユーザーと複数の MAC 認証ユーザーがログインできます。

このモードでは、ポートは最初に 802.1X 認証を実行します。デフォルトでは、802.1X 認証が失敗した場合、MAC 認証が実行されます。

ただし、次の条件が存在する場合、このモードのポートは認証を異なる方法で処理します。

- ポートは、MAC認証および802.1X認証の並列処理でイネーブルにされます。
- ポートは802.1Xユニキャストトリガーでイネーブルになっています。
- ポートが未知のMACアドレスからパケットを受信しました。

このような状況では、ポートはユニキャスト EAP-Request/Identity パケットを MAC アドレスに送信して 802.1X 認証を開始します。その後、ポートは 802.1X 認証の結果を待つことなく、ただちに MAC 認証を処理します。

- **macAddressOrUserLoginSecureExt**

このモードは macAddressOrUserLoginSecure モードに似ていますが、複数の 802.1X および MAC 認証ユーザーをサポートする点が異なります。

- **macAddressElseUserLoginSecure**

このモードは、macAddressWithRadius モードと userLoginSecure モードを組み合わせたもので、Else キーワードが示すように、MAC 認証のプライオリティが高くなっています。このモードでは、1人の 802.1X 認証ユーザーと複数の MAC 認証ユーザーがログインできます。

このモードでは、ポートは 802.1X 以外のフレームを受信すると MAC 認証を実行します。802.1X フレームを受信すると、ポートは MAC 認証を実行し、認証が失敗した場合は 802.1X 認証を実行します。

- **macAddressElseUserLoginSecureExt**

このモードは macAddressElseUserLoginSecure モードに似ていますが、Ext キーワードが示すように、複数の 802.1X および MAC 認証ユーザーをサポートする点が異なります。

## 制約事項および注意事項:ポートセキュリティ設定

この機能は、WLAN など、ポート上のユーザーごとに異なる認証方式を必要とするネットワークに適用されます。

802.1X 認証または MAC 認証だけが必要なシナリオでは、ポートセキュリティではなく、802.1X 認証または MAC 認証機能を使用することをお勧めします。802.1X および MAC 認証の詳細については、「802.1X の設定」および「MAC 認証の設定」を参照してください。

ポートセキュリティモードの **autolearn**、**secure**、**userlogin-withoui**、および **secure MAC** アドレス設定は、レイヤー2 集約インターフェースではサポートされません。その他のポートセキュリティ設定は、レイヤー2 イーサネットインターフェースとレイヤー2 集約インターフェースの両方でサポートされます。

レイヤー2 イーサネットインターフェースが集約グループに追加されると、インターフェースのポートセキュリティ設定は有効になりません。

インターフェースにオンラインの 802.1X または MAC 認証ユーザーがいる場合は、レイヤー2 集約インターフェースを削除しないでください。

# ポートセキュリティタスクの概要

ポートセキュリティを設定するには、次の作業を実行します。

1. ポートセキュリティの基本機能の設定
  - ポートセキュリティのイネーブル化
  - ポートセキュリティモードの設定
  - ポート上のセキュアMACアドレス数に対するポートセキュリティの制限の設定
  - セキュアMACアドレスの設定
  - (任意)NTKの設定
  - (任意)侵入防御の設定
2. (任意)ポートセキュリティの拡張機能の設定
  - サーバーからの許可情報を無視する
  - MAC移動の有効化
  - authorization-fail-offline機能のイネーブル化
  - ポート上の特定のVLANのMACアドレス数に対するポートセキュリティの制限の設定
  - オープン認証モードの有効化
  - ポートセキュリティのためのフリーVLANの設定
  - ポートセキュリティへのNAS-IDプロファイルの適用
  - エスケープクリティカルVSI機能の設定

拡張ポートセキュリティ機能は、ポートセキュリティがディセーブルで、802.1X または MAC 認証がイネーブルの場合にも有効になります。

3. (任意)ポートセキュリティのSNMP通知のイネーブル化
4. (任意)ポートセキュリティユーザーのロギングのイネーブル化

## ポートセキュリティのイネーブル化

### 制約事項とガイドライン

ポートセキュリティを設定する場合は、次の制約事項および注意事項に従ってください。

- ポートセキュリティがイネーブルになっている場合、802.1XまたはMAC認証をイネーブルにしたり、アクセスコントロールモードまたはポート認可ステートを変更したりすることはできません。ポートセキュリティは、異なるセキュリティモードでこれらの設定を自動的に変更します。
- **undo port-security enable**コマンドを使用すると、ポートセキュリティをディセーブルにできます。このコマンドはオンラインユーザーをログオフするため、オンラインユーザーが存在しないことを確認してください。
- ポートセキュリティをイネーブルまたはディセーブルにすると、次のセキュリティ設定がデフォルトにリセットされます。
  - MACベースの802.1Xアクセスコントロールモード。
  - ポートの許可ステート(auto)。

802.1X 認証および MAC 認証設定の詳細については、「802.1X の設定」および「MAC 認証の設定」を参照してください。

### 前提条件

ポートセキュリティをイネーブルにする前に、802.1X および MAC 認証をグローバルにディセーブルにします。

## 手順

1. システムビューを開始します。

### System-view

2. ポートセキュリティをイネーブルにします。

### Port-security enable

デフォルトでは、ポートセキュリティはディセーブルです。

# ポートセキュリティモードの設定

## 制約事項とガイドライン

ポートセキュリティがディセーブルになっていても、設定を有効にできない場合は、ポートセキュリティモードを指定できます。

ポートのポートセキュリティモードを変更すると、そのポートのオンラインユーザーがログオフされます。

ポートセキュリティがイネーブルになっているポートでは、802.1X 認証または MAC 認証をイネーブルにしないでください。

ポートセキュリティをイネーブルにした後、ポートが noRestrictions (デフォルト)モードで動作している場合に限り、ポートのポートセキュリティモードを変更できます。その他のモードのポートのポートセキュリティモードを変更するには、最初に **undo port-security port-mode** コマンドを使用して、デフォルトのポートセキュリティモードに戻します。

デバイスは、次のポートセキュリティモードで RADIUS サーバーによって割り当てられた URL アトリビュートをサポートします。

- mac-authentication
- mac-else-userlogin-secure
- mac-else-userlogin-secure-ext
- userlogin-secure
- userlogin-secure-ext
- userlogin-secure-or-userlogin-mac
- userlogin-secure-or-mac-ext
- userlogin:withoui

認証中、ユーザーの HTTP または HTTPS 要求は、サーバーに割り当てられた URL 属性によって指定された Web インターフェースにリダイレクトされます。ユーザーが Web 認証に合格すると、RADIUS サーバーはユーザーの MAC アドレスを記録し、DM(切断メッセージ)を使用してユーザーをログオフします。ユーザーが 802.1X または MAC 認証を再度開始すると、認証に合格し、正常にオンラインになります。

ポートセキュリティユーザーの HTTPS 要求をリダイレクトするには、デバイス上の HTTPS リダイレクトリスニングポートを指定します。詳細については、『Layer 3 IP Services Configuration Guide』の「HTTP redirect」を参照してください。

## 前提条件

ポートのポートセキュリティモードを設定する前に、次の作業を実行します。

- 802.1XおよびMAC認証をディセーブルにします。

- 自動学習モードを設定する場合は、ポートセキュリティのセキュアMACアドレス数の制限を設定します。ポートが自動学習モードで動作している場合は、この設定を変更できません。

## 手順

1. システムビューを開始します。

### System-view

2. ユーザー認証の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、ユーザー認証用の OUI 値は設定されていません。このコマンドが必要なのは、**userlogin-withoui** モードの場合だけです。

複数の OUI を設定できますが、ポートセキュリティモードが **userlogin-withoui** の場合、ポートでは 1 人の 802.1X ユーザーと、指定された OUI のいずれかに一致する 1 人のユーザーだけが許可されます。

3. インターフェイスビューを開始します。

**interface *interface-type* *interface-number***

4. ポートセキュリティモードを設定します。

**port-security port-mode { autolearn | mac-authentication | mac-else-userlogin-secure | mac-else-userlogin-secure-ext | secure | userlogin | userlogin-secure | userlogin-secure-ext | userlogin-secure-or-mac | userlogin-secure-or-mac-ext | userlogin-withoui }**

デフォルトでは、ポートは noRestrictions モードで動作します。

# ポート上のセキュアMACアドレス数に対するポートセキュリティの制限の設定

## ポート上のセキュア MAC アドレス数に関するポートセキュリティの制限について

次の目的のために、ポートセキュリティがポート上で許可するセキュア MAC アドレスの最大数を設定できます。

- ポート上の同時ユーザー数の制御。

セキュリティモード( autoLearn および secure を除く)で動作しているポートの場合、上限は次の値のうち小さい方になります。

- ポートセキュリティで許可されるセキュアMACアドレスの制限。
- 使用中の認証モードで許可される同時ユーザーの制限。

- 自動学習モードのポート上のセキュアMACアドレスの数を制御する。

また、ポートセキュリティが特定の VLAN またはポート上の各 VLAN に許可するセキュア MAC アドレスの最大数を設定することもできます。

ポート上のセキュア MAC アドレス数に対するポートセキュリティの制限は、「MAC アドレステーブルの設定」で説明されている MAC 学習制限とは無関係です。MAC アドレステーブルの設定の詳細については、『レイヤー2 LAN スイッチングコンフィギュレーションガイド』を参照してください。

## 手順

1. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

```
interface interface-type interface-number
```

3. ポートで許可されるセキュアMACアドレスの最大数を設定します。

```
port-security max-mac-count max-count [ vlan [ vlan-id-list ] ]
```

デフォルトでは、ポートセキュリティはポート上のセキュア MAC アドレスの数を制限しません。

## セキュアMACアドレスの設定

### セキュア MAC アドレスについて

セキュア MAC アドレスは、自動学習モードで設定または学習されます。セキュア MAC アドレスが保存されている場合は、デバイスのリブート後も保持されます。セキュア MAC アドレスをバインドできるのは、VLAN 内の 1 つのポートだけです。

セキュア MAC アドレスには、スタティック、スティッキ、およびダイナミックセキュア MAC アドレスがありません。

表 2 スタティック、スティッキ、およびダイナミックセキュア MAC アドレスの比較

種類	アドレスソース	エージングのメカニズム	保存して、デバイスの再起動後も使用できますか。
static	手動で追加(sticky キーワードを指定せずにport-security mac-address security コマンドを使用)。	<p>利用できません。</p> <p>スタティックセキュアMACアドレスは、次のいずれかのタスクを実行しない限り、期限切れになりません。</p> <ul style="list-style-type: none"> <li>これらのMACアドレスを手動で削除します。</li> <li>ポートセキュリティモードを変更します。</li> <li>ポートセキュリティ機能をディセーブルにします。</li> </ul>	はい。
Sticky	<ul style="list-style-type: none"> <li>手動で追加(port-security mac-address security コマンド (sticky キーワードを指定)。</li> <li>ダイナミックセキュアMACアドレスから変換。</li> <li>ダイナミックセキュアMAC機能がディセーブルの場合、自動的に学習されます。</li> </ul>	<p>デフォルトでは、スティッキMACアドレスはエージングアウトしません。ただし、古いスティッキMACアドレスを削除するには、エージングタイマーを設定するか、非アクティブエージング機能とともにエージングタイマーを使用します。</p> <p>エージングタイマーだけが設定されている場合、エージングタイマーはSticky MACアドレスからトラフィックデータが送信されたかどうかに関係なく、アップします。</p> <ul style="list-style-type: none"> <li>エージングタイマーと非アクティブエージング機能の両方が設定されている場合、スティッ</li> </ul>	はい。 セキュアMACエージングタイマーは、リブート時に再起動します。

		キMACアドレスからトラフィックデータが検出されると、エージングタイマーが再起動されま す。	
Dynamic	<ul style="list-style-type: none"> <li>• ステイツキMACアドレスから変換されます。</li> <li>• ダイナミックセキュアMAC機能をイネーブ ルにした後、自動的に学習 されます。</li> </ul>	Sticky MACアドレスと同じです。	いいえ。 すべてのダイナミック セキュアMACアドレス は、リポート時に失わ れます。

セキュア MAC アドレスエントリの最大数に達すると、ポートはセキュアモードに変更されます。セキュアモードでは、ポートはこれ以上セキュア MAC アドレスを追加または学習できません。ポートは、セキュア MAC アドレスから送信されたフレーム、または **mac-address dynamic** または **mac-address static** コマンドを使用して設定された MAC アドレスから送信されたフレームだけを通させることができます。

## 前提条件

セキュア MAC アドレスを設定する前に、次の作業を実行します。

- ポート上のMACアドレス数に対するポートセキュリティの制限を設定します。自動学習モードをイネーブ  
ルにする前に、この作業を実行します。
- ポートセキュリティモードをautoLearnに設定します。
- 指定されたVLANのパケットがVLANにポートを通または追加できるようにポートを設定します。  
VLANがすでに存在することを確認してください。

## セキュア MAC アドレスの追加

1. システムビューを開始します。  
**System-view**
2. セキュアMACエージングタイマーを設定します。  
**port-security timer autolearn aging [ second ] time-value**  
デフォルトでは、セキュア MAC アドレスは期限切れになりません。
3. セキュアMACアドレスを設定します。
  - システムビューでセキュアMACアドレスを設定します。  
**port-security mac-address security [ sticky ] mac-address interface interface-type  
interface-number vlan vlan-id**
  - インターフェイスビューでセキュアMACアドレスを設定するには、次のコマンドを順番に  
実行します。

**interface interface-type interface-number**

**port-security mac-address security [ sticky ] mac-address vlan vlan-id**

デフォルトでは、手動で設定されたセキュア MAC アドレスは存在しません。

VLAN では、MAC アドレスをスタティックセキュア MAC アドレスとスティッキ MAC アドレスの両方として指定することはできません。

## セキュア MAC アドレスの非アクティブエージングのイネーブル化

1. システムビューを開始します。

**System-view**

2. インターフェイスビューを開始します。

**interface interface-type interface-number**

3. セキュアMACアドレスの非アクティブエージングをイネーブルにします。

**port-security mac-address aging-type inactivity**

デフォルトでは、セキュア MAC アドレスの非アクティブエージング機能はディセーブルです。

## ダイナミックセキュア MAC 機能のイネーブル化

1. システムビューを開始します。

**System-view**

2. インターフェイスビューを開始します。

**interface interface-type interface-number**

3. ダイナミックセキュアMAC機能をイネーブルにします。

**port-security mac-address dynamic**

デフォルトでは、ダイナミックセキュア MAC 機能はディセーブルになっています。スティッキ MAC アドレスはコンフィギュレーションファイルに保存できます。保存されると、デバイスのリブート後も保持されます。

## NTKの設定

### NTK 機能について

NTK 機能は、発信フレームの宛先 MAC アドレスをチェックして、フレームが認証されたデバイスだけに転送されるようにします。

NTK 機能は、次のモードをサポートします。

- **ntkonly**: 認証された宛先MACアドレスを持つユニキャストフレームだけを転送します。
- **ntk-withbroadcasts**: 認証された宛先MACアドレスを持つブロードキャストフレームおよびユニキャストフレームだけを転送します。
- **ntk-withmulticasts**: 認証された宛先MACアドレスを持つブロードキャストフレーム、マルチキャストフレーム、およびユニキャストフレームだけを転送します。

### 制約事項とガイドライン

NTK 機能は、宛先 MAC アドレスが不明なユニキャストフレームをドロップします。



すべてのポートセキュリティモードが NTK 機能のトリガーをサポートしているわけではありません。詳細については、表 21 を参照してください。

## 手順

1. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

3. NTK機能を設定します。

**port-security ntk-mode { ntk-withbroadcasts | ntk-withmulticasts | ntkonly }**

デフォルトでは、NTK はポート上でディセーブルにされ、すべてのフレームの送信が許可されます。

# 侵入保護の設定

## 侵入保護について

侵入保護により、デバイスは不正なフレームに対して次のいずれかのアクションを実行できます。

- **Blockmac:** 不正なフレームの送信元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、フレームを廃棄します。ブロックされたMACアドレスを送信元とする後続のすべてのフレームはドロップされます。ブロックされたMACアドレスは、3分間ブロックされた後、通常の状態に復元されます。間隔は固定されており、変更できません。
- **disableport:** 手動で起動するまでポートをディセーブルにします。
- **disableport-temporarily:** 一定期間、ポートを一時的に無効にします。この期間は、**port-security timer disableport**コマンドで設定できます。

## 制約事項とガイドライン

macAddressElseUserLoginSecure モードまたは macAddressElseUserLoginSecureExt モードで動作しているポートでは、同じフレームに対する MAC 認証と 802.1X 認証の両方が失敗した場合にだけ、侵入保護がトリガーされます。

## 手順

1. システムビューを開始します。

### System-view

2. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

3. 侵入保護機能を設定します。

**port-security intrusion-mode { blockmac | disableport | disableport-temporarily }**

デフォルトでは、侵入保護はディセーブルです。

4. (任意)ポートがディセーブルのままになる無音タイムアウト時間を設定します。

### a. quit

**b. port-security timer disableport** *time-value*

デフォルトでは、ポートの無音タイムアウト時間は 20 秒です。

# サーバーからの許可情報を無視する

## サーバーからの許可情報の無視について

802.1X または MAC 認証ユーザーが認証を通過した後、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ポートを設定できます。

### 手順

1. システムビューを開始します。

#### **System-view**

2. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

3. 認証サーバーから受信した認可情報を無視します。

**port-security authorization ignore**

デフォルトでは、ポートは認証サーバーから受信した認可情報を使用します。

# MAC移動の有効化

## MAC 移動について

MAC 移動を使用すると、802.1X または MAC で認証されたユーザーは、デバイス上のポート間を移動できます。たとえば、認証された 802.1X ユーザーがデバイス上の別の 802.1X 対応ポートに移動すると、認証セッションは最初のポートから削除されます。ユーザーは新しいポートで再認証されます。

MAC 移動がディセーブルの場合、1つのポートで認証された 802.1X または MAC ユーザーは、別のポートに移動した後、認証を通過できません。

認証サーバー(ローカルまたはリモート)上のオンラインユーザーの数が上限に達した場合、802.1X または MAC 認証ユーザーはデバイス上のポート間を移動できません。

## 制約事項とガイドライン

ベストプラクティスとして、ネットワークにアクセスするためにポート間をローミングするユーザーに対して MAC 移動をイネーブルにします。

### 手順

1. システムビューを開始します。

#### **System-view**

2. MAC移動をイネーブルにします。

**port-security mac-move permit**

デフォルトでは、MAC 移動はディセーブルです。

# authorization-fail-offline機能のイネーブル化

## Authorization-fail-offline 機能について

authorization-fail-offline 機能は、ACL またはユーザープロファイル許可に失敗したポートセキュリティユーザーをログオフします。

ユーザーは、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。

- デバイスが、指定されたACLまたはユーザープロファイルをユーザーに認可できませんでした。
- サーバーは、存在しないACLまたはユーザープロファイルをユーザーに割り当てます。

この機能は、VLAN 許可に失敗したユーザーには適用されません。デバイスはこれらのユーザーを直接ログオフします。

Authorization-fail-offline 機能によってログオフされた 802.1X または MAC 認証ユーザーに対して、待機タイマー機能をイネーブルにすることもできます。デバイスは、これらのユーザーを 802.1X または MAC 認証待機キューに追加します。デバイスは、待機タイマーが期限切れになるまで、これらのユーザーからのパケットを処理したり、認証したりしません。待機タイマー機能をイネーブルにしない場合、デバイスは、これらのユーザーからパケットを受信するとすぐにこれらのユーザーを認証します。

## 前提条件

待機タイマー機能を有効にするには、次のタスクを実行します。

- 802.1Xユーザーの場合、dot1x quiet-periodコマンドを使用して待機タイマーをイネーブルにし、dot1x timer quiet-periodコマンドを使用してタイマーを設定します。
- MAC認証ユーザーの場合、mac-authentication timer quietコマンドを使用して、MAC認証のクワイエットタイマーを設定します。

## 手順

1. システムビューを開始します。

### System-view

2. authorization-fail-offline機能をイネーブルにします。

### port-security authorization-fail offline [ quiet-period ]

デフォルトでは、この機能はディセーブルになっており、デバイスは ACL またはユーザープロファイルの認可に失敗したユーザーをログオフしません。

# ポート上の特定のVLANのMACアドレス数に対するポートセキュリティの制限の設定

## ポート上の特定の VLAN の MAC アドレス数に対するポートセキュリティの制限について

通常、ポートセキュリティを使用すると、ポート上の次のタイプの MAC アドレスにアクセスできます。

- 802.1XまたはMAC認証を通過するMACアドレス。
- MAC認証ゲストVLANまたはMAC認証クリティカルVLANのMACアドレス、およびMAC認証ゲストVSIまたはMAC認証クリティカルVSIのMACアドレス。
- 802.1XゲストVLAN、802.1X認証失敗VLAN、または802.1XクリティカルVLANのMACアドレス、および802.1XゲストVSI、802.1X認証失敗VSI、または802.1XクリティカルVSIのMACアドレス。

この機能は、ポートセキュリティが特定の VLAN を介してポートにアクセスすることを許可する MAC アドレスの数を制限します。この機能を使用して、MAC アドレス間のリソース競合を回避し、ポート上の各アクセスユーザーに対して信頼性の高いパフォーマンスを確保します。ポート上の VLAN 内の MAC アドレスの数が上限に達すると、デバイスはポート上の VLAN 内の後続の MAC アドレスを拒否します。

## 制約事項とガイドライン

ポートでは、VLAN 内の MAC アドレスの最大数を VLAN 内の既存の MAC アドレスの数より小さくすることはできません。指定された最大数より小さい場合、設定は有効になりません。

## 手順

1. システムビューを開始します。  
**System-view**
2. インターフェイスビューを開始します。  
**interface** *interface-type interface-number*
3. ポート上の特定のVLANのMACアドレス数に対するポートセキュリティの制限を設定します。  
**port-security mac-limit** *max-number per-vlan vlan-id-list*  
デフォルト設定は 2147483647 です。

# オープン認証モードの有効化

## オープン認証モードについて

この機能により、ポートのアクセスユーザー(802.1X または MAC 認証ユーザー)は、存在しないユーザー名や不正なパスワードを使用している場合でも、オンラインになり、ネットワークにアクセスできます。

オープン認証モードでオンラインになったアクセスユーザーは、オープンユーザーと呼ばれます。オープンユーザーは、承認およびアカウントリングを利用できません。オープンユーザーの情報を表示するには、次のコマンドを使用します。

- **display dot1x connection open**
- **display mac-authentication connection open**

この機能は、正しいユーザー情報を使用するユーザーのアクセスには影響しません。

## 制約事項とガイドライン

オープン認証モードを設定する場合は、次の制約事項および注意事項に従ってください。

- グローバルオープン認証モードがイネーブルの場合、ポート固有のオープン認証モード設定に関係なく、すべてのポートがオープン認証モードでイネーブルになります。グローバルオープン認証モードがディセーブルの場合、ポートがオープン認証モードでイネーブルになるかどうかは、ポート固有のオープン認証モード設定によって決まります。
- オープン認証モードの設定は、802.1X認証失敗VLANおよびMAC認証ゲストVLANよりも優先順位が低くなります。ポートが802.1X認証失敗VLANまたはMAC認証ゲストVLANでも設定されている場合、オープン認証モードはポートで有効になりません。

802.1X 認証および MAC 認証について詳しくは、「802.1X の概要」、「802.1X の設定」および「MAC 認証の設定」を参照してください。

- オープン認証モードの設定は、802.1X Auth-Fail VSIおよびMAC認証ゲストVSIよりも優先順位が低くなります。ポートが802.1X Auth-Fail VSIまたはMAC認証ゲストVSIでも設定されている場合、オープン認証モードはポートで有効になりません。

802.1X 認証および MAC 認証について詳しくは、「802.1X の概要」、「802.1X の設定」および「MAC 認証の設定」を参照してください。

## 手順

1. システムビューを開始します。  
**System-view**
2. グローバルオープン認証モードをイネーブルにします。  
**port-security authentication open global**

デフォルトでは、グローバルオープン認証モードはディセーブルです。

3. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

4. ポートでオープン認証モードをイネーブルにします。

**port-security authentication open**

デフォルトでは、ポートのオープン認証モードはディセーブルです。

## ポートセキュリティのためのフリーVLANの設定

### 空き VLAN の概要

この機能を使用すると、指定された VLAN からのパケットが、次のいずれかの機能で設定されたポートで 802.1X または MAC 認証をトリガーしないようにできます。

- 802.1X 認証。
- MAC 認証。
- 次のポートセキュリティモードのいずれか。
  - userLogin
  - userLoginSecure
  - userLoginWithOUI
  - userLoginSecureExt
  - macAddressWithRadius
  - macAddressOrUserLoginSecure
  - macAddressElseUserLoginSecure
  - macAddressOrUserLoginSecureExt
  - macAddressElseUserLoginSecureExt

### 手順

1. システムビューを開始します。

**System-view**

2. インターフェイスビューを開始します。

**interface** *interface-type interface-number*

3. ポートセキュリティ用にフリーVLANを設定します。

**port-security free-vlan** *vlan-id-list*

デフォルトでは、ポートセキュリティ用の空き VLAN はポート上に存在しません。

## ポートセキュリティへのNAS-IDプロファイルの適用

### NAS-ID プロファイルについて

デフォルトでは、デバイスはすべての RADIUS 要求の NAS-Identifier アトリビュートでデバイス名を送信します。

NAS-ID プロファイルを使用すると、異なる VLAN からの RADIUS 要求で異なる NAS-Identifier 属性文字列を送信できます。文字列は、管理要件に応じて、組織名、サービス名、または任意のユーザー分類基準になります。

たとえば、NAS-ID **companyA** を会社 A のすべての VLAN にマッピングします。デバイスは、RADIUS サーバーの NAS-Identifier アトリビュートで **companyA** を送信して、会社 A のユーザーからの要求を識別します。

## 制約事項とガイドライン

NAS-ID プロファイルは、グローバルまたはポート上のポートセキュリティに適用できます。ポート上では、デバイスは次の順序で NAS-ID プロファイルを選択します。

1. ポート固有のNAS-IDプロファイル。
2. グローバルに適用されるNAS-IDプロファイル。

NAS-ID プロファイルが適用されていない場合、または選択されたプロファイルで一致するバインディングが見つからない場合、デバイスはデバイス名を NAS-ID として使用します。

NAS-ID プロファイル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. システムビューを開始します。

### System-view

2. NAS-IDプロファイルを適用します。

- NAS-IDプロファイルをグローバルに適用します。

**port-security nas-id-profile profile-name**

- 次のコマンドを順番に実行して、NAS-IDプロファイルをインターフェースに適用します。

**interface interface-type interface-number**

**port-security nas-id-profile profile-name**

デフォルトでは、システムビューまたはインターフェイスビューに NAS-ID プロファイルは適用されません。

# エスケープクリティカルVSI機能の設定

## エスケープクリティカル VSI 機能について

この機能は、次の条件が存在する VXLAN ネットワークで使用します。

- デバイスは、802.1XまたはMAC認証ユーザーの認証および認可にリモートRADIUSサーバーを使用します。
- 802.1XまたはMAC認証ユーザーは、デバイスによって選択されたりリモートRADIUSサーバーが正しく機能しないため、認証または認可に失敗します。

エスケープクリティカル VSI 機能は、認可 URL が割り当てられたオンライン MAC 認証ユーザーをログオフします。

ユーザーの 802.1X または MAC 認証がポートでトリガーされると、エスケープクリティカル VSI 機能により、デバイスは次の操作を実行できます。

1. ユーザーのアクセスポート上のユーザーのアクセスVLANおよびMACアドレスと一致するイーサネットサービスインスタンスを動的に作成します。
2. イーサネットサービスインスタンスをポート上の802.1XまたはMAC認証クリティカルVSIにマッピングします。

ユーザーは、対応するクリティカル VSI に割り当てられます。ユーザーは、認証を実行せずにオンラインになり、クリティカル VSIに関連付けられた VXLAN 内のリソースにアクセスできます。

## 制約事項とガイドライン

エスケープクリティカル VSI 機能は、この機能をイネーブルにする前にすでにオンラインになっていた 802.1X または MAC 認証ユーザーには影響しません。

エスケープクリティカル VSI 機能がポートで正常に機能するためには、ポートに次の設定がないことを確認します。

- Web認証。
- 802.1XゲストVLAN、802.1X認証失敗VLAN、および802.1XクリティカルVLAN。
- MAC認証ゲストVLANおよびMAC認証クリティカルVLAN。

エスケープクリティカル VSI 機能は、次のいずれかの条件が存在する場合、新しい 802.1X または MAC 認証ユーザーでは有効になりません。

- 802.1Xクライアントとデバイスでは、EAPメッセージの処理方法が異なります。
- 802.1X MACアドレスバインディングはユーザーのアクセスポートでイネーブルになっていますが、802.1XユーザーのMACアドレスはポートにバインドされていません。
- ユーザーのMACアドレスは、すべてゼロ、すべてF、またはマルチキャストMACアドレスです。

この機能は、グローバルにイネーブルにすることも、ポート上でイネーブルにすることもできます。グローバルなエスケープクリティカル VSI 機能はすべてのポートで有効になり、ポート固有のエスケープクリティカル VSI 機能は指定されたポートでのみ有効になります。

エスケープクリティカル VSI をグローバルにもポート上でもディセーブルにすると、デバイスはポート上の 802.1X クリティカル VSI および MAC 認証クリティカル VSI のユーザーをログオフします。ユーザーがポート上で再びオンラインになるには、認証を実行する必要があります。

## 前提条件

エスケープクリティカル VSI 機能をイネーブルにする前に、各 802.1X または MAC 認証ユーザーのアクセスポートに 802.1X クリティカル VSI および MAC 認証 VSI を設定します。

## 手順

1. システムビューを開始します。

### System-view

2. エスケープクリティカルVSI機能をイネーブルにします。

- グローバルエスケープクリティカルVSI機能をイネーブルにします。

#### **port-security global escape critical-vsi**

- 次のコマンドを順番に実行して、ポート上でエスケープクリティカルVSI機能をイネーブルにします。

**interface** *interface-type interface-number*

#### **port-security escape critical-vsi**

デフォルトでは、エスケープクリティカル VSI 機能はディセーブルです。

# ポートセキュリティのSNMP通知のイネーブル化

## ポートセキュリティの SNMP 通知について

この機能を使用して、重要なポートセキュリティイベントを NMS に報告します。ポートセキュリティイベント通知を正しく送信するには、デバイスで SNMP も設定する必要があります。SNMP 設定の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

### 手順

1. システムビューを開始します。

#### System-view

2. ポートセキュリティのSNMP通知をイネーブルにします。

```
snmp-agent trap enable port-security [ address-learned | dot1x-failure | dot1x-logoff | dot1x-logon | intrusion | mac-auth-failure | mac-auth-logoff | mac-auth-logon ] *
```

デフォルトでは、ポートセキュリティの SNMP 通知はディセーブルになっています。

# ポートセキュリティユーザーのロギングのイネーブル化

## ポートセキュリティユーザーのロギングについて

この機能を使用すると、デバイスでポートセキュリティユーザーのログを生成し、そのログを Information Center に送信できます。ログを正しく出力するには、デバイスに Information Center も設定する必要があります。Information Center の設定の詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

### 制約事項とガイドライン

ポートセキュリティユーザーの過剰なログ出力を防ぐために、この機能をディセーブルにすることを推奨します。

### 手順

1. システムビューを開始します。

#### System-view

2. ポートセキュリティユーザーのロギングをイネーブルにします。

```
port-security access-user log enable [ failed-authorization | mac-learning | violation ] *
```

デフォルトでは、ポートセキュリティユーザーのすべてのタイプのロギングがディセーブルになっています。

パラメーターを指定しない場合、このコマンドはポートセキュリティユーザーのすべてのタイプのロギングをイネーブルにします。



# ポートセキュリティの表示およびメンテナンスコマンド

任意のビューで **display** コマンドを実行します。

タスク	コマンド
ポートセキュリティ設定、動作情報、および統計情報を表示します。	<b>display port-security</b> [ interface <i>interface-type interface-number</i> ]
ブロックされたMACアドレスに関する情報を表示します。	<b>display port-security mac-address block</b> [ interface <i>interface-type interface-number</i> ] [ vlan <i>vlan-id</i> ] [ count ]
セキュアMACアドレスに関する情報を表示します。	<b>display port-security mac-address security</b> [ interface <i>interface-type interface-number</i> ] [ vlan <i>vlan-id</i> ] [ count ]

## ポートセキュリティの設定例

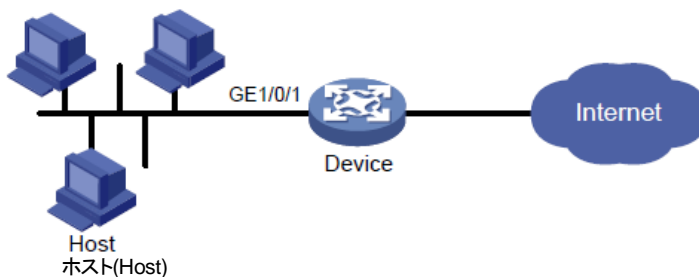
### 例:autoLearn モードでのポートセキュリティの設定

#### ネットワーク構成

図 1 に示すように、次の要件を満たすように、デバイスに GigabitEthernet 1/0/1 を設定します。

- 認証なしで最大64人のユーザーを受け入れます。
- MACアドレスを学習し、スティックMACアドレスとして追加することを許可し、セキュアMACエージングタイマーを30分に設定します。
- セキュアMACアドレスの数が64に達したら、MACアドレスの学習を停止します。未知のMACアドレスを持つフレームが到着すると、侵入保護が開始され、ポートはシャットダウンし、30秒間サイレント状態になります。

図 1 ネットワークダイアグラム



#### 手順

#ポートセキュリティを有効にします。

```
<Device> system-view
```

```
[Device] port-security enable
```

#セキュア MAC エージングタイマーを 30 分に設定します。

```
[Device] port-security timer autolearn aging 30
```

#ポートセキュリティのセキュア MAC アドレス数の制限を、GigabitEthernet 1/0/1 で 64 に設定します。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

#ポートセキュリティモードを autoLearn に設定します。

```
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
```

#Intrusion Protection Feature がトリガーされてから 30 秒間、ポートをサイレントに設定します。

```
[Device-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

```
[Device-GigabitEthernet1/0/1] quit
```

```
[Device] port-security timer disableport 30
```

## 設定の確認

#ポートセキュリティの設定を確認します。

```
[Device] display port-security interface gigabitethernet 1/0/1
```

Global port security parameters:

Port security : Enabled

AutoLearn aging time : 30 min

Disableport timeout : 30 s

MAC move : Denied

Authorization fail : Online

NAS-ID profile : Not configured

Dot1x-failure trap : Disabled

Dot1x-logon trap : Disabled

Dot1x-logoff trap : Disabled

Intrusion trap : Disabled

Address-learned trap : Disabled

Mac-auth-failure trap : Disabled

Mac-auth-logon trap : Disabled

Mac-auth-logoff trap : Disabled

Open authentication : Disabled

OUI value list :

Index : 1 Value : 123401

GigabitEthernet1/0/1 is link-up

Port mode : autoLearn

NeedToKnow mode : Disabled

Intrusion protection mode : DisablePortTemporarily

Security MAC address attribute

Learning mode : Sticky

Aging type : Periodical

Max secure MAC addresses : 64

```
Current secure MAC addresses    : 0
Authorization                   : Permitted
NAS-ID profile                  : Not configured
Free VLANs                     : Not configured
Open authentication            : Disabled
```

このポートではMACアドレスの学習が可能であり、学習されたMACアドレスの数を[Current secure MAC addresses]フィールドに表示できます。

#学習された MAC アドレスに関する追加情報を表示します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] display this
#
interface GigabitEthernet1/0/1
port-security max-mac-count 64
port-security port-mode autolearn
port-security mac-address security sticky 0002-0000-0015 vlan 1
port-security mac-address security sticky 0002-0000-0014 vlan 1
port-security mac-address security sticky 0002-0000-0013 vlan 1
port-security mac-address security sticky 0002-0000-0012 vlan 1
284
port-security mac-address security sticky 0002-0000-0011 vlan 1
#
[Device-GigabitEthernet1/0/1] quit
```

#ポートによって学習された MAC アドレスの数が 64 に達した後、ポートセキュリティモードがセキュアに変更されることを確認します。

```
[Device]display port-security interface gigabitethernet 1/0/1
```

#未知の MAC アドレスを持つフレームを受信した後、ポートが 30 秒間無効になることを確認します (詳細は省略)。

#ポートが再度有効になったら、いくつかのセキュア MAC アドレスを削除します。

```
[Device] undo port-security mac-address security sticky 0002-0000-0015 vlan 1
```

```
[Device] undo port-security mac-address security sticky 0002-0000-0014 vlan 1
```

...

#ポートのポートセキュリティモードが autoLearn に変更され、ポートが MAC アドレスを再度学習できることを確認します(詳細は省略)。

# 例:userLoginWithOUI モードでのポートセキュリティの設定

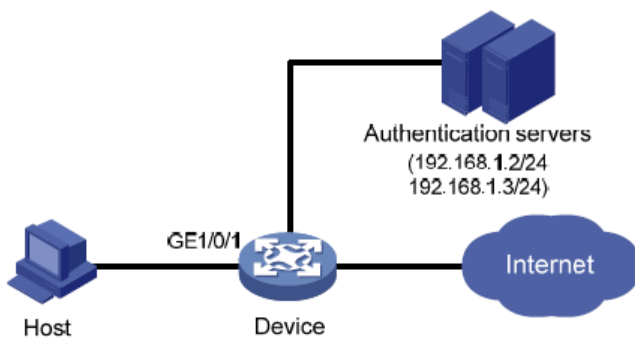
## ネットワーク構成

図 2 に示すように、クライアントは GigabitEthernet 1/0/1 を介してデバイスに接続されています。デバイスは、ISP ドメイン sun の RADIUS サーバーを使用してクライアントを認証します。認証が成功すると、クライアントはインターネットへのアクセスを許可されます。

- 192.168.1.2のRADIUSサーバーは、プライマリ認証サーバーおよびセカンダリアカuntingサーバーとして機能します。192.168.1.3のRADIUSサーバーは、セカンダリ認証サーバーおよびプライマリアカuntingサーバーとして機能します。認証用の共有キーはnameで、アカunting用の共有キーはmoneyです。
- すべてのユーザーは、ISPドメインsunの認証、認可、およびアカunting方式を使用します。
- RADIUSサーバーの応答タイムアウト時間は5秒です。RADIUSパケット再送信の最大試行回数は5です。デバイスは、リアルタイムアカuntingパケットを15分間隔でRADIUSサーバーに送信し、ドメイン名を含まないユーザー名をRADIUSサーバーに送信します。

1 人の 802.1X ユーザーと、指定された OUI 値のいずれかを使用するユーザーだけが認証されるように、GigabitEthernet 1/0/1 を設定します。

図2 ネットワークダイアグラム



## 手順

次の設定手順では、一部の AAA/RADIUS コンフィギュレーションコマンドについて説明します。コマンドの詳細については、『Security Command Reference』を参照してください。

ホストと RADIUS サーバーが相互に到達できることを確認します。

1. AAAを設定します。

#radsun という名前の RADIUS スキームを設定します。

```
<Device> system-view
```

```
[Device] radius scheme radsun
```

```
[Device-radius-radsun] primary authentication 192.168.1.2
```

```
[Device-radius-radsun] primary accounting 192.168.1.3
```

```
[Device-radius-radsun] secondary authentication 192.168.1.3
```

```
[Device-radius-radsun] secondary accounting 192.168.1.2
```

```
[Device-radius-radsun] key authentication simple name
```

```
[Device-radius-radsun] key accounting simple money
```

```
[Device-radius-radsun] timer response-timeout 5
```

```
[Device-radius-radsun] retry 5
```

```
[Device-radius-radsun] timer realtime-accounting 15
```

```
[Device-radius-radsun] user-name-format without-domain
[Device-radius-radsun] quit
#ISPドメイン sun を設定します。
[Device] domain sun

[Device-isp-sun] authentication lan-access radius-scheme radsun
[Device-isp-sun] authorization lan-access radius-scheme radsun
[Device-isp-sun] accounting lan-access radius-scheme radsun
[Device-isp-sun] quit
```

2. 802.1Xの設定:

#802.1X 認証方式を CHAP に設定します。デフォルトでは、802.1X の認証方式は CHAP です。

```
[Device] dot1x authentication-method chap
#ISPドメイン sun を、GigabitEthernet 1/0/1 上の 802.1X ユーザーの必須認証ドメインとして指定します。
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] dot1x mandatory-domain sun
[Device-GigabitEthernet1/0/1] quit
```

3. ポートセキュリティを設定します。#ポートセキュリティを有効にします。

```
[Device] port-security enable
#5 つの OUI 値を追加します。(最大 16 の OUI 値を追加できます。ポートでは、いずれかの OUI に一致する 1 人のユーザーだけが認証を通過できます。)
[Device] port-security oui index 1 mac-address 1234-0100-1111
[Device] port-security oui index 2 mac-address 1234-0200-1111
[Device] port-security oui index 3 mac-address 1234-0300-1111
[Device] port-security oui index 4 mac-address 1234-0400-1111
[Device] port-security oui index 5 mac-address 1234-0500-1111
#ポートセキュリティモードを userLoginWithOUI に設定します。
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] port-security port-mode userlogin-withoui
[Device-GigabitEthernet1/0/1] quit
```

### 設定の確認

#GigabitEthernet 1/0/1 で認証できる 802.1X ユーザーが 1 人だけであることを確認します。

```
[Device] display port-security interface gigabitethernet 1/0/1
```

Global port security parameters:

Port security : Enabled

AutoLearn aging time : 30 min

```

Disableport timeout      : 30 s
MAC move                 : Denied
Authorization fail       : Online
NAS-ID profile           : Not configured
Dot1x-failure trap      : Disabled
Dot1x-logon trap        : Disabled
Dot1x-logoff trap       : Disabled
Intrusion trap          : Disabled
Address-learned trap    : Disabled
Mac-auth-failure trap   : Disabled
Mac-auth-logon trap     : Disabled
Mac-auth-logoff trap    : Disabled
Open authentication     : Disabled
OUI value list :
Index : 1                Value : 123401
Index : 2                Value : 123402
Index : 3                Value : 123403
Index : 4                Value : 123404
Index : 5                Value : 123405
GigabitEthernet1/0/1 is link-up
Port mode                : userLoginWithOUI
NeedToKnow mode         : Disabled
Intrusion protection mode : NoAction
Security MAC address attribute
Learning mode           : Sticky
Aging type              : Periodical
Max secure MAC addresses : Not configured
Current secure MAC addresses : 1
Authorization           : Permitted
NAS-ID profile          : Not configured
Free VLANs              : Not configured
Open authentication     : Disabled

```

# オンラインの 802.1X ユーザーに関する情報を表示して、802.1X 構成を確認します。

```
[Device] display dot1x
```

# ポートが、指定された OUI の中で OUI を持つ MAC アドレスを持つ 1 人のユーザーも認証を通過できることを確認します。

```
[Device] display mac-address interface gigabitethernet 1/0/1
```

MAC Address	VLAN ID	State	Port/NickName	Aging
1234-0300-0011	1		Learned	GE1/0/1 Y

## 例:macAddressElseUserLoginSecure モードでのポートセキュリティの設定

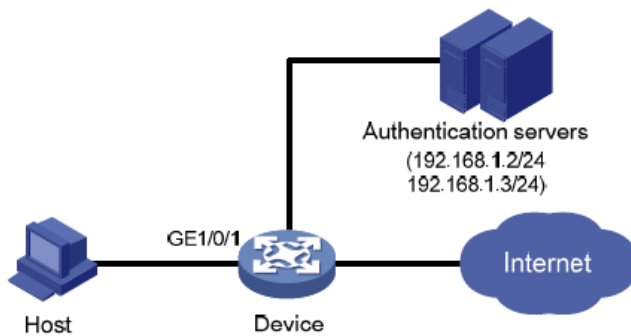
### ネットワーク構成

図 3 に示すように、クライアントは GigabitEthernet 1/0/1 を介してデバイスに接続されています。デバイスは、ISP ドメイン sun の RADIUS サーバーによってクライアントを認証します。認証が成功すると、クライアントはインターネットへのアクセスを許可されます。

次の要件を満たすように、デバイスの GigabitEthernet 1/0/1 を設定します。

- 複数の MAC 認証ユーザーがログオンできるようにします。
- 802.1X ユーザーの場合は、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。ログオンできる 802.1X ユーザーは 1 人だけです。
- 認証用のユーザー名およびパスワードとして、各ユーザーの MAC アドレスを使用します。MAC アドレスは、ハイフン付きの 16 進表記で、文字は大文字です。
- MAC 認証ユーザーと 802.1X 認証ユーザーの合計数を 64 に設定します。
- NTK(ntkonly モード)をイネーブルにして、不明な MAC アドレスにフレームが送信されないようにします。

図3 ネットワークダイアグラム



## 手順

ホストと RADIUS サーバーが相互に到達できることを確認します。

1. RADIUS認証/アカウンティングおよびISPドメイン設定を設定します (「例:userLoginWithOUIモードでのポートセキュリティの設定」を参照)。
2. ポートセキュリティを設定します。

#ポートセキュリティを有効にします。

```
<Device> system-view
```

```
[Device] port-security enable
```

#MAC 認証に MAC ベースのアカウントを使用します。各 MAC アドレスは、ハイフンを含む 16 進表記で指定する必要があります。文字は大文字で指定します。

```
[Device] mac-authentication user-name-format mac-address with-hyphen uppercase
```

#MAC 認証ドメインを指定します。

```
[Device] mac-authentication domain sun
```

#802.1X 認証方式を CHAP に設定します。デフォルトでは、802.1X の認証方式は CHAP です。

```
[Device] dot1x authentication-method chap
```

#ポートセキュリティの MAC アドレス数の制限を、ポート上で 64 に設定します。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64
```

#ポートセキュリティモードを macAddressElseUserLoginSecure に設定します。

```
[Device-GigabitEthernet1/0/1] port-security port-mode mac-else-userlogin-secure
```

#ISPドメイン sun を 802.1X ユーザーの必須認証ドメインとして指定します。

```
[Device-GigabitEthernet1/0/1]dot1x mandatory-domain sun
```

#ポートの NTK モードを ntkonly に設定します。

```
[Device-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

```
[Device-GigabitEthernet1/0/1] quit
```

## 設定の確認

#ポートセキュリティの設定を確認します。



[Device] display port-security interface gigabitethernet 1/0/1

Global port security parameters:

Port security : Enabled  
AutoLearn aging time : 30 min  
Disableport timeout : 30 s  
MAC move : Denied  
Authorization fail : Online  
NAS-ID profile : Not configured  
Dot1x-failure trap : Disabled  
Dot1x-logon trap : Disabled  
Dot1x-logoff trap : Disabled  
Intrusion trap : Disabled  
Address-learned trap : Disabled  
Mac-auth-failure trap : Disabled  
Mac-auth-logon trap : Disabled  
Mac-auth-logoff trap : Disabled  
Open authentication : Disabled

OUI value list

GigabitEthernet1/0/1 is link-up

Port mode : macAddressElseUserLoginSecure  
NeedToKnow mode : NeedToKnowOnly  
Intrusion protection mode : NoAction  
Security MAC address attribute  
Learning mode : Sticky  
Aging type : Periodical  
Max secure MAC addresses : 64  
Current secure MAC addresses : 0  
Authorization : Permitted  
NAS-ID profile : Not configured  
Free VLANs : Not configured  
Open authentication : Disabled

#ユーザーが認証に合格した後、MAC 認証情報を表示します。GigabitEthernet 1/0/1 で複数の MAC 認証ユーザーを認証できることを確認します。

[Device] display mac-authentication interface gigabitethernet 1/0/1

Global MAC authentication parameters:

MAC authentication : Enabled  
User name format : MAC address in uppercase(XX-XX-XX-XX-XX-XX)  
Username : mac  
Password : Not configured  
Offline detect period : 300 s  
Quiet period : 180 s  
Server timeout : 100 s

```

Reauth period          : 3600 s
Authentication domain  : sun
Online MAC-auth users  : 3
Silent MAC users:
MAC address VLAN ID From port Port index
GigabitEthernet1/0/1 is link-up
MAC authentication     : Enabled
Carry User-IP         : Disabled
Authentication domain  : Not configured
Auth-delay timer      : Disabled
Periodic reauth       : Disabled
Re-auth server-unreachable : Logoff
Guest VLAN            : Not configured
Guest VLAN auth-period : 30 s
Critical VLAN         : Not configured
Critical voice VLAN   : Disabled
Host mode             : Single VLAN
Offline detection     : Enabled
Authentication order  : Default
Guest VSI            : Not configured
Guest VSI auth-period : 30 s
Critical VSI         : Not configured
Max online users     : 4294967295
Authentication attempts : successful 3, failed 7
Current online users  : 3
    MAC address      Auth state
    1234-0300-0011   Authenticated
    1234-0300-0012   Authenticated
    1234-0300-0013   Authenticated

```

#802.1X 認証情報を表示します。GigabitEthernet 1/0/1 で認証できる 802.1X ユーザーが 1 人だけであることを確認します。

```
[Device] display dot1x interface
```

```
gigabitethernet 1/0/1
```

```
Global 802.1X parameters:
```

```

802.1X authentication      : Enabled
CHAP authentication       : Enabled
Max-tx period             : 30 s
Handshake period          : 15 s
Quiet timer               : Disabled
Quiet period              : 60 s
Supp timeout              : 30 s

```

Server timeout : 100 s  
 Reauth period : 3600 s  
 Max auth requests : 2  
 EAD assistant function : Disabled  
 EAD timeout : 30 min  
 Domain delimiter : @  
 Online 802.1X users : 1  
 GigabitEthernet1/0/1 is link-up  
 802.1X authentication : Enabled  
 Handshake : Enabled  
 Handshake reply : Disabled  
 Handshake security : Disabled  
 Unicast trigger : Disabled  
 Periodic reauth : Disabled  
 Port role : Authenticator  
 Authorization mode : Auto  
 Port access control : MAC-based  
 Multicast trigger : Enabled  
 Mandatory auth domain : sun  
 Guest VLAN : Not configured  
 Auth-Fail VLAN : Not configured  
 Critical VLAN : Not configured  
 Critical voice VLAN : Disabled  
 Add Guest VLAN delay : Disabled  
 Re-auth server-unreachable : Logoff  
 Max online users : 4294967295  
 User IP freezing : Disabled  
 Reauth period : 60 s  
 Send Packets Without Tag : Disabled  
 Max Attempts Fail Number : 0  
 Auth-Fail VSI : Not configured  
 Critical VSI : Not configured  
 Add Guest VSI delay : Disabled  
 EAPOL packets : Tx 16331, Rx 102  
 Sent EAP Request/Identity packets : 16316  
 EAP Request/Challenge packets: 6  
 EAP Success packets : 4  
 EAP Failure packets : 5

Received EAPOL Start packets : 6  
EAPOL LogOff packets : 2  
EAP Response/Identity packets : 80  
EAP Response/Challenge packets: 6  
Error packets: 0  
Online 802.1X users : 1  
MAC address Auth state  
0002-0000-0011 Authenticated

#不明な宛先 MAC アドレス、マルチキャストアドレス、またはブロードキャストアドレスを持つフレームが廃棄されることを確認します(詳細は省略)。

## ポートセキュリティのトラブルシューティング

### ポートセキュリティモードを設定できません

#### 症状

ポートのポートセキュリティモードを設定できません。

#### 解析

noRestrictions 以外のポートセキュリティモードで動作しているポートの場合、port-security port-mode コマンドを使用してポートセキュリティモードを変更できません。

#### 解決策

この問題を解決するには、次の手順に従います

1. ポートセキュリティモードをnoRestrictionsに設定します。  
[Device-GigabitEthernet1/0/1] undo port-security port-mode
2. ポートに新しいポートセキュリティモード(autoLearnなど)を設定します。  
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn
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。

### セキュア MAC アドレスを設定できません。

#### 症状

セキュア MAC アドレスを設定できません。

#### 解析

autoLearn 以外のポートセキュリティモードで動作するポートには、セキュア MAC アドレスを設定できません。

#### 解決策

この問題を解決するには、次の手順に従います

1. ポートセキュリティモードをautoLearnに設定します。

```
[Device-GigabitEthernet1/0/1] undo port-security port-mode  
[Device-GigabitEthernet1/0/1] port-security max-mac-count 64  
[Device-GigabitEthernet1/0/1] port-security port-mode autolearn  
[Device-GigabitEthernet1/0/1] port-security mac-address security 1-1-2 vlan 1
```

2. 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。

# 攻撃の検出と防御の設定

## 概要

攻撃の検出と防止により、デバイスは着信パケットを検査することで攻撃を検出し、プライベートネットワークを保護するための防止アクション(パケットドロップなど)を実行できます。

## デバイスが防止できる攻撃

この項では、デバイスが検出および防止できる攻撃について説明します。

### TCP フラグメント攻撃

攻撃者は、RFC 1858 で定義されている攻撃 TCP フラグメントを送信することによって、TCP フラグメント攻撃を開始します。

- TCP ヘッダーが 20 バイトより小さい最初のフラグメント。
- フラグメントオフセットが 8 バイト(FO=1)の先頭以外のフラグメント。

通常、パケットフィルタは、TCP パケットの最初のフラグメントの送信元 IP アドレスと宛先 IP アドレス、送信元ポートと宛先ポート、およびトランスポート層プロトコルを検出します。最初のフラグメントが検出に合格すると、TCP パケットの後続のすべてのフラグメントの通過が許可されます。

攻撃 TCP パケットの最初のフラグメントは、パケットフィルタ内のどの一致にもヒットしないため、後続のフラグメントはすべて通過できます。受信ホストがフラグメントを再構成した後、TCP フラグメント攻撃が発生します。

TCP フラグメント攻撃を防止するには、TCP フラグメント攻撃防止をイネーブルにして、攻撃 TCP フラグメントをドロップします。

### ログイン辞書攻撃

ログインディクショナリ攻撃は、事前に用意された値のリスト(ディクショナリ)から可能なすべてのパスワードを試行してログインを試行する自動プロセスです。短時間に複数回のログイン試行が発生する可能性があります。

ログイン遅延機能を設定して、ログインディクショナリ攻撃を遅らせることができます。この機能を使用すると、デバイスは、ユーザーの失敗したログイン試行を検出した後、別のログイン要求の受け入れを遅延できます。

## TCPフラグメント攻撃防止の設定

TCP フラグメント攻撃防止機能は、受信した TCP フラグメントの長さおよびフラグメントオフセットを検出し、攻撃 TCP フラグメントをドロップします。デバイスは、CPU を介して転送された TCP フラグメントの検証だけをサポートします。

TCP フラグメント攻撃防止を設定するには、次の手順を実行します。

ステップ	コマンド	備考
3. システムビューに入ります。	<code>system-view</code>	該当なし

ステップ	コマンド	備考
4. TCPフラグメント攻撃防止をイネーブルにします。	<b>attack-defense tcp fragment enable</b>	デフォルトでは、TCPフラグメント攻撃防止はイネーブルになっています。

## ログイン遅延の有効化

ログイン遅延機能は、ユーザーがログイン試行に失敗した後、デバイスがユーザーからのログイン要求を受け入れるのを遅延させます。この機能は、ログインディクショナリ攻撃を遅らせることができます。

ログイン遅延をイネーブルにするには、次の手順を実行します

ステップ	コマンド	備考
1. システムビューに入ります。	<b>system-view</b>	該当なし
2. ログイン遅延機能をイネーブルにします。	<b>attack-defense login reauthentication-delay</b> <i>seconds</i>	デフォルトでは、ログイン遅延機能はディセーブルになっています。デバイスは、ログイン試行に失敗したユーザーからのログイン要求の受け入れを遅延させません。

# TCP 攻撃防止の設定

## TCP攻撃防止について

TCP 攻撃防止では、TCP 接続確立プロセスを不正利用する攻撃を検出して防止できます。

## Naptha攻撃防止の設定

### Naptha 攻撃防止について

Naptha は、オペレーティングシステムを標的とした DDoS 攻撃である。TCP/IP スタックやネットワークアプリケーションプロセスのリソース消費の脆弱性を悪用する。攻撃者は、短時間に多数の TCP 接続を確立し、データを要求せずに特定の状態のままにする。これらの TCP 接続は、被害者のシステムリソースを枯渇させ、システム障害を引き起こす。

Naptha 攻撃防止を有効にすると、デバイスは各状態(CLOSING、ESTABLISHED、FIN\_WAIT\_1、FIN\_WAIT\_2、および LAST\_ACK)の TCP 接続の数を定期的にチェックします。状態の TCP 接続の数が制限を超えると、デバイスはその状態の TCP 接続のエイジングを加速して、Naptha 攻撃を軽減します。

### 手順

1. システムビューに入ります。

```
system-view
```

2. Naptha 攻撃防止をイネーブルにします。

```
tcp anti-naptha enable
```

デフォルトでは、Naptha 攻撃防止はディセーブルになっています。

3. (任意)ステート内の TCP 接続の最大数を設定します。

```
tcp state { closing | established | fin-wait-1 | fin-wait-2 |  
last-ack } connection-limit number
```

デフォルトでは、各状態(CLOSING、ESTABLISHED、FIN\_WAIT\_1、FIN\_WAIT\_2、および LAST\_ACK)の TCP 接続の最大数は 50 です。

デバイスがある状態の TCP 接続のエイジングを加速しないようにするには、値を 0 に設定します。

4. (任意)各ステートの TCP 接続数をチェックする間隔を設定します。

```
tcp check-state interval interval
```

デフォルトでは、各状態の TCP 接続数をチェックする間隔は 30 秒です。



# IP ソースガードの設定

## IPSGについて

IP Source Guard (IPSG) は、IPSG バインディングテーブルを使用して不正なパケットをフィルタリングすることで、スプーフィング攻撃を防止します。この機能は通常、ユーザー側のインターフェイスで設定されます。

## IPSG 動作メカニズム

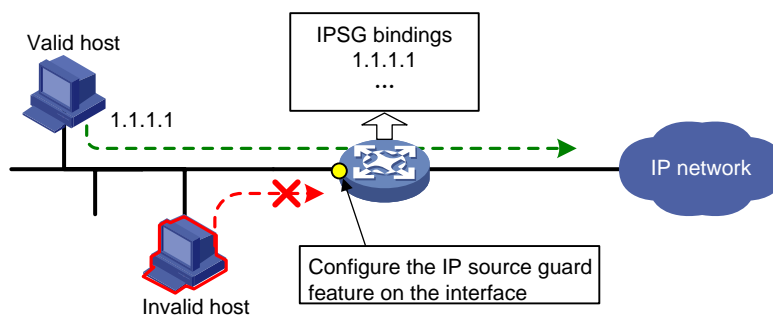
IPSG バインディングテーブルには、IP アドレス、MAC アドレス、VLAN、または任意の組み合わせをバインドするバインディングが含まれています。IPSG はバインディングを使用して着信パケットを照合します。一致が見つかった場合、パケットは転送されます。一致が見つからなかった場合、パケットは廃棄されます。

IPSG は、インターフェイス単位のパケットフィルタです。あるインターフェイスでこの機能を設定しても、別のインターフェイスでのパケット転送には影響しません。

IPSG バインディングには、スタティックバインディングとダイナミックバインディングがあります。

図 1 に示すように、IPSG は IPSG バインディングと一致するパケットだけを転送します。

図 1 IPSG アプリケーション



## スタティック IPSG バインディング

スタティック IPSG バインディングは、手動で設定します。LAN 上に存在するホストが少なく、その IP アドレスが手動で設定されているシナリオに適しています。たとえば、サーバーに接続するインターフェイスにスタティック IPSG バインディングを設定できます。このバインディングにより、インターフェイスはサーバーからのパケットだけを受信できます。

インターフェイスのスタティック IPSG バインディングには、次の機能が実装されています。

- インターフェイス上の着信 IPv4 または IPv6 パケットをフィルタリングします。
- IPv4 の ARP 攻撃検出と連携して、ユーザーの有効性をチェックします。ARP 攻撃検出の詳細については、「ARP 攻撃保護の設定」を参照してください。
- IPv6 の ND 攻撃検出と連携して、ユーザーの有効性をチェックします。ND 攻撃検出の詳細については、「ND 攻撃防御の構成」を参照してください。

スタティック IPSG バインディングは、グローバルまたはインターフェイス固有にすることができます。

- グローバルスタティックバインディングシステムビューで IP アドレスと MAC アドレスをバインドします。バインディングはすべてのインターフェイスで有効になり、ユーザースプーフィング攻撃を防止するためにパケットをフィルタリングします。

- インターフェイス固有のスタティックバインディング IP アドレス、MAC アドレス、VLAN、またはインターフェイスビュー内の項目の任意の組み合わせをバインドします。バインディングは、インターフェイスにアクセスしようとしているユーザーの有効性をチェックするために、インターフェイス上でのみ有効になります。

## ダイナミック IPSG バインディング

IPSG は、他のモジュールからユーザー情報を自動的に取得して、ダイナミックバインディングを生成します。ダイナミック IPSG バインディングには、MAC アドレス、IPv4 または IPv6 アドレス、VLAN タグ、入力インターフェイス、およびバインディングタイプを含めることができます。バインディングタイプは、DHCP スヌーピング、DHCPv6 スヌーピング、DHCP リレーエージェント、DHCPv6 リレーエージェントなど、バインディングの送信元モジュールを識別します。

たとえば、DHCP ベースの IPSG バインディングは、LAN 上のホストが DHCP を介して IP アドレスを取得するシナリオに適しています。IPSG は、DHCP サーバー、DHCP スヌーピングデバイス、または DHCP リレーエージェントで設定されます。IPSG は、DHCP サーバー上のクライアントバインディング、DHCP スヌーピングエントリ、または DHCP リレーエントリに基づいて、ダイナミックバインディングを生成します。IPSG は、DHCP クライアントからのパケットだけを通過させます。

### ダイナミック IPv4SG

さまざまなソースモジュールに基づいて生成された動的バインディングは、さまざまな用途に使用されます。

インターフェイスの種類	ソースモジュール	バインドの使用方法
レイヤ2イーサネットインターフェイス	DHCPスヌーピング 802.1X	パケットフィルタリング。
	ARPスヌーピング	セキュリティサービスを提供するためのモジュール(ARP攻撃検出モジュールなど)との連携。
レイヤ3イーサネットインターフェイス VLANインターフェイス	DHCPリレーエージェント ARPフラッド抑制	パケットフィルタリング。
	DHCPサーバー	セキュリティサービスを提供するためのモジュール(認可されたARPモジュールなど)との連携。

802.1X の詳細については、「802.1X の設定」を参照してください。ARP フラッド抑制の詳細については、『VXLAN Configuration Guide』を参照してください。ARP スヌーピング、DHCP スヌーピング、DHCP リレー、および DHCP サーバーの詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。

### ダイナミック IPv6SG

次のソースモジュールに基づいて生成されたダイナミック IPv6SG バインディングは、パケットフィルタリング用です。

インターフェイスの種類	ソースモジュール
レイヤ2イーサネットインターフェイス	DHCPv6スヌーピング NDスヌーピング 802.1X
レイヤ3イーサネットインターフェイス/VLANインターフェイス	DHCPv6リレーエージェント ND抑制

DHCPv6 スヌーピングの詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。ND スヌーピングの詳細については、『Layer 3 IP Services Configuration Guide』の「IPv6 basics configuration」を参照してください。DHCPv6 リレーエージェントの詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。

## IPSGタスクの概要

IPv4SGを設定するには、次の作業を実行します。

1. インターフェイスでの IPv4SG のイネーブル化
2. (任意)インターフェイスでの IPv4SG のイネーブル化
3. (任意)IPSG フィルタリングからの IPv4 パケットの除外

IPv6SGを設定するには、次の作業を実行します。

4. インターフェイスでの IPv6SG のイネーブル化
5. (オプション)スタティック IPv6SG バインディングの設定

## IPv4SG機能の設定

### インターフェイスでの IPv4SG のイネーブル化

#### インターフェイス上の IPv4SG 機能について

インターフェイスで IPSG をイネーブルにすると、スタティック IPSG とダイナミック IPSG の両方がイネーブルになります。

- スタティック IPv4SG は、ip source binding コマンドを使用して設定されたスタティックバインディングを使用します。詳細については、「スタティック IPv4SG バインディングの設定」を参照してください。
- ダイナミック IPv4SG は、関連するソースモジュールからダイナミックバインディングを生成します。IPv4SG は、バインディングを使用して、ip verify source コマンドで指定された一致基準に基づいて着信 IPv4 パケットをフィルタリングします。

#### 制限事項およびガイドライン

ダイナミック IPv4SG を実装するには、802.1X、ARP スヌーピング、DHCP スヌーピング、DHCP リレーエージェント、または DHCP サーバーがネットワーク上で正常に動作していることを確認します。

#### 手順

1. システムビューに入ります。  
**system-view**
2. インターフェイスビューを入力します。  
**interface interface-type interface-number**  
次のインターフェイスタイプがサポートされています。
  - レイヤ 2 イーサネットインターフェイス。
  - レイヤ 3 イーサネットインターフェイス。
  - VLAN インターフェイス。
3. IPv4SG 機能をイネーブルにします。  
**ip verify source { ip-address | ip-address mac-address | mac-address }**  
デフォルトでは、IPv4SG 機能はインターフェイスでディセーブルになっています。

# 静的 IPv4SG バインディングの設定

## 静的 IPv4SG バインディングについて

グローバルなスタティックおよびインターフェイス固有のスタティック IPv4SG バインディングを設定できます。インターフェイス固有のスタティックおよびダイナミックバインディングは、グローバルなスタティックバインディングよりも優先されます。インターフェイスは、最初にインターフェイス上のスタティックおよびダイナミックバインディングを使用してパケットを照合します。一致が見つからない場合、インターフェイスはグローバルバインディングを使用します。

## 制限事項およびガイドライン

グローバルスタティックバインディングは、デバイス上のすべてのインターフェイスで有効になります。

ARP 攻撃検出機能のスタティック IPv4SG バインディングを設定するには、次の条件が満たされていることを確認します。

- **ip-address** *ip-address* オプション、**mac-address** *mac-address* オプション、および **vlan** *vlan-id* オプションを指定する必要があります。
- 指定した VLAN に対して ARP 攻撃検出をイネーブルにする必要があります。

## グローバルスタティック IPv4SG バインディングの設定

1. システムビューに入ります。

```
system-view
```

2. グローバルスタティック IPv4SG バインディングを設定します。

```
ip source binding ip-address ip-address mac-address mac-address
```

## インターフェイスでのスタティック IPv4SG バインディングの設定

1. システムビューに入ります。

```
system-view
```

2. インターフェイスビューを入力します。

```
interface interface-type interface-number
```

次のインターフェイスタイプがサポートされています。

- レイヤ 2 イーサネットインターフェイス。
- レイヤ 3 イーサネットインターフェイス。
- VLAN インターフェイス。

3. スタティック IPv4SG バインディングを設定します。

```
ip source binding { ip-address ip-address | ip-address ip-address mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
```

異なるインターフェイスに同じスタティック IPv4SG バインディングを設定できます。

# IPSG フィルタリングからの IPv4 パケットの除外

## IPSG フィルタリングからの IPv4 パケットの除外について

デフォルトでは、IPv4SG はインターフェイス上のすべての着信 IPv4 パケットを処理し、IPSG バインディングと一致しないパケットを廃棄します。IPSG バインディングと一致しない特定の IPv4 パケットがインターフェイスを通過できるようにするには、IPSG フィルタリング免除のパケットの送信元項目を指定します。指定された送信元項目を持つすべての IPv4 パケットは、IPSG によって処理されずに転送されます。

## 手順

1. システムビューに入ります。  
**system-view**
2. 指定された送信元項目を含む IPv4 パケットを IPSG フィルタリングから除外します。  
**ip verify source exclude vlan start-vlan-id [to end-vlan-id]**  
デフォルトでは、除外されたソース項目は設定されません。  
このコマンドを複数回実行して、複数の除外 VLAN を指定できます。指定した除外 VLAN はオーバーラップできません。

# IPv6SG機能の設定

## インターフェイスでの IPv6SG のイネーブル化

### インターフェイス上の IPv6SG 機能について

インターフェイスで IPv6SG をイネーブルにすると、スタティック IPv6SG とダイナミック IPv6SG の両方がイネーブルになります。

- 静的 IPv6SG は、**ipv6 source binding** コマンドを使用して構成された静的バインディングを使用します。詳細は、「静的 IPv6SG バインディングの構成」を参照してください。
- ダイナミック IPv6SG は、関連する送信元モジュールからダイナミックバインディングを生成します。IPv6SG はバインディングを使用して、**ipv6 verify source** コマンドで指定された一致基準に基づいて着信 ipv6 パケットをフィルタリングします。

### 制限事項およびガイドライン

ダイナミック IPv6SG を実装するには、DHCPv6 スヌーピング、DHCPv6 リレーエージェント、または ND スヌーピングがネットワーク上で正常に動作することを確認します。

## 手順

1. システムビューに入ります。  
**system-view**
2. インターフェイスビューを入力します。  
**interface interface-type interface-number**  
次のインターフェイスタイプがサポートされています。
  - レイヤ 2 イーサネットインターフェイス。
  - レイヤ 3 イーサネットインターフェイス。
  - VLAN インターフェイス。
3. IPv6SG 機能をイネーブルにします。  
**ipv6 verify source { ip-address | ip-address mac-address | mac-address }**  
デフォルトでは、IPv6SG 機能はインターフェイスでディセーブルになっています。

# 静的 IPv6SG バインディングの設定

## スタティック IPv6SG バインディングについて

グローバルスタティックおよびインターフェイス固有のスタティック IPv6SG バインディングを設定できます。インターフェイス固有のスタティックおよびダイナミックバインディングは、グローバルスタティックバインディングよりも優先されます。インターフェイスは、最初にインターフェイス上のスタティックおよびダイナミックバインディングを使用してパケットを照合します。一致が見つからない場合、インターフェイスはグローバルバインディングを使用します。

## 制限事項およびガイドライン

グローバルスタティックバインディングは、デバイス上のすべてのインターフェイスで有効になります。

ND 攻撃検出機能のスタティック IPv6SG バインディングを設定するには、`vlan vlan-id` オプションを指定し、指定した VLAN に対して ND 攻撃検出をイネーブルにする必要があります。

## グローバルスタティック IPv6SG バインディングの設定

1. システムビューに入ります。

```
system-view
```

2. グローバルスタティック IPv6SG バインディングを設定します。

```
ipv6 source binding ip-address ipv6-address mac-address mac-address
```

## インターフェイスでのスタティック IPv6SG バインディングの設定

1. システムビューに入ります。

```
system-view
```

2. インターフェイスビューを入力します。

```
interface interface-type interface-number
```

次のインターフェイスタイプがサポートされています。

- レイヤ 2 イーサネットインターフェイス。
- レイヤ 3 イーサネットインターフェイス。
- VLAN インターフェイス。

3. スタティック IPv6SG バインディングを設定します。

```
ipv6 source binding { ip-address ipv6-address | ip-address ipv6-address  
mac-address mac-address | mac-address mac-address } [ vlan vlan-id ]
```

異なるインターフェイスに同じスタティック IPv6SG バインディングを設定できます。

# IPSGの表示コマンドおよびメンテナンスコマンド

任意のビューで `display` 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
IPv4SGバインディングを表示します。	<pre>display ip source binding [ static   [ vpn-instance vpn-instance-name ] [ arp-snooping   arp- suppression   dhcp-relay   dhcp-server   dhcp- snooping   dot1x ] ] [ ip-address ip-address ] [ mac-address mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ] [ slot slot-number ]</pre>

タスク	コマンド
IPSGフィルタリングから除外するように設定されているソース項目を表示します。	<code>display ip verify source excluded [ vlan start-vlan-id [ to end-vlan-id ] ] [ slot slot-number ]</code>
IPv6SGアドレスバインディングを表示します。	<code>display ipv6 source binding [ static   [ vpn-instance vpn-instance-name ] [ dhcpv6-relay   dhcpv6-snooping   dot1x   nd-suppression ] ] [ ip-address ipv6-address ] [ mac-address mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ] [ slot slot-number ]</code>
IPv6SGプレフィクスバインディングを表示します。	<code>display ipv6 source binding pd [ vpn-instance vpn-instance-name ] [ prefix prefix/prefix-length ] [ mac-address mac-address ] [ vlan vlan-id ] [ interface interface-type interface-number ] [ slot slot-number ]</code>

## IPSGの設定例

### 例:スタティック IPv4SG の設定

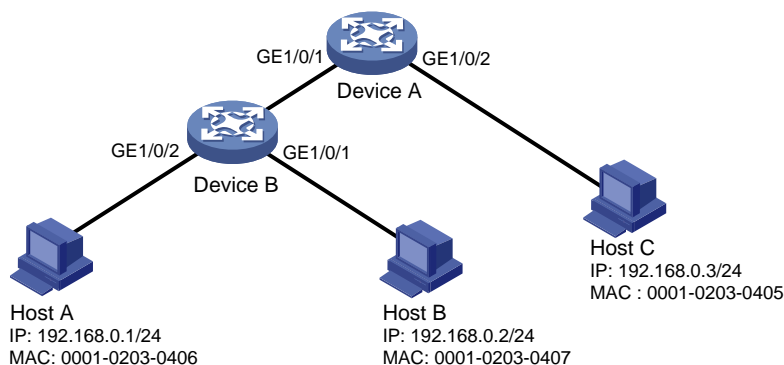
#### ネットワーク構成

図 2 に示すように、すべてのホストは静的 IP アドレスを使用します。

次の要件を満たすように、デバイス A およびデバイス B に静的 IPv4SG バインディングを設定します。

- デバイス A の GigabitEthernet 1/0/2 は、ホスト C からの IP パケットだけを通過させます。
- デバイス A の GigabitEthernet 1/0/1 は、ホスト A からの IP パケットのみを通過させます。
- デバイス B のすべてのインターフェイスは、ホスト A からの IP パケットの通過を許可します。
- GigabitEthernet 1/0/1 は、ホスト B からの IP パケットを通過させます。

図 2 ネットワークダイアグラム



#### 手順

1. デバイス A を構成します。

#インターフェイスの IP アドレスを設定します(詳細は表示されません)。

# GigabitEthernet 1/0/2 で IPv4SG を有効にします。

```
<DeviceA> system-view
```

```
[DeviceA] interface gigabitethernet 1/0/2
```

```
[DeviceA-GigabitEthernet1/0/2] ip verify source ip-address mac-address
#GigabitEthernet 1/0/2 で、ホスト C の静的 IPv4SG バインディングを設定します。
[DeviceA-GigabitEthernet1/0/2] ip source binding ip-address 192.168.0.3 mac-
address 0001-0203-0405
[DeviceA-GigabitEthernet1/0/2] quit
# GigabitEthernet 1/0/1 で IPv4SG を有効にします。
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip verify source ip-address mac-address
# GigabitEthernet 1/0/1 で、ホスト A の静的 IPv4SG バインディングを設定します。
[DeviceA-GigabitEthernet1/0/1] ip source binding ip-address 192.168.0.1 mac-
address 0001-0203-0406
[DeviceA-GigabitEthernet1/0/1] quit
```

## 2. デバイス B を構成します。

#インターフェイスごとに IP アドレスを設定します(詳細は省略)。

# GigabitEthernet 1/0/2 で IPv4SG を有効にします。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip verify source ip-address mac-address
[DeviceB-GigabitEthernet1/0/2] quit
```

#ホスト A の静的 IPv4SG バインディングを設定します。

```
[DeviceB] ip source binding ip-address 192.168.0.1 mac-address 0001-0203-0406
```

# GigabitEthernet 1/01 で IPv4SG を有効にします。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

# GigabitEthernet 1/01 で、ホスト B の静的 IPv4SG バインディングを設定します。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip source binding mac-address 0001-0203-0407
[DeviceB-GigabitEthernet1/0/1] quit
```

## 設定の確認

#スタティック IPv4SG バインディングがデバイス A で正常に設定されていることを確認します。

```
<DeviceA> display ip source binding static
Total entries found: 2
IP Address      MAC Address      Interface          VLAN Type
192.168.0.1     0001-0203-0405  GE1/0/2           N/A Static
192.168.0.3     0001-0203-0406  GE1/0/1           N/A Static
```

#スタティック IPv4SG バインディングがデバイス B で正常に設定されていることを確認します。

```
<DeviceB> display ip source binding static
Total entries found: 2
IP Address      MAC Address      Interface          VLAN Type
192.168.0.1     0001-0203-0406  N/A               N/A Static
N/A             0001-0203-0407  GE1/0/1           N/A Static
```



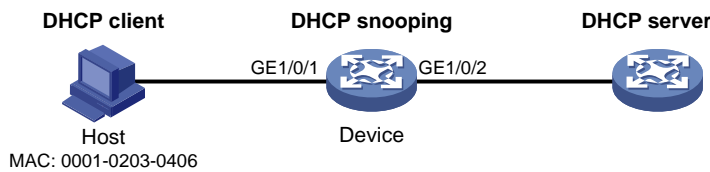
# 例:DHCP スヌーピングベースのダイナミック IPv4SG の設定

## ネットワーク構成

図 3 に示すように、ホスト(DHCP クライアント)は DHCP サーバーから IP アドレスを取得します。次のタスクを実行します。

- デバイスで DHCP スヌーピングをイネーブルにして、DHCP クライアントが認可された DHCP サーバーから IP アドレスを取得するようにします。DHCP クライアントの DHCP スヌーピングエントリを生成するには、DHCP スヌーピングエントリでクライアント情報の記録をイネーブルにします。
- DHCP スヌーピングエントリに基づいて生成された IPv4SG バインディングを使用して着信パケットをフィルタリングするには、GigabitEthernet 1/01 でダイナミック IPv4SG をイネーブルにします。DHCP クライアントからのパケットだけが通過を許可されます。

図 3 ネットワークダイアグラム



## 手順

1. DHCP サーバーを設定します。

DHCP サーバー設定の詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。

2. デバイスを設定します。

#インターフェイスの IP アドレスを設定します(詳細は表示されません)。

#DHCP スヌーピングを有効にします。

```
<Device> system-view
```

```
[Device] dhcp snooping enable
```

# GigabitEthernet 1/02 を信頼できるインターフェイスとして設定します。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] dhcp snooping trust
```

```
[Device-GigabitEthernet1/0/2] quit
```

# GigabitEthernet 1/01 で IPv4SG をイネーブルにし、ダイナミック IPSG の送信元 IP アドレスと MAC アドレスを確認します。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] ip verify source ip-address mac-address
```

# GigabitEthernet 1/01 の DHCP スヌーピングエントリでクライアント情報の記録をイネーブルにします。

```
[Device-GigabitEthernet1/0/1] dhcp snooping binding record
```

```
[Device-GigabitEthernet1/0/1] quit
```

## 設定の確認

#DHCP スヌーピングエントリに基づいて生成されたダイナミック IPSGv4 バインディングを表示します。

```
[Device] display ip source binding dhcp-snooping
```

```
Total entries found: 1
```

IP Address	MAC Address	Interface	VLAN	Type
192.168.0.1	0001-0203-0406	GE1/0/1	1	DHCP snooping

GigabitEthernet 1/0/1 は、IPSGv4 バインディングに基づいてパケットをフィルタリングします。

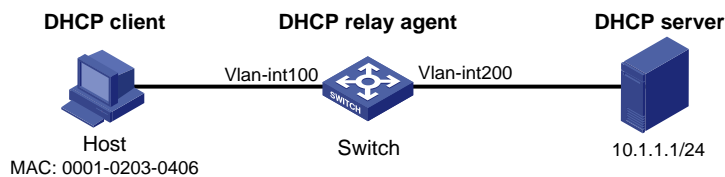
## 例:DHCP リレーエージェントベースのダイナミック IPv4SG の設定

### ネットワーク構成

図 4 に示すように、DHCP リレーエージェントがスイッチでイネーブルになっています。ホストは、DHCP リレーエージェントを介して DHCP サーバーから IP アドレスを取得します。

DHCP リレーエントリに基づいて生成された IPv4SG バインディングを使用して着信パケットをフィルタリングするには、VLAN インターフェイス 100 でダイナミック IPSG をイネーブルにします。

図 4 ネットワークダイアグラム



### 手順

1. ダイナミック IPv4SG を設定します。

#インターフェイスの IP アドレスを設定します(詳細は省略)。

#VLAN インターフェイス 100 で IPv4SG をイネーブルにし、ダイナミック IPSG の送信元 IP アドレスと MAC アドレスを確認します。

```
<Switch> system-view
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] ip verify source ip-address mac-address
[Switch-Vlan-interface100] quit
```

2. DHCP リレーエージェントを設定します。

#DHCP サービスを有効にします。

```
[Switch] dhcp enable
```

#DHCP リレーエントリの記録を有効にします。

```
[Switch] dhcp relay client-information record
```

#VLAN インターフェイス 100 を DHCP リレーモードで動作するように設定します。

```
[Switch] interface vlan-interface 100
[Switch-Vlan-interface100] dhcp select relay
```

#DHCP サーバーの IP アドレスを指定します。

```
[Switch-Vlan-interface100] dhcp relay server-address 10.1.1.1
[Switch-Vlan-interface100] quit
```

### 設定の確認

#DHCP リレーエントリに基づいて生成されたダイナミック IPv4SG バインディングを表示します。

```
[Switch] display ip source binding dhcp-relay
```

Total entries found: 1

IP Address	MAC Address	Interface	VLAN	Type
192.168.0.1	0001-0203-0406	Vlan100	100	DHCP relay

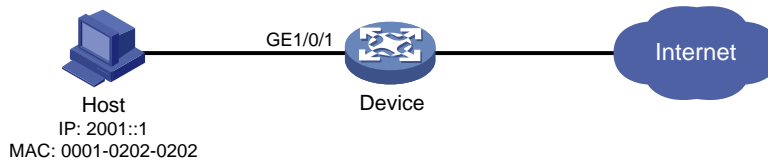
VLAN インターフェイス 100 は、IPSGv4 バインディングに基づいてパケットをフィルタリングします。

## 例:スタティック IPv6SG の設定

### ネットワーク構成

GigabitEthernet 1/0/1 図 5 に示すように、デバイスのスタティック IPv6SG バインディングを設定して、ホストからの IPv6 パケットだけが通過できるようにします。

図 5 ネットワークダイアグラム



### 手順

# GigabitEthernet 1/0/1 で IPv6SG を有効にします。

```
<Device> system-view
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

# GigabitEthernet 1/0/1 で、ホストのスタティック IPv6SG バインディングを設定します。

```
[Device-GigabitEthernet1/0/1] ipv6 source binding ip-address 2001::1 mac-address 0001-0202-0202
[Device-GigabitEthernet1/0/1] quit
```

### 設定の確認

#スタティック IPv6SG バインディングがデバイスで正常に設定されていることを確認します。

```
[Device] display ipv6 source binding static
Total entries found: 1
IPv6 Address          MAC Address          Interface          VLAN Type
2001::1              0001-0202-0202     GE1/0/1           N/A Static
```

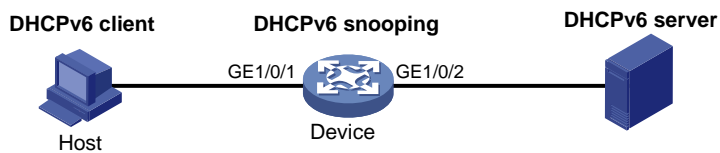
## 例:DHCPv6 スヌーピングベースのダイナミック IPv6SG アドレスバインディングの設定

### ネットワーク構成

図 6 に示すように、ホスト(DHCPv6 クライアント)は DHCPv6 サーバーから IP アドレスを取得します。次のタスクを実行します。

- デバイス上で DHCPv6 スヌーピングをイネーブルにして、DHCPv6 クライアントが認可された DHCPv6 サーバーから IPv6 アドレスを取得できるようにします。DHCPv6 クライアントの DHCPv6 スヌーピングエントリを生成するには、DHCPv6 スヌーピングエントリ内のクライアント情報の記録をイネーブルにします。
- DHCPv6 スヌーピングエントリに基づいて生成された IPv6SG バインディングを使用して着信パケットをフィルタリングするには、GigabitEthernet 1/0/1 でダイナミック IPv6SG をイネーブルにします。DHCPv6 クライアントからのパケットだけが通過を許可されます。

図 6 ネットワークダイアグラム



## 手順

1. DHCPv6 スヌーピングを設定します。

#DHCPv6 スヌーピングをグローバルに有効にします。

```
<Device> system-view
[Device] ipv6 dhcp snooping enable
```

# GigabitEthernet 1/0/2 を信頼できるインターフェイスとして設定します。

```
[Device] interface gigabitethernet 1/0/2
[Device-GigabitEthernet1/0/2] ipv6 dhcp snooping trust
[Device-GigabitEthernet1/0/2] quit
```

2. IPv6SG を有効にします。

# GigabitEthernet 1/0/1 で IPv6SG をイネーブルにし、ダイナミック IPv6SG の送信元 IP アドレスと MAC アドレスを確認します。

```
[Device] interface gigabitethernet 1/0/1
[Device-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

# GigabitEthernet 1/0/1 の DHCPv6 スヌーピングエントリでクライアント情報の記録をイネーブルにします。

```
[Device-GigabitEthernet1/0/1] ipv6 dhcp snooping binding record
[Device-GigabitEthernet1/0/1] quit
```

## 設定の確認

#DHCPv6 スヌーピングエントリに基づいて生成されたダイナミック IP SGv6 バインディングを表示します。

```
[Device] display ipv6 source binding dhcpv6-snooping
Total entries found: 1
IPv6 Address      MAC Address      Interface      VLAN Type
2001::1           040a-0000-0001  GE1/0/1       1      DHCPv6 snooping
```

GigabitEthernet 1/0/1 は、IP SGv6 バインディングに基づいてパケットをフィルタリングします。

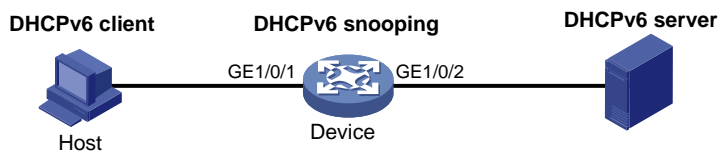
## 例:DHCPv6 スヌーピングベースのダイナミック IPv6SG プレフィックスバインディングの設定

### ネットワーク構成

図 7 に示すように、ホスト(DHCPv6 クライアント)は DHCPv6 サーバーから IPv6 プレフィックスを取得します。次のタスクを実行します。

- デバイス上で DHCPv6 スヌーピングをイネーブルにして、DHCPv6 クライアントが認可された DHCPv6 サーバーから IPv6 プレフィックスを取得するようにします。DHCPv6 クライアントの DHCPv6 スヌーピングプレフィックスエントリを生成するには、DHCPv6 スヌーピングエントリへの IPv6 プレフィックス情報の記録をイネーブルにします。
- GigabitEthernet 1/0/1DHCPv6 スヌーピングプレフィックスエントリに基づいて生成された IPv6SG バインディングを使用して着信パケットをフィルタリングするには、でダイナミック IPv6SG をイネーブルにします。DHCPv6 クライアントからのパケットだけが通過を許可されます。

図 7 ネットワークダイアグラム



## 手順

1. DHCPv6 スヌーピングを設定します。

#DHCPv6 スヌーピングをグローバルに有効にします。

```
<Device> system-view
```

```
[Device] ipv6 dhcp snooping enable
```

# GigabitEthernet 1/0/2 を信頼できるインターフェイスとして設定します。

```
[Device] interface gigabitethernet 1/0/2
```

```
[Device-GigabitEthernet1/0/2] ipv6 dhcp snooping trust
```

```
[Device-GigabitEthernet1/0/2] quit
```

# GigabitEthernet 1/0/1 で DHCPv6 スヌーピングプレフィクスエントリの記録をイネーブルにします。

```
[Device] interface gigabitethernet 1/0/1
```

```
[Device-GigabitEthernet1/0/1] ipv6 dhcp snooping pd binding record
```

2. IPv6SG をイネーブルにします。

# GigabitEthernet 1/0/1 で IPv6SG をイネーブルにし、ダイナミック IPv6SG の送信元 IP アドレスと MAC アドレスを確認します。

```
[Device-GigabitEthernet1/0/1] ipv6 verify source ip-address mac-address
```

```
[Device-GigabitEthernet1/0/1] quit
```

## 設定の確認

#DHCPv6 スヌーピングエントリに基づいて生成されたダイナミック IPSGv6 バインディングを表示します。

```
[Device] display ipv6 source binding pd
```

```
Total entries found: 1
```

IPv6 prefix	MAC address	Interface	VLAN
2001:410:1::/48	0010-9400-0004	GE1/0/1	1

GigabitEthernet 1/0/1 は、IPSGv6 バインディングに基づいてパケットをフィルタリングします。

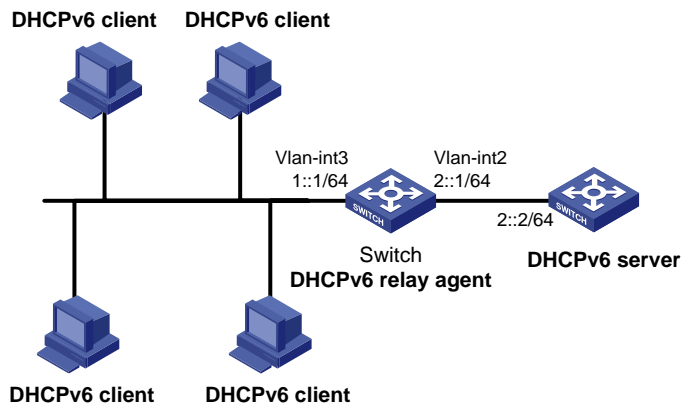
## 例:DHCPv6 リレーエージェントベースのダイナミック IPv6SG の設定

### ネットワーク構成

図 8 に示すように、DHCPv6 リレーエージェントがスイッチ上でイネーブルになっています。クライアントは、DHCPv6 リレーエージェントを介して DHCPv6 サーバーから IPv6 アドレスを取得します。

DHCPv6 リレーエントリに基づいて生成された IPv6SG バインディングを使用して着信パケットをフィルタリングするには、VLAN インターフェイス 3 でダイナミック IPv6SG をイネーブルにします。

図 8 ネットワークダイアグラム



## 手順

1. DHCPv6 リレーエージェントを設定します。  
 #VLAN 2 と VLAN 3 を作成し、VLAN にインターフェイスを割り当て、VLAN-interface 2 と VLAN-interface 3 の IP アドレスを指定します(詳細は表示されていません)。  
 #VLAN インターフェイス 3 で DHCPv6 リレーエージェントをイネーブルにします。  

```
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ipv6 dhcp select relay
```

 #インターフェイスの DHCPv6 リレーエントリの記録を有効にします。  

```
[Switch-Vlan-interface3] ipv6 dhcp relay client-information record
```

 #リレーエージェント上の DHCPv6 サーバアドレス 2::2 を指定します。  

```
[Switch-Vlan-interface3] ipv6 dhcp relay server-address 2::2
[Switch-Vlan-interface3] quit
```
2. VLAN インターフェイス 3 で IPv6SG をイネーブルにし、ダイナミック IPv6SG の送信元 IP アドレスおよび MAC アドレスを確認します。  

```
<Switch> system-view
[Switch] interface vlan-interface 3
[Switch-Vlan-interface3] ipv6 verify source ip-address mac-address
[Switch-Vlan-interface3] quit
```

## 設定の確認

#DHCPv6 リレーエントリに基づいて生成されたダイナミック IPv6SG バインディングを表示します。

```
[Switch] display ipv6 source binding dhcpv6-relay
Total entries found: 1
IP Address      MAC Address      Interface      VLAN Type
1::2           0001-0203-0406 Vlan3          3    DHCPv6 relay
```

# ARP 攻撃からの保護の設定

## ARP攻撃からの保護について

デバイスは、LAN 内の ARP 攻撃およびウイルスを検出して防止するための複数の機能を提供できます。攻撃者は、ARP の脆弱性を不正利用して、次の方法でネットワークデバイスを攻撃できます。

- CPU が過負荷になるまで、IP アドレスの解決で受信デバイスをビジー状態にするために、解決不可能な IP パケットを大量に送信します。解決不可能な IP パケットとは、ARP が対応する MAC アドレスを検出できない IP パケットのことです。
- 大量の ARP パケットを送信して、受信デバイスの CPU を過負荷にします。
- 信頼されたユーザーまたはゲートウェイとして ARP パケットを送信し、受信側デバイスが不正な ARP エントリを取得できるようにします。

## ARP攻撃からの保護タスクの概要

すべての ARP 攻撃保護タスクはオプションです。

- 洪水攻撃の防止
  - 解決不可能な IP 攻撃からの保護の設定
  - ARP パケットレート制限の設定
  - 送信元 MAC ベース ARP 攻撃検出の設定
- ユーザーおよびゲートウェイのスプーフィング攻撃の防止
  - ARP パケットの送信元 MAC 整合性チェックの設定
  - ARP アクティブ確認応答の設定
  - 許可 ARP の設定
  - 例:DHCP リレーエージェントでの許可 ARP の設定
  - ARP 攻撃検出の設定
  - ARP パケットの有効性チェックの設定
  - ARP 制限付き転送の設定
  - ユーザー有効性チェック中に ARP パケットの入力ポートを無視する
  - ARP 攻撃検出ロギングのイネーブル化
  - ARP スキャンおよび固定 ARP の設定
  - ARP ゲートウェイ保護の設定
  - 例:ARP ゲートウェイ保護の設定
  - ARP フィルタリングの設定
  - ARP 送信元 IP アドレスチェックの設定

## 解決不可能なIP攻撃からの保護の設定

### 解決不可能な IP 攻撃からの保護について

デバイスがホストから解決できない IP パケットを大量に受信した場合、次の状況が発生する可能性があります。

- デバイスは大量の ARP 要求を送信し、ターゲットサブネットに過負荷をかけます。
- デバイスは宛先 IP アドレスを解決しようと続け、CPU に過負荷をかけます。

このような IP 攻撃からデバイスを保護するために、次の機能を設定できます。

- ARP 送信元抑制 IP アドレスからの解決できない IP パケットの数が 5 秒以内に上限を超えた場合、IP アドレスからのパケットの解決を停止します。デバイスは、間隔が経過すると ARP 解決を継続します。この機能は、攻撃パケットが同じ送信元アドレスを持つ場合に適用されます。

- ARP ブラックホールルーティング未解決の IP アドレスを宛先とするブラックホールルートを作成します。デバイスは、ブラックホールルートが削除されるまで、一致するすべてのパケットをドロップします。ブラックホールルートは、エージングタイマーに達したとき、またはルートが到達可能になったときに削除されます。

未解決の IP アドレスに対してブラックホールルートが作成された後、デバイスは ARP 要求を送信して最初の ARP ブラックホールルートプローブをただちに開始します。解決に失敗した場合、デバイスはプローブ設定に従ってプローブを続行します。IP アドレス解決がプローブで成功した場合、デバイスはブラックホールルートを通常のルートに変換します。デバイスがすべてのプローブを終了する前に ARP ブラックホールルートが期限切れになった場合、デバイスはブラックホールルートを削除し、残りのプローブは実行しません。

この機能は、攻撃パケットの送信元アドレスが同じかどうかに関係なく適用できます。

## ARP 送信元抑制の設定

1. システムビューに入ります。  
`system-view`
2. ARP 送信元抑制をイネーブルにします。  
`arp source-suppression enable`  
デフォルトでは、ARP 送信元抑制はディセーブルです。
3. デバイスが送信元 IP アドレスごとに 5 秒以内に処理できる解決不可能なパケットの最大数を設定します。  
`arp source-suppression limit limit-value`  
デフォルトでは、最大数は 10 です。

## ARP ブラックホールルーティングの設定

### 制限事項およびガイドライン

ARP ブラックホールルートプローブカウントを 25 などの大きな値に設定します。デバイスが一時的に宛先 IP アドレスに到達できず、プローブカウントが小さすぎる場合、問題が解決される前にすべてのプローブが終了する可能性があります。その結果、攻撃以外のパケットがドロップされます。この設定により、このような状況を回避できます。

### 手順

1. システムビューに入ります。  
`system-view`
2. ARP ブラックホールルーティングをイネーブルにします。  
`arp resolving-route enable`  
デフォルトでは、ARP ブラックホールルーティングはイネーブルです。
3. (任意)未解決の IP アドレスごとに ARP ブラックホールルートプローブの数を設定します。  
`arp resolving-route probe-count count`  
デフォルトの設定は 3 つのプローブです。
4. (任意)デバイスが ARP ブラックホールルートをプローブする間隔を設定します。  
`arp resolving-route probe-interval interval`  
デフォルト設定は 1 秒です。



# 解決不可能な IP 攻撃から保護するための表示コマンドと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ます。

タスク	コマンド
ARP送信元抑制の設定情報を表示します。	<code>display arp source-suppression</code>

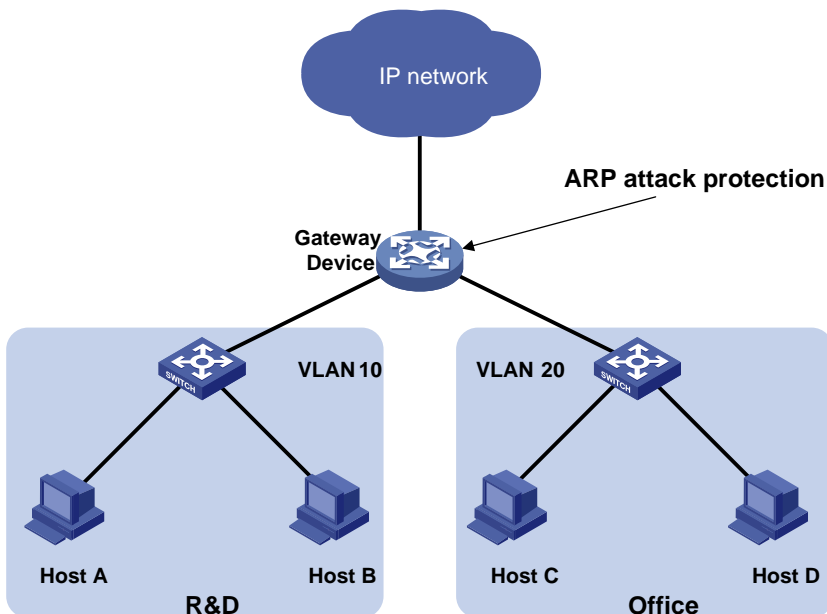
## 例:解決不可能な IP 攻撃からの保護の設定

### ネットワーク構成

図 9 に示すように、LAN には VLAN 10 の研究開発エリアと VLAN 20 のオフィスエリアの 2 つのエリアがあり、各エリアはアクセススイッチを介してゲートウェイ(デバイス)に接続されています。

多数の ARP 要求がオフィスエリアで検出され、解決不可能な IP パケットによって引き起こされた攻撃と見なされます。攻撃を防止するには、ARP 送信元抑制または ARP ブラックホールルーティングを設定します。

図 9 ネットワークダイアグラム



### 手順

- 攻撃パケットの送信元アドレスが同じ場合は、ARP 送信元抑制を設定します。

#ARP 送信元抑制を有効にします。

```
<Device> system-view
```

```
[Device] arp source-suppression enable
```

#5 秒以内に送信元 IP アドレスごとに最大 100 個の解決できないパケットを処理するようにデバイスを設定します。

```
[Device] arp source-suppression limit 100
```

- 攻撃パケットの送信元アドレスが異なる場合は、ARP ブラックホールルーティングを設定します。

#ARP ブラックホールルーティングを有効にします。

# ARPパケットレート制限の設定

## ARP パケットのレート制限について

ARP パケットレート制限機能を使用すると、CPUに配信される ARP パケットのレートを制限できます。ARP 攻撃検出が有効なデバイスは、受信したすべての ARP パケットを検査のために CPU に送信します。過剰な ARP パケットを処理すると、デバイスが誤動作したりクラッシュしたりします。この問題を解決するには、ARP パケットレート制限を設定します。インターフェイス上の ARP パケットの受信レートがレート制限を超えると、これらのパケットは廃棄されます。

SNMP モジュールへの通知の送信をイネーブルにしたり、ARP パケットレート制限のロギングをイネーブルにしたりできます。

- 通知の送信が有効になっている場合、デバイスは送信間隔内で最も高いしきい値を超えた ARP パケットレートを通知として SNMP モジュールに送信します。通知タイプとターゲットホストを設定するには、`snmp-agent target-host` コマンドを使用する必要があります。通知の詳細については、『Network Management and Monitoring Command Reference』を参照してください。
- ARP パケットレート制限のロギングがイネーブルになっている場合、デバイスは送信間隔内で最も高いしきい値を超えた ARP パケットレートをログメッセージで情報センターに送信します。情報センターモジュールを設定して、ログ出力ルールを設定できます。情報センターの詳細については、『Network Management and Monitoring Configuration Guide』を参照してください。

## 制限事項およびガイドライン

ベストプラクティスとして、ARP 攻撃検出、ARP スヌーピング、または MFF がイネーブルの場合、または ARP フラッド攻撃が検出された場合に、この機能を設定します。

ARP パケットレート制限に対して過剰な通知とログメッセージが送信される場合は、通知とログメッセージの送信間隔を増やすことができます。

レイヤ 2 集約インターフェイスで ARP パケットレート制限の通知送信およびロギングをイネーブルにする場合、機能はすべての集約メンバーポートに適用されます。

## 手順

1. システムビューに入ります。  
`system-view`
2. (任意)ARP パケットレート制限の SNMP 通知をイネーブルにします。  
`snmp-agent trap enable arp [ rate-limit ]`  
デフォルトでは、ARP パケットレート制限の SNMP 通知はディセーブルになっています。
3. (任意)ARP パケットレート制限のロギングをイネーブルにします。  
`arp rate-limit log enable`  
デフォルトでは、ARP パケットレート制限のロギングはディセーブルになっています。
4. (任意)通知およびログメッセージの送信間隔を設定します。  
`arp rate-limit log interval interval`  
デフォルトでは、デバイスは 60 秒ごとに通知とログメッセージを送信します。
5. インターフェイスビューを入力します。  
`interface interface-type interface-number`  
サポートされるインターフェイスタイプには、レイヤ 2 イーサネットインターフェイス、レイヤ 3 イーサネットインターフェイス、レイヤ 3 集約インターフェイス、およびレイヤ 2 集約インターフェイスがあります。

6. ARP パケットレート制限をイネーブルにします。

```
arp rate-limit [ pps ]
```

デフォルトでは、ARP パケットのレート制限はイネーブルです。

## 送信元MACベースARP攻撃検出の設定

### 送信元 MAC ベースの ARP 攻撃検出について

この機能は、CPU に配信された ARP パケットの数をチェックします。5 秒以内に同じ MAC アドレスからのパケット数がしきい値を超えた場合、デバイスは MAC アドレスの ARP 攻撃エントリを生成します。ARP ロギング機能がイネーブルの場合、デバイスは、ARP 攻撃エントリが期限切れになる前に、次のいずれかの方法を使用して攻撃を処理します。

- Monitor: ログメッセージだけを生成します。
- Filter: ログメッセージを生成し、MAC アドレスからの後続の ARP パケットをフィルタリングします。

ARP ロギング機能をイネーブルにするには、`arp check log enable` コマンドを使用します。ARP ロギング機能の詳細については、『Layer 3 IP Services Configuration Guide』の「ARP」を参照してください。

ARP 攻撃エントリが期限切れになると、エントリ内の MAC アドレスを送信元とする ARP パケットが正しく処理されます。

### 制限事項およびガイドライン

処理方法を `monitor` から `filter` に変更すると、設定はただちに有効になります。処理方法を `filter` から `monitor` に変更すると、デバイスは既存の攻撃エントリに一致するパケットのフィルタリングを続行します。

一部のゲートウェイおよびサーバーの MAC アドレスをこの検出から除外できます。この機能は、これらのデバイスが攻撃者であっても、これらのデバイスからの ARP パケットを検査しません。

### 手順

1. システムビューに入ります。  
`system-view`
2. 送信元 MAC ベースの ARP 攻撃検出をイネーブルにし、処理方法を指定します。

```
arp source-mac { filter | monitor }
```

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。

3. しきい値を設定します。  
`arp source-mac threshold threshold-value`  
しきい値は 30 です。

4. ARP 攻撃エントリのエイジングタイマーを設定します。  
`arp source-mac aging-time time`

デフォルトでは、ライフタイムは 300 秒です。

5. (任意)この検出から特定の MAC アドレスを除外します。  
`arp source-mac exclude-mac mac-address<1-10>`  
デフォルトでは、MAC アドレスは除外されません。

# 送信元 MAC ベース ARP 攻撃検出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ます。

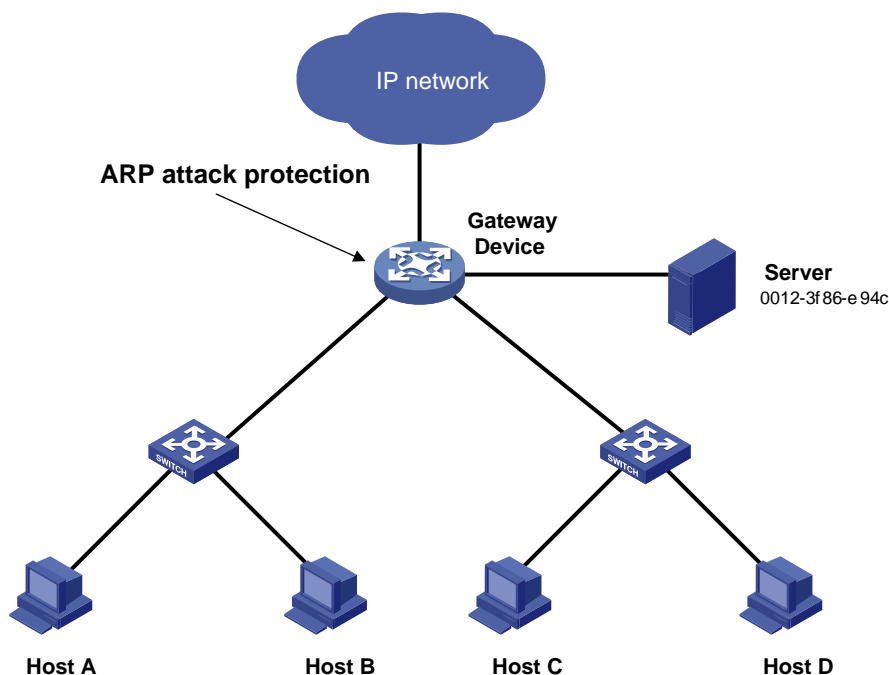
タスク	コマンド
送信元MACベースARP攻撃検出によって検出されたARP攻撃エントリを表示します。	<code>display arp source-mac { interface interface-type interface-number   slot slot-number }</code>

## 例:送信元 MAC ベース ARP 攻撃検出の設定

### ネットワーク構成

図 10 に示すように、ホストはゲートウェイ(デバイス)を介してインターネットにアクセスします。悪意のあるユーザーが大量の ARP 要求をゲートウェイに送信すると、ゲートウェイがクラッシュしてクライアントからの要求を処理できなくなる可能性があります。この問題を解決するには、ゲートウェイで送信元 MAC ベースの ARP 攻撃検出を設定します。

図 10 ネットワークダイアグラム



### 手順

#送信元 MAC ベースの ARP 攻撃検出を有効にし、フィルタとして処理方法を指定します。

```
<デバイス>システムビュー
```

```
<Device> system-view
```

```
[Device] arp source-mac filter
```

# しきい値を 30 に設定します。

```
[Device] arp source-mac threshold 30
```

#ARP 攻撃エントリのライフタイムを 60 秒に設定します。

```
[Device] arp source-mac aging-time 60
```

#この検出から MAC アドレス 0012-3f86-e94c を除外します。

```
[Device] arp source-mac exclude-mac 0012-3f86-e94c
```

## ARPパケットの送信元MAC整合性チェックの設定

### ARP パケットの送信元 MAC 整合性チェックについて

この機能により、ゲートウェイは、イーサネットヘッダー内の送信元 MAC アドレスがメッセージ本文内の送信元 MAC アドレスと異なる ARP パケットをフィルタリングできます。この機能により、ゲートウェイは正しい ARP エントリを学習できます。

#### 手順

1. システムビューに入ります。  
`system-view`
2. ARP パケットの送信元 MAC アドレスの整合性チェックをイネーブルにします。  
`arp valid-check enable`  
デフォルトでは、ARP パケットの送信元 MAC アドレスの整合性チェックはディセーブルです。

## ARPアクティブ確認応答の設定

### ARP アクティブ確認応答について

ゲートウェイでこの機能を設定して、ユーザースプーフィングを防止します。

ARP アクティブ確認応答は、ゲートウェイが不正な ARP エントリを生成するのを防止します。

strict モードでは、ゲートウェイは ARP エントリを作成する前に、より厳密な有効性チェックを実行します。

- ゲートウェイ宛ての ARP 要求を受信すると、ゲートウェイは ARP 応答を送信しますが、ARP エントリは作成しません。
- ARP 応答を受信すると、ゲートウェイは送信元 IP アドレスが解決されたかどうかを判断します。
  - 「はい」の場合、ゲートウェイはアクティブな確認応答を実行します。ARP 応答が有効であることが確認されると、ゲートウェイは ARP エントリを作成します。
  - 「いいえ」の場合、ゲートウェイはパケットを廃棄します。

#### 手順

1. システムビューに入ります。  
`system-view`
2. ARP アクティブ確認応答機能をイネーブルにします。  
`arp active-ack [ strict ] 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。  
ARP アクティブ確認応答を strict モードで有効にするには、ARP ブラックホールルーティングがイネーブルになっていることを確認します。

# 許可ARPの設定

## 認可 ARP について

認可された ARP エントリは、DHCP サーバー上の DHCP クライアントのアドレスリースまたは DHCP リレーエージェント上のダイナミッククライアントエントリに基づいて生成されます。DHCP サーバーおよび DHCP リレーエージェントの詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。

この機能を使用して、ユーザースプーフィングを防止し、認可されたクライアントだけにネットワークリソースへのアクセスを許可します。

## 手順

1. システムビューに入ります。

```
system-view
```

2. インターフェイスビューを入力します。

```
interface interface-type interface-number
```

サポートされるインターフェイスタイプには、レイヤ 3 イーサネットインターフェイス、レイヤ 3 イーサネットサブインターフェイス、レイヤ 3 集約インターフェイス、レイヤ 3 集約サブインターフェイス、および VLAN インターフェイスがあります。

3. インターフェイス上で許可 ARP をイネーブルにします。

```
arp authorized enable
```

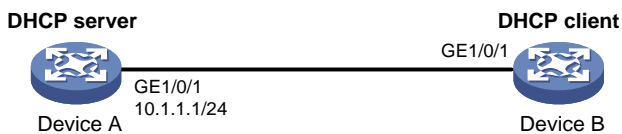
デフォルトでは、許可 ARP はディセーブルになっています。

## 例:DHCP サーバーでの許可 ARP の設定

### ネットワーク構成

GigabitEthernet 1/0/1 図 11 に示すように、デバイス A(DHCP サーバー)で許可された ARP を設定して、ユーザーの有効性を確認します。

図 11 ネットワークダイアグラム



## 手順

1. デバイス A を構成します。

# GigabitEthernet 1/01 の IP アドレスを指定します。

```
<DeviceA> system-view
```

```
[DeviceA] interface gigabitethernet 1/0/1
```

```
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
```

```
[DeviceA-GigabitEthernet1/0/1] quit
```

#DHCP を設定します。

```
[DeviceA] dhcp enable
```

```
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[DeviceA-dhcp-pool-1] quit
```

#レイヤ 3 イーサネットインターフェイスビューを開始します。

```
[DeviceA] interface gigabitethernet 1/0/1
```

#許可された ARP を有効にします。

```
[DeviceA-GigabitEthernet1/0/1] arp authorized enable
[DeviceA-GigabitEthernet1/0/1] quit
```

## 2. デバイス B を構成します。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address dhcp-alloc
[DeviceB-GigabitEthernet1/0/1] quit
```

## 設定の確認

#デバイス A の許可された ARP エントリ情報を表示します。

```
[DeviceA] display arp all
Type: S-Static D-Dynamic O-Openflow R-Rule M-Multiport I-Invalid
IP Address      MAC Address      SVLAN/VSI Interface/Link ID      Aging Type
10.1.1.2        0012-3f86-e94c N/A              GE1/0/1                960 D
```

この出力は、IP アドレス 10.1.1.2 がデバイス B に割り当てられていることを示しています。

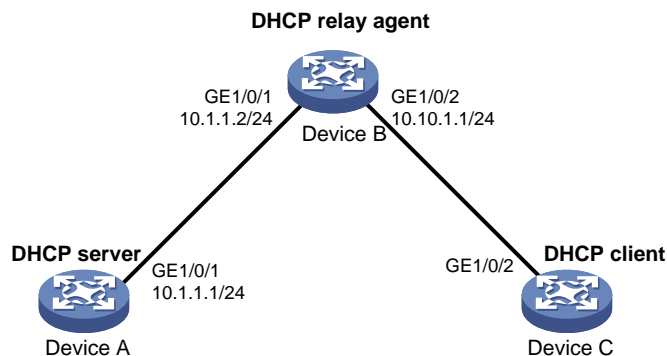
デバイス B は、デバイス A と通信するために、認可された ARP エントリ内の IP アドレスと MAC アドレスを使用する必要があります。そうしないと、通信は失敗します。したがって、ユーザーの有効性が保証されません。

# 例:DHCP リレーエージェントでの許可 ARP の設定

## ネットワーク構成

GigabitEthernet 1/0/2 図 12 に示すように、デバイス B(DHCP リレーエージェント)の許可された ARP を設定して、ユーザーの有効性を確認します。

図 12 ネットワークダイアグラム



## 手順

### 1. デバイス A を構成します。

# GigabitEthernet 1/0/1 の IP アドレスを指定します。

```
<DeviceA> system-view
```

```
[DeviceA] interface gigabitethernet 1/0/1
[DeviceA-GigabitEthernet1/0/1] ip address 10.1.1.1 24
[DeviceA-GigabitEthernet1/0/1] quit
```

**#DHCPを設定します。**

```
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 1
[DeviceA-dhcp-pool-1] network 10.10.1.0 mask 255.255.255.0
[DeviceA-dhcp-pool-1] gateway-list 10.10.1.1
[DeviceA-dhcp-pool-1] quit
[DeviceA] ip route-static 10.10.1.0 24 10.1.1.2
```

## 2. デバイス B を構成します。

**#DHCPを有効にします。**

```
<DeviceB> system-view
[DeviceB] dhcp enable
```

**# GigabitEthernet 1/0/1 および GigabitEthernet 1/0/2 の IP アドレスを指定します。**

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] ip address 10.1.1.2 24
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip address 10.10.1.1 24
```

**# GigabitEthernet 1/0/2 で DHCP リレーエージェントを有効にします。**

```
[DeviceB-GigabitEthernet1/0/2] dhcp select relay
```

**#DHCP サーバー10.1.1.1 を DHCP サーバグループ 1 に追加します。**

```
[DeviceB-GigabitEthernet1/0/2] dhcp relay server-address 10.1.1.1
```

**#許可された ARP を有効にします。**

```
[DeviceB-GigabitEthernet1/0/2] arp authorized enable
[DeviceB-GigabitEthernet1/0/2] quit
```

**#リレーエージェントでリレーエントリの記録をイネーブルにします。**

```
[DeviceB] dhcp relay client-information record
```

## 3. デバイス C を構成します。

```
<DeviceC> system-view
[DeviceC] ip route-static 10.1.1.0 24 10.10.1.1
[DeviceC] interface gigabitethernet 1/0/2
[DeviceC-GigabitEthernet1/0/2] ip address dhcp-alloc
[DeviceC-GigabitEthernet1/0/2] quit
```

## 設定の確認

**#デバイス B の許可された ARP 情報を表示します。**

```
[DeviceB] display arp all
Type: S-Static   D-Dynamic   O-Openflow   R-Rule   M-Multiport   I-Invalid
IP Address      MAC Address    SVLAN/VSI   Interface/Link ID   Aging Type
10.10.1.2       0012-3f86-e94c N/A         GE1/0/2              960   D
```

出力は、デバイス A がデバイス C に IP アドレス 10.10.1.2 を割り当てたことを示しています。

デバイス C は、デバイス B と通信するために、許可された ARP エントリ内の IP アドレスと MAC アドレスを使用する必要があります。そうしないと、通信は失敗します。これにより、ユーザーの有効性が保証されます。



# ARP攻撃検出の設定

## ARP 攻撃の検出について

ARP 攻撃検出を使用すると、アクセスデバイスは、許可されていないクライアントからの ARP パケットをブロックして、ユーザースプーフィング攻撃およびゲートウェイスプーフィング攻撃を防止できます。

ARP 攻撃検出には、次の機能があります。

- ユーザー妥当性検査。
- ARP パケットの有効性チェック。
- ARP 制限付き転送。
- ユーザー有効性チェック中に ARP パケット入力ポートが無視する
- VSI の ARP 攻撃検出。
- ARP 攻撃検出ロギング。

ARP パケットの有効性チェックとユーザーの有効性チェックの両方がイネーブルになっている場合、前者が最初に適用され、次に後者が適用されます。

ARP 攻撃検出と ARP スヌーピングを同時に設定しないでください。同時に設定すると、ARP スヌーピングエントリを生成できません。

## ユーザー妥当性検査の構成

### ユーザー妥当性検査について

ユーザー有効性チェックでは、ARP 信頼インターフェイスで受信された ARP パケットはチェックされません。この機能は、ARP 信頼できないインターフェイスで受信された ARP パケットの送信元 IP および送信元 MAC を、次の順序で一致基準と比較します。

1. ユーザー妥当性検査ルール。
  - 一致が見つかった場合、デバイスはルールに従って ARP パケットを処理します。
  - 一致が見つからない場合、またはユーザー有効性チェック規則が設定されていない場合は、ステップ 2 に進みます。
2. スタティック IP ソースガードバインディング、802.1X セキュリティエントリ、および DHCP スヌーピングエントリ。
  - 一致するものが見つかり、デバイスは ARP パケットを転送します。
  - 一致するものが見つからない場合、デバイスは ARP パケットを廃棄します。

IP ソースガード スタティック IP ソースガードバインディングを作成するには、ip source binding コマンドを使用します。詳細については、「Configuring IP source guard」を参照してください。

DHCP スヌーピングエントリは、DHCP スヌーピングによって自動的に生成されます。詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。

802.1X セキュリティエントリは、802.1X クライアントの IP から MAC へのマッピングを記録します。クライアントが 802.1X 認証を通過し、その IP アドレスを ARP 攻撃検出が有効なデバイスにアップロードすると、デバイスは自動的に 802.1X セキュリティエントリを生成します。802.1X クライアントは、その IP アドレスをデバイスにアップロードするために有効にする必要があります。詳細は、「802.1X の構成」を参照してください。

### 制限事項およびガイドライン

ユーザー有効性チェックを設定する場合は、次の項目の 1 つ以上が設定されていることを確認します。

- ユーザー妥当性検査ルール。
- スタティック IP ソースガードバインディング。
- DHCP スヌーピング。
- 802.1X です。

いずれの項目も設定されていない場合、ARP untrusted インターフェイス上のすべての着信 ARP パケットは廃棄されます。

IP ソースガードバインディングに対して ARP 攻撃検出をイネーブルにする IP アドレス、MAC アドレス、および VLAN を指定します。イネーブルにしない場合、IP ソースガードバインディングに一致する ARP パケットはありません。

## 手順

1. システムビューに入ります。  
**system-view**
2. (任意)ユーザー有効性チェック規則を設定します。  
**arp detection rule rule-id { deny | permit } ip { ip-address [ mask ] | any } mac { mac-address [ mask ] | any } [ vlan vlan-id ]**  
デフォルトでは、ユーザー有効性チェック規則は設定されていません。
3. VLAN ビューを開始します。  
**vlan vlan-id**
4. ARP 攻撃検出をイネーブルにします。  
**arp detection enable**  
デフォルトでは、ARP 攻撃検出はディセーブルになっています。
5. (任意)ARP ユーザー有効性チェックを必要としないインターフェイスを、信頼できるインターフェイスとして設定します。
  - a. システムビューに戻ります。  
**quit**
  - b. インターフェイスビューを入力します。  
**interface interface-type interface-number**  
サポートされているインターフェイスタイプには、レイヤ 2 イーサネットインターフェイスおよびレイヤ 2 集約インターフェイスがあります。
  - c. インターフェイスを、ARP 攻撃検出から除外される信頼できるインターフェイスとして設定します。  
**arp detection trust**  
デフォルトでは、インターフェイスは信頼できません。

# ARP パケットの有効性チェックの設定

## ARP パケットの有効性チェックについて

ARP パケットの有効性チェックでは、ARP 信頼インターフェイスで受信された ARP パケットはチェックされません。信頼できないインターフェイスで受信された ARP パケットをチェックするには、次のチェック対象オブジェクトを指定できます。

- **src-mac:** メッセージ本文の送信元 MAC アドレスが、イーサネットヘッダーの送信元 MAC アドレスと同一であるかどうかをチェックします。同一である場合、パケットは転送されます。同一でない場合、パケットは廃棄されます。
- **dst-mac:** ARP 応答のターゲット MAC アドレスをチェックします。ターゲット MAC アドレスがすべて 0、すべて 1、またはイーサネットヘッダーの宛先 MAC アドレスと一致しない場合、パケットは無効と見なされ、廃棄されます。
- **ip:** ARP 応答の送信元と宛先の IP アドレス、および ARP 要求の送信元 IP アドレスをチェックします。すべてが 1 つの IP アドレスまたはマルチキャスト IP アドレスは無効と見なされ、対応するパケットは廃棄されます。

## 前提条件

ARP パケットの有効性チェックを設定する前に、まずユーザーの有効性チェックを設定する必要があります。ユーザーの有効性チェックの設定の詳細については、「ユーザーの有効性チェックの設定」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. VLAN ビューを開始します。  
**vlan *vlan-id***
3. ARP 攻撃検出をイネーブルにします。  
**arp detection enable**  
デフォルトでは、ARP 攻撃検出はディセーブルになっています。
4. ARP パケットの有効性チェックをイネーブルにします。
  - a. システムビューに戻ります。  
**quit**
  - b. ARP パケットの有効性チェックをイネーブルにし、チェックするオブジェクトを指定します。  
**arp detection validate { *dst-mac* | *ip* | *src-mac* } \***  
デフォルトでは、ARP パケットの有効性チェックはディセーブルになっています。
5. (任意)ARP パケットの有効性チェックを必要としないインターフェイスを、信頼できるインターフェイスとして設定します。
  - a. インターフェイスビューを入力します。  
**interface *interface-type interface-number***  
サポートされているインターフェイスタイプには、レイヤ 2 イーサネットインターフェイスおよびレイヤ 2 集約インターフェイスがあります。
  - b. インターフェイスを、ARP 攻撃検出から除外される信頼できるインターフェイスとして設定します。  
**arp detection trust**  
デフォルトでは、インターフェイスは信頼できません。

# ARP 制限付き転送の設定

## ARP 制限付き転送について

ARP 制限付き転送は、ARP 信頼インターフェイスで受信された ARP パケットには影響せず、ARP パケットを正しく転送します。この機能は、信頼できないインターフェイスで受信され、ユーザー有効性チェックに合格した ARP パケットの転送を次のように制御します。

- パケットが ARP 要求の場合は、信頼できるインターフェイスを介して転送されます。
- パケットが ARP 応答の場合は、宛先 MAC アドレスに従って転送されます。MAC アドレステーブルで一致が見つからない場合は、信頼できるインターフェイスを介して転送されます。

## 制限事項およびガイドライン

ARP 制限付き転送は、マルチポート宛先 MAC アドレスを使用する ARP パケットには適用されません。

## 前提条件

ARP 制限付き転送を構成する前に、ユーザー妥当性チェックを構成します。ユーザー妥当性チェックの構成の詳細は、「ユーザー妥当性チェックの構成」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. VLANビューを開始します。  
`vlan vlan-id`
3. ARP 制限転送をイネーブルにします。  
`arp restricted-forwarding enable`  
デフォルトでは、ARP 制限転送はディセーブルになっています。

# ユーザー有効性チェック中に ARP パケットの入力ポートを無視する

## ユーザー有効性チェック中に ARP パケットの入力ポートを無視することについて

ARP 攻撃検出は、ARP 信頼できないインターフェイスからの ARP パケットに対してユーザー有効性チェックを実行します。受信した ARP パケットの送信元 IP および送信元 MAC は、ユーザー有効性チェックに使用されるエントリと比較されます。さらに、ユーザー有効性チェックでは、ARP パケットの入力ポートとエントリ内のポートが比較されます。一致するポートが見つからない場合、ARP パケットは廃棄されます。ユーザー有効性チェックの詳細については、「ユーザー有効性チェックの設定」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. ユーザーの有効性チェック中に ARP パケットの入力ポートを無視します。  
`arp detection port-match-ignore`  
デフォルトでは、ARP パケットの入力ポートは、ユーザーが無効である間にチェックされます。

# VSI の ARP 攻撃検出の設定

## VSI の ARP 攻撃検出について

VXLAN ネットワークでは、VSI で ARP 攻撃検出を実行するように VTEP を設定できます。ARP 攻撃検出は、ARP 信頼できない AC からの ARP パケットに対して、ユーザー有効性チェックと ARP パケット有効性チェックを実行します。AC の詳細については、『VXLAN Configuration Guide』を参照してください。

VSI のユーザー妥当性検査および ARP パケット妥当性検査のメカニズムは、VLAN の場合と同じです。詳細については、「ユーザー妥当性検査の構成」および「ARP パケット妥当性検査の構成」を参照してください。

## VSI のユーザー有効性チェックの設定

1. システムビューに入ります。  
`system-view`
2. (任意)ユーザー有効性チェック規則を設定します。  
`arp detection rule rule-id { deny | permit } ip { ip-address [ mask ] | any } mac { mac-address [ mask ] | any } [ vlan vlan-id ]`  
デフォルトでは、ユーザー有効性チェック規則は設定されていません。
3. VSI ビューに入ります。  
`vsi vsi-name`
4. ARP 攻撃検出をイネーブルにします。  
`arp detection enable`  
デフォルトでは、ARP 攻撃検出はディセーブルになっています。
5. (任意)AC を、ARP 攻撃検出から除外される信頼できる AC として設定します。
  - a. システムビューに戻ります。  
`quit`
  - b. レイヤ 2 イーサネットインターフェイスビューまたはレイヤ 2 集約インターフェイスビューを開始します。  
`interface interface-type interface-number`
  - c. イーサネットサービスインスタンスビューを開始します。  
`service-instance instance-id`
  - d. ARP 攻撃検出から除外された信頼できる AC として AC を設定します。  
`arp detection trust`  
デフォルトでは、AC は信頼されていません。

## VSI の ARP パケット有効性チェックの設定

1. システムビューに入ります。  
`system-view`
2. VSI ビューに入ります。  
`vsi vsi-name`
3. ARP 攻撃検出をイネーブルにします。  
`arp detection enable`  
デフォルトでは、ARP 攻撃検出はディセーブルになっています。
4. システムビューに戻ります。  
`quit`
5. ARP パケットの有効性チェックをイネーブルにし、チェックするオブジェクトを指定します。

```
arp detection validate { dst-mac | ip | src-mac } *
```

デフォルトでは、ARP パケットの有効性チェックはディセーブルになっています。

6. (任意)ARP 攻撃検出から除外された信頼できる AC として AC を設定します。

a. レイヤ 2 イーサネットインターフェイスビューまたはレイヤ 2 集約インターフェイスビューを開始します。

```
interface interface-type interface-number
```

b. イーサネットサービスインスタンスビューを開始します。

```
service-instance instance-id
```

c. ARP 攻撃検出から除外された信頼できる AC として AC を設定します。

```
arp detection trust
```

デフォルトでは、AC は信頼されていません。

## ARP 攻撃検出ロギングのイネーブル化

### ARP 攻撃検出ロギングについて

ARP 攻撃検出ロギング機能を使用すると、不正な ARP パケットが検出されたときに、デバイスで ARP 攻撃検出ログメッセージを生成できます。ARP 攻撃検出ログメッセージには、次の情報が含まれます。

- ARP パケットの受信インターフェイス。
- 送信者の IP アドレス。
- ドロップされた ARP パケットの総数。

### 手順

1. システムビューに入ります。

```
system-view
```

2. ARP 攻撃検出ロギングをイネーブルにします。

```
arp detection log enable [ interval interval ]
```

デフォルトでは、ARP 攻撃検出ロギングはディセーブルになっています。

## ARP 攻撃検出用の表示およびメンテナンスコマンド

任意のビューで display 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。

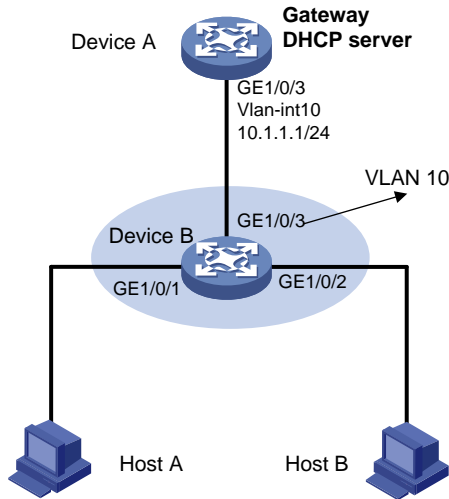
タスク	コマンド
ARP攻撃検出がイネーブルになっているVLANを表示します。	<pre>display arp detection</pre>
ARP攻撃の送信元統計情報を表示します。	<pre>display arp detection statistics attack-source slot slot-number</pre>
ARP攻撃検出によってドロップされたパケットの統計情報を表示します。	<pre>display arp detection statistics packet-drop [ interface interface-type interface-number ]</pre>
ARP攻撃の送信元統計情報をクリアします。	<pre>reset arp detection statistics attack-source [ slot slot-number ]</pre>
ARP攻撃検出によってドロップされたパケットの統計情報をクリアします	<pre>reset arp detection statistics packet-drop [ interface interface-type interface-number ]</pre>

# 例:ユーザー妥当性検査の構成

## ネットワーク構成

図 13 に示すように、接続されたホストの 802.1X セキュリティエントリに基づいてユーザーの有効性チェックを実行するようにデバイス B を設定します。

図 13 ネットワークダイアグラム



## 手順

1. デバイス B のすべてのインターフェイスを VLAN 10 に追加し、デバイス A の VLAN インターフェイス 10 の IP アドレスを指定します(詳細は省略)。
2. デバイス A で DHCP サーバーを設定し、DHCP アドレスプール 0 を設定します。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
```

3. ホスト A とホスト B を 802.1X クライアントとして設定し、ARP 攻撃検出用の IP アドレスをアップロードするように設定します(詳細は省略)。
4. デバイス B を構成します。

```
#802.1X を有効にします。
<DeviceB> system-view
[DeviceB] dot1x
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dot1x
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] dot1x
[DeviceB-GigabitEthernet1/0/2] quit
# ローカルユーザーテストを追加します。
[DeviceB] local-user test
[DeviceB-luser-test] service-type lan-access
[DeviceB-luser-test] password simple test
[DeviceB-luser-test] quit
```

#VLAN 10 の ARP 攻撃検出をイネーブルにして、802.1X エントリに基づいてユーザーの有効性をチェックします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp detection enable
```

#アップストリームインターフェイスを ARP 信頼インターフェイスとして設定します。デフォルトでは、インターフェイスは信頼できないインターフェイスです。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

## 設定の確認

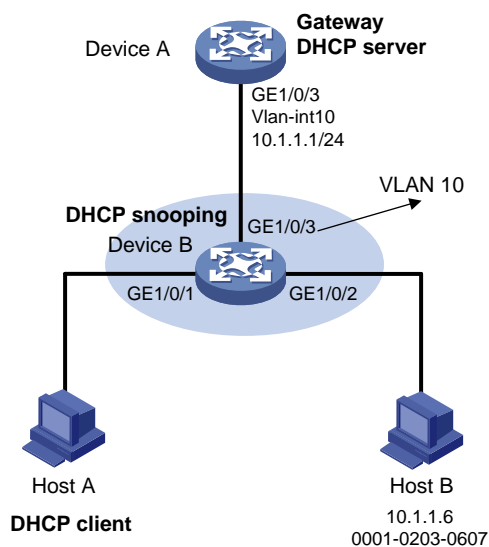
#ARP パケットが GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 インターフェイスで受信され、802.1X エントリに対してチェックされることを確認します。

## 例:ユーザー有効性チェックおよび ARP パケット有効性チェックの設定

### ネットワーク構成

図 14 に示すように、接続されたホストのスタティック IP ソースガードバインディングと DHCP スヌーピング エントリに基づいて、ARP パケットの有効性チェックとユーザーの有効性チェックを実行するようにデバイス B を設定します。

図 14 ネットワークダイアグラム



### 手順

1. デバイス B のすべてのインターフェイスを VLAN 10 に追加し、デバイス A の VLAN インターフェイス 10 の IP アドレスを指定します(詳細は表示されていません)。
2. デバイス A で DHCP サーバーを設定し、DHCP アドレスプール 0 を設定します。

```
<DeviceA> system-view
[DeviceA] dhcp enable
[DeviceA] dhcp server ip-pool 0
[DeviceA-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

3. ホスト A(DHCP クライアント)とホスト B を構成します(詳細は省略)。



#### 4. デバイス B を構成します。

#DHCP スヌーピングを有効にします。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/3] quit
```

# GigabitEthernet 1/0/1 の DHCP スヌーピングエントリでクライアント情報の記録をイネーブルにします。

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] dhcp snooping binding record
[DeviceB-GigabitEthernet1/0/1] quit
```

#VLAN 10 の ARP 攻撃検出を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp detection enable
```

#アップストリームインターフェイスを信頼できるインターフェイスとして設定します。デフォルトでは、インターフェイスは信頼できないインターフェイスです。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

#ユーザーの有効性を確認するために、GigabitEthernet 1/0/2 インターフェイスにスタティック IP ソースガードバインディングエントリを設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

#ARP パケットの MAC アドレスと IP アドレスをチェックすることで、ARP パケットの有効性チェックを有効にします。

```
[DeviceB] arp detection validate dst-mac ip src-mac
```

#### 設定の確認

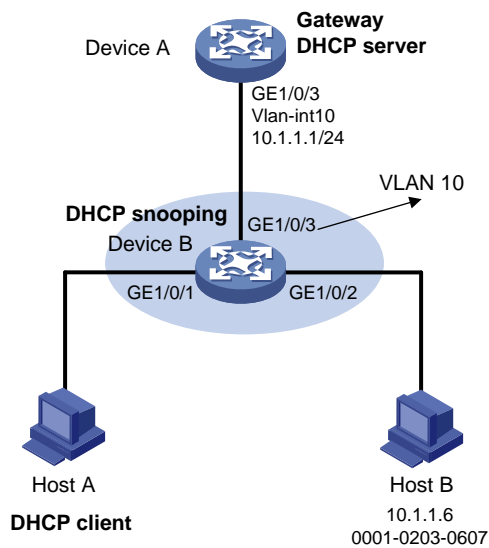
#デバイス B が最初に GigabitEthernet 1/0/1 および GigabitEthernet 1/0/2 で受信した ARP パケットの有効性をチェックすることを確認します。ARP パケットが有効であることが確認された場合、デバイス B はスタティック IP ソースガードバインディングを使用してユーザーの有効性チェックを実行し、最後に DHCP スヌーピングエントリを使用します。

## 例:ARP 制限付きフォワーディングの設定

#### ネットワーク構成

図 15 に示すように、ARP 攻撃検出が設定されているデバイス B に ARP 制限付き転送を設定します。デバイス B に設定されたポート分離は、ブロードキャスト ARP 要求に対して有効になります。

図 15 ネットワークダイアグラム



## 手順

1. VLAN 10 を設定し、VLAN 10 にインターフェイスを追加し、デバイス A の VLAN インターフェイス 10 の IP アドレスを指定します(詳細は省略)。

2. デバイス A で DHCP サーバーを設定し、DHCP アドレスプール 0 を設定します。

```
<DeviceA>システムビュー
[DeviceA]dhcp イネーブル
[DeviceA]dhcp サーバーip-pool 0
[DeviceA-dhcp-pool-0]ネットワーク 10.1.1.0 マスク 255.255.255.0
```

3. ホスト A(DHCP クライアント)とホスト B を構成します(詳細は表示されていません)。

4. デバイス B を構成します。

#DHCP スヌーピングをイネーブルにし、GigabitEthernet 1/0/3 を DHCP 信頼インターフェイスとして設定します。

```
<DeviceB> system-view
[DeviceB] dhcp snooping enable
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] dhcp snooping trust
[DeviceB-GigabitEthernet1/0/3] quit
```

#ユーザーの有効性チェックのために ARP 攻撃検出を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] arp detection enable
```

# GigabitEthernet 1/0/3 を ARP 信頼インターフェイスとして設定します。

```
[DeviceB-vlan10] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] arp detection trust
[DeviceB-GigabitEthernet1/0/3] quit
```

# GigabitEthernet 1/0/2 インターフェイスにスタティック IP ソースガードエントリを設定します。

```
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] ip source binding ip-address 10.1.1.6 mac-address
0001-0203-0607 vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
```

#ARP パケットの MAC アドレスと IP アドレスをチェックすることで、ARP パケットの有効性チェックを有効にします。

```
[DeviceB] arp detection validate dst-mac ip src-mac
```

#隔離ポートを設定します。

```
[DeviceB] port-isolate group 1
```

```
[DeviceB] interface gigabitethernet 1/0/1
```

```
[DeviceB-GigabitEthernet1/0/1] port-isolate enable group 1
```

```
[DeviceB-GigabitEthernet1/0/1] quit
```

```
[DeviceB] interface gigabitethernet 1/0/2
```

```
[DeviceB-GigabitEthernet1/0/2] port-isolate enable group 1
```

```
[DeviceB-GigabitEthernet1/0/2] quit
```

設定が完了すると、デバイス B は最初に GigabitEthernet 1/0/1 および GigabitEthernet 1/0/2 で受信した ARP パケットの有効性をチェックします。ARP パケットが有効であることが確認された場合、デバイス B はスタティック IP ソースガードバインディングを使用してユーザーの有効性チェックを実行し、最後に DHCP スヌーピングエントリを使用します。ただし、ホスト A から送信された ARP ブロードキャスト要求は、デバイス B のチェックを通過してホスト B に到達できます。ポートの分離に失敗しません。

#ARP 制限付き転送を有効にします。

```
[DeviceB] vlan 10
```

```
[DeviceB-vlan10] arp restricted-forwarding enable
```

```
[DeviceB-vlan10] quit
```

## 設定の確認

#デバイス B が、信頼できるインターフェイス GigabitEthernet 1/0/3 を介して、ホスト A からデバイス A に ARP ブロードキャスト要求を転送することを確認します。ホスト B は、このようなパケットを受信できません。ポート分離は正常に動作します。

# ARP スキャンおよび固定 ARP の設定

## ARP スキャンと固定 ARP について

ARP スキャンは、通常、小規模で安定したネットワークで固定 ARP 機能とともに使用されます。

ARP スキャンは、アドレス範囲内のデバイスの ARP エントリを自動的に作成します。デバイスは、次の手順で ARP スキャンを実行します。

1. アドレス範囲内の各 IP アドレスに対して ARP 要求を送信します。
2. 受信した ARP 応答を通じて MAC アドレスを取得します。
3. ダイナミック ARP エントリを作成します。

固定 ARP は、既存のダイナミック ARP エントリ(ARP スキャンによって生成されたものを含む)をスタティック ARP エントリに変換します。これらのスタティック ARP エントリは、手動で設定された ARP エントリと同じ属性を持ちます。この機能は、攻撃者による ARP エントリの変更を防止します。

デフォルトでは、デバイスは指定されたスキャン範囲内のすべての IP アドレスに同時に ARP 要求を送信します。これにより、CPU 使用率が高くなり、ネットワーク負荷が大きくなります。この問題を解決するには、デバイスが ARP スキャンの ARP 要求を送信するレートを設定できます。

## 制限事項およびガイドライン

既存の ARP エントリ内の IP アドレスはスキャンされません。

ARP スキャンには時間がかかります。進行中のスキャンを停止するには、Ctrl+C を押します。ダイナミック ARP エントリは、スキャンが終了する前に受信された ARP 応答に基づいて作成されます。

スタティック ARP エントリの合計数の制限により、一部の動的 ARP エントリが変換に失敗する場合があります。

arp fixup コマンドは 1 回限りの操作です。このコマンドを再度使用して、後で学習した動的 ARP エントリをスタティックに変換できます。

動的 ARP エントリから変換されたスタティック ARP エントリを削除するには、undo arp ip-address[vpn-instance-name]コマンドを使用します。また、reset arp all コマンドを使用してすべての ARP エントリを削除したり、reset arp static コマンドを使用してすべてのスタティック ARP エントリを削除することもできます。

## 手順

1. システムビューに入ります。  
`system-view`
2. インターフェイスビューを入力します。  
`interface interface-type interface-number`
3. ARP スキャンをトリガーし、ARP パケットの送信レートを設定します。  
`arp scan [ start-ip-address to end-ip-address ] [ send-rate pps ]`
4. システムビューに戻ります。  
`quit`
5. 既存の動的 ARP エントリをスタティック ARP エントリに変換します。  
`arp fixup`

# ARPゲートウェイ保護の設定

## ARP ゲートウェイ保護について

ゲートウェイスプーフィング攻撃を防止するには、ゲートウェイに接続されていないインターフェイスでこの機能を設定します。

このようなインターフェイスは、ARP パケットを受信すると、パケット内の送信元 IP アドレスが保護されたゲートウェイの IP アドレスと一致しているかどうかをチェックします。一致している場合は、パケットを破棄します。一致していない場合は、パケットを正しく処理します。

## 制限事項およびガイドライン

ARP ゲートウェイ保護は、インターフェイス上で最大 8 つのゲートウェイに対してイネーブルにできます。

インターフェイス上で arp filter source コマンドと arp filter binding コマンドの両方を設定しないでください。

ARP ゲートウェイ保護が ARP 攻撃検出、MFF、および ARP スヌーピングと連動する場合、ARP ゲートウェイ保護が最初に適用されます。

## 手順

1. システムビューに入ります。  
`system-view`
2. インターフェイスビューを入力します。  
`interface interface-type interface-number`

サポートされているインターフェイスタイプには、レイヤ 2 イーサネットインターフェイスおよびレイヤ 2 集約インターフェイスがあります。

3. 指定されたゲートウェイの ARP ゲートウェイ保護をイネーブルにします。

```
arp filter source ip-address
```

デフォルトでは、ARP ゲートウェイ保護はディセーブルになっています。

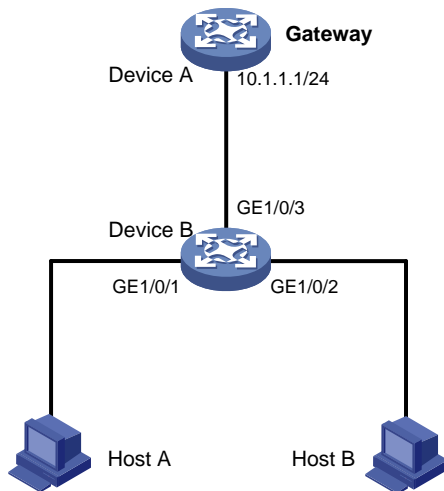
## 例:ARP ゲートウェイ保護の設定

### ネットワーク構成

図 16 に示すように、ホスト B はデバイス B に対してゲートウェイスプーフィング攻撃を開始します。その結果、デバイス B がデバイス A に送信しようとしているトラフィックがホスト B に送信されます。

このような攻撃をブロックするようにデバイス B を設定します。

図 16 ネットワークダイアグラム



### 手順

#デバイス B に ARP ゲートウェイ保護を設定します。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] arp filter source 10.1.1.1
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] arp filter source 10.1.1.1
```

### 設定の確認

# GigabitEthernet 1/0/1 及び GigabitEthernet 1/0/2 を確認し、送信元 IP アドレスがゲートウェイの IP アドレスである着信 ARP パケットを廃棄します。

## ARPフィルタリングの設定

### ARP フィルタリング

ARP フィルタリング機能は、ゲートウェイスプーフィング攻撃とユーザースプーフィング攻撃を防止できます。

この機能を有効にしたインターフェイスは、受信した ARP パケットの送信元 IP アドレスと MAC アドレスを、許可されたエントリと照合します。一致するものが見つかった場合、パケットは正しく処理されます。一致しない場合、パケットは破棄されます。

## 制限事項およびガイドライン

インターフェイスには、最大 8 つの許可エントリを設定できます。

インターフェイス上で `arp filter source` コマンドと `arp filter binding` コマンドの両方を設定しないでください。

ARP フィルタリングが ARP 攻撃検出、MFF、および ARP スヌーピングと連動する場合は、ARP フィルタリングが最初に適用されます。

## 手順

1. システムビューに入ります。

`system-view`

2. インターフェイスビューを入力します。

`interface interface-type interface-number`

サポートされているインターフェイスタイプには、イーサネットインターフェイスとレイヤ 2 集約インターフェイスがあります。

3. ARP フィルタリングをイネーブルにし、許可されるエントリを設定します。

`arp filter binding ip-address mac-address`

デフォルトでは、ARP フィルタリングはディセーブルです。

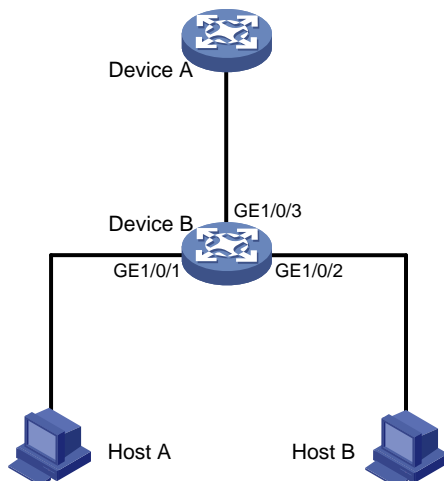
## 例:ARP フィルタリングの設定

### ネットワーク構成

図 17 に示すように、ホスト A の IP アドレスと MAC アドレスは、それぞれ 10.1.1.2 と 000f-e349-1233 です。ホスト B の IP アドレスと MAC アドレスは、それぞれ 10.1.1.3 と 000f-e349-1234 です。

ホスト A およびホスト B からの ARP パケットだけを許可するように、デバイス B の GigabitEthernet 1/0/1 および GigabitEthernet 1/0/2 で ARP フィルタリングを設定します。

図 17 ネットワークダイアグラム



## 手順

#デバイス B に ARP フィルタリングを設定します。

```
<DeviceB> system-view
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] arp filter binding 10.1.1.2 000f-e349-1233
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

## 設定の確認

# GigabitEthernet 1/0/1 がホスト A からの ARP パケットを許可し、その他の ARP パケットを廃棄することを確認します。

# GigabitEthernet 1/0/2 がホスト B からの ARP パケットを許可し、その他の ARP パケットを廃棄することを確認します。

# ARP送信元IPアドレスチェックの設定

## ARP 送信元 IP アドレスの確認について

この機能を使用すると、ゲートウェイは、ARP ラーニングの前に VLAN 内の ARP パケットの送信元 IP アドレスを確認できます。送信元 IP アドレスが許可された IP アドレス範囲内にある場合、ゲートウェイは ARP ラーニングを続行します。送信元 IP アドレスが範囲外にある場合、ゲートウェイは ARP パケットを攻撃パケットと判断し、廃棄します。

## 制限事項およびガイドライン

VLAN がサブ VLAN であり、スーパーVLANに関連付けられている場合は、サブ VLAN だけでこのチェック機能を設定します。

プライマリ VLAN に関連付けられたセカンダリ VLAN 間にレイヤ 3 通信が設定されている場合は、プライマリ VLAN でこの機能を設定します。プライマリ VLAN に関連付けられたセカンダリ VLAN 間にレイヤ 3 通信が設定されていない場合は、目的の VLAN でこの機能を設定します。

## 手順

1. システムビューに入ります。  
**system-view**
2. VLAN ビューを開始します。  
**vlan vlan-id**
3. ARP 送信元 IP アドレスチェック機能をイネーブルにし、IP アドレス範囲を指定します。  
**arp sender-ip-range start-ip-address end-ip-address**  
デフォルトでは、ARP 送信元 IP アドレスチェック機能はディセーブルになっています。

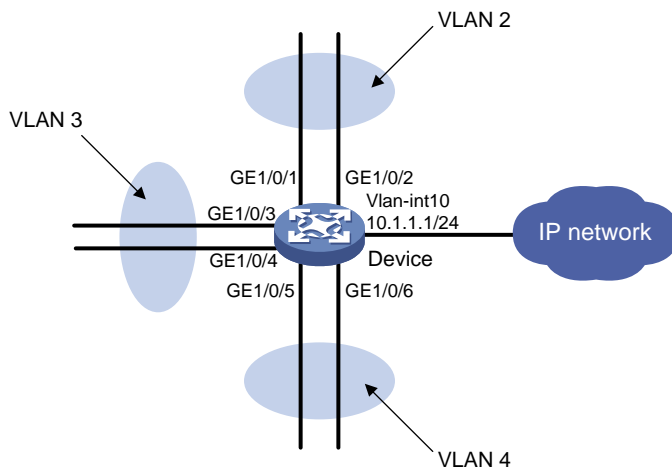
# 例:ARP 送信元 IP アドレスチェックの設定

## ネットワーク構成

図 18 に示すように、次のタスクを実行します。

- スーパーVLAN を作成し、VLAN 2、3、および 4 に関連付けます。VLAN 2、3、および 4 はレイヤ 2 で分離されていますが、レイヤ 3 で相互運用可能です。VLAN 2、3、および 4 のすべてのホストは、レイヤ 3 通信にゲートウェイ IP アドレス 10.1.1.1/24 を使用します。
- VLAN 2 で ARP 送信元 IP アドレスチェック機能を設定し、送信元 IP アドレス範囲 10.1.1.1～10.1.1.10 を指定します。

図 18 ネットワークダイアグラム



## 手順

#VLAN 10 を作成します。

```
<Device> system-view
[Device] vlan 10
[Device-vlan10] quit
```

#VLAN-interface 10 を作成し、IP アドレス 10.1.1.1/24 を割り当てます。

```
[Device] interface vlan-interface 10
[Device-Vlan-interface10] ip address 10.1.1.1 255.255.255.0
[Device] quit
```

#VLAN 2 を作成し、GigabitEthernet 1/0/1 と GigabitEthernet 1/0/2 を VLAN に割り当てます。

```
[Device] vlan 2
[Device-vlan2] port gigabitethernet 1/0/1 gigabitethernet 1/0/2
[Device-vlan2] quit
```

#VLAN 3 を作成し、GigabitEthernet 1/0/3 と GigabitEthernet 1/0/4 を VLAN に割り当てます。

```
[Device] vlan 3
[Device-vlan3] port gigabitethernet 1/0/3 gigabitethernet 1/0/4
[Device-vlan3] quit
```

#VLAN 4 を作成し、GigabitEthernet 1/0/5 と GigabitEthernet 1/0/6 を VLAN に割り当てます。

```
[Device] vlan 4
[Device-vlan4] port gigabitethernet 1/0/5 gigabitethernet 1/0/6
[Device-vlan4] quit
```



#VLAN 10 をスーパーVLAN として設定し、サブ VLAN 2、3、および 4 をスーパーVLAN に関連付けます。

```
[Device] vlan 10
[Device-vlan10] supervlan
[Device-vlan10] subvlan 2 3 4
[Device-vlan10] quit
```

#VLAN 2 で ARP 送信元 IP アドレスチェック機能をイネーブルにし、IP アドレス範囲 10.1.1.1～10.1.1.10 を指定します。

```
[Device] vlan 2
[Device-vlan2] arp sender-ip-range 10.1.1.1 10.1.1.10
```

## 設定の確認

#デバイスが、送信元 IP アドレスが指定されたアドレス範囲 10. 1.1.1～10. 1.1.10 内にある ARP パケットだけを受け入れることを確認します。デバイスは、範囲外の送信元 IP アドレスを持つ ARP パケットを破棄します。

# ND 攻撃防御の設定

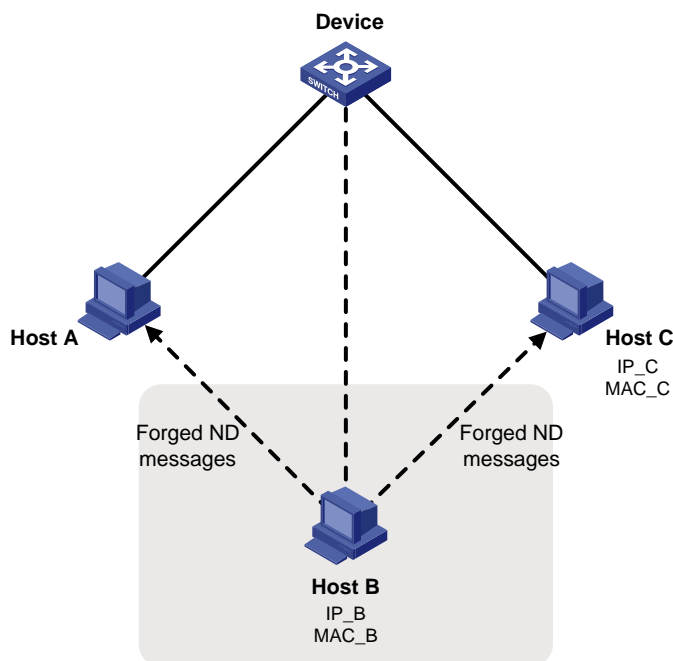
## ND攻撃防御について

IPv6 近隣探索(ND)攻撃防御では、偽造された ND メッセージを識別して、ND 攻撃を防ぐことができる。

IPv6 ND プロトコルはセキュリティメカニズムを提供せず、ネットワーク攻撃に対して脆弱です。図 19 に示すように、攻撃者は ND 攻撃を実行するために次の偽造 ICMPv6 メッセージを送信できます。

- 被害ホストの IPv6 アドレスを持つ偽造された NS/NA/RS メッセージ。ゲートウェイと他のホストは、不正なアドレス情報で被害の ND エントリを更新します。その結果、被害を目的としたすべてのパケットが攻撃端末に送信されます。
- ビクティムゲートウェイの IPv6 アドレスを使用した偽造 RA メッセージ。その結果、ビクティムゲートウェイに接続されているすべてのホストは、不正な IPv6 設定パラメータと ND エントリを保持します。

図 19 ND アタックダイヤグラム



## ND攻撃防御タスク一覧

すべての ND 攻撃防御タスクはオプションです。

- ND メッセージの送信元 MAC 整合性チェックのイネーブル化
- ND 攻撃検出の設定

# NDメッセージの送信元MAC整合性チェックのイネーブル化

## 送信元 MAC 整合性チェックについて

通常、送信元 MAC 整合性チェック機能は、ND 攻撃を防止するためにゲートウェイで設定されます。

この機能は、各着信 ND メッセージの一貫性について、送信元 MAC アドレスと送信元リンクレイヤアドレスをチェックします。

- 送信元 MAC アドレスと送信元リンクレイヤアドレスが同じでない場合、デバイスはパケットをドロップします。
- アドレスが同じ場合、デバイスは ND エントリの学習を継続します。

ND ロギング機能は、送信元 MAC 不一致イベントを記録し、ログメッセージをインフォメーションセンターに送信します。インフォメーションセンターは、さまざまな送信元モジュールからさまざまな宛先にログメッセージを出力できます。インフォメーションセンターの詳細については、『Network Management and Monitoring 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. ND メッセージの送信元 MAC 整合性チェックをイネーブルにします。

```
ipv6 nd mac-check enable
```

デフォルトでは、ND メッセージの送信元 MAC 整合性チェックはディセーブルになっています。

3. (任意)ND ロギング機能をイネーブルにします。

```
ipv6 nd check log enable
```

デフォルトでは、ND ロギング機能はディセーブルになっています。

過剰な ND ログを回避するには、ND ロギング機能をディセーブルにすることを推奨します。

# ND攻撃検出の設定

## ND 攻撃検出について

ND 攻撃検出は、スプーフィング攻撃を防止するために、着信 ND メッセージのユーザー有効性をチェックします。通常、アクセスデバイスで設定されます。

ND 攻撃検出では、次のタイプのインターフェイスが定義されます。

- ND 信頼インターフェイス: デバイスは、ND 信頼インターフェイスで受信した ND メッセージまたはデータパケットを直接転送します。ユーザーの有効性チェックは実行しません。
- ND untrusted インターフェイス: デバイスは RA を廃棄し、ND untrusted インターフェイスで受信されたメッセージをリダイレクトします。ND untrusted インターフェイスで受信された他のタイプの ND メッセージについては、デバイスはユーザーの有効性をチェックします。

ND 攻撃検出では、着信 ND メッセージ内の送信元 IPv6 アドレスと送信元 MAC アドレスが、他のモジュールからのセキュリティエントリと比較されます。

- 一致が検出された場合、デバイスは受信側 VLAN でユーザーが正当であることを確認し、パケットを転送します。

- 一致するものが見つからない場合、デバイスはユーザーが不正であることを確認し、ND メッセージを廃棄します。

ND 攻撃検出では、スタティック IPv6 ソースガードバインディングエントリ、ND スヌーピングエントリ、および DHCPv6 スヌーピングエントリを使用して、ユーザーの有効性をチェックします。

スタティック ipv6 ソースガードバインディングエントリは、ipv6 source binding コマンドを使用して作成されます。ipv6 ソースガードの詳細については、「IP ソースガードの設定」を参照してください。DHCPv6 スヌーピングの詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。ND スヌーピングの詳細については、『Layer 3 IP Services Configuration Guide』を参照してください。

## 制限事項およびガイドライン

ND 攻撃検出を設定する場合は、次の制約事項およびガイドラインに従ってください。

- ND 非信頼インターフェイスが受信したすべての ND メッセージをドロップしないようにするには、IPv6 ソースガードスタティックバインディング、DHCPv6 スヌーピング、および ND スヌーピングのうち 1 つ以上の機能が設定されていることを確認します。
- ND 攻撃の検出で IPv6 ソースガードスタティックバインディングを有効にするには、次の操作を実行する必要があります。
  - ipv6 source binding コマンドに vlan vlan-id オプションを指定します。
  - 同じ VLAN に対して ND 攻撃検出をイネーブルにします。

## 手順

1. システムビューに入ります。  
**system-view**
2. VLAN ビューを開始します。  
**vlan** *vlan-id*
3. ND 攻撃検出をイネーブルにします。  
**ipv6 nd detection enable**  
デフォルトでは、ND 攻撃検出はディセーブルになっています。
4. (任意)インターフェイスを ND trusted インターフェイスとして設定します。
  - a. システムビューに戻ります。  
**quit**
  - b. レイヤ 2 イーサネットまたは集約インターフェイスビューを開始します。  
**interface** *interface-type interface-number*
  - c. インターフェイスを ND trusted インターフェイスとして設定します。  
**ipv6 nd detection trust**  
デフォルトでは、すべてのインターフェイスが ND untrusted インターフェイスです。

# ND 攻撃検出用の表示およびメンテナンスコマンド

任意のビューで display 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。

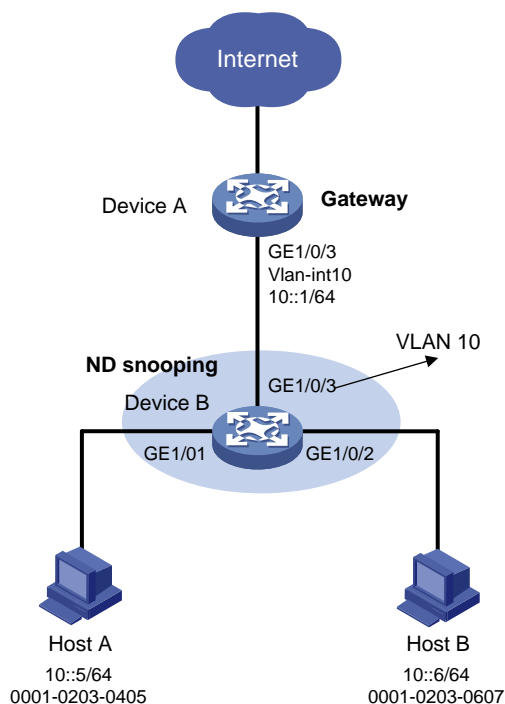
タスク	コマンド
ND攻撃検出によってドロップされたNDメッセージの統計情報を表示します。	<code>display ipv6 nd detection statistics</code> [ <code>interface interface-type interface-number</code> ]
ND攻撃検出統計情報をクリアします。	<code>reset ipv6 nd detection statistics</code> [ <code>interface interface-type interface-number</code> ]

## 例:ND 攻撃検出の設定

### ネットワーク構成

図 20 に示すように、デバイス B で ND 攻撃検出を設定して、ホスト A およびホスト B からの ND メッセージのユーザー有効性をチェックします。

図 20 ネットワークダイアグラム



### 手順

1. デバイス A を構成します。  
#VLAN 10 を作成します。  

```
<DeviceA> system-view  
[DeviceA] vlan 10  
[DeviceA-vlan10] quit
```

  
# GigabitEthernet 1/0/1 で VLAN 10 をトランクするように設定します。  

```
[DeviceA] interface gigabitethernet 1/0/3
```

```
[DeviceA-GigabitEthernet1/0/3] port link-type trunk
[DeviceA-GigabitEthernet1/0/3] port trunk permit vlan 10
[DeviceA-GigabitEthernet1/0/3] quit
```

#IPv6 アドレス 10::1/64 を VLAN インターフェイス 10 に割り当てます。

```
[DeviceA-Vlan-interface10] ipv6 address 10::1/64
[DeviceA-Vlan-interface10] quit
```

## 2. デバイス B を構成します。

#VLAN 10 を作成します。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
```

#VLAN 10 をトランクするように、GigabitEthernet 1/0/1、GigabitEthernet 1/0/3、および GigabitEthernet 1/0/3 を設定します。

```
<DeviceB> system-view
[DeviceB] vlan 10
[DeviceB-vlan10] quit
```

# Configure GigabitEthernet 1/0/1, GigabitEthernet 1/0/2, and GigabitEthernet 1/0/3 to trunk VLAN 10.

```
[DeviceB] interface gigabitethernet 1/0/1
[DeviceB-GigabitEthernet1/0/1] port link-type access
[DeviceB-GigabitEthernet1/0/1] port access vlan 10
[DeviceB-GigabitEthernet1/0/1] quit
[DeviceB] interface gigabitethernet 1/0/2
[DeviceB-GigabitEthernet1/0/2] port link-type access
[DeviceB-GigabitEthernet1/0/2] port access vlan 10
[DeviceB-GigabitEthernet1/0/2] quit
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] port link-type trunk
[DeviceB-GigabitEthernet1/0/3] port trunk permit vlan 10
[DeviceB-GigabitEthernet1/0/3] quit
```

#VLAN 10 の ND 攻撃検出を有効にします。

```
[DeviceB] vlan 10
[DeviceB-vlan10] ipv6 nd detection enable
```

#VLAN 10 で、IPv6 グローバルユニキャストアドレスの ND スヌーピングおよび IPv6 リンクローカルアドレスの ND スヌーピングをイネーブルにします。

```
[DeviceB-vlan10] ipv6 nd snooping enable global
[DeviceB-vlan10] ipv6 nd snooping enable link-local
[DeviceB-vlan10] quit
```

# GigabitEthernet 1/0/3 を ND trusted インターフェイスとして設定します。

```
[DeviceB] interface gigabitethernet 1/0/3
[DeviceB-GigabitEthernet1/0/3] ipv6 nd detection trust
```

## 設定の確認

GigabitEthernet 1/0/1、GigabitEthernet 1/0/2、GigabitEthernet 1/0/3 デバイス B が、ND スヌーピングエントリに基づいて、で受信されたすべての ND メッセージを検査することを確認します(詳細は表示されません)。

# uRPF の設定

## uRPFについて

ユニキャスト Reverse Path Forwarding(uRPF)は、DoS 攻撃や DDoS 攻撃などの送信元アドレススプーフィング攻撃からネットワークを保護します。

## uRPF アプリケーションのシナリオ

攻撃者は、許可されたユーザーまたは管理者の名前で、IPv 4 ベースの認証を使用するシステムにアクセスするために、偽造された送信元アドレスを持つパケットを送信します。攻撃者または他のホストが応答パケットを受信できない場合でも、攻撃は攻撃されたターゲットを混乱させます。

図 21 送信元アドレススプーフィング攻撃

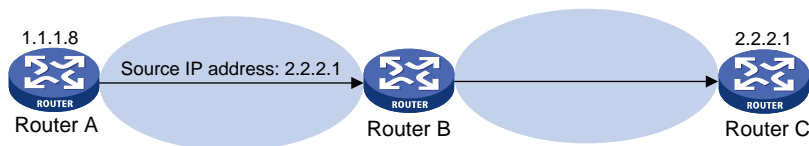


図 21 に示すように、ルーターA の攻撃者は、偽造された送信元 IP アドレス 2.2.2.1 を含むサーバー(ルーターB)要求を高いレートで送信します。ルーターB は、IP アドレス 2.2.2.1(ルーターC)に応答パケットを送信します。その結果、ルーターB とルーターC の両方が攻撃されます。管理者が誤ってルーターC を切断すると、ネットワークサービスが中断されます。

攻撃者は、異なる偽造された送信元アドレスを持つパケットを送信したり、複数のサーバーを同時に攻撃して接続をブロックしたり、ネットワークを破壊したりすることもできます。

uRPF は、これらの送信元アドレススプーフィング攻撃を防ぐことができます。uRPF は、パケットを受信するインターフェイスが、パケットの送信元アドレスと一致する FIB エントリの出カインターフェイスであるかどうかを確認します。一致しない場合、uRPF はスプーフィング攻撃と見なし、パケットを廃棄します。

## uRPF チェックモード

uRPF は、strict モードと loose モードをサポートします。

### 厳密な uRPF チェック

厳密な uRPF チェックに合格するには、パケットの送信元アドレスと受信インターフェイスが、FIB エントリの宛先アドレスと出カインターフェイスに一致する必要があります。一部のシナリオ(非対称ルーティングなど)では、厳密な uRPF によって有効なパケットが廃棄される場合があります。

Strict uRPF は、多くの場合、PE と CE の間に配置されます。

### Loose uRPF チェック

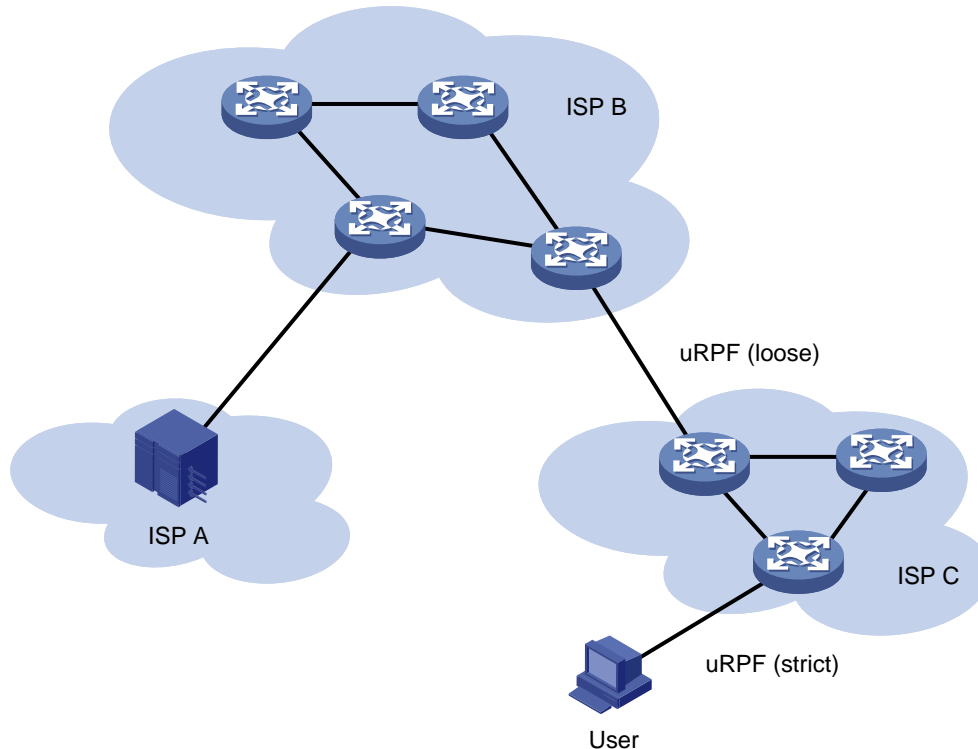
Loose uRPF チェックを通過するには、パケットの送信元アドレスが FIB エントリの宛先アドレスと一致する必要があります。Loose uRPF では、有効なパケットの廃棄を回避できますが、攻撃パケットが廃棄される可能性があります。

Loose uRPF は、特に非対称ルーティングでは、ISP 間で展開されることがよくあります。

## ネットワークアプリケーション

図 22 に示すように、ISP ネットワークとカスタマーネットワークの間には、厳密な uRPF チェックが設定されています。ISP 間には、緩やかな uRPF チェックが設定されています。

図 22 ネットワークダイアグラム



## uRPFのグローバルなイネーブル化

### 制限事項およびガイドライン

グローバル uRPF は、デバイスのすべてのインターフェイスで有効になります。

### 手順

1. システムビューに入ります。

```
system-view
```

2. uRPF をグローバルにイネーブルにします。

```
ip urpf { loose [ acl acl-number ] | strict [ allow-default-route ] [ acl  
acl-number ] }
```

デフォルトでは、uRPF はディセーブルです。

## インターフェイスでのuRPFのイネーブル化

1. システムビューに入ります。

```
system-view
```

2. インターフェイスビューを入力します。



```
interface interface-type interface-number
```

3. uRPFをイネーブルにします。

```
ip urpf { loose [ allow-default-route ] | strict }
```

デフォルトでは、uRPFはディセーブルです。

## uRPF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ます。

タスク	コマンド
uRPF設定を表示します。	<b>display ip urpf</b> [ <b>slot</b> <i>slot-number</i> ]