第 6 編 AccessDefender

1. AccessDefender の機能説明

AccessDefender の機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

1.1 AccessDefender の概要

AccessDefender は、装置と RADIUS サーバーの構成で、内部ネットワークにアクセスできるクライアントを認証する機能です。RADIUS サーバーを認証サーバーとして使用し、アクセスしてきたクライアントを認証したうえで、内部ネットワークへの接続を許可します。これにより、不正なクライアントが、装置のポートを通じて内部ネットワークに接続することを制限できます。

1.2 サポートする認証方法

AccessDefender は、以下の認証方法および DHCP スヌーピングをサポートしています。

表 1-1 AccessDefender がサポートする認証方法

機能	MAC 認証	Web 認証	ゲートウェイ認証	IEEE 802.1X 認証
制御レイヤー	レイヤー 2（MAC アドレスベース）	レイヤー 2（MAC アドレスベース）	レイヤー 3（IP アドレスベース）	レイヤー 2（MAC アドレスベース）
認証の仕組み	端末認証	ユーザー認証	ユーザー認証	ユーザー認証、端末認証
電子証明書の利用	×	○	○	○
認証サーバー	RADIUS	RADIUS	RADIUS	RADIUS（EAP 対応）
ローカルデータベース	○	○	○	×
アプリケーション	なし	Web ブラウザー	Web ブラウザー	IEEE 802.1X 認証対応ソフトウェア（以後、サプリカント）
ダイナミック VLAN*1 *2	○	○	×	○
ユーザーポリシーコントロール（クラス ID）	○	○	×	○
アクセスハブ、無線アクセスポイント	○	○	○	○ *3
ルーター、L3 スイッチ、WAN 経由の認証	×	×	○	×

*1：認証に成功したクライアントごとに、ダイナミックに VLAN を割り当てることができます。VLAN をダイナミックに割り当てる場合、割り当てる VLAN をあらかじめ作成しておく必要があります。

*2：ダイナミック VLAN を使用する際、設定した最大認証クライアント数に満たない場合でも、VLAN 割り当て時にテーブルのエントリーが重複して、ログインに失敗する場合があります。

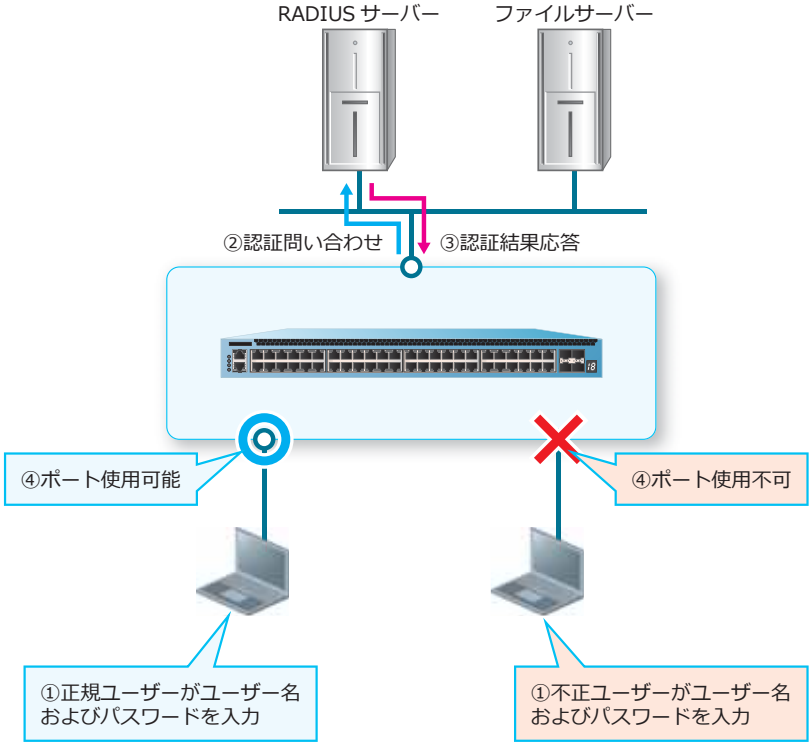
*3：EAPOL 透過スイッチが必要です。

1.2.1 ユーザー認証

ユーザー認証は、未認証状態のユーザーが内部ネットワークに接続する前に、ユーザー名およびパスワードを入力して、正規のユーザーだけに内部ネットワークへのアクセスを許可する仕組みです。

装置は、未認証状態のユーザーからアクセスされると、ユーザー名およびパスワードの入力を要求します。次に、ユーザー名およびパスワードを基に、ユーザーに内部ネットワークへのアクセスを許可してよいかどうかを決定します。

図 1-1 ユーザー認証による不正ユーザーのブロック



1.2.2 端末認証

端末認証は、未認証状態の端末が内部ネットワークに接続する際に、端末の MAC アドレスなどを利用して、正規の端末だけに内部ネットワークへのアクセスを許可する仕組みです。

装置は、未認証状態の端末からアクセスされると、MAC アドレスなどを利用して、端末に内部ネットワークへのアクセスを許可してよいかどうかを決定します。

1.3 認証バイパス

IP 電話の使用時に認証なしで通信を許可したり、Web 認証前に DHCP サーバーから IP アドレスを取得するための通信を許可したりするなど、認証前の状態でも通信ができるようにするには、**認証バイパス設定**を行います。

認証バイパス設定を行うには、認証バイパス設定用のアクセスリストのエントリーを作成します。認証バイパス設定用のアクセスリストのエントリーを作成するには、**`permit`** コマンドで authentication-bypass パラメーターを指定します。

REF: アクセスリストについては、「第 4 編 レイヤー 2」の「アクセスリスト」を参照してください。

NOTE: 認証バイパスは、ingress のアクセスリストでのみサポートしています。

NOTE: MAC 認証と関係なく CPU 宛てにコピーされるパケットは、たとえ認証バイパスにマッチしても CPU コピーされることに注意してください。

1.3.1 Windows ドメイン環境への適用

Windows ドメイン環境において、Web ブラウザーを使用するネットワーク認証を利用する場合は、認証バイパス設定を行い、Windows へログオンする前にドメインコントローラーとの通信を許可します。

1.4 ダイナミック VLAN

認証に成功して属性値として VLAN ID が通知された場合は、認証に成功したクライアントごとに、受信する VLAN をダイナミックに割り当てることができます。これにより、会議室などの共有スペースに設置された装置に接続した場合でも、自分が所属する VLAN に直接接続できるようになります。また、同一ポートに複数の VLAN を割り当てることもできます。

REF: RADIUS サーバーで「ダイナミックに割り当てる VLAN ID」を設定する方法については、「AccessDefender の認証方式」の「RADIUS 認証」を参照してください。

CAUTION: ゲートウェイ認証では、ダイナミック VLAN はサポートしていません。

CAUTION: NP7000、NP5000、NP4000、NP3000、NP2000（1.04.01 より前のバージョン）、および NP2500 では、トランクポートでのダイナミック VLAN はサポートしていません。

CAUTION: NP2100 および NP2000（1.04.01 以降）では、トランクポートでのタグなし形式のフレームに対するダイナミック VLAN をサポートしました。トランクポートで認証に成功してダイナミックに VLAN が割り当てられた場合、その VLAN はアクセスポートとして動作します（タグなしフレームを送受信）。ダイナミックに割り当てられた VLAN が **`switchport trunk allowed vlan`** コマンドで割り当てられていると、当該ポートから送信するフレームがタグ付きフレームになるため、そのポートでは **`switchport trunk allowed vlan`** コマンドで対象の VLAN を割り当てずに使用してください。

NOTE: ダイナミックに割り当てる VLAN は、あらかじめ作成しておく必要があります。

1.4.1 AccessDefender の VLAN モード

`vlan mode` コマンドで、AccessDefender の VLAN モードを変更できます。デフォルト設定の場合は、ダイナミック VLAN により同一ポートに複数の VLAN を割り当てることができます。

VLAN モードを static モードに設定した場合は、ダイナミック VLAN 動作を禁止できます。認証に成功して属性値として VLAN ID が通知された場合でも、ダイナミック VLAN は動作せず、元々対象ポートに設定されていた VLAN が割り当てられます。

VLAN モードを dynamic port-base モードに設定した場合は、2 台目以降の認証クライアントのダイナミック VLAN 動作を制限するモードになります。dynamic port-base モードの場合の動作を以下に示します。

表 1-2 dynamic port-base モードの場合の動作

ログイン中の クライアントの VLAN	同一ポートで後から認証を行うクライアント	ログイン 可否
対象ポートに元々設定されている VLAN	VLAN ID の通知なし	可
	属性値として VLAN ID（ログイン中のクライアントと同じ VLAN）の通知あり	可
	属性値として VLAN ID（ログイン中のクライアントと異なる VLAN）の通知あり	不可
対象ポートに元々設定されている VLAN と異なる VLAN	VLAN ID の通知なし	不可
	属性値として VLAN ID（ログイン中のクライアントと同じ VLAN）の通知あり	可
	属性値として VLAN ID（ログイン中のクライアントと異なる VLAN）の通知あり	不可

1.5 ユーザーポリシーコントロール

認証成功時に割り当てられる属性値にクラス ID が含まれている場合、そのクラス ID が認証済みクライアントに関連付けられます。関連付けられたクラス ID は、アクセスリストの抽出条件として使用することができるため、アクセスリストの **permit** コマンドおよび **deny** コマンドを使用して、クラス ID ごとにアクセス制限を設定できます（ユーザーポリシーコントロール）。

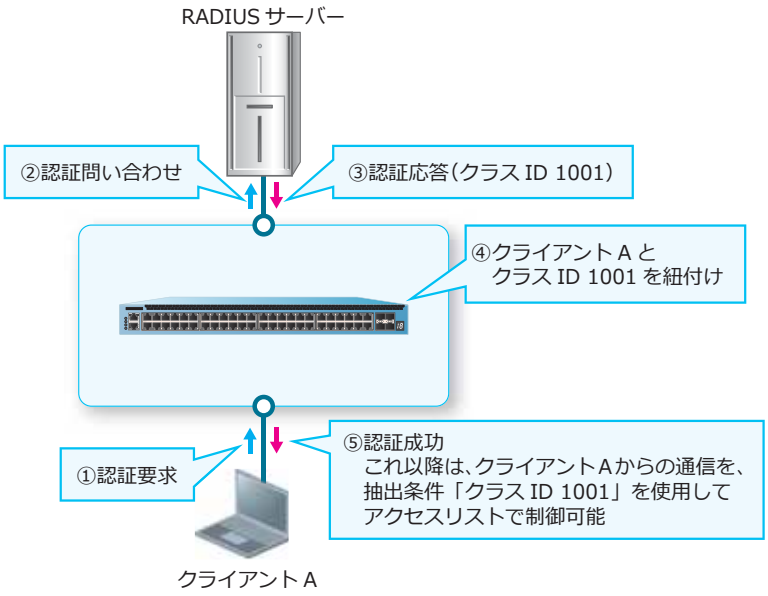
REF: RADIUS サーバーでクラス ID を設定する方法については、「AccessDefender の認証方式」の「RADIUS 認証」を参照してください。

CAUTION: ゲートウェイ認証では、クラス ID の割り当てはサポートしていません。

CAUTION: NP7000、NP5000、および NP3000 では、IP アクセスリストではクラス ID 条件はサポートしていません。

CAUTION: クラス ID 条件は、ingress のアクセスリストでのみサポートしています。

図 1-2 ユーザーポリシーコントロールの動作例



1.6 AccessDefender の主な仕様

AccessDefender の主な仕様は以下のとおりです。

表 1-3 AccessDefender の主な仕様

項目		仕様
認証方法		MAC 認証、Web 認証、ゲートウェイ認証、IEEE 802.1X 認証（EAP-MD5、PEAP、EAP-TTLS、EAP-TLS）
認証サーバー	対応サーバー	RADIUS サーバー
	バックアップ	RADIUS サーバーグループ、ローカルデータベース認証 *1、強制認証 *1
	ローカルデータベース	最大 3,000 アカウント （ファイルサイズは 245,600 バイト以下）
最大接続可能クライアント *2	MAC 認証、Web 認証、ゲートウェイ認証、IEEE 802.1X 認証	NP7000 および NP5000：2,048（IPv4） NP3000：1,536（IPv4） NP4000 および NP2500：768（IPv4） NP2100 および NP2000：768
	ダイナミック VLAN	NP7000 および NP5000：2,048（IPv4） NP3000：1,536（IPv4） NP4000 および NP2500：768（IPv4） NP2100 および NP2000：768
	クラス ID	NP7000：1,024 NP5000：2,048 NP3000：1,536 NP4000、NP2100、NP2000、および NP2500：512
	DHCP スヌーピング	400 クライアント ※ クライアントの最大数は、ダイナミックエントリーとスタティックエントリーで共有です。
その他	Discard 登録数	200*3
	Web 認証の認証ページリダイレクト	HTTP/HTTPS*4 対応 HTTP プロキシ対応 *5 外部 Web サーバーへのリダイレクト
	Web 認証の認証ページカスタマイズ	装置内部の認証ページカスタマイズ対応 外部サーバーの認証ページ対応
	IP アドレス割り当て方式	固定 IP アドレス、DHCP による割り当て *6
	VLAN 環境	固定 VLAN、ダイナミック VLAN
	認証バイパス設定	アクセスリストの許可エントリーを使用して、条件に一致したパケットの認証を省略可能
	認証クライアントの制限	認証拒否、TTL フィルター

*1：ローカルデータベース認証および強制認証は単独で使用できます。

*2：アクセスリストのリソースを使用する他機能の使用状況などにより、使用可能な最大数が異なる場合があります。また、NP2100 の 1.11.01 以降、NP2500 の 1.11.01 以降では、**total-client** コマンドの ipv6-disable オプションを使用すると、接続可能クライアント数は最大 1,024 まで設定できます。

*3：Discard 登録には ACL のリソースは消費しません。

*4：未認証クライアントからの HTTPS アクセスをリダイレクトする場合には、Web ブラウザーに証明書エラーに関わる警告が表示される場合がありますが、これは HTTPS の仕様によるものです。証明書エラーに関わる警告が表示されても、Web ブラウザーで許可する操作を実施することにより、認証ページにリダイレクトされます。

*5：HTTPS はリダイレクトされません。

*6：Web 認証でダイナミック VLAN を使用する場合は、認証後に VLAN が変更されるため、DHCP クライアントでの使用が前提になります。

1.7 アクセスリストグループと最大認証クライアント数

AccessDefender を有効にすると、AccessDefender の制御用および認証クライアント用にアクセスリストの Ingress グループのリソースが使用されます。各機種ごとのアクセスリストグループと最大認証クライアント数について、以下に示します。

1.7.1 アクセスリストグループと最大認証クライアント数（NP7000）

NP7000 で AccessDefender を有効にすると、制御用に 3 個のグループが使用されます。装置全体の最大認証クライアント数を設定するには、**total-client** コマンドを使用します。このときの設定値により、さらに 1 ～ 7 個のグループが使用されます。

total-client コマンドを最大値の 2,048 で設定した場合には、10 個のグループが AccessDefender で使用されます。

AccessDefender で使用するグループは以下のとおりです。

表 1-4 AccessDefender で使用するグループ（NP7000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）*1	257 ～ 512 クライアント
7	認証クライアント用（任意）*1	513 ～ 768 クライアント
8	認証クライアント用（任意）*1	769 ～ 1,024 クライアント
9	認証クライアント用（任意）*1	1,025 ～ 1,536 クライアント
10	認証クライアント用（任意）*1	1,537 ～ 2,048 クライアント

*1：最大認証クライアント数を制限することで、未使用グループにすることができます。未使用グループは、認証バイパス設定やアクセスリストのエントリーなどで使用できます。

NOTE: すべての認証機能（Web 認証、MAC 認証、IEEE 802.1X 認証、および DHCP スヌーピング）を無効にしてから、**`total-client`** コマンドを使用してください。

NOTE: Web 認証の場合は、認証バイパス設定などを利用するために、最大認証クライアント数を 1,536 クライアント以下に設定し、最低 1 グループは未使用グループにすることを推奨します。

NOTE: インターフェースごとに最大認証クライアント数を設定することもできます。インターフェースごとに最大認証クライアント数を設定するには、**`max-client interface`** コマンドを使用します。

DHCP スヌーピングでは、他の認証とアクセスリストの Ingress グループのリソースの使い方が異なります。最大認証クライアント数は 400 です。

DHCP スヌーピングで使用するグループは、以下のとおりです。

表 1-5 DHCP スヌーピングで使用するグループ（NP7000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）	257 ～ 400 クライアント
7	–	
8	–	
9	–	
10	–	

1.7.2 アクセスリストグループと最大認証クライアント数（NP5000）

NP5000 で AccessDefender を有効にすると、制御用に 3 個のグループが使用されます。装置全体の最大認証クライアント数を設定するには、**`total-client`** コマンドを使用します。このときの設定値により、さらに 1 ～ 9 個のグループが使用されます。

`total-client` コマンドを最大値の 2,048 で設定した場合には、12 個のグループが AccessDefender で使用されます。

AccessDefender で使用するグループは以下のとおりです。

表 1-6 AccessDefender で使用するグループ（NP5000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	

使用する グループ数	用途	最大認証クライアント数
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）*1	257 ～ 512 クライアント
7	認証クライアント用（任意）*1	513 ～ 768 クライアント
8	認証クライアント用（任意）*1	769 ～ 1,024 クライアント
9	認証クライアント用（任意）*1	1,025 ～ 1,280 クライアント
10	認証クライアント用（任意）*1	1,281 ～ 1,536 クライアント
11	認証クライアント用（任意）*1	1,537 ～ 1,792 クライアント
12	認証クライアント用（任意）*1	1,793 ～ 2,048 クライアント

*1：最大認証クライアント数を制限することで、未使用グループにすることができます。未使用グループは、認証バイパス設定やアクセスリストのエントリーなどで使用できます。

NOTE: すべての認証機能（Web 認証、MAC 認証、IEEE 802.1X 認証、および DHCP スヌーピング）を無効にしてから、**`total-client`** コマンドを使用してください。

NOTE: Web 認証の場合は、認証バイパス設定などを利用するために、最大認証クライアント数を 1,792 クライアント以下に設定し、最低 1 グループは未使用グループにすることを推奨します。

NOTE: インターフェースごとに最大認証クライアント数を設定することもできます。インターフェースごとに最大認証クライアント数を設定するには、**`max-client interface`** コマンドを使用します。

DHCP スヌーピングでは、他の認証とアクセスリストの Ingress グループのリソースの使い方が異なります。最大認証クライアント数は 400 です。

DHCP スヌーピングで使用するグループは、以下のとおりです。

表 1-7 DHCP スヌーピングで使用するグループ（NP5000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）	257 ～ 400 クライアント
7	–	

使用する グループ数	用途	最大認証クライアント数
8	–	
9	–	
10	–	
11	–	
12	–	

1.7.3 アクセスリストグループと最大認証クライアント数（NP4000）

NP4000 で AccessDefender を有効にすると、制御用に 3 個のグループが使用されます。装置全体の最大認証クライアント数を設定するには、**`total-client`** コマンドを使用します。このときの設定値により、さらに 1 ～ 7 個のグループが使用されます。

`total-client` コマンドを最大値の 768 で設定した場合には、10 個のグループが AccessDefender で使用されます。

AccessDefender で使用するグループは以下のとおりです。

表 1-8 AccessDefender で使用するグループ（NP4000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 128 クライアント
5	認証クライアント用（必須）	1 ～ 128 クライアント
6	認証クライアント用（任意）*1	129 ～ 256 クライアント
7	認証クライアント用（任意）*1	257 ～ 384 クライアント
8	認証クライアント用（任意）*1	385 ～ 512 クライアント
9	認証クライアント用（任意）*1	513 ～ 640 クライアント
10	認証クライアント用（任意）*1	641 ～ 768 クライアント
11	AccessDefender 制御用 III（任意）	*2
12	–	
13	–	
14	–	
15	–	

*1：最大認証クライアント数を制限することで、未使用グループにすることができます。未使用グループは、認証バイパス設定やアクセスリストのエントリーなどで使用できます。

*2：MAC 認証の Discard エントリーが 124 ～ 127 個（ループ検知やポートリダンダントの FDB フラッシュフレーム送受信機能の設定有無によって個数は異なります）以上登録される場合に、追加で割り当てられます。

> ***NOTE:*** すべての認証機能（Web 認証、MAC 認証、IEEE 802.1X 認証、および DHCP スヌーピング）を無効にしてから、**`total-client`** コマンドを使用してください。
>
> ***NOTE:*** インターフェースごとに最大認証クライアント数を設定することもできます。インターフェースごとに最大認証クライアント数を設定するには、**`max-client interface`** コマンドを使用します。

DHCP スヌーピングでは、他の認証とアクセスリストの Ingress グループのリソースの使い方が異なります。最大認証クライアント数は 400 です。

DHCP スヌーピングで使用するグループは以下のとおりです。

表 1-9 DHCP スヌーピングで使用するグループ（NP4000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	AccessDefender 制御用 II（任意）	*1
5	AccessDefender 制御用 II（任意）	*2
6	認証クライアント用（必須）	1 ～ 128 クライアント
7	認証クライアント用（必須）	1 ～ 128 クライアント
8	認証クライアント用（任意）	129 ～ 256 クライアント
9	認証クライアント用（任意）	257 ～ 384 クライアント
10	認証クライアント用（任意）	385 ～ 400 クライアント
11	–	
12	–	
13	–	
14	–	
15	–	

*1：252 ～ 379 クライアント登録時に、追加で割り当てられます。

*2：380 ～ 400 クライアント登録時に、追加で割り当てられます。

1.7.4 アクセスリストグループと最大認証クライアント数（NP3000）

NP3000 で AccessDefender を有効にすると、制御用に 3 個のグループが使用されます。装置全体の最大認証クライアント数を設定するには、**total-client** コマンドを使用します。このときの設定値により、さらに 1 ～ 7 個のグループが使用されます。

total-client コマンドを最大値の 1,536 で設定した場合には、10 個のグループが AccessDefender で使用されます。

AccessDefender で使用するグループは以下のとおりです。

表 1-10 AccessDefender で使用するグループ（NP3000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）*1	257 ～ 512 クライアント
7	認証クライアント用（任意）*1	513 ～ 768 クライアント
8	認証クライアント用（任意）*1	769 ～ 1,024 クライアント
9	認証クライアント用（任意）*1	1,025 ～ 1,280 クライアント
10	認証クライアント用（任意）*1	1,281 ～ 1,536 クライアント

*1：最大認証クライアント数を制限することで、未使用グループにすることができます。未使用グループは、認証バイパス設定やアクセスリストのエントリーなどで使用できます。

> ***NOTE:*** すべての認証機能（Web 認証、MAC 認証、IEEE 802.1X 認証、および DHCP スヌーピング）を無効にしてから、**total-client** コマンドを使用してください。
>
> ***NOTE:*** Web 認証の場合は、認証バイパス設定などを利用するために、最大認証クライアント数を 1,280 クライアント以下に設定し、最低 1 グループは未使用グループにすることを推奨します。
>
> ***NOTE:*** インターフェースごとに最大認証クライアント数を設定することもできます。インターフェースごとに最大認証クライアント数を設定するには、**max-client interface** コマンドを使用します。

DHCP スヌーピングでは、他の認証とアクセスリストの Ingress グループのリソースの使い方が異なります。最大認証クライアント数は 400 です。

DHCP スヌーピングで使用するグループは、以下のとおりです。

表 1-11 DHCP スヌーピングで使用するグループ（NP3000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	

使用する グループ数	用途	最大認証クライアント数
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）	257 ～ 400 クライアント
7	–	
8	–	
9	–	
10	–	

1.7.5 アクセスリストグループと最大認証クライアント数（NP2100）

NP2100 で AccessDefender を有効にすると、制御用に 3 個のグループが使用されます。装置全体の最大認証クライアント数を設定するには、**`total-client`** コマンドを使用します。このときの設定値により、さらに 1 ～ 4 個のグループが使用されます。

> ***NOTE:*** NP2100 の 1.11.01 以降では、**`total-client`** コマンドの ipv6-disable オプションをサポートしています。

NP2100 では、ipv6-disable オプションを使用して **`total-client`** コマンド設定する場合は、最大 1,024 まで設定できます。ipv6-disable オプションを使用しないで **`total-client`** コマンド設定する場合は、最大 768 まで設定できます。

ipv6-disable パラメーターを指定した場合は、IPv6 アドレス認証用のアクセスリストのリソースが予約されなくなります。この場合は IPv6 アドレス認証用のリソースが使えなくなるため、IPv6 アドレスによるゲートウェイ認証は使用できません。

ipv6-disable オプションを使用して **`total-client`** コマンドを最大値の 1,024 で設定した場合には、7 個のグループが AccessDefender で使用されます。AccessDefender で使用するグループは以下のとおりです。

表 1-12 ipv6-disabled オプション使用時の AccessDefender で使用するグループ（NP2100）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（任意）*1	257 ～ 512 クライアント
6	認証クライアント用（任意）*1	513 ～ 768 クライアント
7	認証クライアント用（任意）*1	769 ～ 1,024 クライアント

*1：最大認証クライアント数を制限することで、未使用グループにすることができます。未使用グループは、認証バイパス設定やアクセスリストのエントリーなどで使用できます。

ipv6-disable オプションを使用しないで **total-client** コマンドを最大値の 768 で設定した場合には、7 個のグループが AccessDefender で使用されます。AccessDefender で使用するグループは以下のとおりです。

表 1-13 AccessDefender で使用するグループ（NP2100）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント（IPv6 アドレス）用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）*1	257 ～ 512 クライアント
7	認証クライアント用（任意）*1	513 ～ 768 クライアント

*1：最大認証クライアント数を制限することで、未使用グループにすることができます。未使用グループは、認証バイパス設定やアクセスリストのエントリーなどで使用できます。

> ***NOTE:*** すべての認証機能（Web 認証、MAC 認証、IEEE 802.1X 認証、および DHCP スヌーピング）を無効にしてから、**total-client** コマンドを使用してください。
>
> ***NOTE:*** Web 認証の場合は、認証バイパス設定などを利用するために、最大認証クライアント数を 512 クライアント以下に設定し、最低 1 グループは未使用グループにすることを推奨します。
>
> ***NOTE:*** インターフェースごとに最大認証クライアント数を設定することもできます。インターフェースごとに最大認証クライアント数を設定するには、**max-client interface** コマンドを使用します。

DHCP スヌーピングでは、他の認証とアクセスリストの Ingress グループのリソースの使い方が異なります。最大認証クライアント数は 400 です。

DHCP スヌーピングで使用するグループは、以下のとおりです。

表 1-14 DHCP スヌーピングで使用するグループ（NP2100）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）	257 ～ 400 クライアント
7	–	

1.7.6 アクセスリストグループと最大認証クライアント数（NP2000）

NP2000 で AccessDefender を有効にすると、制御用に 3 個のグループが使用されます。装置全体の最大認証クライアント数を設定するには、**total-client** コマンドを使用します。このときの設定値により、さらに 1 ～ 4 個のグループが使用されます。

total-client コマンドを最大値の 768 で設定した場合には、7 個のグループが AccessDefender で使用されます。

AccessDefender で使用するグループは以下のとおりです。

表 1-15 AccessDefender で使用するグループ（NP2000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント（IPv6 アドレス）用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）*1	257 ～ 512 クライアント
7	認証クライアント用（任意）*1	513 ～ 768 クライアント

*1：最大認証クライアント数を制限することで、未使用グループにすることができます。未使用グループは、認証バイパス設定やアクセスリストのエントリーなどで使用できます。

NOTE: すべての認証機能（Web 認証、MAC 認証、IEEE 802.1X 認証、および DHCP スヌーピング）を無効にしてから、**total-client** コマンドを使用してください。

NOTE: Web 認証の場合は、認証バイパス設定などを利用するために、最大認証クライアント数を 512 クライアント以下に設定し、最低 1 グループは未使用グループにすることを推奨します。

NOTE: インターフェースごとに最大認証クライアント数を設定することもできます。インターフェースごとに最大認証クライアント数を設定するには、**max-client interface** コマンドを使用します。

DHCP スヌーピングでは、他の認証とアクセスリストの Ingress グループのリソースの使い方が異なります。最大認証クライアント数は 400 です。

DHCP スヌーピングで使用するグループは、以下のとおりです。

表 1-16 DHCP スヌーピングで使用するグループ（NP2000）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（必須）	1 ～ 256 クライアント

使用する グループ数	用途	最大認証クライアント数
6	認証クライアント用（任意）	257 ～ 400 クライアント
7	–	

1.7.7 アクセスリストグループと最大認証クライアント数（NP2500）

NP2500 で AccessDefender を有効にすると、制御用に 3 個のグループが使用されます。装置全体の最大認証クライアント数を設定するには、**total-client** コマンドを使用します。このときの設定値により、さらに 1 ～ 4 個のグループが使用されます。

> ***NOTE:*** NP2500 の 1.11.01 以降では、**total-client** コマンドの ipv6-disable オプションをサポートしています。

NP2500 では、ipv6-disable オプションを使用して **total-client** コマンド設定する場合は、最大 1,024 まで設定できます。ipv6-disable オプションを使用しないで **total-client** コマンド設定する場合は、最大 768 まで設定できます。

ipv6-disable パラメーターを指定した場合は、IPv6 アドレス認証用のアクセスリストのリソースが予約されなくなります。この場合は IPv6 アドレス認証用のリソースが使えなくなるため、IPv6 アドレスによるゲートウェイ認証は使用できません。

ipv6-disable オプションを使用して **total-client** コマンドを最大値の 1,024 で設定した場合には、7 個のグループが AccessDefender で使用されます。AccessDefender で使用するグループは以下のとおりです。

表 1-17 ipv6-disable オプション使用時の AccessDefender で使用するグループ（NP2500）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（任意）*1	257 ～ 512 クライアント
6	認証クライアント用（任意）*1	513 ～ 768 クライアント
7	認証クライアント用（任意）*1	769 ～ 1,024 クライアント

*1：最大認証クライアント数を制限することで、未使用グループにすることができます。未使用グループは、認証バイパス設定やアクセスリストのエントリーなどで使用できます。

ipv6-disable オプションを使用しないで **total-client** コマンドを最大値の 768 で設定した場合には、7 個のグループが AccessDefender で使用されます。AccessDefender で使用するグループは以下のとおりです。

表 1-18 AccessDefender で使用するグループ（NP2500）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント（IPv6 アドレス）用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）*1	257 ～ 512 クライアント
7	認証クライアント用（任意）*1	513 ～ 768 クライアント

*1：最大認証クライアント数を制限することで、未使用グループにすることができます。未使用グループは、認証バイパス設定やアクセスリストのエントリーなどで使用できます。

NOTE: すべての認証機能（Web 認証、MAC 認証、IEEE 802.1X 認証、および DHCP スヌーピング）を無効にしてから、**`total-client`** コマンドを使用してください。

NOTE: Web 認証の場合は、認証バイパス設定などを利用するために、最大認証クライアント数を 512 クライアント以下に設定し、最低 1 グループは未使用グループにすることを推奨します。

NOTE: インターフェースごとに最大認証クライアント数を設定することもできます。インターフェースごとに最大認証クライアント数を設定するには、**`max-client interface`** コマンドを使用します。

DHCP スヌーピングでは、他の認証とアクセスリストの Ingress グループのリソースの使い方が異なります。最大認証クライアント数は 400 です。

DHCP スヌーピングで使用するグループは、以下のとおりです。

表 1-19 DHCP スヌーピングで使用するグループ（NP2500）

使用する グループ数	用途	最大認証クライアント数
1	AccessDefender 制御用 I（必須）	
2	AccessDefender 制御用 II（必須）	
3	AccessDefender 制御用 III（必須）	
4	認証クライアント用（必須）	1 ～ 256 クライアント
5	認証クライアント用（必須）	1 ～ 256 クライアント
6	認証クライアント用（任意）	257 ～ 400 クライアント
7	–	

1.8 ログアウト方法

認証済みクライアントは様々な原因でログアウトします。認証済みクライアントをログアウトする方法および原因は、認証方法によって異なります。また、ログアウト方法や原因によって、SYSLOG サーバーに送信される文字列が異なります。

表 1-20 ログアウト処理

ログアウト方法または原因	SYSLOG 表示	MAC 認証	Web 認証、ゲートウェイ認証	IEEE 802.1X 認証	DHCP スヌーピング
ユーザーが認証ページのログアウトボタンをクリックする（常に有効）	web	–	○	–	–
装置の認証ポートがリンクダウンした	link down	○	○	○	–
一定時間通信が行われなかった	aging	○	○	○	–
認証後一定時間が経過した	maxtime	○	○	○	–
指定したログアウト時刻になった	clock	○	○	○	–
access-defender logout コマンドによるログアウト	cli	○	○	○	○
認証関連または認証ポートの設定を変更した	config change	○	○	○	○
同一の認証情報でクライアントがログインした	overwrite	○	○	○	○
サプリカントからの logoff を受信した	logoff	–	–	○	–
再認証に失敗した	reauth failure	–	–	○	–
再認証時にサプリカントからの応答がない	reauth failure (supp-timeout)	–	–	○	–
再認証時に VLAN が変更された	reauth vlan change	–	–	○	–
再認証時にユーザー名が変更された	reauth user name change	–	–	○	–
再認証時にクラス ID の変更を検知した	reauth class change	–	–	○	–
ポート設定が初期化された	Port initialization	–	–	○	–

ログアウト方法または原因	SYSLOG 表示	MAC 認証	Web 認証、ゲートウェイ認証	IEEE 802.1X 認証	DHCP スヌーピング
DHCP サーバーから割り当てられた IP アドレスがリリースされた	release	–	–	–	○
DHCP サーバーから割り当てられた IP アドレスのリース期間が満了した	expire	–	–	–	○
ping ログアウトが実行された	ping	–	○	–	–

ping ログアウト

特定の IP アドレス宛ての ICMP Echo Request、または特定の TTL（Time To Live）値の ICMP Echo Request を装置が受信すると、それを送信した認証済みクライアントがログアウトするように設定できます。IP アドレス指定の ping ログアウトを有効にするには、**`logout ping dst-ip`** コマンドを使用します。TTL 値指定の ping ログアウトを有効にするには、**`logout ping ttl`** コマンドを使用します。

1.9 ローミング機能

認証済みクライアントが装置内の他の認証ポート配下のハブに接続された場合など、通信ポートが変更されてもログアウトすることなく通信を継続するには、**ローミング機能**を有効に設定し、リンクダウンによる認証済みクライアントのログアウトを無効に設定します。ローミング機能を有効に設定するには、**`roaming enable interface`** コマンドを使用します。また、リンクダウンによる認証済みクライアントのログアウトを無効に設定するには、**`logout linkdown disable interface`** コマンドを使用します。

> ***NOTE:*** **`roaming enable interface`** コマンドで指定したインターフェースは、**`logout linkdown disable interface`** コマンドも合わせて設定してください。

1.10 認証クライアントの制限

認証拒否

不正な認証要求を繰り返すクライアントからの認証を一時的に拒否できます。認証を一時的に拒否するには、**`access-defender deny`** コマンドを使用します。

TTL フィルター

Web 認証とゲートウェイ認証において、指定した TTL 値の IP パケットを受信した場合のみ認証を可能とし、指定した TTL 値以外の場合は認証を拒否できます。これにより、ネットワークの距離に応じて、接続を制限できます。TTL フィルターを有効にするには、**`web-authentication ttl`** コマンドを使用します。

Web 認証時の持ち込み端末の制限

RADIUS サーバーの Calling-Station-Id 属性を設定すると、使用する端末の MAC アドレスを、ユーザーごとに制限できます。これにより、ユーザーが許可を受けずに持ち込んだ端末による内部ネットワークへのアクセスを禁止できます。

なお、装置が RADIUS サーバーに送信する RADIUS 要求パケットにおける Calling-Station-Id 属性の MAC アドレス形式は変更できます。たとえば、「XX-XX-XX-XX-XX-XX」（大文字、ハイフン区切り）にしたり、「xxxxxxxxxxxx」（小文字、区切りなし）にしたりできます。MAC アドレスの形式を変更するには、**`radius-server attribute mac-format`** コマンドを使用します。

1.11 AccessDefender の制限事項および注意事項

スタック機能と AccessDefender 機能との併用時の注意事項

スタック構成で AccessDefender を使用する場合でも、最大認証クライアント数はスイッチ 1 台分の値となります。アクセスリストのリソースを効率的に使用したい場合は、スタック機能と併用せずに、装置単体で AccessDefender 機能を使用してください。

スタック機能と AccessDefender 機能との併用において、認証結果の情報はマスター装置が保持します。また、認証を行った時点で認証結果の情報はバックアップマスター装置にも転送され、バックアップマスターは転送された認証結果の情報を保持します。

- **マスター装置がダウンした場合**

  プリエンプトモードの設定にかかわらず、バックアップマスター装置はマスターになった後、保持していた情報を基にして認証機能の動作を継承します。

- **マスター装置が復旧した場合**

  プリエンプトモードが有効時は、バックアップマスターの保持している認証結果の情報を継承しないため、再認証が必要となります。

  プリエンプトモードが無効時は、マスターの切り替わりが発生しないため、再認証は必要ありません。

認証インターフェースにおける制限事項

スパニングツリープロトコル動作ポートを認証インターフェースに指定することは未サポートです。

2. MAC 認証

MAC 認証の機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

2.1 MAC 認証の機能説明

MAC 認証は、端末認証を利用する認証方法です。未認証状態の端末の MAC アドレスを利用して、正規の端末だけに内部ネットワークへのアクセスを許可します。装置全体で MAC 認証を有効化するには、**`mac-authentication enable`** コマンドを使用します。MAC 認証を有効にするインターフェースの設定には、**`authentication interface`** コマンドを使用します。

MAC 認証のユーザー名には端末の MAC アドレスが使用されます。デフォルト設定では「小文字、区切り文字を使用しない形式（例：aabbccddeeff）」がユーザー名になります。MAC 認証で使用するユーザー名の形式を設定するには、**`mac-authentication username mac-format`** コマンドを使用します。

MAC 認証のパスワードは、デフォルト設定ではユーザー名と同じ文字列が使用されます。MAC 認証のパスワードを設定するには、**`mac-authentication password`** コマンドを使用します。

ユーザー名およびパスワードを RADIUS またはローカルデータベースで確認し、認証の成否を決定します。

なお、認証に失敗した場合は、Discard 端末として一定時間（デフォルト設定は 300 秒）登録されます。Discard 端末として登録されている間は、その端末から任意のパケットを受信しても MAC 認証は行われず破棄されます。

2.2 MAC 認証の認証フロー

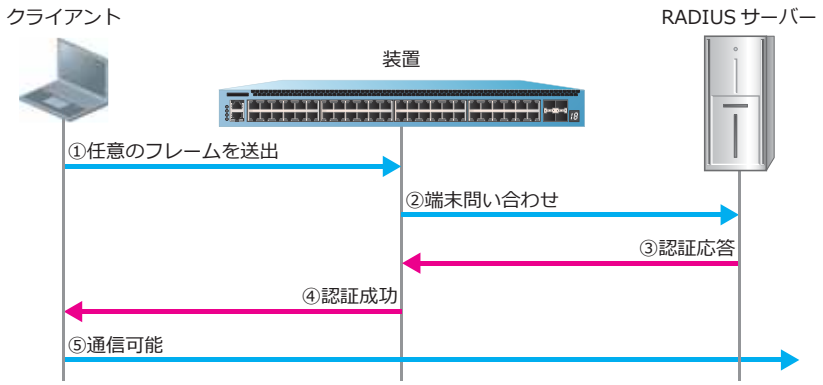
以下に示すパターンの MAC 認証の認証フローについて説明します。

- ダイナミック VLAN を使用しない場合
- ダイナミック VLAN を使用する場合

2.2.1 ダイナミック VLAN を使用しない場合

ダイナミック VLAN を使用しない場合の、MAC 認証の認証フローを以下に示します。

図 2-1 ダイナミック VLAN を使用しない場合の MAC 認証の認証フロー

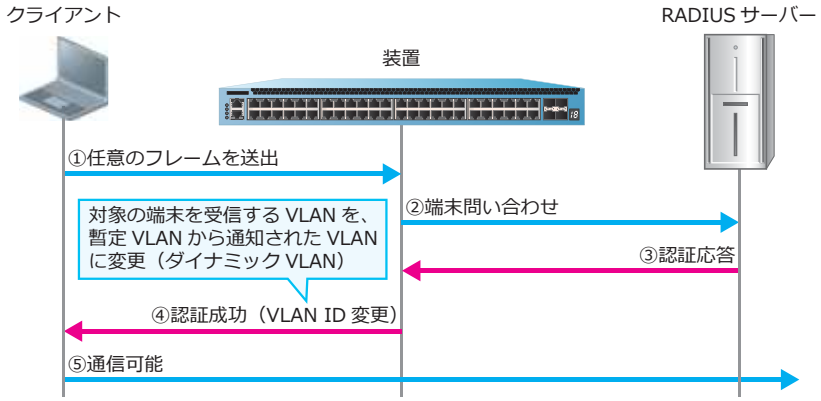


2.2.2 ダイナミック VLAN を使用する場合

ダイナミック VLAN を使用する場合、認証ポートには暫定 VLAN を割り当てておきます。認証に成功して属性値として VLAN ID が通知された場合、その認証済みクライアントは通知された VLAN で受信するように割り当てられます。

ダイナミック VLAN を使用する場合の、MAC 認証の認証フローを以下に示します。

図 2-2 ダイナミック VLAN を使用する場合の MAC 認証の認証フロー



2.3 MAC 認証のオプション機能

MAC 認証に関連するオプション機能を以下に示します。

- MAC 認証のユーザー名の形式設定
- Discard 端末の登録時間設定
- DHCP パケットの MAC 認証除外設定

2.3.1 MAC 認証のユーザー名の形式設定

MAC 認証のユーザー名の形式は、以下の 20 パターンから選択できます。ユーザー名の形式を設定するには、**mac-authentication username mac-format** コマンドを使用します。

表 2-1 MAC 認証のユーザー名の形式一覧

大文字／小文字	区切り文字	区切り文字数	例
小文字	none	-	aabbccddeeff（デフォルト設定）
	hyphen（-）	1	aabbcc-ddeeff
		2	aabb-ccdd-eeff
		5	aa-bb-cc-dd-ee-ff
	colon（:）	1	aabbcc:ddeeff
		2	aabb:ccdd:eeff
		5	aa:bb:cc:dd:ee:ff
	dot（.）	1	aabbcc.ddeeff
		2	aabb.ccdd.eeff
		5	aa.bb.cc.dd.ee.ff
大文字	none	-	AABBCCDDEEFF
	hyphen（-）	1	AABBCC-DDEEFF
		2	AABB-CCDD-EEFF
		5	AA-BB-CC-DD-EE-FF
	colon（:）	1	AABBCC:DDEEFF
		2	AABB:CCDD:EEFF
		5	AA:BB:CC:DD:EE:FF
	dot（.）	1	AABBCC.DDEEFF
		2	AABB.CCDD.EEFF
		5	AA.BB.CC.DD.EE.FF

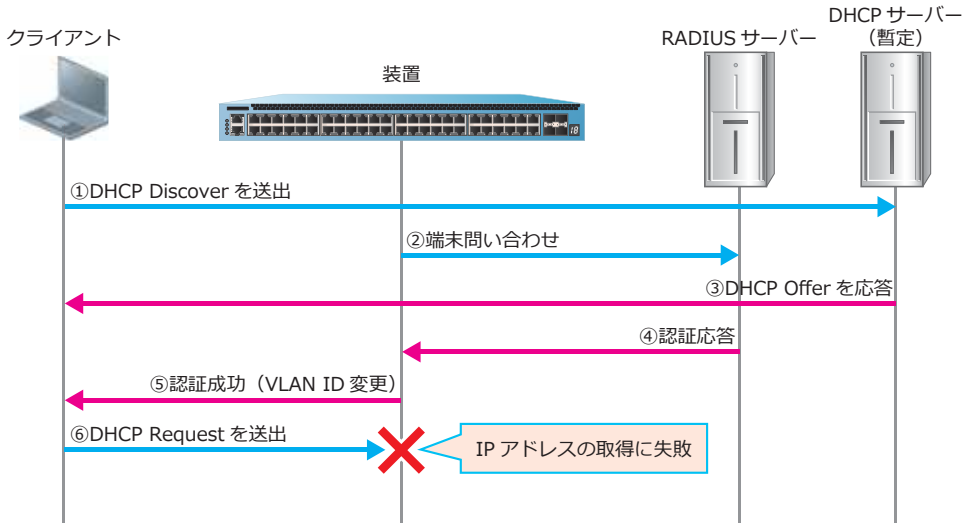
2.3.2 Discard 端末の登録時間設定

Discard 端末の登録時間は、デフォルト設定では 300 秒です。Discard 端末として登録されている時間を設定するには、**mac-authentication discard-time** コマンドを使用します。

2.3.3 DHCP パケットの MAC 認証除外設定

MAC 認証を利用していると、DHCP サーバーから IP アドレスを取得するパケット（DHCP Discover）でも MAC 認証が行われます。その際、RADIUS サーバーから属性値として VLAN ID が通知された場合は、DHCP サーバーから IP アドレスを取得している途中で VLAN ID が切り替わり、IP アドレスの取得に失敗します。

図 2-3 DHCP パケットを MAC 認証の対象としている場合のフロー



これを避けるには、DHCP サーバーから IP アドレスを取得するパケットでは、MAC 認証が行われないように設定します（DHCP パケットの除外設定）。DHCP パケットの除外設定を行うには、**`mac-authentication ignore-dhcp`** コマンドを使用します。

3. Web 認証

Web 認証の機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

3.1 Web 認証の機能説明

Web 認証は、ユーザー認証を利用する認証方法です。未認証状態のユーザーが内部ネットワークに接続する前に、ユーザー名およびパスワードを入力して、正規のユーザーだけに内部ネットワークへのアクセスを許可します。装置全体で Web 認証を有効化するには、**`web-authentication enable`** コマンドを使用します。Web 認証を有効にするインターフェースの設定には、**`authentication interface`** コマンドを使用します。

Web 認証用の Web サーバーの IPv4 アドレス／ IPv6 アドレスを設定するには、**`web-authentication http-ip`** コマンドを使用します。Web 認証用の Web サーバーのポート番号を設定するには、**`web-authentication http-port`** コマンドまたは **`web-authentication https-port`** コマンドを使用します。なお、Web 認証用の Web サーバーとして外部 Web サーバーを利用することもできます。外部 Web サーバーを利用する場合は、**`web-authentication redirect url`** コマンドを使用します。

ユーザーが入力したユーザー名およびパスワードは、RADIUS サーバーまたはローカルデータベースで確認し、認証の成否を決定します。

NOTE: Web 認証を使用する場合は、少なくとも 1 つは IP アドレスを設定した任意の VLAN インターフェースを作成してください。また、IP アドレスを設定した VLAN インターフェースが 1 つもアップしていない場合は、認証ページは応答できません。

NOTE: Web 認証を有効にしたインターフェースでは、アドレス解決のための ARP/NDP は、認証状態にかかわらず自動的に許可されます。

3.2 Web 認証の認証フロー

以下に示すパターンの Web 認証の認証フローについて説明します。

- ダイナミック VLAN を使用しない場合
- ダイナミック VLAN を使用する場合

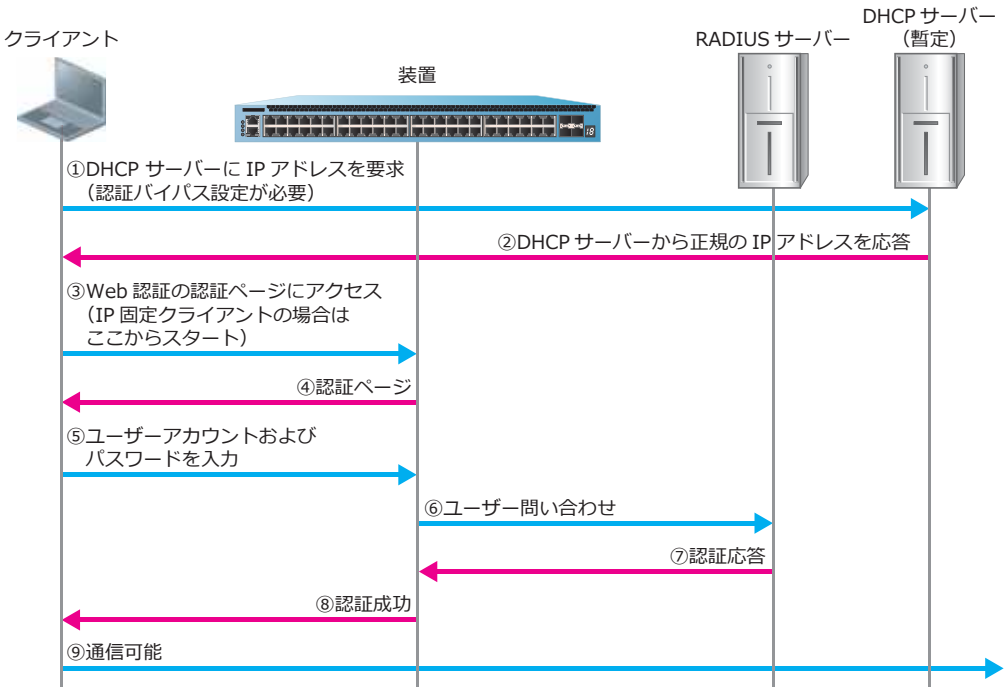
また、Web 認証の応答の仕組みについて説明します。

3.2.1 ダイナミック VLAN を使用しない場合

ダイナミック VLAN を使用しない場合の、Web 認証の認証フローを以下に示します。この例では認証クライアントが DHCP クライアントのため、認証バイパス機能を使用して DHCP パケットをバイパスしています。

NOTE: クライアントが使用する Web ブラウザーのリダイレクト回数制限により、認証成功・失敗ページを表示できないことがあります。その場合は、Web ブラウザーの更新ボタンを一回クリックし、再読み込みを行ってください。

図 3-1 ダイナミック VLAN を使用しない場合の Web 認証の認証フロー



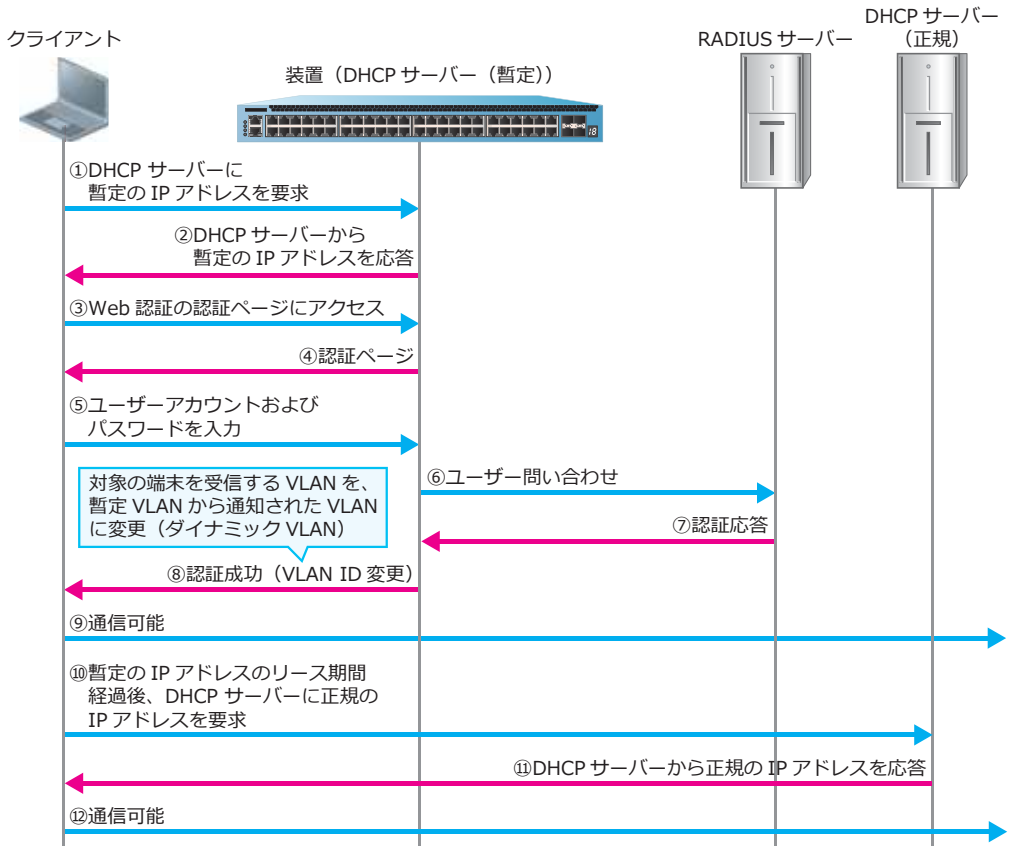
3.2.2 ダイナミック VLAN を使用する場合

Web 認証でダイナミック VLAN を使用する場合は、認証後に VLAN が変更されるため、DHCP クライアントでの使用が前提になります。

ダイナミック VLAN を使用する場合、認証ポートには暫定 VLAN を割り当てておきます。認証に成功して属性値として VLAN ID が通知された場合、その認証済みクライアントは通知された VLAN で受信するように割り当てられます。

ダイナミック VLAN を使用する場合の、Web 認証の認証フローを以下に示します。この例では認証前のクライアントに暫定的に IP を割り当てる暫定 DHCP サーバーは、装置に設定しています。

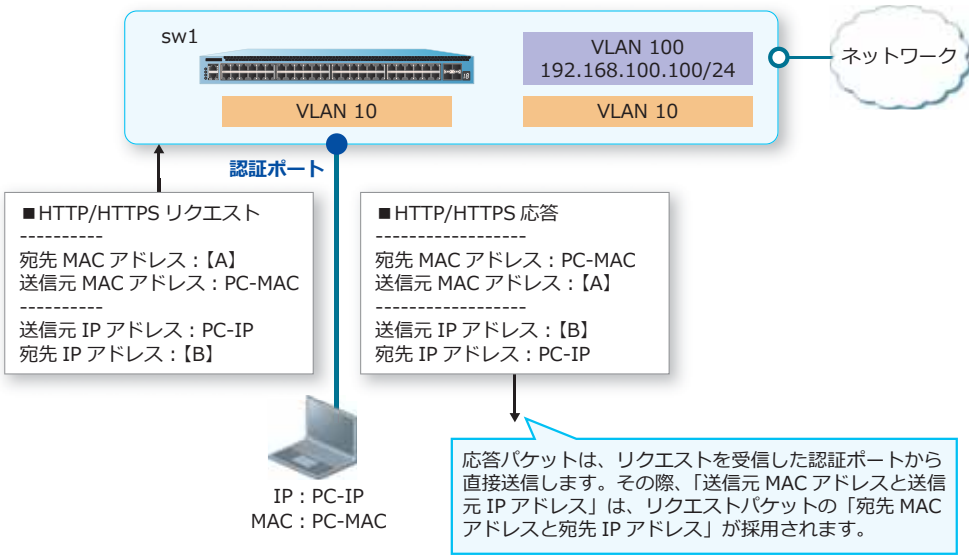
図 3-2 ダイナミック VLAN を使用する場合の Web 認証の認証フロー



3.2.3 Web 認証の応答の仕組み

Web 認証ポートにおいて、認証前のクライアントから HTTP/HTTPS リクエストを受信すると、応答パケットは、リクエストを受信した Web 認証ポートから直接送信されます。その際、「送信元 MAC アドレスと送信元 IP アドレス」は、リクエストパケットの「宛先 MAC アドレスと宛先 IP アドレス」が採用されます。

図 3-3 Web 認証の応答の仕組み



3.3 認証ページリダイレクト

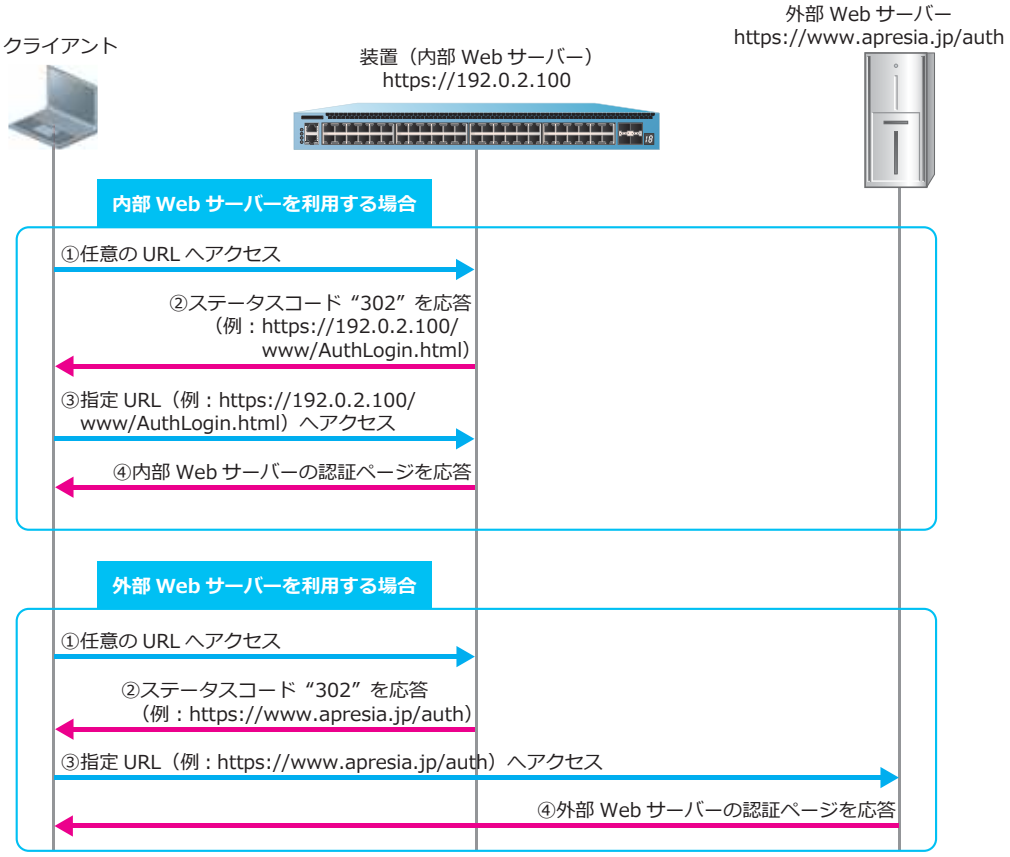
ユーザーが認証前のクライアントから任意の Web サーバーにアクセスしたときに（装置を経由し、任意の URL に対して HTTP/HTTPS リクエストが送信されたときに）、自動的に装置または外部 Web サーバーの認証ページにリダイレクトできます。これにより、ユーザーに対して認証ページの URL を通知する必要がなくなるため、認証ネットワークをスムーズに運用できます。

このリダイレクト動作はデフォルトで動作し、ユーザーが HTTP でアクセスした際には HTTP、また HTTPS でアクセスした際には HTTPS の装置の認証ページにリダイレクトされます。リダイレクト先を HTTP または HTTPS のいずれか 1 つに固定したい場合、または外部 Web サーバーに設定する場合には、**`web-authentication redirect url`** コマンドでリダイレクト先の認証ページの URL を指定します。

> ***NOTE:*** リダイレクト動作が有効の場合は、Web ブラウザー以外からの HTTP または HTTPS の通信負荷によって、認証性能が著しく低下する可能性があります。
>
> ***NOTE:*** 認証前のクライアントからの HTTPS アクセスをリダイレクトする場合には、Web ブラウザーに証明書エラーに関わる警告が表示される場合がありますが、これは HTTPS の仕様によるものです。証明書エラーに関わる警告が表示されても、Web ブラウザーで許可する操作を実施することにより、認証ページにリダイレクトされます。
>
> ***NOTE:*** 外部 Web サーバーにリダイレクトする際にリダイレクト先の URL を FQDN で設定している場合は、認証バイパス機能を使用して、外部サーバーへの通信だけでなく DNS の通信をバイパスするように設定してください。

認証ページリダイレクトの例を以下に示します。

図 3-4 認証ページリダイレクトの動作例



3.3.1 リダイレクト動作を無効にする場合の設定

web-authentication redirect disable コマンドで、HTTP または HTTPS のリダイレクト動作を無効にできます。

3.3.2 リダイレクト先の装置の認証ページを HTTP に固定する場合の設定

web-authentication redirect url コマンドで、リダイレクト先の装置の認証ページを HTTP に固定できます。HTTP に固定する場合は、リダイレクト先の URL を以下のように設定します。

http://「**web-authentication http-ip** コマンドの設定値」:「**web-authentication http-port** コマンドの設定値」/www/AuthLogin.html

リダイレクト先を「http://192.0.2.100:8080/www/AuthLogin.html」に設定する場合の設定例を以下に示します。

```
(config)# access-defender
(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
(config-a-def)# web-authentication http-port 8080
(config-a-def)# web-authentication redirect url http://192.0.2.100:8080/www/AuthLogin.html
```

NOTE: リダイレクト先が装置の認証ページの場合の「/www/AuthLogin.html」は、装置内部の設定値を参照しており、変更できません。

3.3.3 リダイレクト先の装置の認証ページを HTTPS に固定する場合の設定

web-authentication redirect url コマンドで、リダイレクト先の装置の認証ページを HTTPS に固定できます。HTTPS に固定する場合は、リダイレクト先の URL を以下のように設定します。

https://「**web-authentication http-ip** コマンドの設定値」:「**web-authentication https-port** コマンドの設定値」/www/AuthLogin.html

リダイレクト先を「https://192.0.2.100:8443/www/AuthLogin.html」に設定する場合の設定例を以下に示します。

```
(config)# access-defender
(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
(config-a-def)# web-authentication https-port 8443
(config-a-def)# web-authentication redirect url https://192.0.2.100:8443/www/AuthLogin.html
```

NOTE: リダイレクト先が装置の認証ページの場合の「/www/AuthLogin.html」は、装置内部の設定値を参照しており、変更できません。

3.3.4 HTTP プロキシ使用環境での認証ページリダイレクト

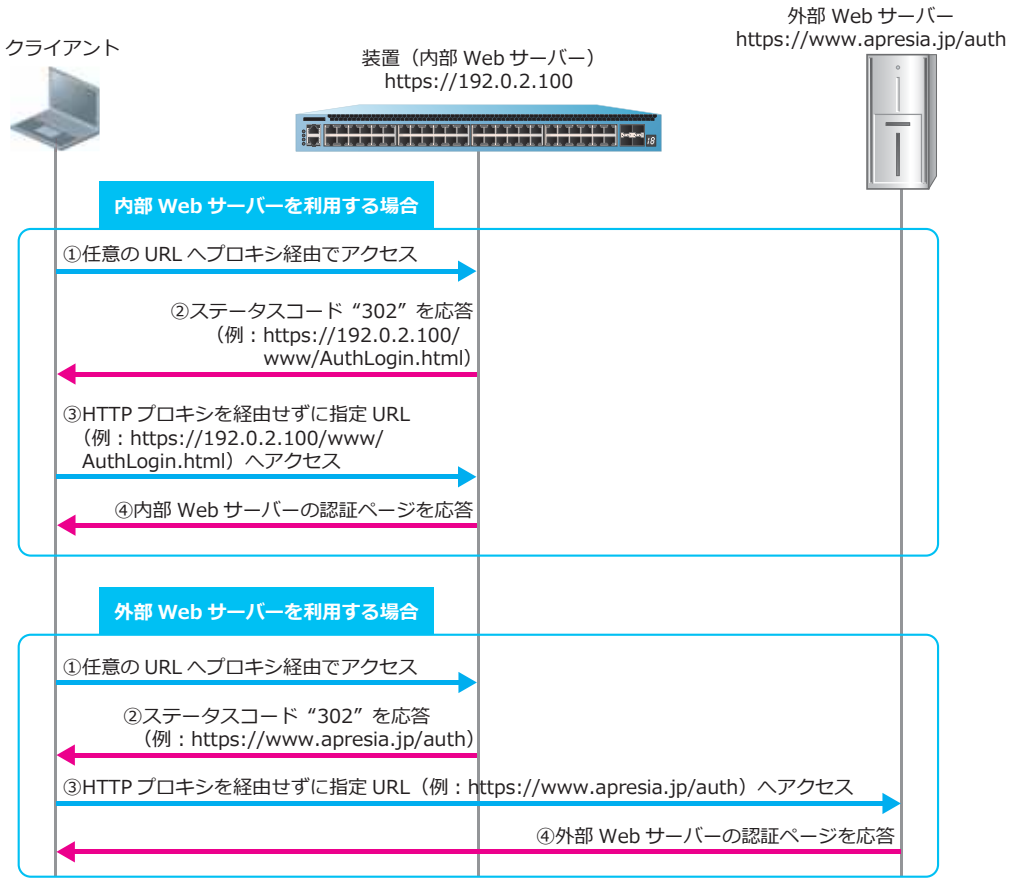
HTTP プロキシ使用環境で HTTP プロキシ経由のアクセスをリダイレクトするためには、**web-authentication redirect proxy-port** コマンドを使用します。

NOTE: プロキシ経由の HTTPS アクセスはリダイレクトできません。

NOTE: **web-authentication redirect proxy-port** コマンドを使用して、Web 認証のプロキシリダイレクト機能を有効にした際は、Web ブラウザーのプロキシ設定で、リダイレクト先の URL を例外指定する必要があります。

HTTP プロキシ使用環境での、認証ページリダイレクトの例を以下に示します。

図 3-5 HTTP プロキシ使用環境での認証ページリダイレクトの動作例



3.4 認証ページのカスタマイズ

AccessDefender で使用する以下の認証ページは、カスタマイズできます。

- ログイン認証ページ
- 認証成功ページ
- 認証失敗ページ
- ログアウト成功ページ
- ログアウト失敗ページ
- リダイレクト失敗ページ

デフォルトのページについては、実際に表示される認証ページを確認してください。カスタマイズした認証ページを装置に保存するには、**copy** コマンドを使用します。また、保存した認証ページを削除するには、**access-defender erase** コマンドを使用します。削除後はデフォルトのページが使用されます。

ログイン用のフォームの例を以下に示します。

表 3-1 ログイン用のフォームの例

```
<form method="POST" action="/cgi-bin/adeflogin.cgi">
<table>
<tr><th width="184">User Account:</th><td width="220">
<input name="name" type="text" value="" size="30" maxlength="63"></td></tr>
<tr><th width="184">Password:</th><td width="220">
<input name="pass" type="password" size="30" maxlength="63"></td></tr></table>
<input type="submit" name="action" value="login">
<input type="reset" value="reset">
</form>
```

NOTE: form タグの method 属性を「POST」に設定します。

NOTE: ユーザー名を入力するフォームの name 属性を「name」に、パスワードを入力するフォームの name 属性を「pass」に設定します。

REF: 認証 ID ごとの認証方式を使用する場合のフォームについては、「AccessDefender の認証方式」の「Web 認証の認証方式選択機能」を参照してください。

また、AccessDefender で使用する認証ページを外部 Web サーバーの任意のページ（以後、ユーザー認証用外部ページ）に埋め込むこともできます。任意のページに埋め込む場合は、ユーザー認証用外部ページの form タグの action 属性を「http://（AccessDefender 認証用 IP アドレス）:（ポート番号）/cgi-bin/adeflogin.cgi」に設定します。

AccessDefender 認証用 IP アドレスが「192.0.2.100」、ポート番号が「8080」の場合のログイン用のフォームの例を以下に示します。

表 3-2 ログイン用のフォームの例

```
<form method="POST" action="http://192.0.2.100:8080/cgi-bin/adeflogin.cgi">
<table>
<tr><th width="184">User Account:</th><td width="220">
<input name="name" type="text" value="" size="30" maxlength="63"></td></tr>
<tr><th width="184">Password:</th><td width="220">
<input name="pass" type="password" size="30" maxlength="63"></td></tr></table>
<input type="submit" name="action" value="login">
<input type="reset" value="reset">
</form>
```

NOTE: form タグの method 属性を「POST」に設定します。

NOTE: ユーザー名を入力するフォームの name 属性を「name」に、パスワードを入力するフォームの name 属性を「pass」に設定します。

REF: 認証 ID ごとの認証方式を使用する場合のフォームについては、「AccessDefender の認証方式」の「Web 認証の認証方式選択機能」を参照してください。

認証ページのカスタマイズ（画像表示）

認証ページで画像を表示させることも可能です。認証ページで画像を表示させる場合、ローカルフラッシュに画像ファイルを webpage-image として格納する必要があります。webpage-image は webpage-image01 から webpage-image10 の 10 個まで格納できます。なお、画像ファイルのサイズは、1 ファイルにつき 1 メガバイト未満としてください。

表 3-3 画像ファイル（img7.gif）をローカルフラッシュに webpage-image01 としてコピーする際の例

```
# copy tftp: webpage-image01

Address of remote host []? 10.249.234.137
Source filename []? img7.gif
Destination filename webpage-image01? [y/n]:  y

 Accessing tftp://10.249.234.137/img7.gif...
 Transmission start...
 Transmission finished, file length 4807 bytes.
 Please wait, programming flash............. Done.
```

NOTE: 画像ファイルを格納する前に、ローカルフラッシュに十分な空き容量があることを確認してください。

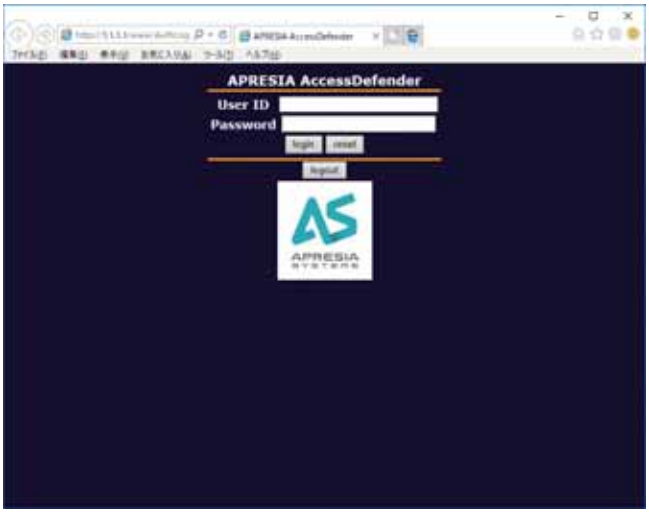
NOTE: 画像ファイルの格納時に、”webpage-image01” ～ ”webpage-image10” という画像ファイルを **copy** コマンドでローカルフラッシュに単純にコピーすることはサポートしていません。必ず、**copy** コマンドでパラメーターを ”webpage-image01” ～ ”webpage-image10” を指定して画像ファイルを格納してください。

ローカルフラッシュに格納した webpage-image を認証ページに表示させるには、<img src = “”> タグでファイルを指定してください。

表 3-4 認証ページでローカルフラッシュの webpage-image01 を中央揃えで表示させる場合のタグの例

```
<div style="text-align:center;">
<img src="/webpage-image01">
</div>
```

図 3-6 画像を表示させたログインページの例



3.5 Web 認証のオプション機能

Web 認証に関連するオプション機能を以下に示します。

- TTL フィルター
- HTTP セッションタイムアウト
- Web 認証の上書きログイン機能
- Web 認証のスヌーピングプロキシ機能
- Web 認証のサーバー証明書と秘密鍵の変更
- 証明書要求と秘密鍵の作成
- 個別 Web 認証ページ

3.5.1 TTL フィルター

Web 認証とゲートウェイ認証において、指定した TTL 値の IP パケットを受信した場合のみ認証を可能とし、指定した TTL 値以外の場合は認証を拒否できます。これにより、ネットワークの距離に応じて、接続を制限できます。TTL フィルターを有効にするには、**`web-authentication ttl`** コマンドを使用します。

3.5.2 HTTP セッションタイムアウト

Web 認証で HTTP クライアント用に予約された HTTP セッション数は制限されています。すべての HTTP セッションが占有されている場合は、新しい HTTP クライアントが Web 認証を開始できません。

そこで、一定時間応答がない HTTP セッションを自動的に切断して解放することで、新しい HTTP クライアントが Web 認証を開始できるようにしています。

HTTP セッションのタイムアウトを設定するには、**`web-authentication http-session-timeout`** コマンドを使用します。

3.5.3 Web 認証の上書きログイン機能

認証済みクライアントから装置の認証ページにアクセスすると、通常は認証成功ページ（login-success-page）が表示されますが、認証成功ページではなくログインページ（login-page）を表示させて、ユーザー名の上書きログインが行えるように変更できます。

Web 認証のユーザー名の上書きログインを有効にするには、**`web-authentication overwrite enable`** コマンドを使用します。

3.5.4 Web 認証のスヌーピングプロキシ機能

認証クライアントが指定したプロキシポート番号を経由して任意の Web ページを参照したときに、装置はリダイレクトを行わず、強制的に認証ページを表示できます。これにより、ユーザーに対して装置の認証ページの URL を通知する必要がなくなるため、認証ネットワークをスムーズに運用できます。

プロキシポート番号を経由して任意の Web ページを参照したときに、強制的に認証ページを表示するには、**`web-authentication snooping proxy-port`** コマンドを使用します。

3.5.5 Web 認証のサーバー証明書と秘密鍵の変更

Web 認証のサーバー証明書と秘密鍵を変更する方法を以下に示します。

NOTE: Web 認証が有効な状態では、サーバー証明書と秘密鍵の削除、およびダウンロードはできません。

NOTE: サーバー証明書と秘密鍵の両方をダウンロードすると、**`show ssl https-certificate`** コマンドと **`show ssl https-private-key`** コマンドに反映されます。片方のみダウンロードした状態では反映されません。

1. 新しいサーバー証明書と秘密鍵を用意します。
2. **`no web-authentication enable`** コマンドで Web 認証を無効にします。
3. **`access-defender erase ssl-files`** コマンドで、以前にダウンロードしたサーバー証明書と秘密鍵を削除します。
4. **`copy {tftp: | flash:} https-certificate`** コマンド、**`copy {tftp: | flash:} https-private-key`** コマンドで、TFTP または SD カードから新しいサーバー証明書と秘密鍵をダウンロードします。
5. **`web-authentication enable`** コマンドで Web 認証を有効にします。

3.5.6 証明書要求と秘密鍵の作成

新しいサーバー証明書の作成には、装置で作成した CSR（証明書署名要求）と秘密鍵を利用することもできます。装置で作成した CSR（証明書署名要求）と秘密鍵をもとにサーバー証明書を作成する方法を以下に示します。

1. **`ssl gencsr rsakey`** コマンドで CSR（証明書署名要求）と秘密鍵を作成します。
2. **`copy csr-certificate tftp:`** コマンド、**`copy csr-private-key tftp:`** コマンドで、TFTP 経由で CSR（証明書署名要求）と秘密鍵を取り出します。
3. 取り出した CSR（証明書署名要求）に認証局（CA）による署名を行い、サーバー証明書を作成します。
4. 手順 3 で作成したサーバー証明書と、手順 2 で取り出した秘密鍵を、Web 認証のサーバー証明書の変更手順に従って装置にダウンロードします。

3.5.7 個別 Web 認証ページ

個別 Web 認証ページを使用すると、指定したインターフェースに個別の Web 認証ページを適用できます。個別 Web 認証ページを使用する場合は、事前に個別 Web 認証ページを装置にダウンロードしてください。指定した ID の個別 Web 認証ページが存在しない場合は、「デフォルト Web 認証ページ」が適用されます。デフォルト Web 認証ページがユーザーによってカスタマイズされて装置にダウンロードされている場合は、「カスタマイズされたデフォルト Web 認証ページ」が適用されます。

NOTE: 個別 Web 認証ページ ID は、1 ～ 30 の範囲で指定できます。

NOTE: 個別 Web 認証ページは、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降でサポートしています。

個別 Web 認証ページを適用するには、**`web-authentication interface`** コマンドを使用します。

個別 Web 認証ページのダウンロード

個別 Web 認証ページを装置にダウンロードするには、**`copy`** コマンドで webpages パラメーターを使用し、個別 Web 認証ページ ID を指定して実施します。

個別 Web 認証ページの削除

装置にダウンロードした個別 Web 認証ページを削除するには、**`access-defender erase`** コマンドで webpages パラメーターを使用し、個別 Web 認証ページ ID を指定して実施します。

4. ゲートウェイ認証

ゲートウェイ認証の機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

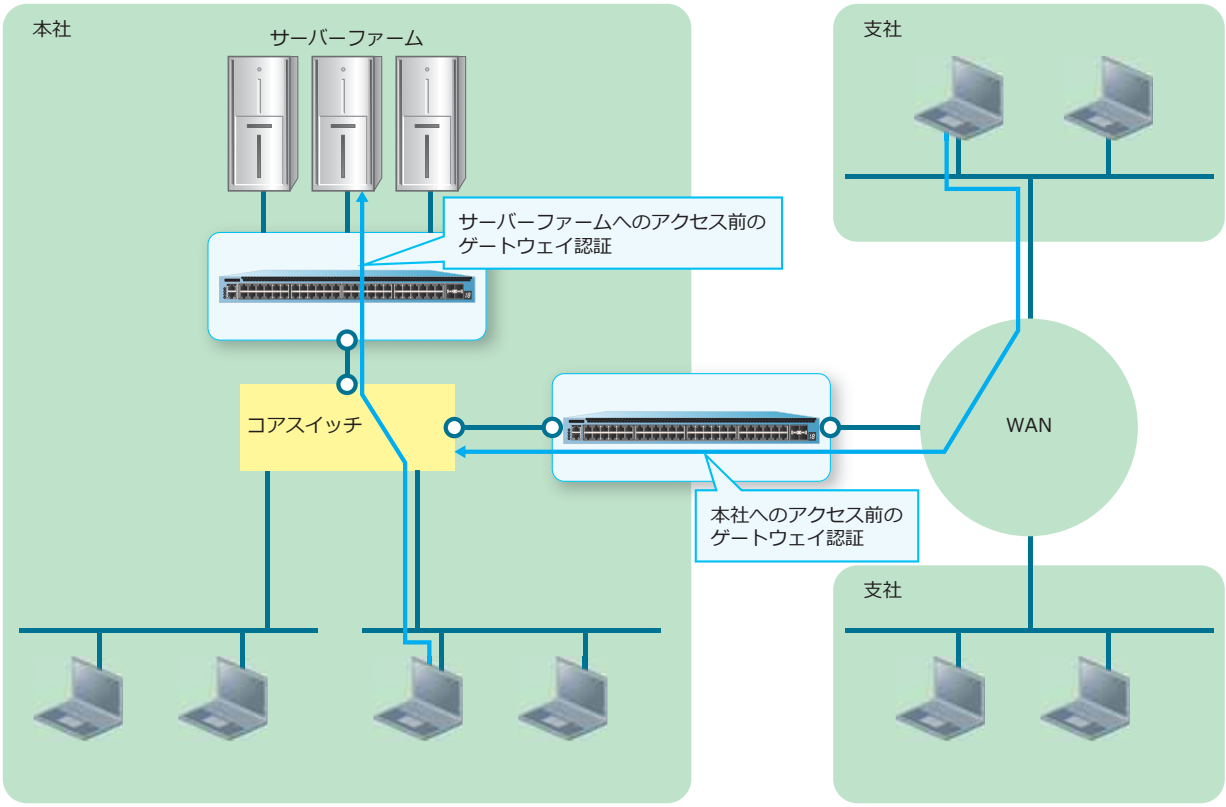
4.1 ゲートウェイ認証の機能説明

ゲートウェイ認証は、認証するクライアントと装置が、異なるネットワークに存在する場合に使用します。Web 認証と同様の仕組みで、正規のユーザーだけに内部ネットワークへのアクセスを許可します。たとえば、サーバーファームの手前に設置した装置で、サーバー群にアクセスできるユーザーを認証したり、中央拠点の手前に設置した装置で、本社ネットワークにアクセスできるユーザーを認証したりできます。装置全体でゲートウェイ認証を有効化するには、**`web-authentication enable`** コマンドを使用します。ゲートウェイ認証を有効にするインターフェースの設定には、**`authentication interface`** コマンドを使用します。

CAUTION: ゲートウェイ認証を有効にしたインターフェースでは、他の認証機能は併用できません。

CAUTION: ゲートウェイ認証では、ダイナミック VLAN はサポートしていません。

図 4-1 ゲートウェイ認証



5. IEEE 802.1X 認証

IEEE 802.1X 認証の機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

5.1 IEEE 802.1X 認証の機能説明

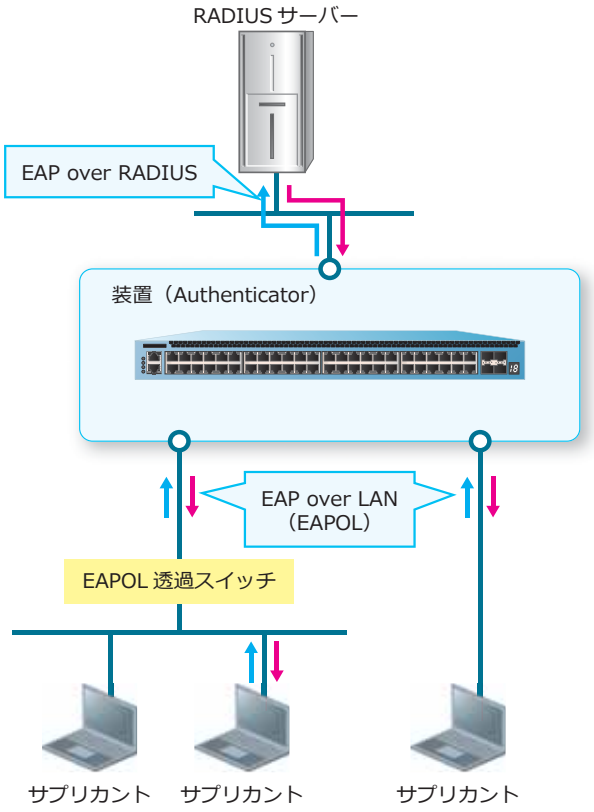
IEEE 802.1X 認証は、電子証明書や、ユーザー名およびパスワードを使用して、正規のユーザーだけに内部ネットワークへのアクセスを許可します。装置全体で IEEE 802.1X 認証を有効化するには、**`dot1x enable`** コマンドを使用します。IEEE 802.1X 認証を有効にするインターフェースの設定には、**`authentication interface`** コマンドを使用します。

IEEE 802.1X 認証には、装置（Authenticator）のほかに、認証するクライアントソフトウェア（サプリカント）、IEEE 802.1X 認証に対応した RADIUS サーバーが必要です。また、装置（Authenticator）と認証クライアントの間に L2 スイッチなどが存在する場合、その L2 スイッチでは EAPOL 透過機能が必要です。

CAUTION: タグ付きの IEEE 802.1X 認証フレームに対しては認証できません。

CAUTION: IEEE 802.1X 認証では、ローカルデータベースによる認証は未サポートです。

図 5-1 IEEE 802.1X 認証



- **サプリカント**

  サプリカントは、IEEE 802.1X 認証に対応した端末用のソフトウェアです。Windows は、標準で IEEE 802.1X 認証に対応しています。

- **RADIUS サーバー**

  RADIUS サーバーは、ユーザー名およびパスワードを確認し、サプリカントに内部ネットワークへのアクセスを許可してよいかどうかを決定します。

- **EAPOL 透過スイッチ**

  IEEE 802.1X 認証で使用する EAP メッセージは、特殊なマルチキャストアドレスを使用する MAC フレーム（EAPOL フレーム）で送受信されます。一般的なスイッチでは EAPOL フレームが破棄されてしまうため、装置（Authenticator）の 1 つの認証ポートに複数のサプリカントを接続したい場合は、EAPOL フレームを透過することができる L2 スイッチを経由して接続します。

IEEE 802.1X 認証で使用される EAP 認証方式

装置がサポートする EAP の認証方式は、以下のとおりです。

表 5-1 AccessDefender がサポートする EAP 認証方式

	EAP-MD5（Message Digest 5）	PEAP（Protected EAP）	EAP-TTLS（Tunneled TLS）	EAP-TLS（Transport Level Security）
サーバー電子証明書	不要	要	要	要
クライアント電子証明書	不要	不要	不要	要
ユーザー識別	ユーザー名およびパスワード	ユーザー名およびパスワード	ユーザー名およびパスワード	電子証明書
サーバー認証	なし	電子証明書	電子証明書	電子証明書
セキュリティー	AccessDefender が対応する EAP 認証方式の中で、セキュリティーレベルが最も低い	• 通信経路が TLS トンネルで暗号化される（TLS トンネル内でさらに EAP を使用する） • 強固な認証が可能である	• 通信経路が TLS トンネルで暗号化される（TLS トンネル内でさらに様々な認証プロトコルを使用できる） • 強固な認証が可能である	AccessDefender が対応する EAP 認証方式の中で、セキュリティーレベルが最も高い
導入および運用管理	Web 認証と同程度に容易である	運用管理の負担が比較的小さい	運用管理の負担が比較的小さい	電子証明書の導入や運用管理の負担が大きい
備考		端末の OS が、基本的に Windows に限定される	OS に標準搭載されていないため、別途サプリカントを用意する必要がある	

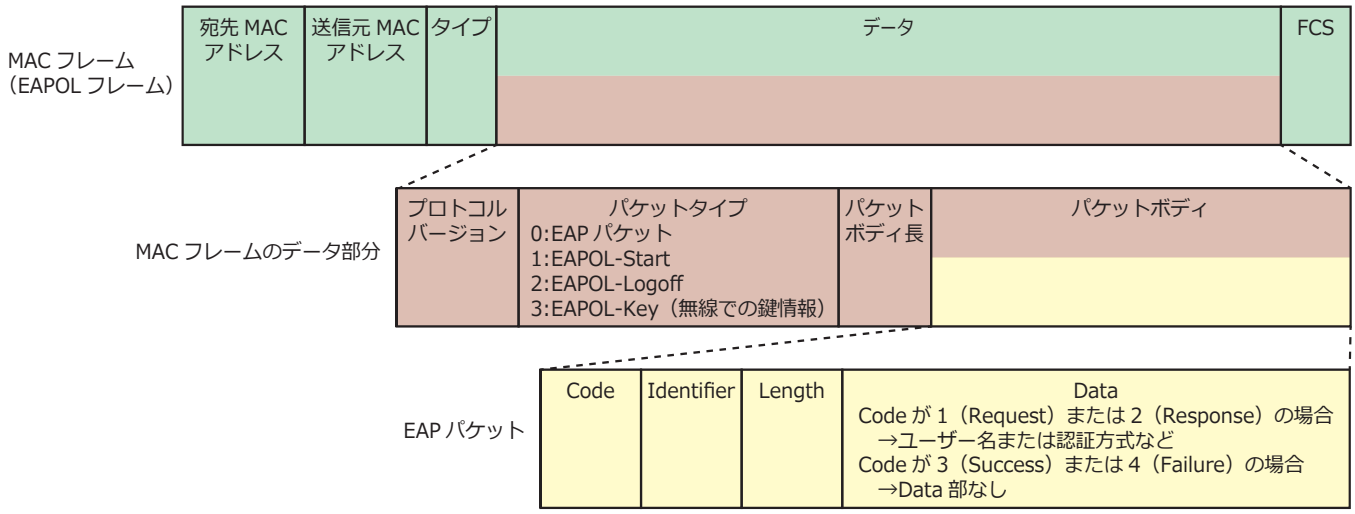
EAP のフレーム形式

EAP では、EAP パケットを使用して各種認証情報をやりとりします。

サプリカントと Authenticator の間では、EAPOL フレームに EAP パケットを格納して情報をやりとりします。また、Authenticator と RADIUS サーバーの間では、RADIUS パケットに EAP パケットを格納して情報をやりとりします。

EAPOL フレームのフレーム形式は下図のとおりです。

図 5-2 EAPOL フレームのフレーム形式



5.2 IEEE 802.1X 認証の認証フロー

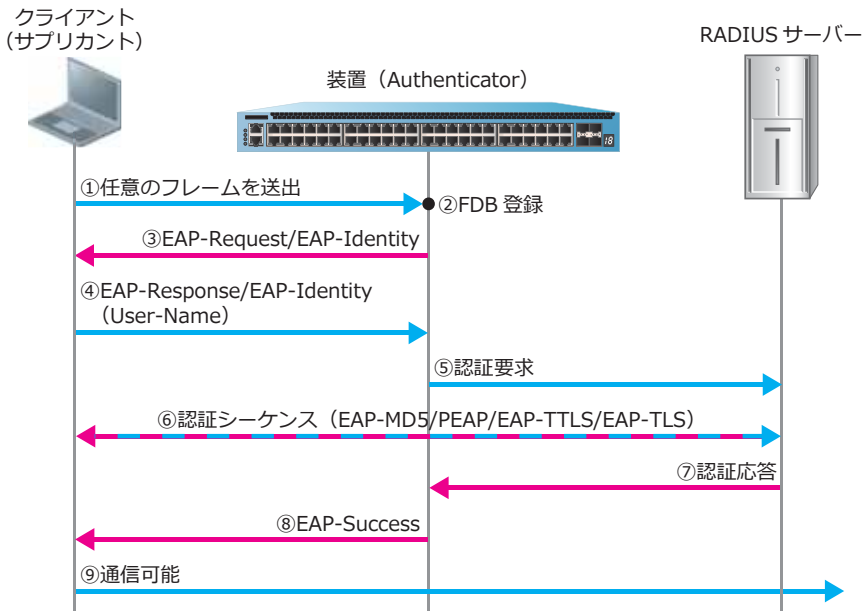
以下に示すパターンの IEEE 802.1X 認証の認証フローについて説明します。

- ダイナミック VLAN を使用しない場合
- ダイナミック VLAN を使用する場合

5.2.1 ダイナミック VLAN を使用しない場合

ダイナミック VLAN を使用しない場合の、IEEE 802.1X 認証の認証フローを以下に示します。

図 5-3 ダイナミック VLAN を使用しない場合の IEEE 802.1X 認証の認証フロー

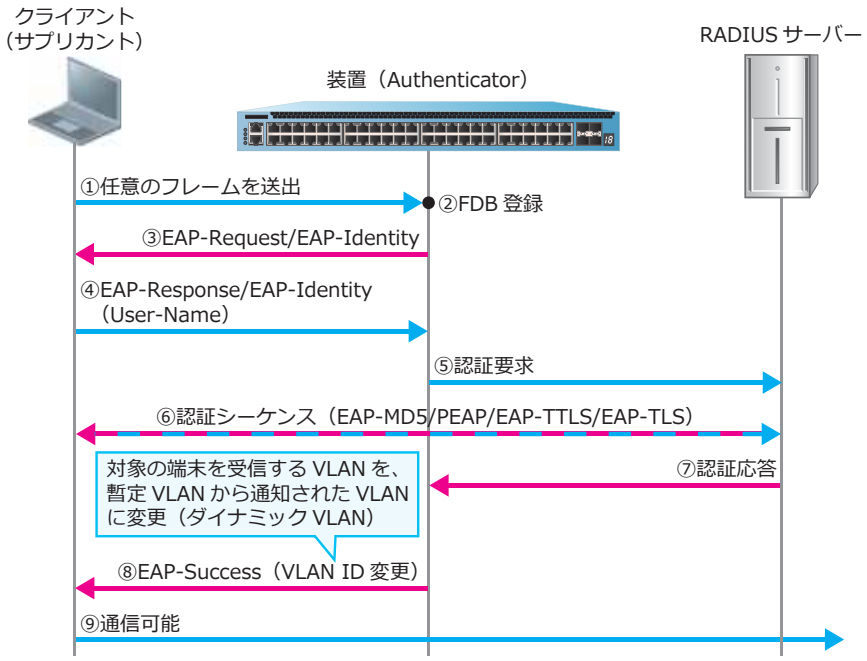


5.2.2 ダイナミック VLAN を使用する場合

ダイナミック VLAN を使用する場合、認証ポートには暫定 VLAN を割り当てておきます。認証に成功して属性値として VLAN ID が通知された場合、その認証済みクライアントは通知された VLAN で受信するように割り当てられます。

ダイナミック VLAN を使用する場合の、IEEE 802.1X 認証の認証フローを以下に示します。

図 5-4 ダイナミック VLAN を使用する場合の IEEE 802.1X 認証の認証フロー



5.3 IEEE 802.1X 認証のオプション機能

IEEE 802.1X 認証に関連するオプション機能を以下に示します。

- 認証開始時の EAP-Request/EAP-Identity の送信間隔の変更
- 認証失敗時のステータス保持時間の変更
- EAPOL-Start 受信による認証の抑止機能
- EAPOL フレームの転送機能

5.3.1 認証開始時の EAP-Request/EAP-Identity の送信間隔の変更

認証開始時の、サプリカントに対する EAP-Request/EAP-Identity の送信間隔を変更できます。
EAP-Request/EAP-Identity の送信間隔を変更するには、**`dot1x timeout tx-period`** コマンドを使用します。

5.3.2 認証失敗時のステータス保持時間の変更

IEEE 802.1X 認証に失敗した場合、デフォルト設定では 60 秒間ステータスを認証失敗状態として保持します。その期間中に対象のサプリカントから EAPOL-Start を受信しても、認証処理は行われません。認証失敗時のステータス保持時間を変更するには、**`dot1x timeout quiet-period`** コマンドを使用します。

5.3.3 EAPOL-Start 受信による認証の抑止機能

サプリカントから EAPOL-Start を受信しても、EAP-Request/EAP-Identity を応答せず、認証を抑止できます。EAPOL-Start 受信による認証の抑止機能を使用するには、**`dot1x ignore-eapol-start interface`** コマンドを使用します。

5.3.4 EAPOL フレームの転送機能

デフォルト設定では、IEEE 802.1X 認証が無効のインターフェースでは、EAPOL フレームは破棄され中継されませんが、これを中継するように変更できます。IEEE 802.1X 認証が無効のインターフェースで EAPOL フレームを転送する機能を有効にするには、**`fwd-eapol enable`** コマンドを使用します。

6. スタティック認証

スタティック認証の機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

6.1 スタティック認証の機能説明

スタティック認証クライアントとして登録されると、常にアクセスが許可されるようになります。なお、スタティック認証だけでは未認証クライアントからの通信を破棄しないため、使用する場合は他の認証機能と併用して使用してください。

CAUTION: スタティック認証とゲートウェイ認証は併用できません。

NOTE: 登録可能なスタティック認証端末数は最大 64 台です。

スタティック認証を有効にするインターフェースの設定には、**`authentication interface`** コマンドを使用します。また、スタティック認証クライアントとして登録するには、**`access-defender static mac`** コマンドを使用します。

NOTE: スタティック認証が有効なインターフェースにおいて、他認証で認証済み、または Discard 登録されたクライアントを、**`access-defender static mac`** コマンドで登録すると、スタティック認証クライアントとして上書きされます。

7. DHCP スヌーピング

DHCP スヌーピングの機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

7.1 DHCP スヌーピングの機能説明

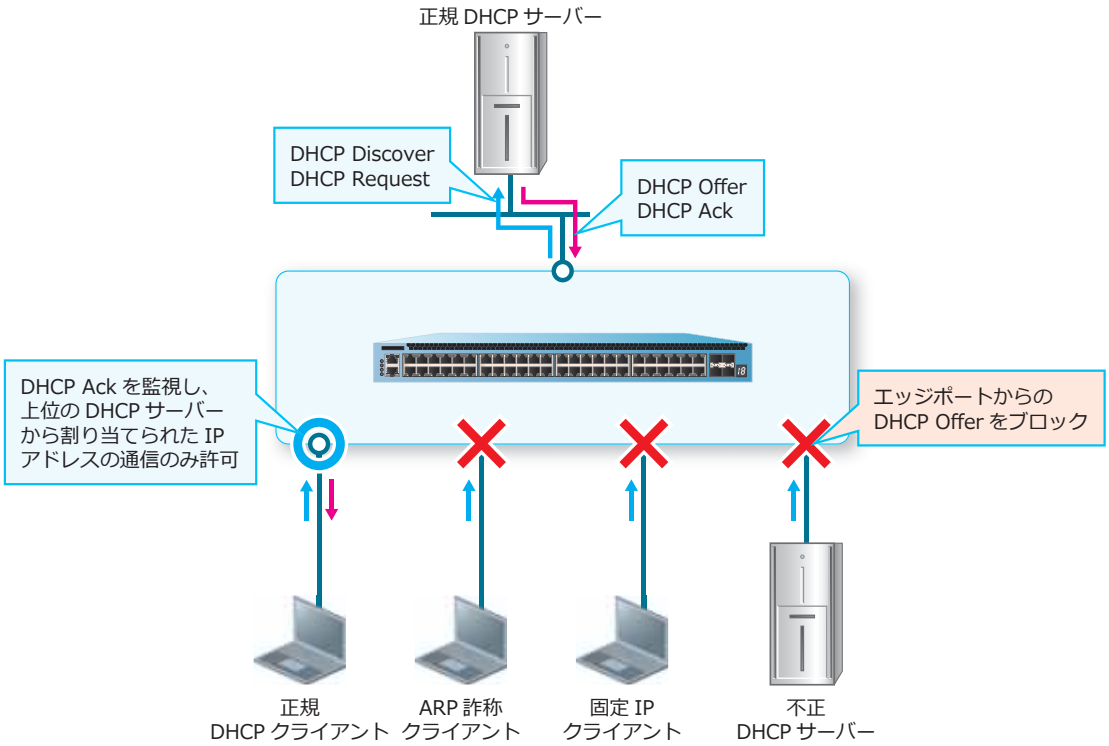
DHCP スヌーピングは、正規の DHCP サーバーから IP アドレスを配布された DHCP クライアントにのみ、内部ネットワークへのアクセスを許可する機能です。装置全体で DHCP スヌーピングを有効化するには、**`dhcp-snooping enable`** コマンドを使用します。DHCP スヌーピングを有効にするインターフェースの設定には、**`dhcp-snooping interface`** コマンドを使用します。

CAUTION: DHCPv6 スヌーピングは未サポートです。

DHCP スヌーピングでは、DHCP サーバーと DHCP クライアントの間でやりとりされる DHCP パケットをのぞき見る（スヌーピングする）ことで、以下の内容を実現します。

- DHCP スヌーピングを有効にしたインターフェースで DHCP offer パケットの受信をブロックすることにより、不正に設置された DHCP サーバーによる IP アドレスの配布を禁止
- 固定 IP アドレス端末や、正規 DHCP サーバー以外から IP アドレスを取得した不正 DHCP クライアントからのアクセスを禁止
- ARP 詐称（ARP スプーフィング）を起点とした盗聴の防止

図 7-1 DHCP スヌーピング



7.1.1 DHCP スヌーピングのスタティックエントリー

DHCP スヌーピングを有効にしたインターフェースに固定 IP アドレス端末を接続すると、デフォルトではアクセスが禁止されますが、スタティックエントリーを登録することにより、固定 IP アドレス端末を許可できます。スタティックエントリーを登録するには、**`dhcp-snooping static-entry`** コマンドを使用します。

7.2 DHCP スヌーピングの仕組み

DHCP スヌーピングには、DENY モードと PERMIT モードの 2 つの動作モードがあります。DHCP スヌーピングを有効にしたインターフェースが DENY モードの場合は、登録されたクライアントからの通信（IPv4、ARP）が許可され、それ以外のクライアントからの通信（IPv4、ARP）が制限されます。PERMIT モードの場合は、未登録クライアントからの通信（IPv4、ARP）も許可されます。

> ***NOTE:*** DHCP スヌーピングの動作モードにかかわらず、DHCP スヌーピングだけを有効にしたインターフェースでは、非 IP パケットは制限されません。
>
> ***NOTE:*** DHCP スヌーピングの動作モードにかかわらず、DHCP スヌーピングを有効にしたインターフェースでは、DHCP サーバーからの DHCP offer パケットを破棄します。
>
> ***NOTE:*** DHCPv6 スヌーピングは未サポートです。IPv6 パケットは、動作モードが DENY モードの場合は制限されますが、PERMIT モードの場合は制限されません。なお、DENY モードの場合でも NDP の一部のパケットは制限されません。

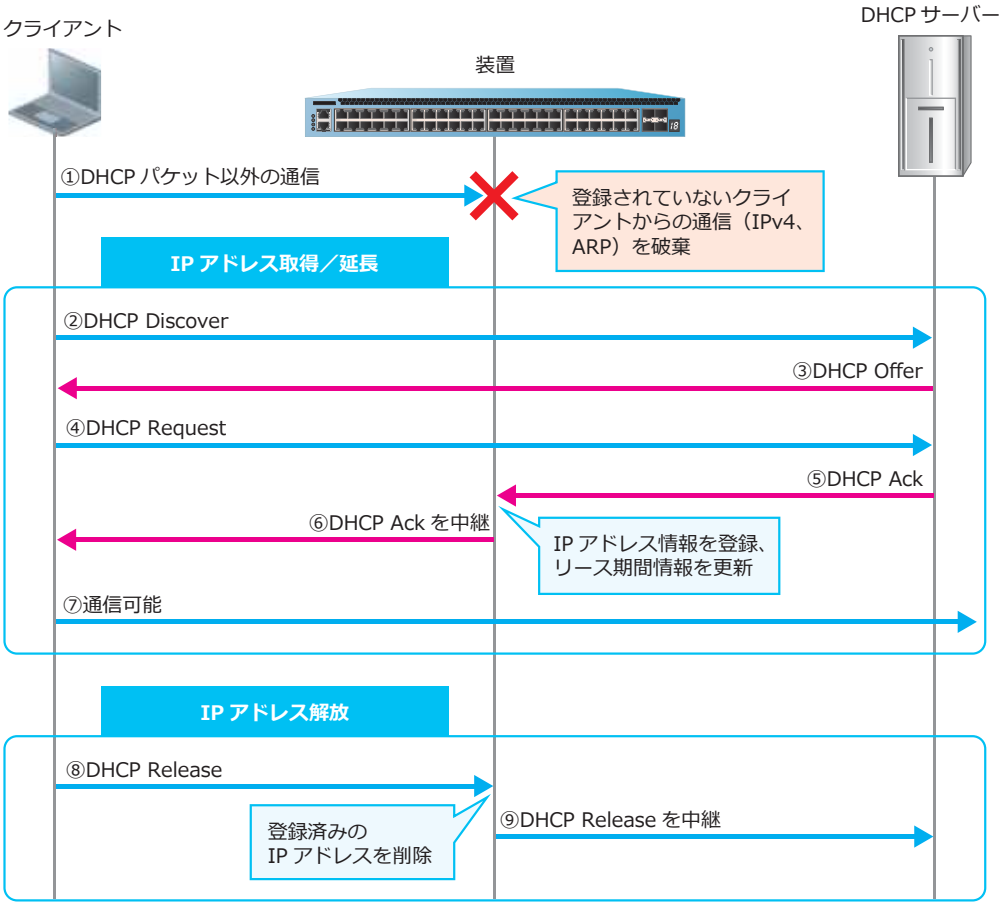
動作モードは手動で DENY モードに設定するか、または自動切り替えタイマーで PERMIT モードから DENY モードに切り替えることができます。自動切り替えタイマーを設定すると、装置が起動して DHCP スヌーピングが有効になってから一定時間は PERMIT モードで動作し、自動切り替えタイマーが満了すると DENY モードに切り替わります。手動で DENY モードに設定するには、**`dhcp-snooping mode deny`** コマンドを使用します。自動切り替えタイマーを設定するには、**`dhcp-snooping mode timer`** コマンドを使用します。

登録された DHCP スヌーピングエントリーは、クライアントから DHCP Release パケットを受信すると削除されます。また、DHCP Release パケットを受信しなかった場合でも、DHCP サーバーから払い出されたリース期間が経過すると、DHCP スヌーピングエントリーは削除されます。

7.2.1 DENY モード

DENY モードの場合は、登録されたクライアントからの通信（IPv4、ARP）が許可され、それ以外のクライアントからの通信（IPv4、ARP）が制限されます。DENY モードの動作フローは下図のとおりです。

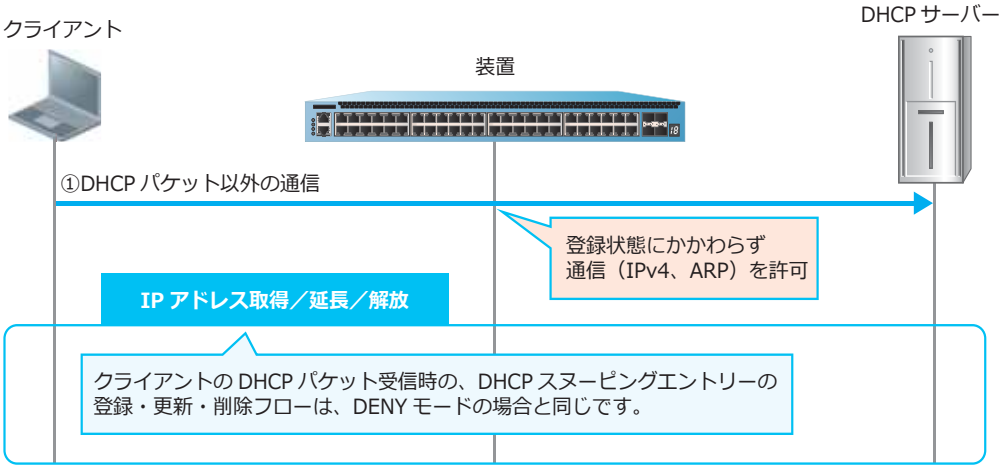
図 7-2 DENY モードの動作フロー



7.2.2 PERMIT モード

PERMIT モードの場合は、登録されたクライアントだけでなく、未登録クライアントからの通信（IPv4、ARP）も許可されます。

図 7-3 PERMIT モードの動作フロー



7.3 DHCP スヌーピングと他の認証機能の併用

DHCP スヌーピングと他の認証機能を併用したインターフェースでは、他の認証機能で認証に成功しないと通信が許可されなくなります。また、制限動作もより IPv4 パケットに特化した制限動作になります。具体的には、以下のように変更されます。

- DHCP スヌーピング（DENY モード）と他の認証機能を併用したインターフェースでは、非 IP パケットと IPv6 パケット（NDP の一部のパケットは除く）は、認証状態にかかわらず制限。
- DHCP スヌーピングエントリーとして登録されると、登録された IP アドレスからの ARP を許可。
- 他の認証機能で認証に成功すると、認証済みクライアントの MAC アドレスからの IPv4 パケットを許可。

CAUTION: DHCP スヌーピングとゲートウェイ認証は併用できません。

NOTE: DHCP スヌーピングの動作モードが PERMIT モードの場合は、認証状態にかかわらずすべての通信（DHCP offer を除く）が許可されます。

7.3.1 DHCP スヌーピングの MAC 認証モード

DHCP スヌーピングと MAC 認証を併用したインターフェースにおいて、DHCP スヌーピングの MAC 認証モードを有効にすると、MAC 認証に成功した場合のみ DHCP スヌーピングの処理を開始させるようにすることができます。DHCP スヌーピングの MAC 認証モードを有効にするには、**`dhcp-snooping mode mac-authentication`** コマンドを使用します。

8. OR 認証（1 ポート複数認証）

OR 認証（1 ポート複数認証）の機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

8.1 OR 認証（1 ポート複数認証）の機能説明

AccessDefender では、同一インターフェースで複数の認証機能を有効にすること（**OR 認証**）ができます。いずれか 1 つの認証機能で認証に成功すると、アクセスが許可されます。OR 認証の併用可能な組み合わせを以下に示します。

表 8-1 OR 認証（1 ポート複数認証）の併用可能な組み合わせ

OR 認証の併用可能な組み合わせ	動作概要
Web 認証、MAC 認証	• 同一ポートで Web 認証と MAC 認証を併用し、どちらか 1 つの認証機能で認証に成功した場合にアクセスが許可される。 • MAC 認証に失敗して Discard 登録された状態でも、MAC 認証以外の認証機能は処理可能。 • その他、スタティック認証や DHCP スヌーピングも、同一ポートで併用可能。
Web 認証、IEEE 802.1X 認証	• 同一ポートで Web 認証と IEEE 802.1X 認証を併用し、どちらか 1 つの認証機能で認証に成功した場合に許可される。 • その他、スタティック認証や DHCP スヌーピングも、同一ポートで併用可能。
IEEE 802.1X 認証、MAC 認証	• 同一ポートで IEEE 802.1X 認証と MAC 認証を併用し、どちらか 1 つの認証機能で認証に成功した場合に許可される。 • MAC 認証に失敗して Discard 登録された状態でも、MAC 認証以外の認証機能は処理可能。 • その他、スタティック認証や DHCP スヌーピングも、同一ポートで併用可能。
Web 認証、IEEE 802.1X 認証、MAC 認証	• 同一ポートで Web 認証、IEEE 802.1X 認証、および MAC 認証を併用し、いずれか 1 つの認証機能で認証に成功した場合にアクセスが許可される。 • MAC 認証に失敗して Discard 登録された状態でも、MAC 認証以外の認証機能は処理可能。 • その他、スタティック認証や DHCP スヌーピングも、同一ポートで併用可能。

CAUTION: ゲートウェイ認証を有効にしたインターフェースでは、他の認証機能は併用できません。

8.2 OR 認証（1 ポート複数認証）のオプション機能

OR 認証（1 ポート複数認証）に関連するオプション機能を以下に示します。

- MAC 認証に失敗した場合のみ IEEE 802.1X 認証を開始させる設定
- DHCP スヌーピングと MAC 認証併用時のオプション機能については、「DHCP スヌーピング」の「DHCP スヌーピングの MAC 認証モード」を参照

8.2.1 MAC 認証に失敗した場合のみ IEEE 802.1X 認証を開始させる設定

MAC 認証と IEEE 802.1X 認証を併用しているインターフェースで、MAC 認証に失敗した場合のみ IEEE 802.1X 認証を開始させるように変更できます。これにより、MAC 認証に成功した端末に対して IEEE 802.1X 認証処理が動作するのを防ぎます。

MAC 認証に失敗した場合のみ IEEE 802.1X 認証を開始させるように設定するには、**`dot1x mode mac-authentication-fail`** コマンドを使用します。

9. AND 認証

AND 認証の機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

9.1 AND 認証の機能説明

AND 認証は、同一インターフェースに複数の認証機能を設定し、そのすべての認証機能で認証に成功した場合にアクセスを許可する機能です。設定した複数の認証機能のうち 1 つでも認証に失敗した場合、アクセスは拒否されます。以下に、使用可能な AND 認証を示します。

表 9-1 AND 認証

AND 認証 パラメーター名 *1	動作概要
Web/MAC 認証（AND） web-mac	• 同一ポートで Web 認証と MAC 認証を併用し、すべての認証機能で認証に成功した場合にアクセスが許可される。 • スタティック認証は同一ポートで併用可能。
Web/IEEE 802.1X 認証（AND） web-dot1x	• 同一ポートで Web 認証と IEEE 802.1X 認証を併用し、すべての認証機能で認証に成功した場合にアクセスが許可される。 • スタティック認証は同一ポートで併用可能。
IEEE 802.1X/MAC 認証（AND） dot1x-mac	• 同一ポートで IEEE 802.1X 認証と MAC 認証を併用し、すべての認証機能で認証に成功した場合にアクセスが許可される。 • スタティック認証は同一ポートで併用可能。
Web/IEEE 802.1X/MAC 認証（AND） web-dot1x-mac	• 同一ポートで Web 認証、IEEE 802.1X 認証、および MAC 認証を併用し、すべての認証機能で認証に成功した場合にアクセスが許可される。 • スタティック認証は同一ポートで併用可能。

*1：**`authentication interface`** コマンドで有効にする場合のパラメーター名です。

CAUTION: 一部の例外を除き、AND 認証を有効にしたインターフェースでは、他の認証機能、DHCP スヌーピングは併用できません。

NOTE: AND 認証は、すべての認証で成功した場合に **`show access-defender client`** コマンドで認証済みクライアントとして表示されます。一部の認証でのみ成功した状態では、**`show access-defender client`** コマンドで表示されません。

9.1.1 AND 認証と MAC 認証の併用

AND 認証を有効にしたインターフェースでは、基本的には他の認証機能を併用できませんが、Web/MAC 認証（AND）または Web/IEEE 802.1 認証（AND）を有効にしたインターフェースでは、MAC 認証を併用（OR 認証）できます。それぞれ併用した場合の動作は以下のとおりです。

- Web/MAC 認証（AND）と MAC 認証を同一インターフェースで併用（OR 認証）した場合、MAC 認証は通常の MAC 認証の動作になりますが、Web/MAC 認証（AND）は動作が変更されます。このケースでの Web/MAC 認証（AND）は、Web 認証ページにアクセスしてユーザー名 / パスワードを入力すると、「① MAC 認証のユーザー名 / パスワードで認証問い合わせ」、「② Web 認証のユーザー名 / パスワードで認証問い合わせ」の 2 回認証の問い合わせを行い、両方で認証に成功した場合にアクセスが許可されます。

- Web/IEEE 802.1X 認証（AND）と MAC 認証を同一インターフェースで併用（OR 認証）した場合、MAC 認証は通常の MAC 認証の動作になり、Web/IEEE 802.1X 認証（AND）も通常の Web/IEEE 802.1X 認証（AND）の動作になります。

9.2 AND 認証の認証フロー

以下に示すパターンの AND 認証の認証フローについて説明します。

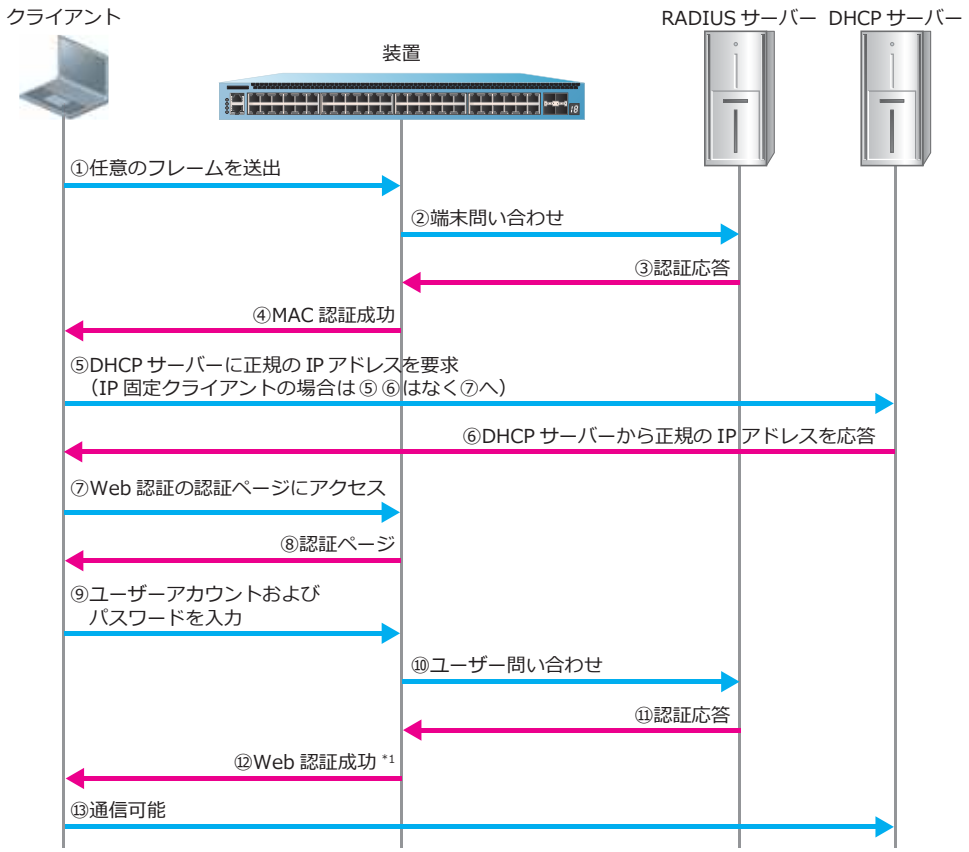
- Web/MAC 認証（AND）
- Web/IEEE 802.1X 認証（AND）
- IEEE 802.1X/MAC 認証（AND）
- Web/IEEE 802.1X/MAC 認証（AND）

9.2.1 Web/MAC 認証（AND）

Web/MAC 認証（AND）は、MAC 認証、Web 認証の順番で、両方の認証に成功した場合にアクセスが許可されます。なお、個々の認証機能は独立して動作しているため、RADIUS サーバーからの応答遅延などで認証の順番が逆になる可能性もありますが、MAC 認証に成功していない状態で Web 認証に成功しても、ログイン失敗となりアクセスは拒否されます。

ダイナミック VLAN を使用しない場合の、Web/MAC 認証（AND）の認証フローを以下に示します。この例では認証クライアントが DHCP クライアントのため、認証バイパス機能を使用して DHCP パケットをバイパスしています。

図 9-1 Web/MAC 認証（AND）の認証フロー



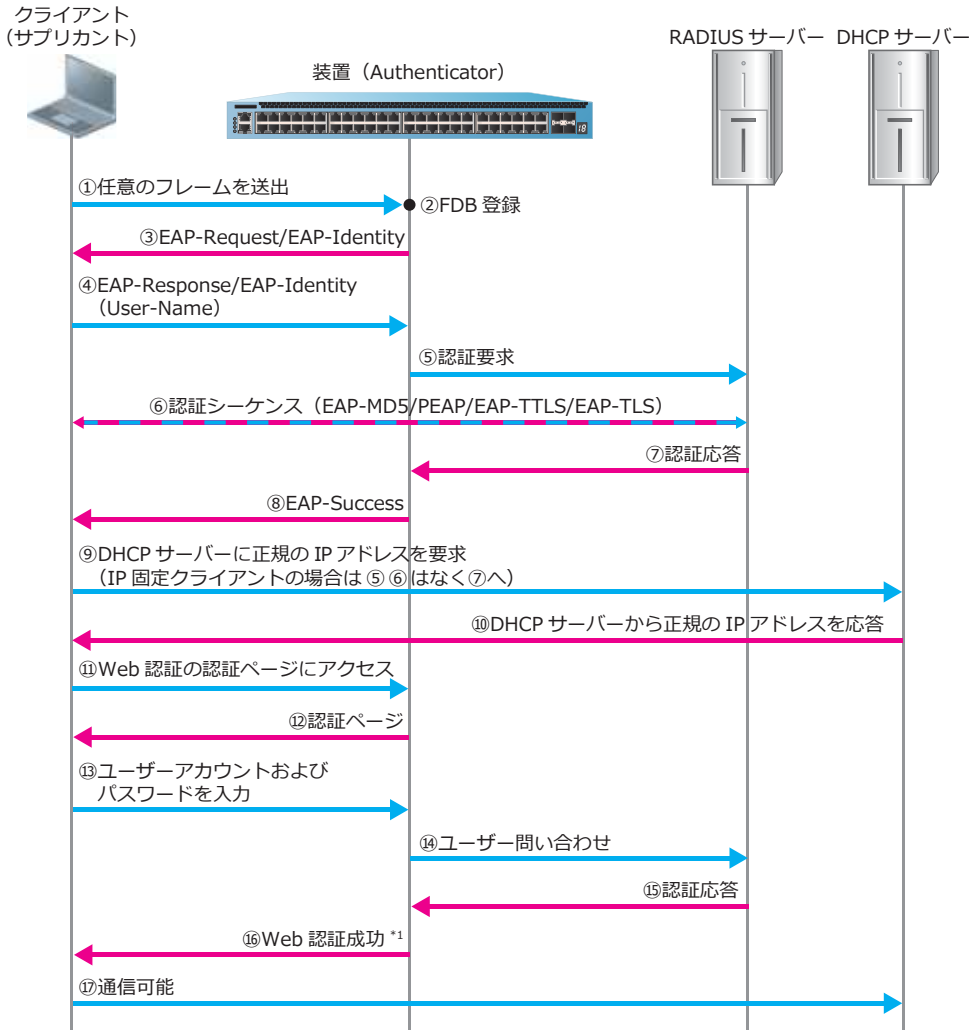
*1：ダイナミック VLAN 使用時は、VLAN ID が変更されます。

9.2.2 Web/IEEE 802.1X 認証（AND）

Web/IEEE 802.1X 認証（AND）は、IEEE 802.1X 認証、Web 認証の順番で、両方の認証に成功した場合にアクセスが許可されます。なお、個々の認証機能は独立して動作しているため、RADIUS サーバーからの応答遅延などで認証の順番が逆になる可能性もありますが、IEEE 802.1X 認証に成功していない状態で Web 認証に成功しても、ログイン失敗となりアクセスは拒否されます。

ダイナミック VLAN を使用しない場合の、Web/IEEE 802.1X 認証（AND）の認証フローを以下に示します。この例では認証クライアントが DHCP クライアントのため、認証バイパス機能を使用して DHCP パケットをバイパスしています。

図 9-2 Web/IEEE 802.1X 認証（AND）の認証フロー



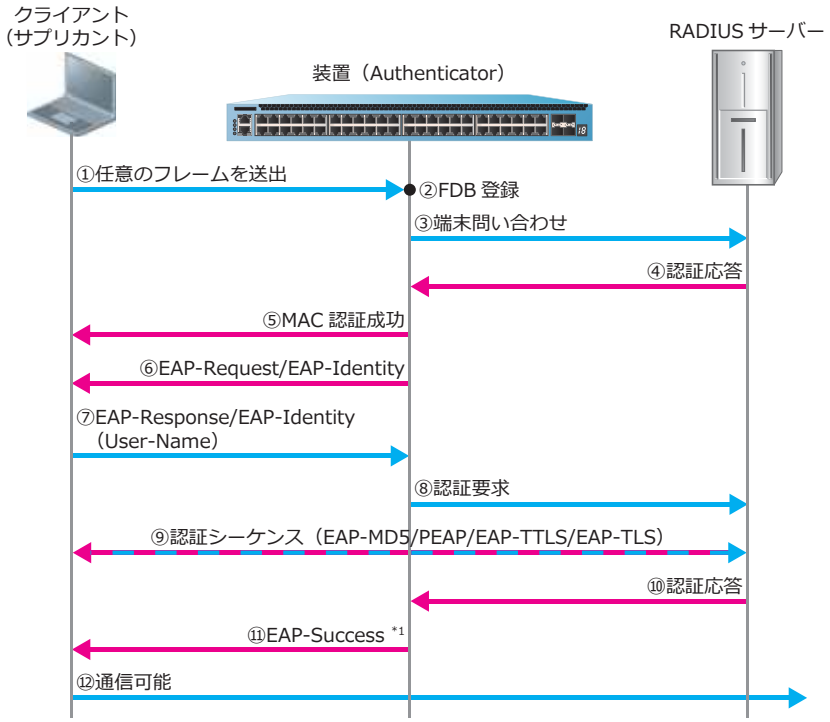
*1：ダイナミック VLAN 使用時は、VLAN ID が変更されます。

9.2.3 IEEE 802.1X/MAC 認証（AND）

IEEE 802.1X/MAC 認証（AND）は、MAC 認証、IEEE 802.1X 認証の順番で、両方の認証に成功した場合にアクセスが許可されます。なお、個々の認証機能は独立して動作しているため、RADIUS サーバーからの応答遅延などで認証の順番が逆になる可能性もありますが、MAC 認証に成功していない状態で IEEE 802.1X 認証に成功しても、ログイン失敗となりアクセスは拒否されます。

ダイナミック VLAN を使用しない場合の、IEEE 802.1X/MAC 認証（AND）の認証フローを以下に示します。

図 9-3 IEEE 802.1X/MAC 認証（AND）の認証フロー



*1：ダイナミック VLAN 使用時は、VLAN ID が変更されます。

9.2.4 Web/IEEE 802.1X/MAC 認証（AND）

Web/IEEE 802.1X/MAC 認証（AND）は、MAC 認証、IEEE 802.1X、Web 認証の順番で、すべての認証に成功した場合にアクセスが許可されます。なお、個々の認証機能は独立して動作しているため、RADIUS サーバーからの応答遅延などで認証の順番が逆になる可能性もありますが、MAC 認証や IEEE 802.1X 認証に成功していない状態で Web 認証に成功しても、ログイン失敗となりアクセスは拒否されます。

9.3 AND 認証のオプション機能

AND 認証に関連するオプション機能を以下に示します。

- 適用する属性値（VLAN ID やクラス ID）の取得元の選択機能
- アドバンスド VLAN 設定モード
- MAC 認証失敗クライアントへの Web 認証ページ応答抑止

9.3.1 適用する属性値（VLAN ID やクラス ID）の取得元の選択機能

AND 認証に成功したクライアントに適用する認証属性（VLAN ID やクラス ID）は、デフォルトでは以下の動作になります。

- Web/MAC 認証（AND）、Web/IEEE 802.1X 認証（AND）、Web/IEEE 802.1X/MAC 認証（AND）では、デフォルトでは Web 認証で取得した属性値（VLAN ID やクラス ID）が反映される。
- IEEE 802.1X/MAC 認証（AND）では、デフォルトでは IEEE 802.1X 認証で取得した属性値（VLAN ID やクラス ID）が反映される。

適用される属性値（VLAN ID やクラス ID）を、他の認証機能で取得した属性値に変更できます。適用する属性値の取得元を変更するには、**`authentication prefer-attribute`** コマンドを使用します。

9.3.2 アドバンスド VLAN 設定モード

アドバンスド VLAN 設定モードを有効にした Web/IEEE 802.1X 認証（AND）の場合、IEEE 802.1X 認証処理で認証に成功した時点で、通信が許可されない状態で IEEE 802.1X 認証処理で取得した属性値（VLAN ID、クラス ID）が、装置に反映されるようになります。

同様に、アドバンスド VLAN 設定モードを有効にした Web/MAC 認証（AND）の場合、MAC 認証処理で認証に成功した時点で、通信が許可されない状態で MAC 認証処理で取得した属性値（VLAN ID、クラス ID）が、装置に反映されるようになります。

アドバンスド VLAN 設定モードを使用すると、以下のような運用ができます。

- たとえば Web/IEEE 802.1X 認証（AND）でダイナミック VLAN を使用する場合に、IEEE 802.1X 認証に成功した時点で暫定 VLAN ではなく最終的な正規 VLAN を割り当てることにより、暫定 DHCP サーバーを使わない設計が可能になります。
- たとえば Web/IEEE 802.1X 認証（AND）で Web 認証ページを外部 Web サーバーにリダイレクトしている場合に、IEEE 802.1X 認証に成功したクライアントにクラス ID を割り当て、そのクラス ID にマッチした場合のみ外部 Web サーバーへのリダイレクトをバイパスすることにより、外部 Web サーバーへのバイパス対象を絞り込むことができます。

  CAUTION: IEEE 802.1X/MAC 認証（AND）と、Web/IEEE 802.1X/MAC 認証（AND）では、アドバンス VLAN 設定モードは使用できません。

アドバンスド VLAN 設定モードを有効にするには、**`authentication web-dot1x advanced-vlan-setting`** コマンドまたは **`authentication web-mac advanced-vlan-setting`** コマンドを使用します。

9.3.3 MAC 認証失敗クライアントへの Web 認証ページ応答抑止

Web/MAC 認証（AND）において、MAC 認証処理で認証に失敗したクライアントに対して Web 認証ページを応答しないようにできます。

> ***CAUTION:*** Web/IEEE 802.1X 認証（AND）、IEEE 802.1X/MAC 認証（AND）、Web/IEEE 802.1X/MAC 認証（AND）では、本機能は使用できません。
>
> ***CAUTION:*** AND 認証と MAC 認証の併用インターフェースでは、本機能は動作しません。
>
> ***NOTE:*** 本機能は、NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降でサポートしています。

MAC 認証処理で認証に失敗したクライアントに対して、Web 認証ページを応答しないようにするには、**`authentication web-mac abort-if-failure`** コマンドを使用します。

10. AccessDefender の認証方式

AccessDefender の認証方式の機能について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

10.1 AccessDefender の認証方式の機能説明

AccessDefender では、以下の方法により認証可否を決定できます。

- RADIUS 認証
- ローカルデータベース認証
- 強制認証

複数の RADIUS サーバーを設定した場合は、登録リストの先頭から問い合わせを行います。タイムアウトなどで問い合わせた RADIUS サーバーからの応答がない場合には、次に登録された RADIUS サーバーに問い合わせします。

MAC 認証で使用する認証方式を設定するには、**`aaa authentication mac-auth`** コマンドを使用します。Web 認証またはゲートウェイ認証で使用する認証方式を設定するには、**`aaa authentication web-auth`** コマンドを使用します。IEEE 802.1X 認証で使用する認証方式を指定するには、**`aaa authentication dot1x`** コマンドを使用します。

NOTE: AccessDefender のユーザー名とパスワードは、最大 63 文字で指定します。ASCII コードの印字可能な文字のうち、; , | " ? 空白文字 を除いた文字のみ使用可能です。

NOTE: **`aaa authentication mac-auth`** コマンドのインターフェースごとの設定は、NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降でサポートしています。

NOTE: **`aaa authentication web-auth`** コマンドのインターフェースごとの設定は、NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降でサポートしています。

10.2 RADIUS 認証

AccessDefender では、RADIUS サーバーを認証サーバーとして使用できます。

RADIUS サーバーを設定するには、**`radius-server host`** コマンドを使用します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

RADIUS サーバーグループを設定するには、**`aaa group server radius`** コマンドを使用します。そして、**`server`** コマンドで所属する RADIUS サーバーを指定します。

10.2.1 ベンダー独自属性による VLAN ID、クラス ID の設定

認証成功後に動的に VLAN を変更する場合やクラス ID を割り当てる場合は、認証成功時に ApresiaNP シリーズに引き渡す VLAN ID およびクラス ID を、あらかじめ RADIUS サーバーに登録しておく必要があります。VLAN ID およびクラス ID を RADIUS サーバーに登録する際は、ベンダー独自属性（Vendor Specific Attribute）として登録します。なお、ベンダー独自属性の値は、アクセス許可属性として各ユーザーに紐付けて登録してください。

ユーザーからの認証要求を受信すると、ベンダー独自属性に設定した VLAN ID およびクラス ID が ApresiaNP シリーズに引き渡されます。動的に VLAN を変更する場合やクラス ID を割り当てる場合に、RADIUS サーバーに登録するベンダー独自属性は以下のとおりです。

表 10-1 RADIUS サーバーに登録するベンダー独自属性

属性	ベンダー独自属性値	動的な VLAN 変更の設定値	クラス ID 割り当ての設定値
Vendor-Specific	ベンダー ID	278	278
	ベンダー属性番号	192*1	193
	値	割り当てる VLAN ID	割り当てるクラス ID
	属性の型	整数（INTEGER）	整数（INTEGER）

*1：ベンダー独自属性による動的な VLAN 変更は、Web 認証および MAC 認証のみサポートしています。

10.2.2 Tunnel-Private-Group-Id による VLAN 設定

MAC 認証、Web 認証、および IEEE 802.1X 認証において、Tunnel-Private-Group-Id により動的に VLAN を変更する機能をサポートしています。

動的に VLAN を変更する場合は、認証成功時に ApresiaNP シリーズに引き渡す VLAN ID または VLAN 名称を、あらかじめ RADIUS サーバーに登録しておく必要があります。VLAN ID または VLAN 名称を RADIUS サーバーに登録する際は、Tunnel-Private-Group-Id に登録します。なお、Tunnel-Private-Group-Id は、アクセス許可属性として各ユーザーに登録してください。

ユーザーからの認証要求を受信すると、Tunnel-Private-Group-Id に設定した VLAN ID または VLAN 名称が ApresiaNP シリーズに引き渡されます。Tunnel-Private-Group-Id により動的に VLAN を変更する場合に、RADIUS サーバーに登録する属性は以下のとおりです。

表 10-2 Tunnel-Private-Group-Id による VLAN 変更で使用する属性

属性	属性値	設定値	備考
Tunnel-Type	使用するトンネリングプロトコル	13（VLAN）	固定
Tunnel-Medium-Type	データ転送媒体のプロトコル	6（IEEE 802）	固定
Tunnel-Private-Group-Id	トンネルが属するグループ ID	割り当てる VLAN ID または VLAN 名称	変更可能

10.2.3 AccessDefender で使用する RADIUS 属性

AccessDefender でサポートしている RADIUS 属性を以下に示します。

表 10-3 MAC 認証、Web 認証で使用する RADIUS 属性

属性	説明
User-Name	認証されるユーザー名
User-Password	パスワード

属性	説明
NAS-IP-Address	認証要求している RADIUS クライアントの IP アドレス（IPv4 のみ）
Calling-Station-Id	認証端末の MAC アドレス
NAS-Identifier	認証された端末が属している VLAN ID
NAS-Port	認証端末が接続されているインターフェース番号

表 10-4 IEEE 802.1X 認証で使用する RADIUS 属性

属性	説明
User-Name	認証されるユーザー名
NAS-IP-Address	認証要求しているオーセンティケーターの IP アドレス（IPv4 のみ）
Framed-MTU	サプリカントとオーセンティケーター間の最大フレームサイズ（1466 固定）
NAS-Port	サプリカントが接続されているオーセンティケーターのインターフェース番号
NAS-Port-Type	ユーザー認証に使用しているインターフェースのタイプ（Ethernet(15) 固定）
Service-Type	提供するサービスタイプ（Framed(2) 固定）
Calling-Station-Id	サプリカントの MAC アドレス
EAP-Message	EAP メッセージの送受信に使用
Message-Authenticator	RADIUS パケットの内容を保証するために使用
State	オーセンティケーターと RADIUS サーバー間の State 情報の保持
Tunnel-Type	動的 VLAN 割り当て用応答属性（VLAN(13) に設定）
Tunnel-Medium-Type	動的 VLAN 割り当て用応答属性（IEEE 802(6) に設定）
Tunnel-Private-Group-Id	動的 VLAN 割り当て用応答属性（割り当てる VLAN ID または VLAN 名称）

10.2.4 NAS 属性による制限

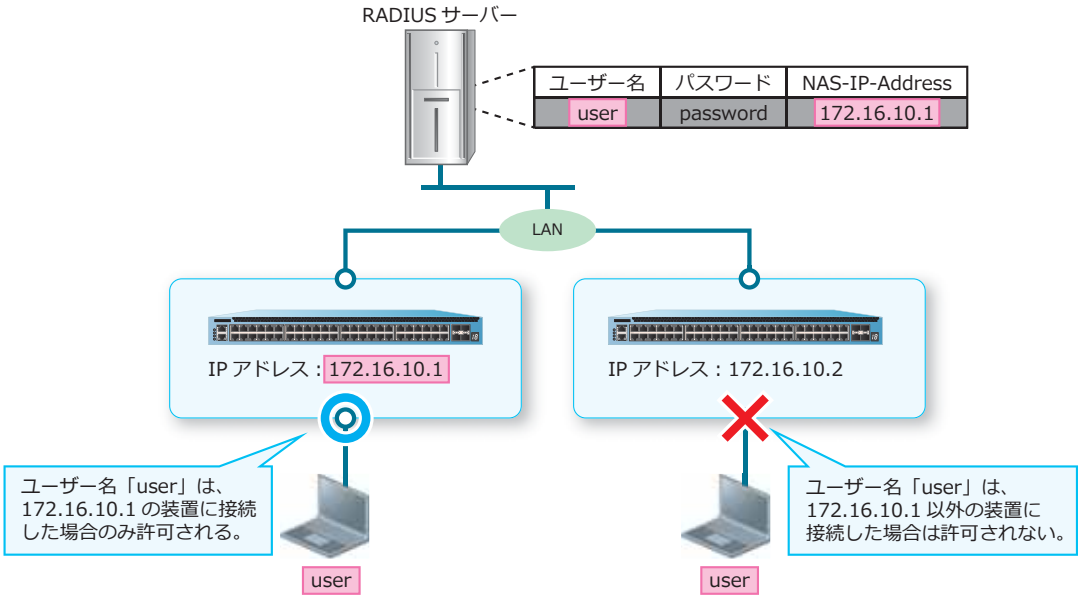
NAS（Network Access Server）属性による制限

RADIUS サーバーの以下の NAS 属性を設定すると、ユーザーアカウントごとにアクセスできる内部ネットワークを制限できます。各属性を単独で設定して制限するだけでなく、属性を組み合わせて制限することもできます。設定できる NAS 属性は、以下のとおりです。

- **NAS-IP-Address**

  NAS-IP-Address は、認証クライアントが接続している装置の IP アドレスです。そのユーザーアカウントでは、登録した装置に接続している認証クライアントで認証を行った場合のみ、内部ネットワークへのアクセスを許可します。

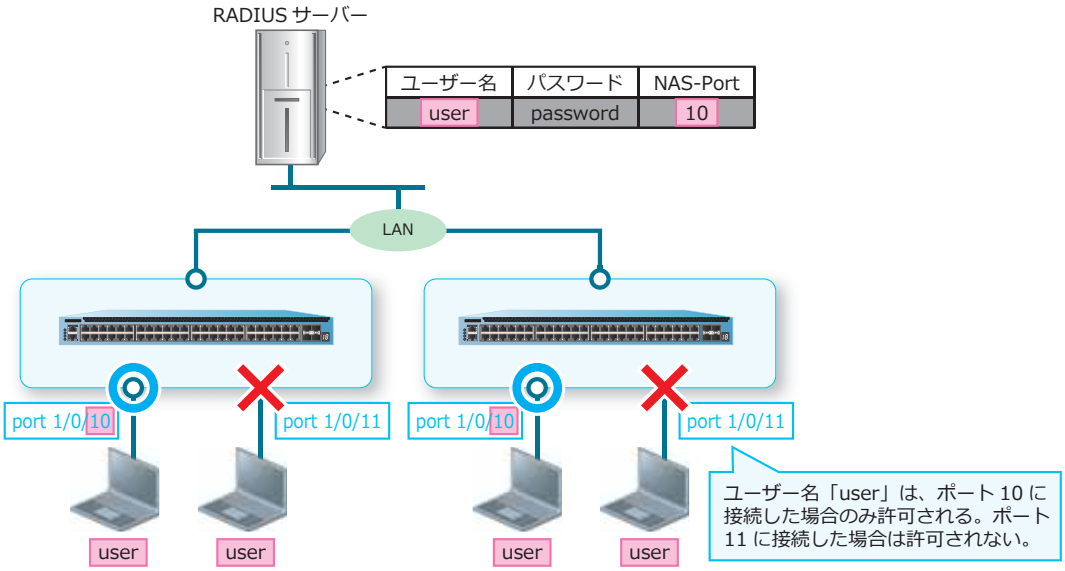
図 10-1 NAS-IP-Address 設定時のアクセス制限



- **NAS-Port**

  NAS-Port は、認証クライアントが接続している装置のポートです。そのユーザーアカウントでは、登録したポートに接続している認証クライアントで認証を行った場合のみ、内部ネットワークへのアクセスを許可します。

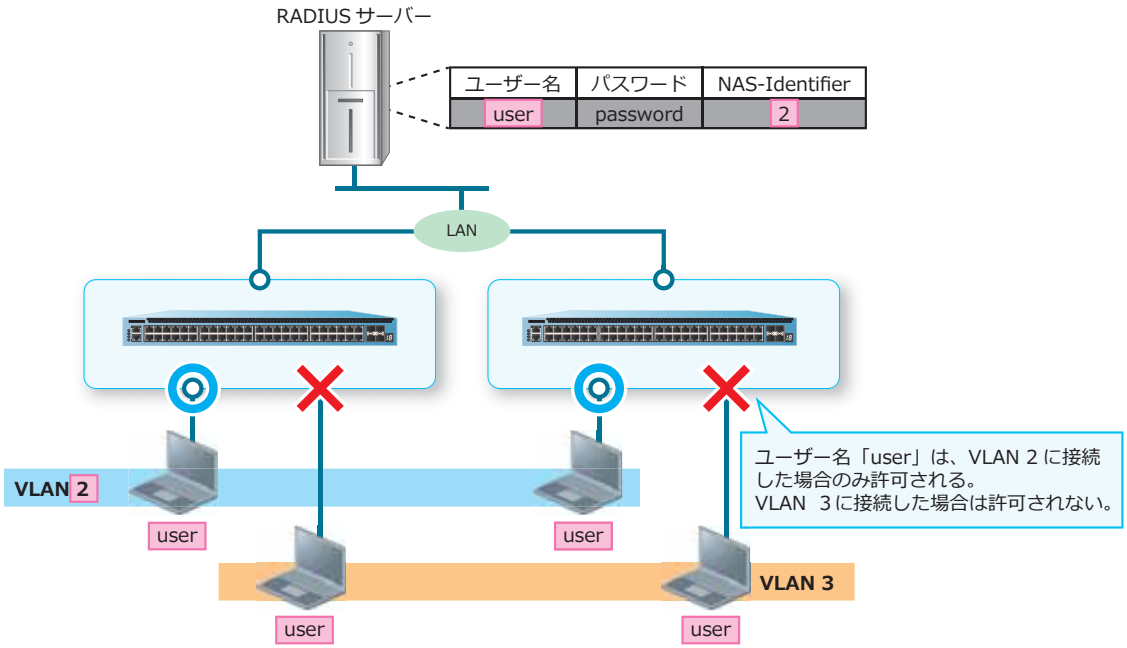
図 10-2 NAS-Port 設定時のアクセス制限



- **NAS-Identifier**

  NAS-Identifier は、認証クライアントが接続している装置の該当ポートの VLAN ID です。そのユーザーアカウントでは、登録した VLAN ID に接続している認証クライアントで認証を行った場合のみ、内部ネットワークへのアクセスを許可します。

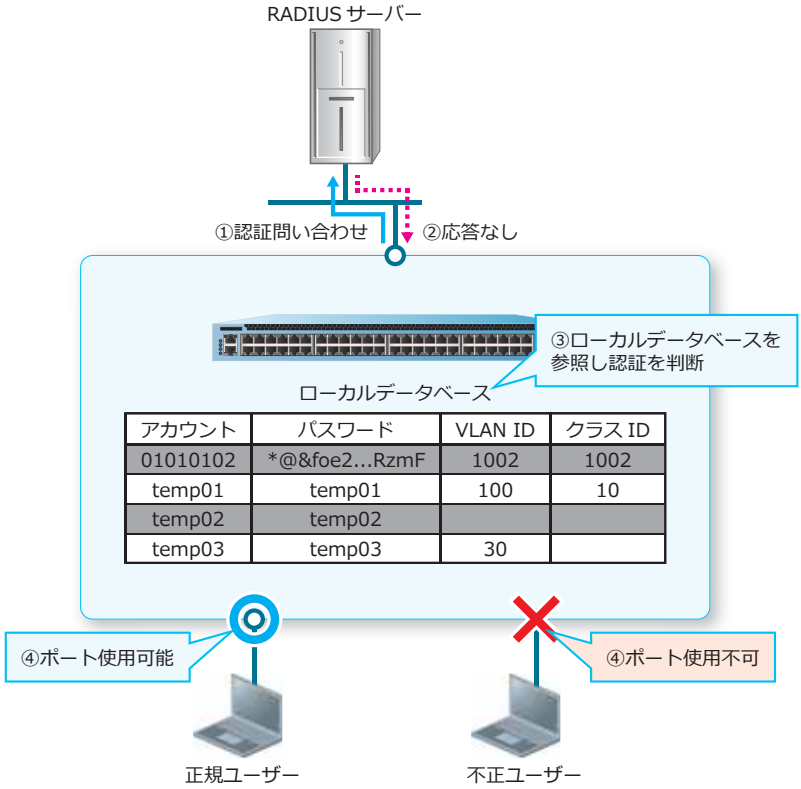
図 10-3 NAS-Identifier 設定時のアクセス制限



10.3 ローカルデータベース認証

ローカルデータベース認証が有効の場合は、RADIUS サーバーからの応答がタイムアウトした際に、装置の構成情報に**ローカルデータベース**として保存されたユーザーアカウントを利用して認証できます。ローカルデータベースには、ユーザー名、パスワード、VLAN ID、およびクラス ID が記載されています。

図 10-4 ローカルデータベース認証の構成例



CAUTION: ローカルデータベースは装置の構成情報として保存されます。変更を保存する場合は、**`write memory`** コマンドを使用してください。

NOTE: IEEE 802.1X 認証のローカルデータベース認証は未サポートです。

ローカルデータベースフォーマット

装置に保存するローカルデータベースは、csv 形式のファイルです。ローカルデータベースの入力例を以下に示します。

表 10-5 ローカルデータベースの入力例

```
 (1)       (2)                                  (3)   (4)   (5)
01010102,*@&foe2zgl6pwJiXjVe0+amVwAAAAC+RzmF,1002,1002,*
temp01,temp01,100,10
temp02,temp02
temp03,temp03,30
```

各項目の説明は、以下のとおりです。

表 10-6 ローカルデータベースの入力項目

項番	説明
(1)	ユーザー名を入力します。
(2)	パスワードを平文または暗号化した形式で入力します。
(3)	VLAN ID を入力します（省略可能）。
(4)	クラス ID を入力します（省略可能）。
(5)	その行のパスワードを暗号化した形式で入力する場合は、行末に「,*」を入力します（省略可能）。

ローカルデータベースの登録（ダウンロード）およびバックアップ（アップロード）

PC で作成したローカルデータベースを、TFTP サーバーまたは SD カードを使用して装置に登録（ダウンロード）できます。逆に、装置に登録されているローカルデータベースを、TFTP サーバーまたは SD カードにバックアップ（アップロード）することもできます。ローカルデータベースを登録（ダウンロード）またはバックアップ（アップロード）するには、**copy** コマンドを使用します。

ローカルデータベースの削除

装置に登録されているローカルデータベースを削除します。この場合は、すべてのユーザーアカウントが削除されます。ローカルデータベースを削除するには、**access-defender erase aaa-local-db** コマンドを使用します。

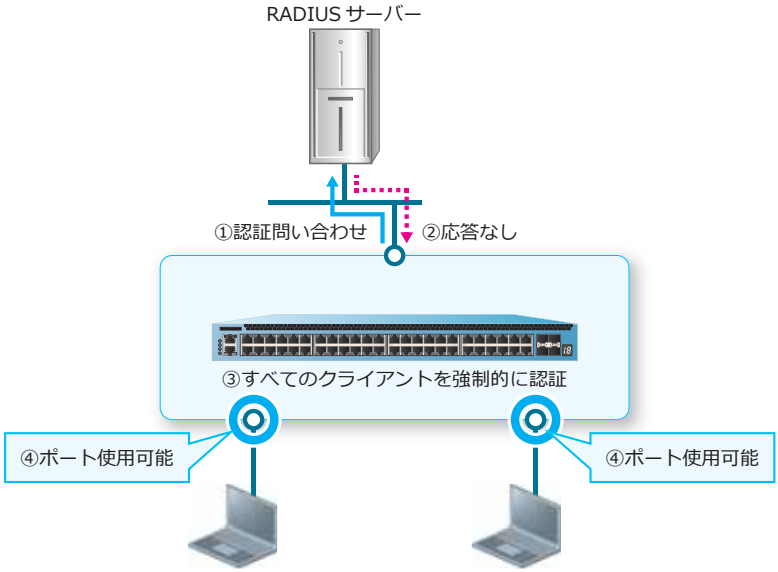
ユーザーアカウントの追加および削除

装置に保存されているローカルデータベースに、ユーザーアカウントを追加したり、削除したりできます。ユーザーアカウントを追加および削除するには、**aaa-local-db user** コマンドを使用します。

10.4 強制認証

MAC 認証、Web 認証、および IEEE 802.1X 認証で認証する際、RADIUS サーバーからの応答がタイムアウトしたときに、強制的に認証を成功させ、クライアントに内部ネットワークへのアクセスを許可できます。MAC 認証で強制認証を行う場合は、**`aaa authentication mac-auth`** コマンドで force パラメーターを指定します。Web 認証で強制認証を行う場合は、**`aaa authentication web-auth`** コマンドで force パラメーターを指定します。IEEE 802.1X 認証で強制認証を行う場合は、**`aaa authentication dot1x`** コマンドで force パラメーターを指定します。

図 10-5 強制認証の構成例



CAUTION: 強制認証は、セキュリティー上の問題となる可能性があります。強制認証を使用する前に、十分に検討してください。

10.5 認証方式の優先順位設定

MAC 認証、Web 認証、および IEEE 802.1X 認証では、以下の認証方式を使用できます。

- **local**

  AccessDefender のローカルデータベース認証（MAC 認証、Web 認証のみ）

- **group radius**

  `radius-server host` コマンドで設定したすべての RADIUS サーバー

- **group グループ名**

  `aaa group server radius` コマンドで設定した RADIUS サーバーグループに登録されている RADIUS サーバー

- **force**

  強制認証

認証方式は認証方法ごとに最大で 4 個まで指定できます。認証方式を設定するには、**`aaa authentication mac-auth`** コマンド、**`aaa authentication web-auth`** コマンド、または **`aaa authentication dot1x`** コマンドを使用します。

> ***NOTE:*** IEEE 802.1X 認証ではローカルデータベース認証は未サポートです。IEEE 802.1X 認証を使用する際は必ず **`aaa authentication dot1x`** コマンドで RADIUS サーバーグループまたは強制認証を設定してください。

移行条件変更機能を有効に設定した場合には、複数の認証方式を指定した順番で使用できるようになります。

10.5.1 移行条件変更機能

複数の認証方式を指定していても、デフォルトでは先に指定した認証方式で認証が拒否されると内部ネットワークへのアクセスが許可されません。ただし、**移行条件変更機能**を有効にすると、1 つの認証方式で認証が拒否されても次の認証方式に移行します。そして他の認証方式で認証されたときは、内部ネットワークへのアクセスが許可されます。移行条件変更機能を有効化するには、**`aaa authentication control sufficient`** コマンドを使用します。

> ***CAUTION:*** IEEE 802.1X 認証では移行条件変更機能は使用できません。
>
> ***NOTE:*** 移行条件変更機能が有効な場合でも、他の認証方式で明示的に認証拒否と判定されて認証失敗になった場合には、強制認証は行われません。
>
> ***NOTE:*** 移行条件変更機能が無効の場合でも、RADIUS サーバーへの問い合わせがタイムアウトした場合には次の認証方式に移行します。

10.6 Web 認証の認証方式選択機能

Web 認証では、認証 ID ごとに認証方式を選択できます。認証 ID と認証方式を関連付けるには、**aaa authentication web-auth** コマンドを使用します。

ユーザーが認証方式を選択できるようにするためには、認証ページのログイン用フォームで認証 ID を指定するように認証ページをカスタマイズします。ログイン用のフォームの例を以下に示します。

> ***NOTE:*** デフォルトのログインページのようにユーザーが認証 ID を指定しない場合は、**aaa authentication web-auth 1** コマンドで設定した認証方式が使用されます。

表 10-7 認証方法選択用のフォーム（ユーザー選択型）の例

```
                (1)
<form method="POST" action="/cgi-bin/adeflogin.cgi">
<table>
<tr><th width="184">User Account:</th><td width="220">
               (2)
<input name="name" type="text" value="" size="30" maxlength="63"></td></tr>
<tr><th width="184">Password:</th><td width="220">
               (3)
<input name="pass" type="password" size="30" maxlength="63"></td></tr></table>
<tr><th width="184">Authentication method:</th><td width="220">
                           (4)             (5)
<input type="radio" name="authid" value="1">RADIUS Server 1<br>
<input type="radio" name="authid" value="2">RADIUS Server 2<br>
<input type="radio" name="authid" value="3">Forced Authentication<br>
<input type="radio" name="authid" value="4">Local Database<br>
</td></tr>
<input type="submit" name="action" value="login">
<input type="reset" value="reset">
</form>
```

各項目の説明は、以下のとおりです。

表 10-8 認証方法選択用のフォーム（ユーザー選択型）のポイント

項番	説明
(1)	form タグの method 属性に「POST」を設定します。
(2)	ユーザー名を入力するフォームの name 属性に「name」を設定します。
(3)	パスワードを入力するフォームの name 属性に「pass」を設定します。
(4)	認証 ID を指定するフォームの name 属性に「authid」を設定します。
(5)	認証 ID を指定するフォームの value 属性に認証 ID を設定します。

次に、認証ページを表示したときに、認証 ID が「2」に設定されている場合（ユーザーが選択できない場合）のログイン用のフォームの例を以下に示します。

表 10-9 ログイン用のフォーム（埋め込み型）の例

```
                (1)
<form method="POST" action="http://192.0.2.100:8080/cgi-bin/adeflogin.cgi">
<table>
<tr><th width="184">User Account:</th><td width="220">
              (2)
<input name="name" type="text" value="" size="30" maxlength="63"></td></tr>
<tr><th width="184">Password:</th><td width="220">
              (3)
<input name="pass" type="password" size="30" maxlength="63"></td></tr></table>
              (4)            (5)            (6)
<input type="hidden" name="authid" value="2">
<input type="submit" name="action" value="login">
<input type="reset" value="reset">
</form>
```

各項目の説明は、以下のとおりです。

表 10-10 ログイン用のフォーム（埋め込み型）のポイント

項番	説明
(1)	form タグの method 属性に「POST」を設定します。
(2)	ユーザー名を入力するフォームの name 属性に「name」を設定します。
(3)	パスワードを入力するフォームの name 属性に「pass」を設定します。
(4)	認証 ID を指定するフォームの type 属性に「hidden」を設定します。
(5)	認証 ID を指定するフォームの name 属性に「authid」を設定します。
(6)	認証 ID を指定するフォームの value 属性に認証 ID を設定します。

11. AccessDefender の show コマンド

AccessDefender の **show** コマンドについて説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

11.1 AccessDefender の設定の表示

AccessDefender の設定を確認する方法を説明します。

11.1.1 ポートの AccessDefender 設定の表示

show access-defender port-configuration コマンドで、ポートの AccessDefender の設定を確認できます。

表示例を以下に示します。

```
# show access-defender port-configuration

AccessDefender Port Configuration:
  mac = mac-authentication, 802.1X = IEEE802.1X,
  web = web-authentication, gateway = web-authentication gateway,
  web/mac = web/mac authentication,
  web/.1X = web/IEEE802.1X authentication,
  .1X/mac = IEEE802.1X/mac authentication,
  w/.1X/m = web/IEEE802.1X/mac authentication,
  DHCPSNP = DHCP snooping,
  linkdown = linkdown logout, TTL = web-authentication ttl filter,
  ld time = logout linkdown time,
  o = enable, x = disable
(1)
Type      C Port
            1       8 9      16 17     24 25
            +------+ +------+ +------+ +---
mac       1 ........ oooo.... oooooooo ....
802.1X    1 ........ ........ oooooooo ....
web       1 oooooooo ........ oooooooo ....
gateway   1 ........ ........ ........ oo..
web/mac   1 ........ ......oo ........ ....
web/.1X   1 ........ ....oo.. ........ ....
.1X/mac   1 ........ ........ ........ ....
w/.1X/m   1 ........ ........ ........ ....
DHCPSNP   1 ........ ........ ........ ....
roaming   1 ........ oooooooo ........ ....
static    1 ........ ........ ........ ....
linkdown  1 xxxxxxxx xxxxxxxx ........ ....
ld time   1 ........ ........ oooooooo ....
TTL       1 oooooooo ........ ........ ....
```

各項目の説明は、以下のとおりです。

表 11-1 `show access-defender port-configuration` コマンドの表示項目

項番	説明
(1)	ポートごとに、AccessDefender 設定の各機能の有効／無効を表示します。 • mac：MAC 認証 • 802.1X：IEEE 802.1X 認証 • web：Web 認証 • gateway：ゲートウェイ認証 • web/mac：Web/MAC 認証（AND） • web/.1X：Web/IEEE 802.1X 認証（AND） • .1X/mac：IEEE 802.1X/MAC 認証（AND） • w/.1X/m：Web/IEEE 802.1X/MAC 認証（AND） • DHCPSNP：DHCP スヌーピング • roaming：ローミング機能 • static：スタティック認証 • linkdown：x 表示の場合、リンクダウンによるログアウトが無効 • ld time：リンクダウン監視時間の設定 • TTL：Web 認証の TTL フィルター機能 "C" 列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。

11.1.2 ポートチャネルの AccessDefender 設定の表示

show access-defender port-channel-configuration コマンドで、ポートチャネルの AccessDefender の設定を確認できます。

表示例を以下に示します。

```
# show access-defender port-channel-configuration

AccessDefender Port-channel Configuration:
  mac = mac-authentication, 802.1X = IEEE802.1X,
  web = web-authentication, gateway = web-authentication gateway,
  web/mac = web/mac authentication,
  web/.1X = web/IEEE802.1X authentication,
  .1X/mac = IEEE802.1X/mac authentication,
  w/.1X/m = web/IEEE802.1X/mac authentication,
  DHCPSNP = DHCP snooping,
  linkdown = linkdown logout, TTL = web-authentication ttl filter,
  ld time = logout linkdown time,
  o = enable, x = disable
(1)
Type      C Port-channel ID
            1      8 9     16 17    24 25    32 33    40 41    48
            +------+ +------+ +------+ +------+ +------+ +------+
mac       1 oooooo.. ........ ........ ........ ........ ........
802.1X    1 ........ ........ ........ oooo.... ........ ........
web       1 oooooo.. ........ ........ ........ ........ ........
gateway   1 ........ ........ oo...... ........ ........ ........
web/mac   1 .......o ........ ........ ........ ........ ........
web/.1X   1 ......o. ........ ........ ........ ........ ........
.1X/mac   1 ........ o....... ........ ........ ........ ........
w/.1X/m   1 ........ .o...... ........ ........ ........ ........
DHCPSNP   1 ........ ........ ....oooo ........ ........ ........
roaming   1 oooooo.. ........ ........ ........ ........ ........
static    1 ........ ........ ........ ........ ........ ........
linkdown  1 xxxxxx.. ........ ........ ........ ........ ........
ld time   1 ........ ........ oo...... ........ ........ ........
TTL       1 oooooo.. ........ ........ ........ ........ ........
```

各項目の説明は、以下のとおりです。

表 11-2 show access-defender port-channel-configuration コマンドの表示項目

項番	説明
(1)	ポートチャネルごとに、AccessDefender 設定の各機能の有効／無効を表示します。 • mac：MAC 認証 • 802.1X：IEEE 802.1X 認証 • web：Web 認証 • gateway：ゲートウェイ認証 • web/mac：Web/MAC 認証（AND） • web/.1X：Web/IEEE 802.1X 認証（AND） • .1X/mac：IEEE 802.1X/MAC 認証（AND） • w/.1X/m：Web/IEEE 802.1X/MAC 認証（AND） • DHCPSNP：DHCP スヌーピング • roaming：ローミング機能 • static：スタティック認証 • linkdown：x 表示の場合、リンクダウンによるログアウトが無効 • ld time：リンクダウン監視時間の設定 • TTL：Web 認証の TTL フィルター機能 "C" 列はスタックのボックス ID を示しますが、本コマンドでは常に 1 が表示されます。

11.1.3 ローカルデータベースの情報の表示

show access-defender aaa-local-db コマンドで、ローカルデータベース情報を確認できます。表示例を以下に示します。

```
# show access-defender aaa-local-db
(1) (2)                                                                (3)    (4)
-------------------------------------------------------------------------------
No. Username                                                          VID   Class
-------------------------------------------------------------------------------
1   user1                                                              10
2   user2                                                              20
3   user3                                                              30
4   user4                                                              40      40
5   user5                                                              50
6   user6                                                              60      60
```

各項目の説明は、以下のとおりです。

表 11-3 show access-defender aaa-local-db コマンドの表示項目

項番	説明
(1)	通し番号を表示します。
(2)	ユーザー名を表示します。
(3)	VLAN ID を表示します。
(4)	クラス ID を表示します。

11.1.4 Web 認証ページの情報の表示

show access-defender webpages コマンドで、装置にダウンロードした Web 認証ページの情報を確認できます。

> ***NOTE:*** 本コマンドは、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降でサポートしています。

表示例を以下に示します。

```
# show access-defender webpages

WEBPAGES-ID:Default ...(1)
(2)                              (3)                  (4)
Filename                        Size                 Date
-------------------------------------------------------
login-failure-page               300 Jan 21 2017 09:00:00
login-page                      1000 Jan 21 2017 09:00:00
login-success-page              1000 Jan 21 2017 09:00:00
logout-failure-page              500 Jan 21 2017 09:00:00
logout-success-page              500 Jan 21 2017 09:00:00
redirect-error-page              500 Jan 21 2017 09:00:00

WEBPAGES-ID:1 ...(1)
(2)                              (3)                  (4)
Filename                        Size                 Date
-------------------------------------------------------
01-login-failure-page            500 Dec 12 2019 11:14:17
01-login-page                   2000 Dec 12 2019 11:15:20
01-login-success-page           1000 Dec 12 2019 11:17:26
01-logout-failure-page           500 Dec 12 2019 11:19:40
01-logout-success-page           500 Dec 12 2019 11:20:21
01-redirect-error-page           500 Dec 12 2019 11:22:37

WEBPAGES-ID:5 ...(1)
(2)                              (3)                  (4)
Filename                        Size                 Date
-------------------------------------------------------
05-login-page                   2000 Dec 12 2019 12:22:37
05-login-success-page           1000 Dec 12 2019 12:24:10
05-logout-success-page           500 Dec 12 2019 12:27:21
```

各項目の説明は、以下のとおりです。

表 11-4 show access-defender webpages コマンドの表示項目

項番	説明
(1)	個別 Web 認証ページ ID を表示します。 「カスタマイズされたデフォルト Web 認証ページ」の場合は Default と表示されます。なお、カスタマイズされていない「デフォルト Web 認証ページ」は表示されません。
(2)	ファイル名を表示します。
(3)	ファイルサイズを表示します。
(4)	ファイルの更新日時を表示します。

11.2 AccessDefender の動作状態の表示

AccessDefender の動作状態を確認する方法を説明します。

11.2.1 認証済みクライアントおよび認証失敗クライアントの表示

show access-defender client コマンドで、認証済みクライアントと、MAC 認証に失敗して Discard 登録されたクライアントを確認できます。

表示例を以下に示します。

```
# show access-defender client
Total number of Clients           :    4 ...(1)
Total number of Discarded Clients :    1 ...(2)

   Codes: W = Web authentication, G = Gateway authentication,
          M = MAC authentication, - = MAC authentication (discard),
          X = IEEE802.1X, D(S) = DHCP snooping (static),
          S = Static authentication
    Port: C = port-channel, * = roaming,
(3) (4)               (5)                                        (6)    (7)   (8)
T   MAC address       IP                                        Port   VID   Cls
(9)                                                                (10)    (11)
User                                                               Time    Aging
-------------------------------------------------------------------------------
-   00-17-A4-F6-D3-04 0.0.0.0                                   1/0/3   200
0017a4f6d304                                                    0:00:21 0:00:00

WD  00-17-A4-D6-B3-A4 172.170.100.100                           1/0/1 4094    10
webuser01                                                       0:20:39 0:00:00

WM  00-17-A4-D6-F3-C4 172.170.1.1                               1/0/2 4094    10
webuser03                                                       0:20:39 0:00:15

G   N/A               2000:adb8:85a3:85a2:aba3:8a2e:a370:7334  1/0/5*4094    10
webuser02                                                          5d1hr 0:00:24

D   00-17-29-7F-6F-2A 172.170.2.100                              C/1   300
N/A                                                             0:00:36 0:00:00
```

各項目の説明は、以下のとおりです。

表 11-5 show access-defender client コマンドの表示項目

項番	説明
(1)	認証済みクライアントの数を表示します。
(2)	MAC 認証に失敗して Discard 登録されたクライアントの数を表示します。

項番	説明
(3)	認証済みクライアント、MAC 認証に失敗して Discard 登録されたクライアントのタイプコードを表示します。タイプコードが複数ある場合は、そのクライアントが AND 認証に成功したことを意味します。 • W：Web 認証 • G：ゲートウェイ認証 • M：MAC 認証 • -：MAC 認証に失敗して Discard 登録されたクライアント • X：IEEE 802.1X 認証 • D：DHCP スヌーピング • S：スタティック認証
(4)	クライアントの MAC アドレスを表示します。
(5)	クライアントの IP アドレスを表示します。
(6)	クライアントが接続されたポート番号またはポートチャネル番号を表示します。
(7)	クライアントが所属する VLAN ID を表示します。
(8)	クライアントに関連付けられたクラス ID を表示します。クラス ID が関連付けられていない場合は表示されません。
(9)	クライアントのユーザー名を表示します。
(10)	クライアントが認証されてからの経過時間、MAC 認証に失敗して Discard 登録されてからの経過時間を表示します。経過時間が 10 時間より短い場合は（時）:（分）:（秒）形式で表示され、10 時間以上の場合は（日）d（時）hr 形式で表示されます。
(11)	認証済みクライアントの無通信時間（最後に通信してからの経過時間）を表示します。経過時間が 10 時間より短い場合は（時）:（分）:（秒）形式で表示され、10 時間以上の場合は（日）d（時）hr 形式で表示されます。

11.2.2 認証拒否クライアントの表示

show access-defender deny コマンドで、認証拒否クライアントの情報を確認できます。

表示例を以下に示します。

```
# show access-defender deny

Total number of Denied Clients     :    3 ...(1)
(2)                (3)                                        (4)
MAC address        IP                                         Timer
-------------------------------------------------------------------
00-00-11-11-22-22 -                                           0:29:04
-                  100.100.100.100                            0:29:04
-                  1111:2222:3333:4444:5555:6666:7777:8888 0:29:05
```

各項目の説明は、以下のとおりです。

表 11-6 show access-defender deny コマンドの表示項目

項番	説明
(1)	認証拒否クライアントの数を表示します。
(2)	認証拒否クライアントの MAC アドレスを表示します。
(3)	認証拒否クライアントの IP アドレスを表示します。
(4)	認証拒否クライアントの、認証を拒否する残り時間を表示します。

11.2.3 AccessDefender に関連するアクセスリストルールの使用状態の表示

show access-defender rule-statistics コマンドで、AccessDefender に関連するアクセスリストルールの使用状態を確認できます。

表示例を以下に示します。

```
# show access-defender rule-statistics

 Total Rules  : 768 ...(1)
 Unused Rules : 767 ...(2)
 Used Rules   :   1 ...(3)                (4)     (5)
                                         Rule   Client
              ----------------------------------------
               web-authentication           1        1
               web-authentication gateway   0        0
               mac-authentication           0        0
               static-authentication        0        0
               IEEE802.1X                   0        0
               DHCPv4 snooping              0        0
               DHCPv6 snooping              0        0
              ----------------------------------------

 Total Discard Rules  :  200 ...(6)
 Unused Discard Rules :  199 ...(7)
 Used Discard Rules   :    1 ...(8)       (9)     (10)
                                         Rule   Client
              ----------------------------------------
               Discarded MAC address        1        1
              ----------------------------------------

 Total VFP Rules          : 1024 ...(11)
 Unused VFP Rules         : 1024 ...(12)
 Authorization VFP Rules  :    0 ...(13)
```

各項目の説明は、以下のとおりです。

表 11-7 show access-defender rule-statistics コマンドの表示項目

項番	説明
(1)	ルール数を表示します。
(2)	未使用のルール数を表示します。

項番	説明
(3)	使用済みルール数を表示します。
(4)	認証機能ごとのルール数を表示します。
(5)	認証機能ごとのクライアント数を表示します。
(6)	Discard クライアント用のルール数を表示します。
(7)	未使用の Discard クライアント用のルール数を表示します。
(8)	使用済みの Discard クライアント用のルール数を表示します。
(9)	MAC 認証に失敗して Discard 登録されたクライアント用のルール数を表示します。
(10)	MAC 認証に失敗して Discard 登録されたクライアント数を表示します。
(11)	VFP テーブルのルール数を表示します。
(12)	未使用の VFP ルール数を表示します。
(13)	使用済みの VFP ルール数を表示します。VFP ルールはクラス ID を使用すると消費します。

11.3 IEEE 802.1X 認証の設定および動作状態の表示

IEEE 802.1X 認証の設定および動作状態を確認する方法を説明します。

11.3.1 IEEE 802.1X 認証の設定の表示

show access-defender dot1x interface コマンドで、IEEE 802.1X 認証の設定を確認できます。

ポートの IEEE 802.1X 認証の設定の表示

show access-defender dot1x interface port コマンドで、ポートの IEEE 802.1X 認証の設定を確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show access-defender dot1x interface port 1/0/1

Interface           : Port1/0/1 ...(1)
PAE                 : Authenticator ...(2)
Port Control        : Auto ...(3)
Ignore EAPOL start  : Disabled ...(4)
Quiet Period        : 60 sec ...(5)
Tx Period           : 30 sec ...(6)
Supp Timeout        : 30 sec ...(7)
Server Timeout      : 30 sec ...(8)
Max-req             : 2 times ...(9)
Re-Authenticate     : Disabled ...(10)
Re-Auth Period      : 3600 sec ...(11)
```

各項目の説明は、以下のとおりです。

表 11-8 show access-defender dot1x interface port コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	Port Access Entity（PAE）の現在の状態を表示します。
(3)	ポートコントロールを表示します。
(4)	EAPOL-Start 受信による認証の抑止機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(5)	認証が失敗したときのステータスの保持時間を表示します。
(6)	EAP-Request/EAP-Identity をサプリカントに送信する間隔を表示します。
(7)	RADIUS サーバーからの EAP メッセージを受信後、サプリカントからの応答がない場合に EAP-Request を再送信する間隔を表示します。
(8)	RADIUS サーバーからの応答待ち時間を表示します。
(9)	EAP-Request/EAP-Identity をサプリカントに再送信する回数を表示します。
(10)	IEEE 802.1X 認証の再認証の有効 (Enabled) ／無効 (Disabled) を表示します。
(11)	再認証の間隔を表示します。

ポートチャネルの IEEE 802.1X 認証の設定の表示

show access-defender dot1x interface port-channel コマンドで、ポートチャネルの IEEE 802.1X 認証の設定を確認できます。

ポートチャネル 1 を指定した場合の表示例を以下に示します。

```
# show access-defender dot1x interface port-channel 1

Interface          : Port-channel1 ...(1)
PAE                : Authenticator ...(2)
Port Control       : Auto ...(3)
Ignore EAPOL start: Disabled ...(4)
Quiet Period       : 60    sec ...(5)
Tx Period          : 30    sec ...(6)
Supp Timeout       : 30    sec ...(7)
Server Timeout     : 30    sec ...(8)
Max-req            : 2     times ...(9)
Re-Authenticate    : Disabled ...(10)
Re-Auth Period     : 3600  sec ...(11)
```

各項目の説明は、以下のとおりです。

表 11-9 show access-defender dot1x interface port-channel コマンドの表示項目

項番	説明
(1)	ポート番号またはポートチャネル番号を表示します。
(2)	Port Access Entity（PAE）の現在の状態を表示します。
(3)	ポートコントロールを表示します。
(4)	EAPOL-Start 受信による認証の抑止機能の有効 (Enabled) ／無効 (Disabled) を表示します。
(5)	認証が失敗したときのステータスの保持時間を表示します。
(6)	EAP-Request/EAP-Identity をサプリカントに送信する間隔を表示します。
(7)	RADIUS サーバーからの EAP メッセージを受信後、サプリカントからの応答がない場合に EAP-Request を再送信する間隔を表示します。
(8)	RADIUS サーバーからの応答待ち時間を表示します。
(9)	EAP-Request/EAP-Identity をサプリカントに再送信する回数を表示します。
(10)	IEEE 802.1X 認証の再認証の有効 (Enabled) ／無効 (Disabled) を表示します。
(11)	再認証の間隔を表示します。

11.3.2 登録されたサプリカント情報の表示

show access-defender dot1x コマンドで、登録されたサプリカント情報を確認できます。

表示例を以下に示します。

```
# show access-defender dot1x

802.1X Port-Based Authentication Enabled ...(1)
802.1X info for Port-channel1 ...(2)
  Supplicant name: user1 ...(3)
  Supplicant address: 00-0C-29-8F-8F-2A ...(4)
  (5)                  (6)
  portEnabled: true - portControl: Auto
  portStatus: authorized - currentId: 1 ...(7)
  protocol version: 2 ...(8)
  reAuthenticate: Disabled ...(9)
  reAuthPeriod: 3600 ...(10)
       (11)                    (12)
  PAE: state: Authenticated - portMode: Auto
  PAE: reAuthCount: 0 ...(13)
       (14)               (15)            (16)
  PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30
  BE: state: Idle ...(17)
      (18)               (19)
  BE: suppTimeout: 30 - serverTimeout: 30
      (20)                             (21)
  CD: adminControlledDirections: In - operControlledDirections: In
  CD: bridgeDetected: false
  KR: rxKey: false
  KT: keyAvailable: false - keyTxEnabled: false
```

各項目の説明は、以下のとおりです。

表 11-10 show access-defender dot1x コマンドの表示項目

項番	説明
(1)	IEEE 802.1X 認証の有効 (Enabled) ／無効 (Disabled) を表示します。
(2)	情報を表示するポート番号またはポートチャネル番号を表示します。
(3)	サプリカントのユーザー名を表示します。
(4)	サプリカントの MAC アドレスを表示します。
(5)	サプリカントのリンクステータスを表示します。 常に「true」が表示されます。
(6)	サプリカントの認証モードを表示します。 常に「Auto」が表示されます。
(7)	サプリカントの現在の認証セッション ID を表示します。
(8)	IEEE 802.1X 認証 /EAPOL プロトコルバージョンを表示します。
(9)	サプリカントの再認証状態設定の有効／無効を表示します。
(10)	サプリカントの再認証期間設定を表示します。

項番	説明
(11)	サプリカントの Port Access Entity（PAE）の現在のステータスを表示します。 • Down：ダウン状態 • Initialize：初期化中 • Disconnecting：接続なし • Connecting：接続済み • Authenticating：認証中 • Aborting：中断中 • Held：EAP-Failure 送信
(12)	サプリカントの Port Access Entity（PAE）のポートモードを表示します。 常に「Auto」が表示されます。
(13)	サプリカントへの request-ID の再送信試行回数を表示します。
(14)	サプリカントの休止期間の設定を表示します。
(15)	サプリカントに許可されている再認証試行回数を表示します。 常に「2」が表示されます。
(16)	サプリカントの送信期間設定を表示します。
(17)	バックエンド認証のステータスを表示します。 • Invalid：無効 • Request：リクエスト送信 • Response：応答受信 • Success：認証成功 • Fail：認証失敗 • Timeout：応答タイムアウト • Idle：待機中 • Initialize：初期化
(18)	サプリカントのタイムアウト設定を表示します。
(19)	RADIUS サーバーの応答待ち時間を表示します。
(20)	非認証サプリカントのパケット破棄方向の設定を表示します。 常に「In」が表示されます。
(21)	非認証サプリカントの使用可能なパケット破棄方向を表示します。 常に「In」が表示されます。

11.3.3 IEEE 802.1X 認証の統計情報の表示

show access-defender dot1x statistics コマンドで、IEEE 802.1X 認証の統計情報を確認できます。

ポートの IEEE 802.1X 認証の統計情報の表示

show access-defender dot1x statistics interface port コマンドで、ポートの IEEE 802.1X 認証の統計情報を確認できます。

ポート 1/0/1 を指定した場合の表示例を以下に示します。

```
# show access-defender dot1x statistics interface port 1/0/1

Port1/0/1 dot1x statistics information:
EAPOL Frames RX                        : 1 ...(1)
EAPOL Frames TX                        : 4 ...(2)
EAPOL-Start Frames RX                  : 0 ...(3)
EAPOL-Req/Id Frames TX                 : 6 ...(4)
EAPOL-Logoff Frames RX                 : 0 ...(5)
EAPOL-Req Frames TX                    : 0 ...(6)
EAPOL-Resp/Id Frames RX                : 0 ...(7)
EAPOL-Resp Frames RX                   : 0 ...(8)
Invalid EAPOL Frames RX                : 0 ...(9)
EAP-Length Error Frames RX             : 0 ...(10)
Last EAPOL Frame Version               : 0 ...(11)
Last EAPOL Frame Source                : 00-10-28-00-19-78 ...(12)
```

各項目の説明は、以下のとおりです。

表 11-11 show access-defender dot1x statistics interface port コマンドの表示項目

項番	説明
(1)	受信した EAPOL フレームのフレーム数を表示します。
(2)	送信した EAPOL フレームのフレーム数を表示します。
(3)	受信した EAPOL-Start フレームのフレーム数を表示します。
(4)	送信した EAP-Request/EAP-Identity フレームのフレーム数を表示します。
(5)	受信した EAPOL-Logoff フレームのフレーム数を表示します。
(6)	送信した EAP-Request フレームのフレーム数を表示します。
(7)	受信した EAP-Response/EAP-Identity フレームのフレーム数を表示します。
(8)	受信した EAP-Response フレームのフレーム数を表示します。
(9)	受信した無効な EAPOL フレームのフレーム数を表示します。
(10)	受信した EAP フレームのうち、Length に誤りがあるフレームのフレーム数を表示します。
(11)	最後に送受信した EAPOL フレームのプロトコルバージョンを表示します。
(12)	最後に送受信した EAPOL フレームの送受信相手の MAC アドレスを表示します。

ポートチャネルの IEEE 802.1X 認証の統計情報の表示

show access-defender dot1x statistics interface port-channel コマンドで、ポートチャネルの IEEE 802.1X 認証の統計情報を確認できます。

ポートチャネル 1 を指定した場合の表示例を以下に示します。

```
# show access-defender dot1x statistics interface port-channel 1

Port-channel1 dot1x statistics information:
EAPOL Frames RX                        : 1 ...(1)
EAPOL Frames TX                        : 4 ...(2)
EAPOL-Start Frames RX                  : 0 ...(3)
EAPOL-Req/Id Frames TX                 : 6 ...(4)
EAPOL-Logoff Frames RX                 : 0 ...(5)
EAPOL-Req Frames TX                    : 0 ...(6)
EAPOL-Resp/Id Frames RX                : 0 ...(7)
EAPOL-Resp Frames RX                   : 0 ...(8)
Invalid EAPOL Frames RX                : 0 ...(9)
EAP-Length Error Frames RX             : 0 ...(10)
Last EAPOL Frame Version               : 0 ...(11)
Last EAPOL Frame Source                : 00-10-28-00-19-78 ...(12)
```

各項目の説明は、以下のとおりです。

表 11-12 show access-defender dot1x statistics interface port-channel コマンドの表示項目

項番	説明
(1)	受信した EAPOL フレームのフレーム数を表示します。
(2)	送信した EAPOL フレームのフレーム数を表示します。
(3)	受信した EAPOL-Start フレームのフレーム数を表示します。
(4)	送信した EAP-Request/EAP-Identity フレームのフレーム数を表示します。
(5)	受信した EAPOL-Logoff フレームのフレーム数を表示します。
(6)	送信した EAP-Request フレームのフレーム数を表示します。
(7)	受信した EAP-Response/EAP-Identity フレームのフレーム数を表示します。
(8)	受信した EAP-Response フレームのフレーム数を表示します。
(9)	受信した無効な EAPOL フレームのフレーム数を表示します。
(10)	受信した EAP フレームのうち、Length に誤りがあるフレームのフレーム数を表示します。
(11)	最後に送受信した EAPOL フレームのプロトコルバージョンを表示します。
(12)	最後に送受信した EAPOL フレームの送受信相手の MAC アドレスを表示します。

11.4 DHCP スヌーピングの設定および動作状態の表示

DHCP スヌーピングの設定および動作状態を確認する方法を説明します。

11.4.1 DHCP スヌーピングの設定の表示

show access-defender dhcp-snooping configuration コマンドで、DHCP スヌーピングの設定を確認できます。

表示例を以下に示します。

```
# show access-defender dhcp-snooping configuration

 Port configuration (o: snooping ON) ...(1)
         C Port
           1      8 9     16 17    24 25    32 33    40 41    48
           +------+ +------+ +------+ +------+ +------+ +------+
         1 oooooooo ........ ........ ........ ........ ........

           49    56 57    64 65    72
           +------+ +------+ +------+
         1 ........ ........ ........

 Snooping : ENABLE ...(2)
 Mode     : PERMIT ...(3)
 Mode     : MAC Authentication Mode ...(4)
 Timer    : 1800 ...(5)

 Port-channel configuration (o: snooping ON) ...(6)
                  C Port-channel ID
                    1      8 9     16 17    24 25    32 33    40 41    48
                    +------+ +------+ +------+ +------+ +------+ +------+
 Port-channel     1 o....... ........ ........ ........ ........ ........
                    49    56 57    64 65    72 73    80 81    88 89    96
                    +------+ +------+ +------+ +------+ +------+ +------+
                    ........ ........ ........ ........ ........ ........
                    97   104 105  112 113  120 121
                    +------+ +------+ +------+ +------
                    ........ ........ ........ .......
 (7)
 Static Entry :
 Port            IP Address
 -------------------------------------------------------
 Port1/0/1       192.168.2.2
 Port-channel1   192.168.255.255
```

各項目の説明は、以下のとおりです。

表 11-13 show access-defender dhcp-snooping configuration コマンドの表示項目

項番	説明
(1)	ポートごとの DHCP スヌーピングの有効／無効を表示します。 "C" 列はスタックのボックス ID を示します。スタックが無効な場合は 1 が表示されます。
(2)	DHCP スヌーピングの有効 (ENABLE) ／無効 (DISABLE) を表示します。
(3)	DHCP スヌーピングの動作モード手動切り替えコマンド（**dhcp-snooping mode deny** コマンド）の設定を表示します。 DENY：コマンド設定時 PERMIT：コマンド未設定時

項番	説明
(4)	DHCP スヌーピングの MAC 認証モードが有効な場合に表示されます。無効な場合には表示されません。
(5)	DHCP スヌーピングの動作モード自動切り替えタイマーの設定を表示します。
(6)	ポートチャネルごとの DHCP スヌーピングの有効／無効を表示します。 "C" 列はスタックのボックス ID を示しますが、ここでは常に 1 が表示されます。
(7)	スタティックエントリーを表示します。

11.4.2 DHCP スヌーピングの動作モードの表示

show access-defender dhcp-snooping mode-status コマンドで、DHCP スヌーピングの動作モードを確認できます。

表示例を以下に示します。

```
# show access-defender dhcp-snooping mode-status
 (1)        (2)            (3)
 Mode       Timer          Remaining time
 -------------------------------------
 PERMIT     0:00:30:00     0:00:05:20
 MAC AUTH   -:--:--:--     -:--:--:--
```

各項目の説明は、以下のとおりです。

表 11-14 show access-defender dhcp-snooping mode-status コマンドの表示項目

項番	説明
(1)	DHCP スヌーピングの動作モードを表示します。MAC AUTH 行は DHCP スヌーピングの MAC 認証モードが有効な場合に表示されます。無効な場合には表示されません。
(2)	DHCP スヌーピングの動作モード自動切り替えタイマーの設定を表示します。
(3)	PERMIT モードから DENY モードに自動的に切り替えるまでの残り時間を表示します。

11.4.3 DHCP スヌーピングエントリーの表示

show access-defender dhcp-snooping status コマンドで、DHCP スヌーピングエントリーを確認できます。

表示例を以下に示します。

```
# show access-defender dhcp-snooping status

 Snooping : ENABLE ...(1)
 Mode     : DENY ...(2)
 Mode     : MAC Authentication Mode ...(3)

 C = port-channel, LE = Lease Expiration

 Total    : 4 (static 1, dynamic 3) ...(4)
 (5)        (6)                                  (7)                 (8)
 Port       IP Address                           MAC Address         LE
 ---------------------------------------------------------------------------
 Port1/0/2  172.17.100.150                       00-1D-09-D1-15-9F   0:4:12
 C/1        172.17.100.155                       00-21-70-70-7E-C5   1:1:11
 Port1/0/5  191.168.1.1                          N/A
```

各項目の説明は、以下のとおりです。

表 11-15 show access-defender dhcp-snooping status コマンドの表示項目

項番	説明
(1)	DHCP スヌーピングの有効 (ENABLE) ／無効 (DISABLE) を表示します。
(2)	DHCP スヌーピングの動作モードを表示します。 DENY：DENY モード（登録されたクライアントからの通信は許可、それ以外は制限） PERMIT：PERMIT モード（未登録クライアントからの通信も許可）
(3)	DHCP スヌーピングの MAC 認証モードが有効な場合に表示されます。無効な場合には表示されません。
(4)	DHCP スヌーピングのエントリー数（スタティックエントリー数とダイナミックエントリー数）を表示します。
(5)	DHCP スヌーピングエントリーのポート番号またはポートチャネル番号を表示します。
(6)	DHCP サーバーによって提供されるクライアント IP アドレスを表示します。
(7)	DHCP スヌーピングエントリーの MAC アドレスを表示します。スタティックエントリーでは MAC アドレスは表示されません。
(8)	DHCP スヌーピングエントリーのリース期間を表示します。スタティックエントリーではリース期間は表示されません。 10 時間未満の場合は、9:33:12 のように（時）:（分）:（秒）の形式で表示されます。10 時間を超える場合は、3d5hr のように（日）d（時）hr の形式で表示されます。

11.5 SSL 情報の表示

SSL の情報を確認する方法を説明します。

11.5.1 SSL サーバーの証明書情報の表示

show ssl https-certificate コマンドで、SSL サーバーの証明書情報を確認できます。

表示例を以下に示します。

```
# show ssl https-certificate

Certificate Information:
Certificate Version :3 ...(1)
Serial Number :00:80:2D:5E:A8:BD:8D:53:C3 ...(2)
Issuer Name   :C=JP, ST=Tokyo, L=Chiyoda-ku, O=Example Domain., OU=Example Group.,
CN=Apresia, emailAddress=example@example.com ...(3)
Subject Name  :C=JP, ST=Tokyo, L=Chiyoda-ku, O=Example Domain., OU=Example Group.,
CN=Apresia, emailAddress=example@example.com ...(4)
Not Before    :2017-02-16 06:54:58 ...(5)
Not After     :2037-02-11 06:54:58 ...(6)
Public Key Alg:rsaEncryption ...(7)
Signed Using  :RSA+SHA256 ...(8)
RSA Key Size  :2048 bits ...(9)
```

各項目の説明は、以下のとおりです。

表 11-16 show ssl https-certificate コマンドの表示項目

項番	説明
(1)	バージョンを表示します。
(2)	シリアル番号を表示します。
(3)	発行者を表示します。
(4)	サブジェクトを表示します。
(5)	有効期間の開始日時を表示します。
(6)	有効期間の終了日時を表示します。
(7)	公開鍵アルゴリズムを表示します。
(8)	署名アルゴリズムを表示します。
(9)	公開鍵 (RSA キー) のサイズを表示します。

11.5.2 SSL サーバーの秘密鍵情報の表示

show ssl https-private-key コマンドで、SSL サーバーの秘密鍵情報を確認できます。

表示例を以下に示します。

```
# show ssl https-private-key

Private key is embedded in firmware. ...(1)
```

各項目の説明は、以下のとおりです。

表 11-17 show ssl https-private-key コマンドの表示項目

項番	説明
(1)	SSL サーバーの証明書と、その証明書に一致する秘密鍵の両方をユーザーがダウンロードした状態では、「Private key is installed by user.」と表示されます。

11.5.3 CSR（証明書署名要求）の表示

show ssl csr コマンドで、CSR（証明書署名要求）を確認できます。

表示例を以下に示します。

```
# show ssl csr

Certificate Request: ...(1)
    Data:
        Version: 1 (0x1)
        Subject: C=jp, ST=tokyo, L=chiyoda-ku, O=apresia, OU=network, CN=www.apresia.jp/
emailAddress=xxx@apresia.jp
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (1024 bit)
                Modulus:
                    00:9d:f3:98:37:f2:c5:7f:e0:89:b3:6a:6f:b6:9a:
                    f3:b1:76:48:c3:91:20:9f:b4:7c:d8:91:ac:6a:a3:
                    6b:df:da:7a:2e:93:9e:0e:56:92:6f:01:84:6f:bd:
                    c5:61:21:7a:a0:29:42:c7:5b:79:22:7c:cb:2e:4a:
                    9a:8a:5a:c0:45:9e:43:b4:8e:6b:2f:11:6d:a1:12:
                    17:d7:bf:ec:ca:72:ca:ea:2b:2f:df:e4:e7:03:14:
                    ee:e8:97:4a:a7:ba:67:b9:2b:ce:a2:f5:28:1c:fa:
                    a7:67:b3:59:96:0a:6f:91:fd:fc:bd:1c:86:79:b8:
                    41:d9:04:74:01:d5:b3:63:61
                Exponent: 65537 (0x10001)
        Attributes:
            a0:00
    Signature Algorithm: sha256WithRSAEncryption
        8c:c6:69:d7:65:56:e8:80:5d:3b:58:fa:3f:86:91:01:aa:97:
        aa:92:58:ba:1f:8c:b8:e4:99:77:f8:b1:c3:1e:1e:29:7a:e2:
        98:ad:f1:59:28:3b:df:50:32:a5:d7:9a:db:65:01:a4:26:c8:
        28:db:a4:d3:6a:2b:7b:53:44:0d:c9:22:d7:16:39:fa:bf:ec:
        2d:54:4d:bd:33:03:ec:c1:4e:c6:f9:8d:ac:8b:9d:c8:71:ba:
        99:48:e9:a2:85:db:59:22:35:e5:f0:2e:e6:dd:19:76:dd:25:
        5a:b1:d3:95:41:c4:bf:9e:47:82:e1:98:82:c3:14:95:ac:e3:
        cf:ce
```

各項目の説明は、以下のとおりです。

表 11-18 show ssl csr コマンドの表示項目

項番	説明
(1)	CSR（証明書署名要求）を表示します。

11.6 AccessDefender に関連するテクニカルサポート情報の表示

show tech-support access-defender コマンドで、AccessDefender に関連するテクニカルサポート情報を確認できます。

表示例を以下に示します。

```
# show tech-support access-defender

********************************
There is AD techsupport
********************************


 Snooping : ENABLE
 Mode: 1 (0:permit,1:deny)

 Total : 3 (static 2, dynamic 1)

 Binding Entry
 ip address:10.92.0.2, mac address:00-50-BA-6B-35-19, vlan id:1, interface_id:5,
lifetime:85958 , dhcp_type:0, timer_start_time:1513

 BST Entry

 IPSG-binding Entry
 ip address:1.1.1.1, mac address:00-00-00-00-00-00, vlan id:0, interface_id:1,
 ip address:1.1.1.2, mac address:00-00-00-00-00-00, vlan id:0, interface_id:1,
 ip address:0.0.0.0, mac address:00-00-00-00-00-00, vlan id:0, interface_id:1,
 ip address:10.92.0.2, mac address:00-00-00-00-00-00, vlan id:1, interface_id:5,

 IPSG Static Entry
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

12. AccessDefender の構成例と設定例

AccessDefender の構成例と設定例について説明します。

REF: コマンドの詳細については、『コマンドリファレンス』を参照してください。

12.1 MAC 認証の構成例と設定例

MAC 認証の構成例と設定例を示します。

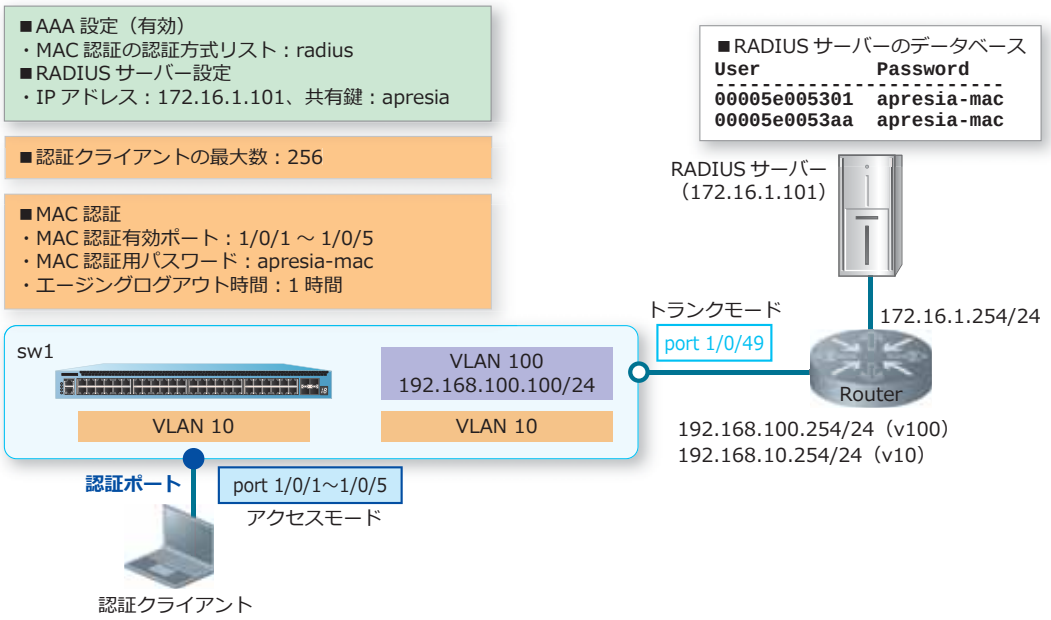
12.1.1 MAC 認証の設定例

MAC 認証の構成例と設定例を示します。この例では以下のように設定しています。

表 12-1 MAC 認証の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac
エージングログアウト時間	1 時間

図 12-1 MAC 認証の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で MAC 認証を有効に、MAC 認証用パスワードを［apresia-mac］に設定します。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# logout aging-time 0 0 1 mac
sw1(config-a-def)# exit
sw1(config)#
```

7. MAC 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)# end
sw1#
```

8. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication mac-auth default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 mac

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable
```

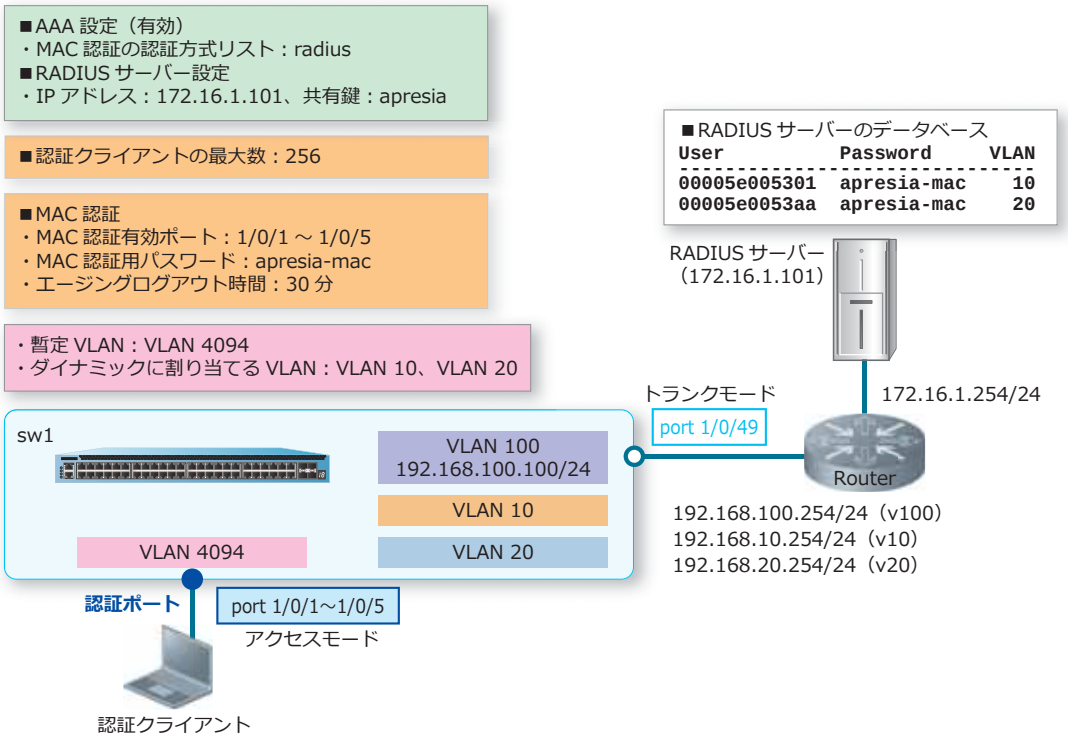
12.1.2 MAC 認証でダイナミック VLAN を使用する場合

MAC 認証でダイナミック VLAN を使用する場合の構成例と設定例を示します。この例では、認証ポートには暫定 VLAN 4094 を割り当てておき、ダイナミック VLAN を使用して、ユーザーごとに VLAN 10 または VLAN 20 が割り当てられるようにしています。

表 12-2 MAC 認証でダイナミック VLAN を使用する場合の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac
エージングログアウト時間	30 分

図 12-2 MAC 認証でダイナミック VLAN を使用する場合の構成例



1. VLAN 10、VLAN 20、VLAN 100、VLAN 4094 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,20,100,4094
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 4094
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,20,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で MAC 認証を有効に、MAC 認証用パスワードを［apresia-mac］に設定します。また、エージングログアウト時間を［30 分］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# logout aging-time 0 30 mac
sw1(config-a-def)# exit
sw1(config)#
```

7. MAC 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)# end
sw1#
```

8. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication mac-auth default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 30 mac

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable
```

12.2 Web 認証の構成例と設定例

Web 認証の構成例と設定例を示します。

12.2.1 Web 認証の設定例

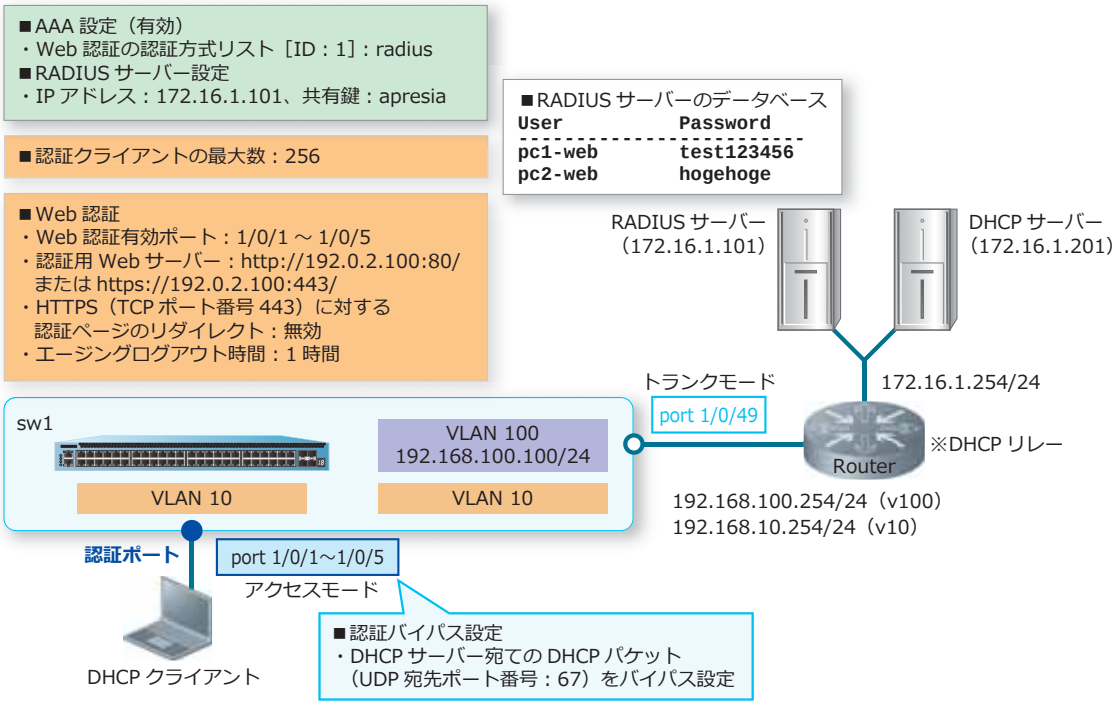
Web 認証の構成例と設定例を示します。この例では以下のように設定しています。

表 12-3 Web 認証の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
Web 認証有効ポート	ポート 1/0/1 からポート 1/0/5
認証用 Web サーバー	http://192.0.2.100:80/、または https://192.0.2.100:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
HTTPS（TCP ポート番号 443）に対する認証ページのリダイレクト	無効
エージングログアウト時間	1 時間

また、未認証クライアントが認証前に DHCP で IP アドレスを取得できるように、「DHCP サーバー宛ての DHCP パケット（UDP 宛先ポート番号：67）をバイパス」する認証バイパスを設定しています。

図 12-3 Web 認証の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、Web 認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で Web 認証を有効に、認証用 Web サーバーの IP アドレスを［192.0.2.100］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 web
sw1(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
sw1(config-a-def)# logout aging-time 0 0 1 web
sw1(config-a-def)#
```

7. HTTPS（TCP ポート番号 443）に対する認証ページのリダイレクトを無効にします。

```
sw1(config-a-def)# web-authentication redirect disable https
sw1(config-a-def)# exit
sw1(config)#
```

8. Web 認証を有効にします。

```
sw1(config)# web-authentication enable
sw1(config)#
```

9. 認証バイパス設定のために、拡張 IP アクセスリスト［IPv4-EX-ACL］を作成し、以下のルールを設定します。

ルール 10（authentication-bypass）：宛先 UDP ポート番号［67］

```
sw1(config)# ip access-list extended IPv4-EX-ACL
sw1(config-ip-ext-acl)# 10 permit authentication-bypass udp any any eq 67
sw1(config-ip-ext-acl)# exit
sw1(config)#
```

10. 設定したアクセスリストを認証ポート（ポート 1/0/1 からポート 1/0/5）に適用します。

```
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# ip access-group IPv4-EX-ACL in

The remaining applicable IP related access entries are 255
sw1(config-if-port-range)# end
sw1#
```

11. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 web

# WEB-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 web
 web-authentication http-ip ipv4 192.0.2.100
 web-authentication redirect disable https
web-authentication enable
```

12. 実施後のアクセスリスト関連の設定を以下に抜粋します。

```
# ACL

ip access-list extended IPv4-EX-ACL 3999
 10 permit authentication-bypass udp any any eq bootps
interface port 1/0/1
 ip access-group IPv4-EX-ACL in
interface port 1/0/2
 ip access-group IPv4-EX-ACL in
interface port 1/0/3
 ip access-group IPv4-EX-ACL in
interface port 1/0/4
 ip access-group IPv4-EX-ACL in
interface port 1/0/5
 ip access-group IPv4-EX-ACL in
```

12.2.2 Web 認証でダイナミック VLAN を使用する場合

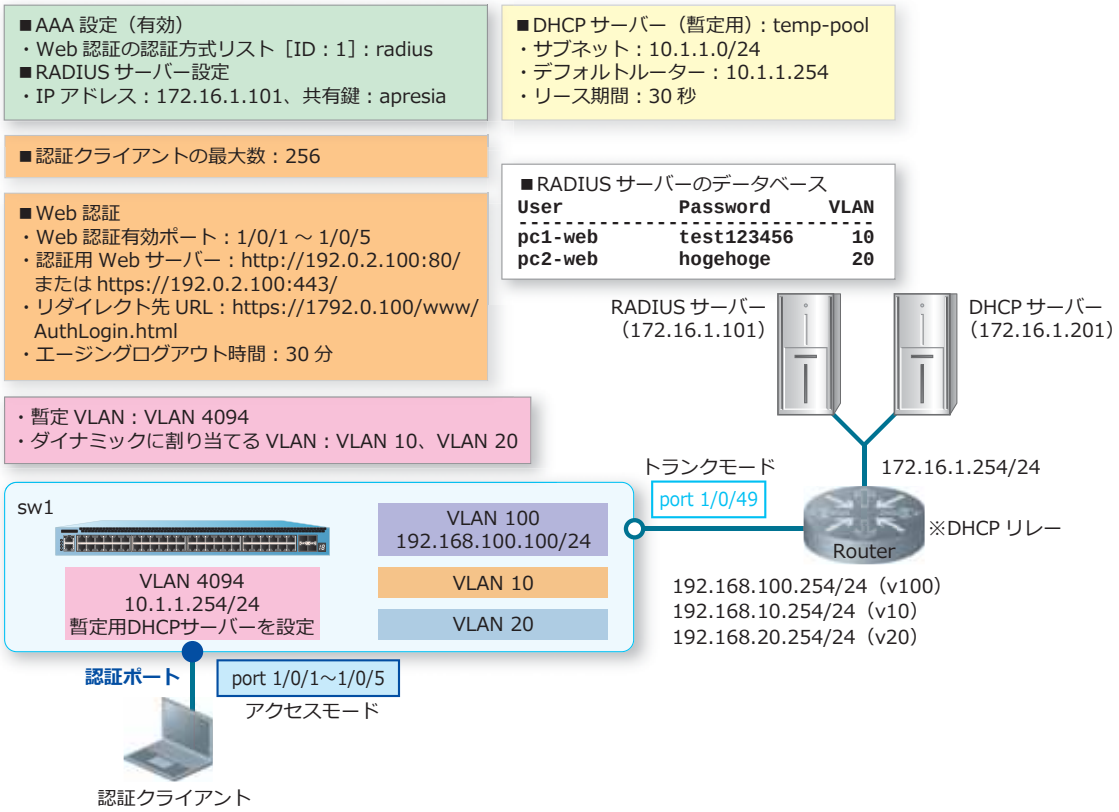
Web 認証でダイナミック VLAN を使用する場合の構成例と設定例を示します。この例では、認証ポートには暫定 VLAN 4094 を割り当てておき、ダイナミック VLAN を使用して、ユーザーごとに VLAN 10 または VLAN 20 が割り当てられるようにしています。

表 12-4 Web 認証でダイナミック VLAN を使用する場合の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
Web 認証有効ポート	ポート 1/0/1 からポート 1/0/5
認証用 Web サーバー	http://192.0.2.100:80/、または https://192.0.2.100:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
リダイレクト先 URL	（自装置の認証ページ）https://192.0.2.100:443/www/AuthLogin.html
エージングログアウト時間	1 時間

また、暫定 VLAN で未認証クライアントに IP アドレスを割り当てるための暫定 DHCP サーバーは、この例では自装置に設定しています。

図 12-4 Web 認証でダイナミック VLAN を使用する場合の構成例



1. VLAN 10、VLAN 20、VLAN 100、VLAN 4094 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,20,100,4094
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 4094
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,20,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、Web 認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で Web 認証を有効に、認証用 Web サーバーの IP アドレスを［192.0.2.100］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。また、エージングログアウト時間を［30 分］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 web
sw1(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
sw1(config-a-def)# logout aging-time 0 30 web
sw1(config-a-def)#
```

7. リダイレクト先の自装置の認証ページを HTTPS に固定するために、リダイレクト先 URL を［https://192.0.2.100:443/www/AuthLogin.html］に設定します。
※ 設定例が 1 行に収まるように、コマンドを省略形式で実施しています。

```
sw1(config-a-def)# web-a red url https://192.0.2.100:443/www/AuthLogin.html
sw1(config-a-def)# end
sw1#
```

8. Web 認証が無効な状態で、自装置の Web サーバー用の証明書と秘密鍵を TFTP サーバーからダウンロードします。この例では、TFTP サーバーの IP アドレス［172.16.1.202］、証明書のファイル名［test.crt］、秘密鍵のファイル名［test.key］として実施しています。また、実施前の状態が不明な場合を想定し、**access-defender erase ssl-files** コマンドを実施してからダウンロードしています。
※ ダウンロード済みの SSL サーバー証明書および秘密鍵が装置上に存在する場合、**access-defender erase ssl-files** コマンドで既存のファイルを削除してから証明書、秘密鍵をダウンロードしてください。

```
sw1# access-defender erase ssl-files
Erasing SSL files in FLASH.......... Done.


sw1# copy tftp: https-certificate

Address of remote host []? 172.16.1.202
Source filename []? test.crt
Destination filename https-certificate? [y/n]:  y

% Importing certificate PEM file...
Reading file from tftp://172.16.1.202/test.crt
Loading test.crt from 172.16.1.202 (via Port1/0/49):!
[OK - 4474 bytes]


sw1# copy tftp: https-private-key

Address of remote host []? 172.16.1.202
Source filename []? test.key
Destination filename https-privatekey? [y/n]:  y

% Importing private key PEM file...
Reading file from tftp://172.16.1.202/test.key
Loading test.key from 172.16.1.202 (via Port1/0/49):!
[OK - 1679 bytes]


sw1#
```

9. Web 認証を有効にします。

```
sw1# configure terminal
sw1(config)# web-authentication enable
sw1(config)#
```

10. 未認証クライアントに暫定的に IP アドレスを付与するための暫定 DHCP サーバーを設定します。まずは、VLAN 4094 インターフェースに IP アドレス［10.1.1.254/24］を設定します。

```
sw1(config)# interface vlan 4094
sw1(config-if-vlan)# ip address 10.1.1.254/24
sw1(config-if-vlan)# exit
sw1(config)#
```

11. 暫定 DHCP サーバー用の DHCP アドレスプール［temp-pool］を作成し、以下の内容で設定して有効にします。

サブネット［10.1.1.0/24］、デフォルトルーター［10.1.1.254］、リース期間［30 秒］

```
sw1(config)# ip dhcp pool temp-pool
sw1(config-dhcp-pool)# network 10.1.1.0/24
sw1(config-dhcp-pool)# default-router 10.1.1.254
sw1(config-dhcp-pool)# lease 0 0 0 30
sw1(config-dhcp-pool)# exit
sw1(config)# service dhcp
sw1(config)# end
sw1#
```

12. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 30 web

# WEB-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 web
 web-authentication http-ip ipv4 192.0.2.100
 web-authentication redirect url https://192.0.2.100:443/www/AuthLogin.html
web-authentication enable
```

12.2.3 外部 Web サーバーの認証ページにリダイレクトする場合

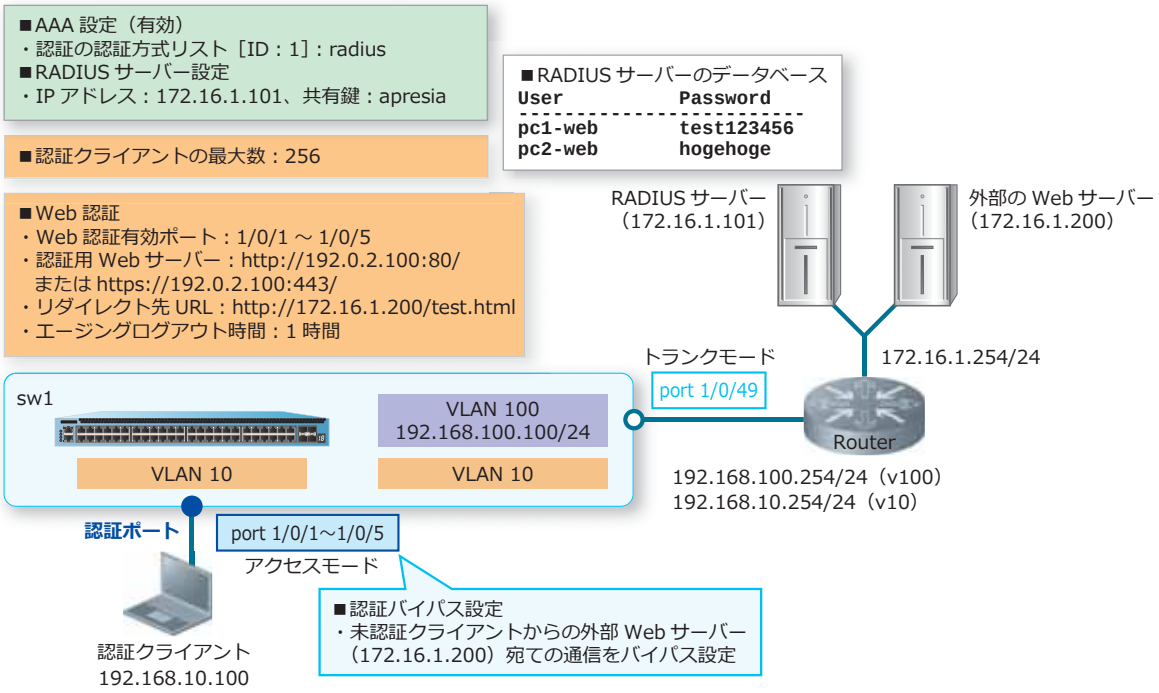
外部 Web サーバーの認証ページにリダイレクトする場合の構成例と設定例を示します。この例では以下のように設定しています。

表 12-5 外部 Web サーバーの認証ページにリダイレクトする場合の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
Web 認証有効ポート	ポート 1/0/1 からポート 1/0/5
自装置の認証用 Web サーバー	http://192.0.2.100:80/、または https://192.0.2.100:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
リダイレクト先 URL	（外部 Web サーバーの認証ページ）http://172.16.1.200/test.html
エージングログアウト時間	1 時間

また、未認証クライアントが認証前に外部 Web サーバーの認証ページを取得できるように、「外部 Web サーバー宛ての通信をバイパス」する認証バイパスも設定しています。

図 12-5 外部 Web サーバーの認証ページにリダイレクトする場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、Web 認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で Web 認証を有効に、認証用 Web サーバーの IP アドレスを［192.0.2.100］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 web
sw1(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
sw1(config-a-def)# logout aging-time 0 0 1 web
sw1(config-a-def)#
```

7. リダイレクト先 URL を、外部 Web サーバーの認証ページ［http://172.16.1.200/test.html］に設定します。

```
sw1(config-a-def)# web-authentication redirect url http://172.16.1.200/test.html
sw1(config-a-def)# exit
sw1(config)#
```

8. Web 認証を有効にします。

```
sw1(config)# web-authentication enable
sw1(config)#
```

9. 認証バイパス設定のために、標準 IP アクセスリスト［IPv4-ACL］を作成し、以下のルールを設定します。

ルール 10（authentication-bypass）：宛先 IP アドレス［172.16.1.200］

```
sw1(config)# ip access-list IPv4-ACL
sw1(config-ip-acl)# 10 permit authentication-bypass any host 172.16.1.200
sw1(config-ip-acl)# exit
sw1(config)#
```

10. 設定したアクセスリストを認証ポート（ポート 1/0/1 からポート 1/0/5）に適用します。

```
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# ip access-group IPv4-ACL in

The remaining applicable IP related access entries are 255
sw1(config-if-port-range)# end
sw1#
```

11. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 web

# WEB-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 web
 web-authentication http-ip ipv4 192.0.2.100
 web-authentication redirect url http://172.16.1.200/test.html
web-authentication enable
```

12. 実施後のアクセスリスト関連の設定を以下に抜粋します。

```
# ACL

ip access-list IPv4-ACL 1999
 10 permit authentication-bypass any host 172.16.1.200
interface port 1/0/1
 ip access-group IPv4-ACL in
interface port 1/0/2
 ip access-group IPv4-ACL in
interface port 1/0/3
 ip access-group IPv4-ACL in
interface port 1/0/4
 ip access-group IPv4-ACL in
interface port 1/0/5
 ip access-group IPv4-ACL in
```

12.2.4 個別 Web 認証ページを使用する場合

「Web 認証の設定例」において、ポート 1/0/3 で以下を使用する場合の構成例と設定例を示します。

- 個別 Web 認証ページ
- Web 認証のインターフェースごとの認証方式設定

NOTE: 個別 Web 認証ページは、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降でサポートしています。

NOTE: Web 認証のインターフェースごとの認証方式設定は、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降でサポートしています。

この例では以下のように設定しています。

表 12-6 個別 Web 認証ページの設定例

項目	設定
ポート 1/0/3 用 Web 認証の認証方式設定	• RADIUS サーバーグループ「PORT-AUTH」を使用 – RADIUS サーバー：172.16.1.102 – 共有鍵：test-apresia
ポート 1/0/3 用 個別 Web 認証ページ	• 個別 Web 認証ページ ID：3 • 以下のページを個別 Web 認証ページとして、TFTP サーバー：172.16.1.10 からダウンロードして使用する – ログイン認証ページ：test_login.html – 認証成功ページ：test_login-success.html – 認証失敗ページ：test_login-failure.html • それ以外の認証ページはデフォルトのページを使用する

1. 「Web 認証の設定例」を実施します。

2. RADIUS サーバーを、IP アドレス［172.16.1.102］、共有鍵［test-apresia］で設定します。

```
sw1# configure terminal
sw1(config)# radius-server host 172.16.1.102 key test-apresia
sw1(config)#
```

3. RADIUS サーバーグループ「PORT-AUTH」を作成し、前の手順で設定した RADIUS サーバーを、このグループに所属するように設定します。

```
sw1(config)# aaa group server radius PORT-AUTH
sw1(config-sg-radius)# server 172.16.1.102
sw1(config-sg-radius)# exit
sw1(config)#
```

4. ポート 1/0/3 の Web 認証で使用する認証方式リスト［ID：1］を、ユーザー設定の RADIUS サーバーグループ「PORT-AUTH」に指定します。

```
sw1(config)# aaa authentication web-auth 1 default group PORT-AUTH interface
port 1/0/3
sw1(config)#
```

5. ポート 1/0/3 で使用する個別 Web 認証ページ［ID：3］を設定します。

```
sw1(config-a-def)# web-authentication interface port 1/0/3 webpages 3
sw1(config-a-def)# end
sw1#
```

6. 個別 Web 認証ページ［ID：3］で使用する以下の認証ページを TFTP サーバー［172.16.1.10］からダウンロードします。

ログイン認証ページ：test_login.html

認証成功ページ：test_login-success.html

認証失敗ページ：test_login-failure.html

```
sw1# copy tftp: webpages 3 login-page

Address of remote host []? 172.16.1.10
Source filename []? test_login.html
Destination filename 03-login-page? [y/n]:  y

 Accessing tftp://172.16.1.10/test_login.html...
 Transmission start...
 Transmission finished, file length 2427 bytes.
 Please wait, programming flash............. Done.

sw1#

sw1# copy tftp: webpages 3 login-success-page

Address of remote host []? 172.16.1.10
Source filename []? test_login-success.html
Destination filename 03-login-success-page? [y/n]:  y

 Accessing tftp://172.16.1.10/test_login-success.html...
 Transmission start...
 Transmission finished, file length 1332 bytes.
 Please wait, programming flash............. Done.

sw1#

sw1# copy tftp: webpages 3 login-failure-page

Address of remote host []? 172.16.1.10
Source filename []? test_login-failure.html
Destination filename 03-login-failure-page? [y/n]:  y

 Accessing tftp://172.16.1.10/test_login-failure.html...
 Transmission start...
 Transmission finished, file length 1011 bytes.
 Please wait, programming flash............. Done.

sw1#
```

7. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
radius-server host 172.16.1.102 key test-apresia
aaa group server radius PORT-AUTH
 server 172.16.1.102
aaa authentication web-auth 1 default group radius
aaa authentication web-auth 1 default group PORT-AUTH interface port 1/0/3

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 web

# WEB-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 web
 web-authentication http-ip ipv4 192.0.2.100
 web-authentication redirect disable https
 web-authentication interface port 1/0/3 webpages 3
web-authentication enable
```

8. 設定後の個別 Web 認証ページの情報を確認します。

```
sw1# show access-defender webpages

WEBPAGES-ID:3
Filename                        Size                 Date
-------------------------------------------------------
03-login-page                   2427 Nov 20 2020 16:02:18
03-login-success-page           1332 Nov 20 2020 16:03:26
03-login-failure-page           1011 Nov 20 2020 16:04:03
```

12.3 ゲートウェイ認証の構成例と設定例

ゲートウェイ認証の構成例と設定例を示します。

12.3.1 サーバーファームアクセス時のゲートウェイ認証の設定例

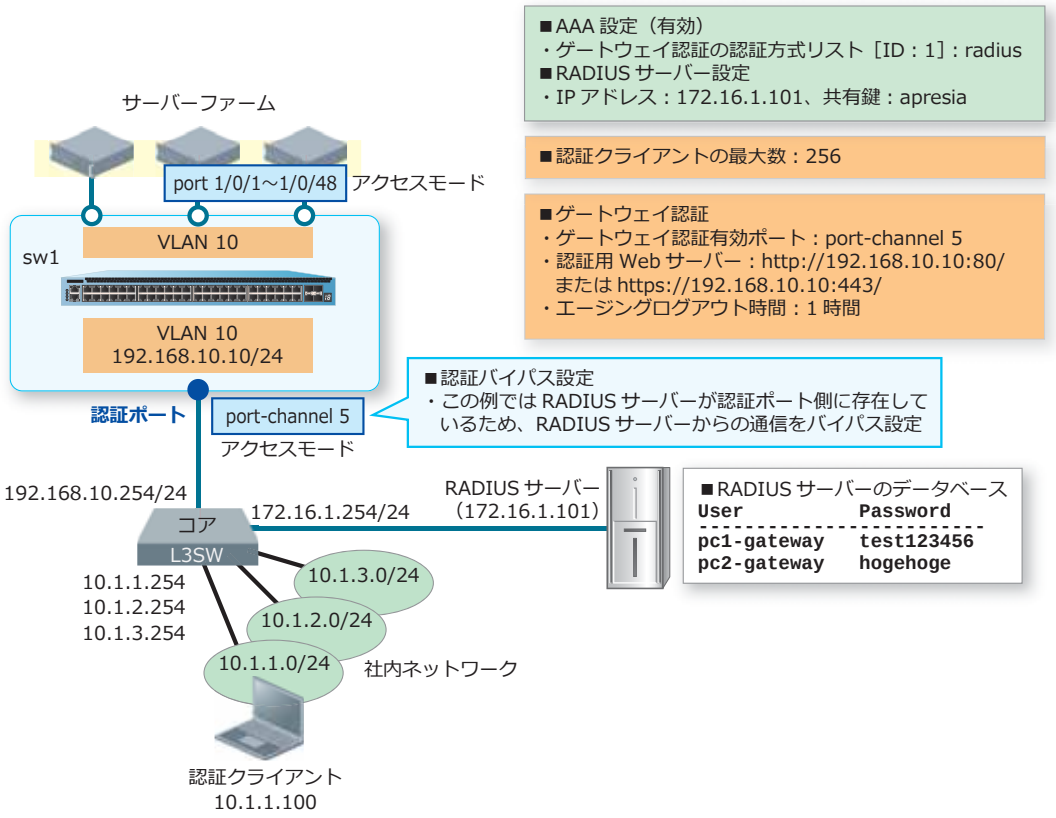
社内ネットワークの端末からサーバーファームへアクセスする際にゲートウェイ認証を実施する場合の構成例と設定例を示します。この例では以下のように設定しています。

表 12-7 サーバーファームアクセス時のゲートウェイ認証の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
ゲートウェイ認証有効ポート	port-channel 5（ポート 1/0/49,1/0/50）
認証用 Web サーバー	http://192.168.10.10:80/、または https://192.168.10.10:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
エージングログアウト時間	1 時間

また、この例では RADIUS サーバーが認証ポート側に存在しているため、認証スイッチと RADIUS サーバーが通信できるように、「RADIUS サーバーからの通信をバイパス」する認証バイパスも設定しています。

図 12-6 サーバーファームアクセス時のゲートウェイ認証の構成例



1. ポート 1/0/49 からポート 1/0/50 をチャネルグループ ID［5］のメンバーポートとして、スタティックモードで設定します。

```
sw1# configure terminal
sw1(config)# interface range port 1/0/49-50
sw1(config-if-port-range)# channel-group 5 mode on
sw1(config-if-port-range)# exit
sw1(config)#
```

2. VLAN 10 を作成し、構成例のように VLAN を割り当てます。

```
sw1(config)# vlan 10
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface port-channel 5
sw1(config-if-port-channel)# switchport mode access
sw1(config-if-port-channel)# switchport access vlan 10
sw1(config-if-port-channel)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-48
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
```

3. VLAN 10 インターフェースに IP アドレス［192.168.10.10/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.10.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ip address 192.168.10.10/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.10.254
sw1(config)#
```

4. 装置の AAA を有効化します。また、ゲートウェイ認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。コマンドは Web 認証と共通です。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

5. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

6. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

7. ポートチャネル 5 でゲートウェイ認証を有効に、認証用 Web サーバーの IP アドレスを［192.168.10.10］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port-channel 5 gateway
sw1(config-a-def)# web-authentication http-ip ipv4 192.168.10.10
sw1(config-a-def)# logout aging-time 0 0 1 gateway
sw1(config-a-def)# exit
sw1(config)#
```

8. ゲートウェイ認証を有効にします。コマンドは Web 認証と共通です。

```
sw1(config)# web-authentication enable
sw1(config)#
```

9. 認証バイパス設定のために、標準 IP アクセスリスト［IPv4-ACL］を作成し、以下のルールを設定します。設定したアクセスリストを認証ポートに適用します。

ルール 10（authentication-bypass）：送信元 IP アドレス［172.16.1.101］

```
sw1(config)# ip access-list IPv4-ACL
sw1(config-ip-acl)# 10 permit authentication-bypass host 172.16.1.101
sw1(config-ip-acl)# exit
sw1(config)#
```

10. 設定したアクセスリストを認証ポート（ポートチャネル 5 のメンバーポートであるポート 1/0/49 からポート 1/0/50）に適用します。

```
sw1(config)# interface range port 1/0/49-50
sw1(config-if-port-range)# ip access-group IPv4-ACL in

The remaining applicable IP related access entries are 255
sw1(config-if-port-range)# end
sw1#
```

11. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 gateway

# WEB-AUTHENTICATION

access-defender
 authentication interface port-channel 5 gateway
 web-authentication http-ip ipv4 192.168.10.10
web-authentication enable
```

12. 実施後のアクセスリスト関連の設定を以下に抜粋します。

```
ip access-list IPv4-ACL 1999
 10 permit authentication-bypass host 172.16.1.101 any
interface port 1/0/49
 ip access-group IPv4-ACL in
interface port 1/0/50
 ip access-group IPv4-ACL in
```

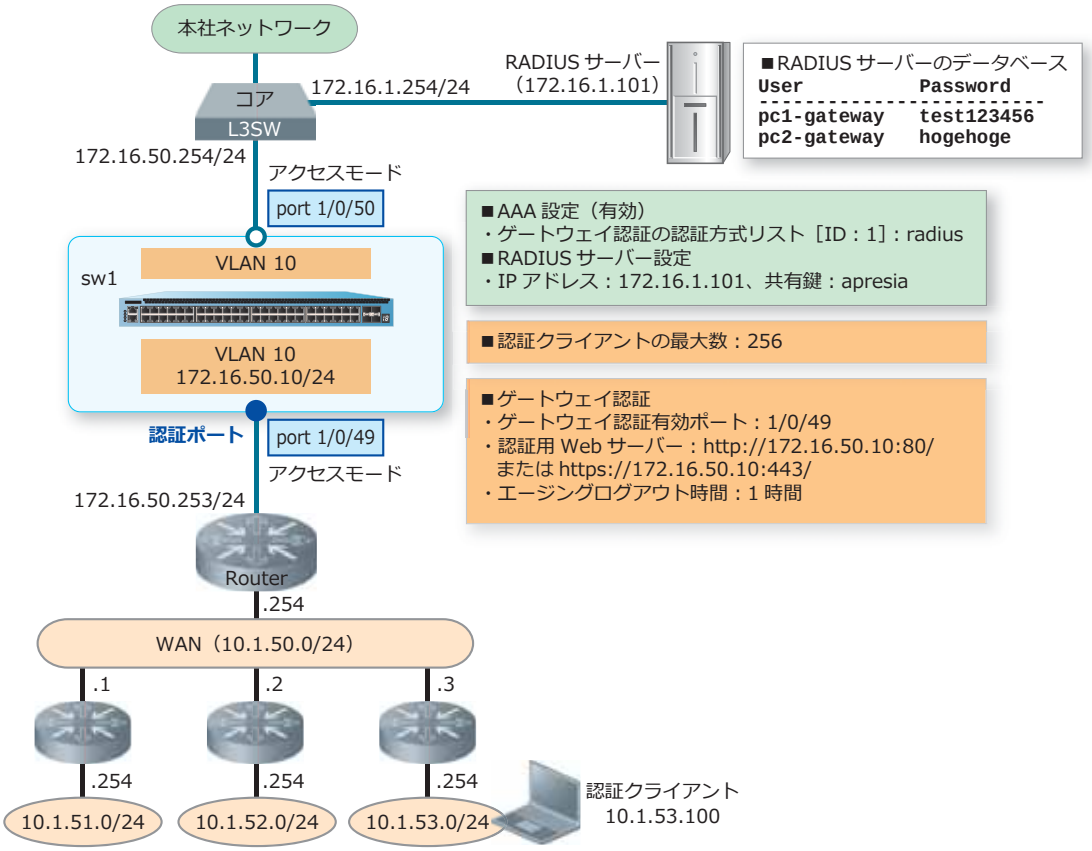
12.3.2 本社アクセス時のゲートウェイ認証の設定例

支社などから本社ネットワークへアクセスする前に、ゲートウェイ認証を実施する場合の構成例と設定例を示します。この例では以下のように設定しています。

表 12-8 本社アクセス時のゲートウェイ認証の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
ゲートウェイ認証有効ポート	ポート 1/0/49
認証用 Web サーバー	http://172.16.50.10:80/、または https://172.16.50.10:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
エージングログアウト時間	1 時間

図 12-7 本社アクセス時のゲートウェイ認証の構成例



1. VLAN 10 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/49-50
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
```

2. VLAN 10 インターフェースに IP アドレス［172.16.50.10/24］を設定します。また、本設定例ではデフォルトスタティックルートを［172.16.50.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 10
sw1(config-if-vlan)# ip address 172.16.50.10/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 172.16.50.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、ゲートウェイ認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。コマンドは Web 認証と共通です。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/49 でゲートウェイ認証を有効に、認証用 Web サーバーの IP アドレスを［172.16.50.10］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/49 gateway
sw1(config-a-def)# web-authentication http-ip ipv4 172.16.50.10
sw1(config-a-def)# logout aging-time 0 0 1 gateway
sw1(config-a-def)# exit
sw1(config)#
```

7. ゲートウェイ認証を有効にします。コマンドは Web 認証と共通です。

```
sw1(config)# web-authentication enable
sw1(config)# end
sw1#
```

8. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 gateway

# WEB-AUTHENTICATION

access-defender
 authentication interface port 1/0/49 gateway
 web-authentication http-ip ipv4 172.16.50.10
web-authentication enable
```

12.4 IEEE 802.1X 認証の構成例と設定例

IEEE 802.1X 認証の構成例と設定例を示します。

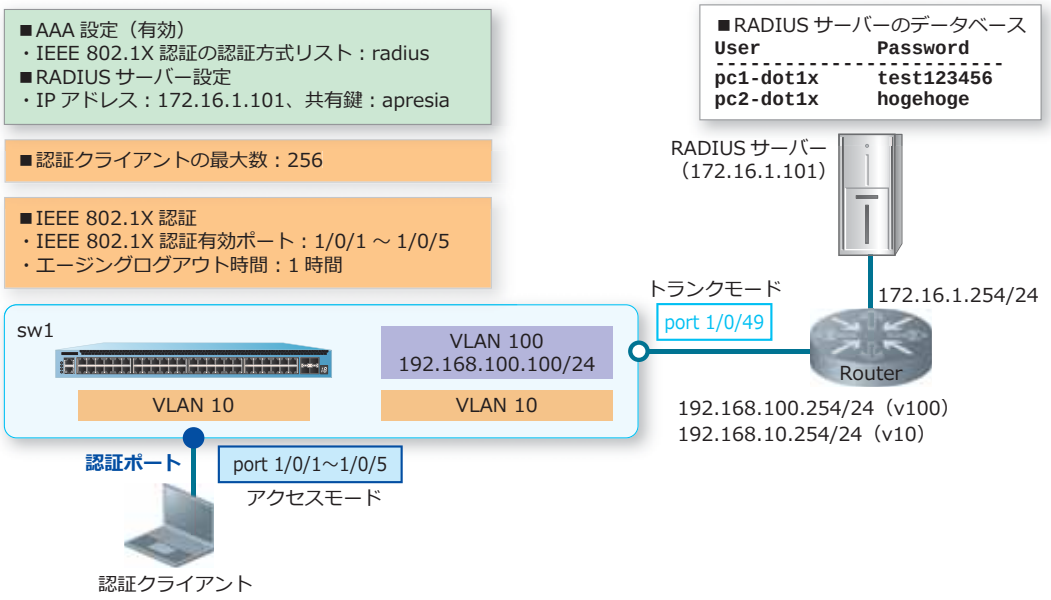
12.4.1 IEEE 802.1X 認証の設定例

IEEE 802.1X 認証の構成例と設定例を示します。この例では以下のように設定しています。

表 12-9 IEEE 802.1X 認証の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
IEEE 802.1X 認証有効ポート	ポート 1/0/1 からポート 1/0/5
エージングログアウト時間	1 時間

図 12-8 IEEE 802.1X 認証の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、IEEE 802.1X 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication dot1x default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で IEEE 802.1X 認証を有効にします。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 dot1x
sw1(config-a-def)# logout aging-time 0 0 1 dot1x
sw1(config-a-def)# exit
sw1(config)#
```

7. IEEE 802.1X 認証を有効にします。

```
sw1(config)# dot1x enable
sw1(config)# end
sw1#
```

8. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication dot1x default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 dot1x

# DOT1X

access-defender
 authentication interface port 1/0/1-1/0/5 dot1x
dot1x enable
```

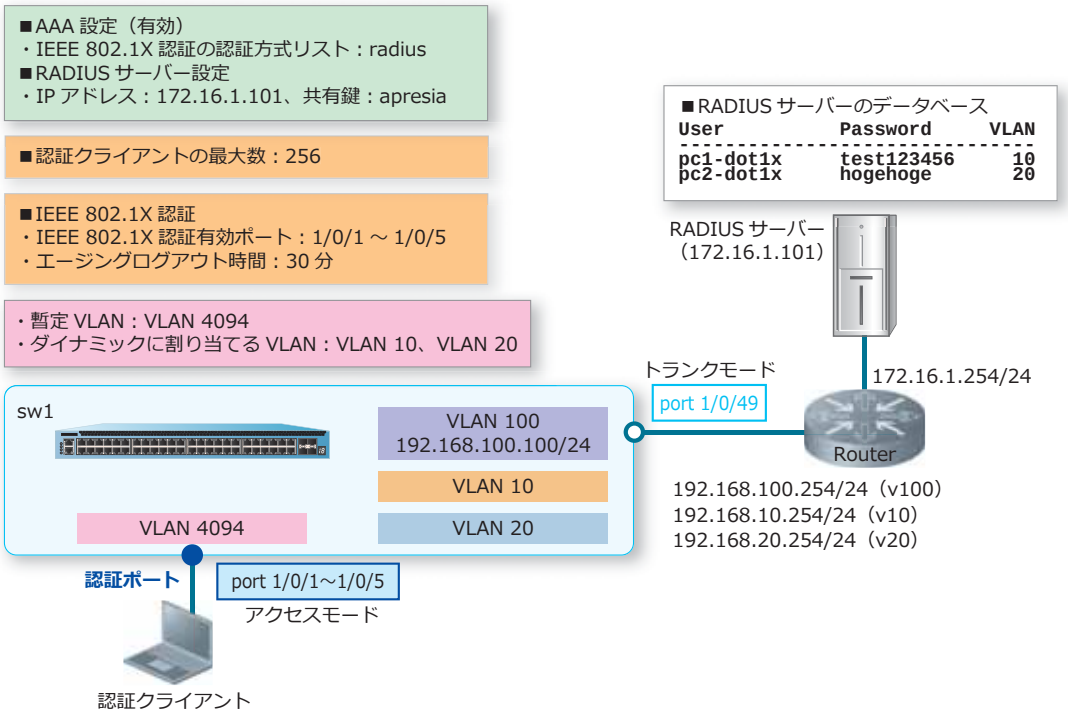
12.4.2 IEEE 802.1X 認証でダイナミック VLAN を使用する場合

IEEE 802.1X 認証でダイナミック VLAN を使用する場合の構成例と設定例を示します。この例では、認証ポートには暫定 VLAN 4094 を割り当てておき、ダイナミック VLAN を使用して、ユーザーごとに VLAN 10 または VLAN 20 が割り当てられるようにしています。

表 12-10 IEEE 802.1X 認証でダイナミック VLAN を使用する場合の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
IEEE 802.1X 認証有効ポート	ポート 1/0/1 からポート 1/0/5
エージングログアウト時間	30 分

図 12-9 IEEE 802.1X 認証でダイナミック VLAN を使用する場合の構成例



1. VLAN 10、VLAN 20、VLAN 100、VLAN 4094 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,20,100,4094
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 4094
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,20,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、IEEE 802.1X 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication dot1x default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で IEEE 802.1X 認証を有効にします。また、エージングログアウト時間を［30 分］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 dot1x
sw1(config-a-def)# logout aging-time 0 30 dot1x
sw1(config-a-def)# exit
sw1(config)#
```

7. IEEE 802.1X 認証を有効にします。

```
sw1(config)# dot1x enable
sw1(config)# end
sw1#
```

8. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication dot1x default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 30 dot1x

# DOT1X

access-defender
 authentication interface port 1/0/1-1/0/5 dot1x
dot1x enable
```

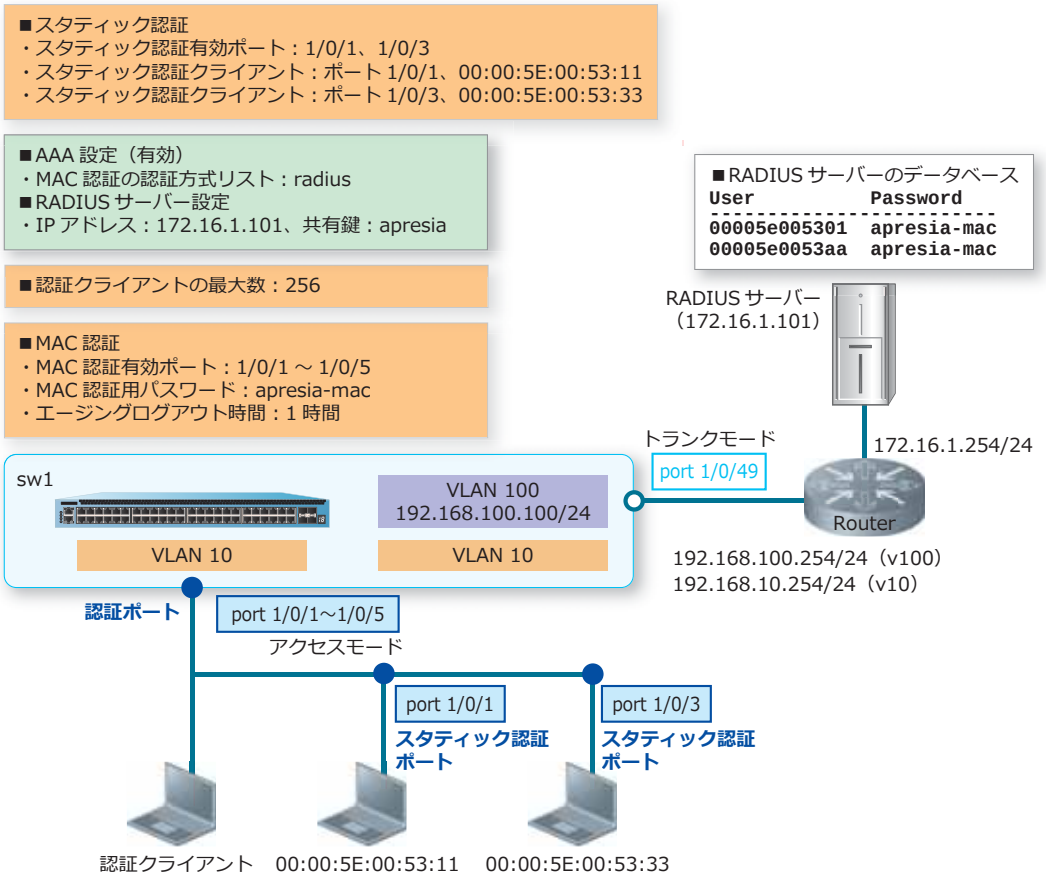
12.5 スタティック認証の構成例と設定例

スタティック認証の構成例と設定例を示します。この例では以下のように設定しています。

表 12-11 スタティック認証の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac
エージングログアウト時間	1 時間
スタティック認証有効ポート	ポート 1/0/1、ポート 1/0/3
スタティック認証端末	ポート 1/0/1、00:00:5E:00:53:11
スタティック認証端末	ポート 1/0/3、00:00:5E:00:53:33

図 12-10 スタティック認証の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で MAC 認証を有効に、MAC 認証用パスワードを［apresia-mac］に設定します。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# logout aging-time 0 0 1 mac
sw1(config-a-def)# exit
sw1(config)#
```

7. MAC 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)#
```

8. ポート 1/0/1 とポート 1/0/3 でスタティック認証を有効に設定し、スタティックエントリー［ポート 1/0/1、00:00:5E:00:53:11］［ポート 1/0/3、00:00:5E:00:53:33］を設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# authentication interface port 1/0/1,1/0/3 static
sw1(config-a-def)# exit
sw1(config)# access-defender static mac 0000.5e00.5311 interface port 1/0/1
sw1(config)# access-defender static mac 0000.5e00.5333 interface port 1/0/3
sw1(config)# end
sw1#
```

9. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication mac-auth default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 mac
 authentication interface port 1/0/1,1/0/3 static
access-defender static mac 00-00-5E-00-53-11 interface port 1/0/1
access-defender static mac 00-00-5E-00-53-33 interface port 1/0/3

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable
```

12.6 DHCP スヌーピングの構成例と設定例

DHCP スヌーピングの構成例と設定例を示します。

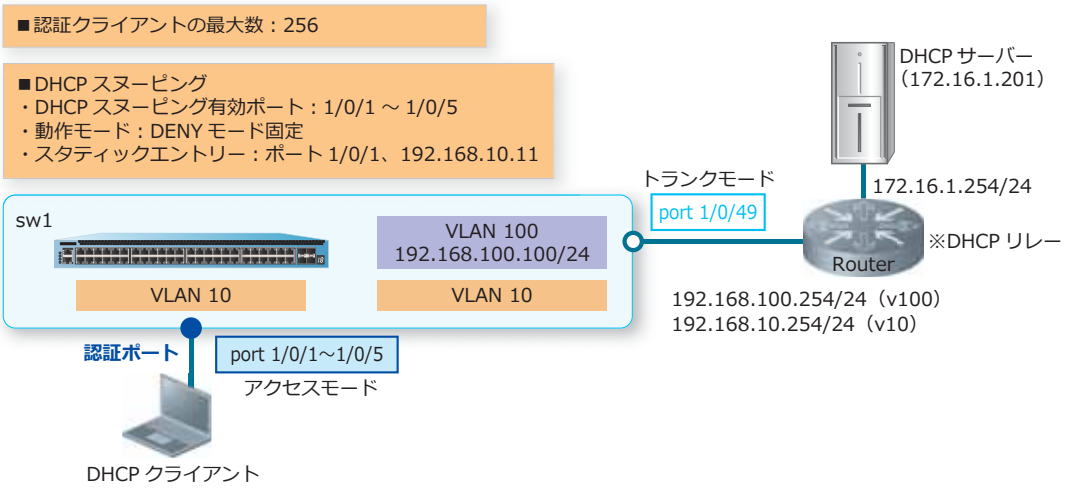
12.6.1 DHCP スヌーピングの設定例

DHCP スヌーピングの構成例と設定例を示します。この例では以下のように設定しています。

表 12-12 DHCP スヌーピングの設定例

項目	設定
認証クライアントの最大数	256
DHCP スヌーピング有効ポート	ポート 1/0/1 からポート 1/0/5
DHCP スヌーピングの動作モード	DENY モード固定
スタティックエントリー	ポート 1/0/1、192.168.10.11

図 12-11 DHCP スヌーピングの構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

4. ポート 1/0/1 からポート 1/0/5 で DHCP スヌーピングを有効に、動作モードを DENY モード固定に設定します。

```
sw1(config-a-def)# dhcp-snooping interface port 1/0/1-5
sw1(config-a-def)# dhcp-snooping mode deny
sw1(config-a-def)#
```

5. DHCP スヌーピングのスタティックエントリー［ポート 1/0/1、192.168.10.11］を設定します。

```
sw1(config-a-def)# dhcp-snooping static-entry interface port 1/0/1
192.168.10.11
sw1(config-a-def)# exit
sw1(config)#
```

6. DHCP スヌーピングを有効にします。

```
sw1(config)# dhcp-snooping enable
sw1(config)# end
sw1#
```

7. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# ACCESS-DEFENDER

access-defender
 total-client 256

# DHCP-SNOOPING

access-defender
 dhcp-snooping interface port 1/0/1-1/0/5
 dhcp-snooping mode deny
 dhcp-snooping static-entry interface port 1/0/1 192.168.10.11
dhcp-snooping enable
```

12.6.2 DHCP スヌーピングと MAC 認証を併用する場合

DHCP スヌーピングと MAC 認証を併用する場合の構成例と設定例を示します。この例では MAC 認証は以下のように設定しています。

表 12-13 MAC 認証の設定例

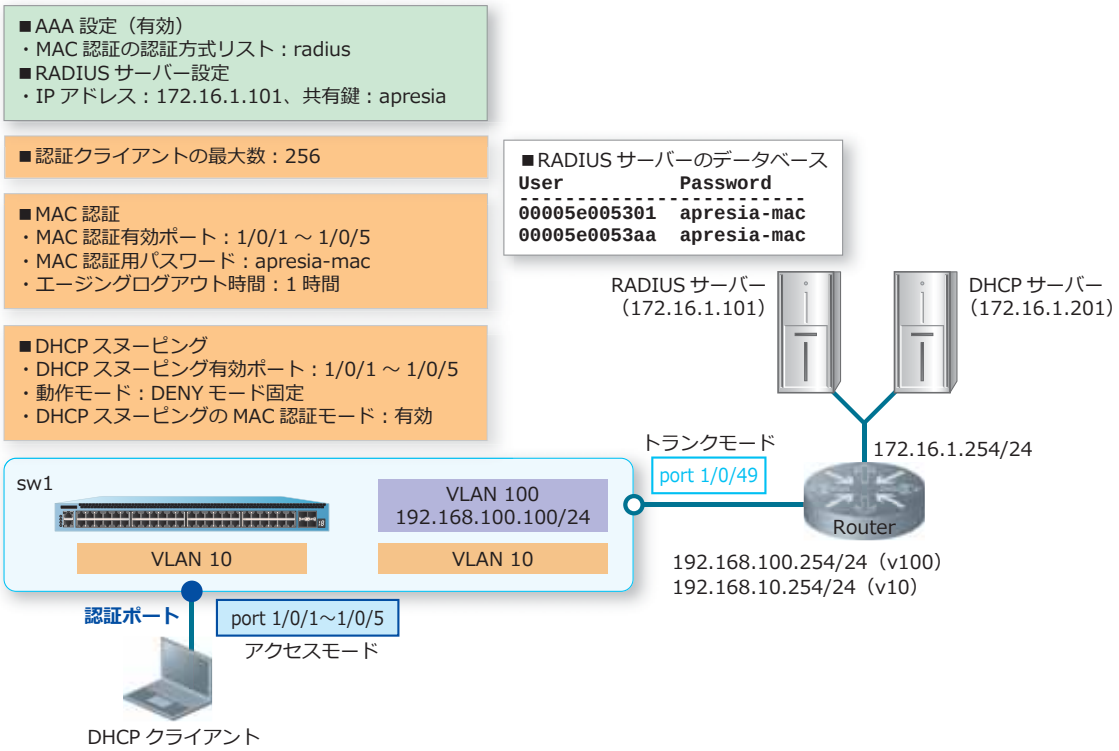
項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac
エージングログアウト時間	1 時間

また、DHCP スヌーピングは以下のように設定しています。

表 12-14 DHCP スヌーピングの設定例

項目	設定
DHCP スヌーピング有効ポート	ポート 1/0/1 からポート 1/0/5
DHCP スヌーピングの動作モード	DENY モード固定
DHCP スヌーピングの MAC 認証モード	有効

図 12-12 DHCP スヌーピングと MAC 認証を併用する場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で MAC 認証を有効に、MAC 認証用パスワードを［apresia-mac］に設定します。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# logout aging-time 0 0 1 mac
sw1(config-a-def)# exit
sw1(config)#
```

7. MAC 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)#
```

8. ポート 1/0/1 からポート 1/0/5 で DHCP スヌーピングを有効に、動作モードを DENY モード固定に、DHCP スヌーピングの MAC 認証モードを有効に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# dhcp-snooping interface port 1/0/1-5
sw1(config-a-def)# dhcp-snooping mode deny
sw1(config-a-def)# dhcp-snooping mode mac-authentication
sw1(config-a-def)# exit
sw1(config)#
```

9. DHCP スヌーピングを有効にします。

```
sw1(config)# dhcp-snooping enable
sw1(config)# end
sw1#
```

10. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication mac-auth default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 mac

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable

# DHCP-SNOOPING

access-defender
 dhcp-snooping interface port 1/0/1-1/0/5
 dhcp-snooping mode deny
 dhcp-snooping mode mac-authentication
dhcp-snooping enable
```

12.6.3 DHCP スヌーピングと Web 認証を併用する場合

DHCP スヌーピングと Web 認証を併用する場合の構成例と設定例を示します。この例では Web 認証は以下のように設定しています。

表 12-15 Web 認証の設定例

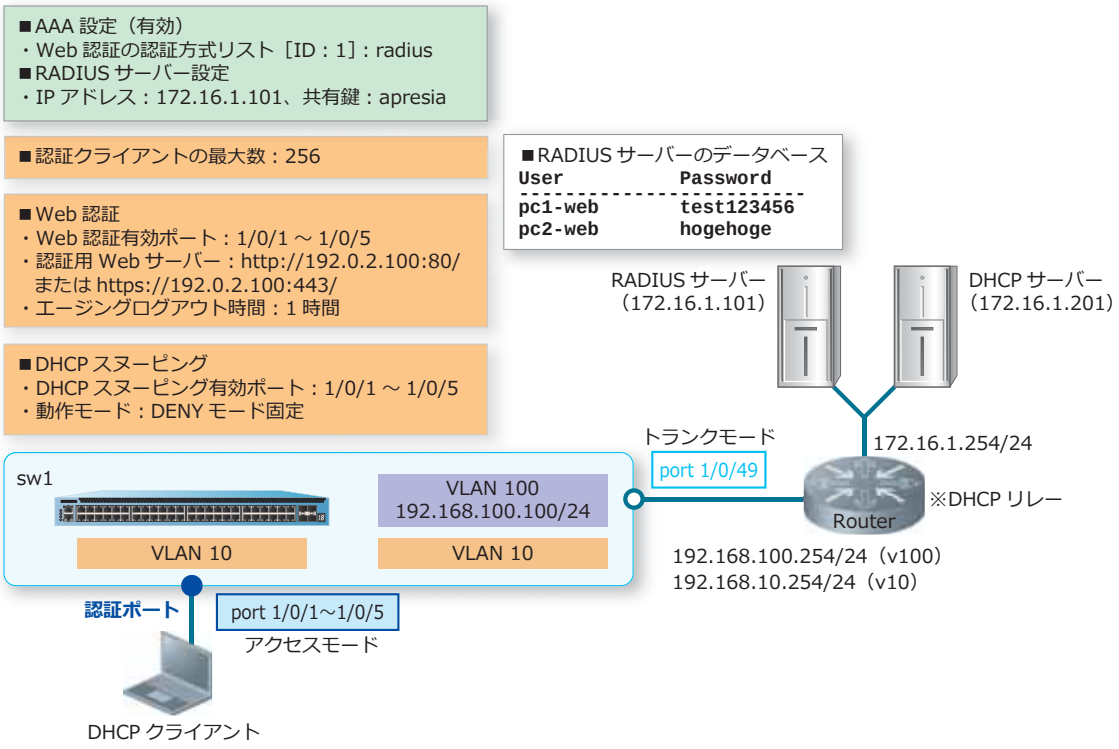
項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
Web 認証有効ポート	ポート 1/0/1 からポート 1/0/5
認証用 Web サーバー	http://192.0.2.100:80/、または https://192.0.2.100:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
エージングログアウト時間	1 時間

また、DHCP スヌーピングは以下のように設定しています。

表 12-16 DHCP スヌーピングの設定例

項目	設定
DHCP スヌーピング有効ポート	ポート 1/0/1 からポート 1/0/5
DHCP スヌーピングの動作モード	DENY モード固定

図 12-13 DHCP スヌーピングと Web 認証を併用する場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、Web 認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で Web 認証を有効に、認証用 Web サーバーの IP アドレスを［192.0.2.100］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 web
sw1(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
sw1(config-a-def)# logout aging-time 0 0 1 web
sw1(config-a-def)# exit
sw1(config)#
```

7. Web 認証を有効にします。

```
sw1(config)# web-authentication enable
sw1(config)#
```

8. ポート 1/0/1 からポート 1/0/5 で DHCP スヌーピングを有効に、動作モードを DENY モード固定に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# dhcp-snooping interface port 1/0/1-5
sw1(config-a-def)# dhcp-snooping mode deny
sw1(config-a-def)# exit
sw1(config)#
```

9. DHCP スヌーピングを有効にします。

```
sw1(config)# dhcp-snooping enable
sw1(config)# end
sw1#
```

10. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 web

# WEB-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 web
 web-authentication http-ip ipv4 192.0.2.100
web-authentication enable

# DHCP-SNOOPING

access-defender
 dhcp-snooping interface port 1/0/1-1/0/5
 dhcp-snooping mode deny
dhcp-snooping enable
```

12.7 OR 認証（1 ポート複数認証）の構成例と設定例

OR 認証（1 ポート複数認証）の構成例と設定例を示します。

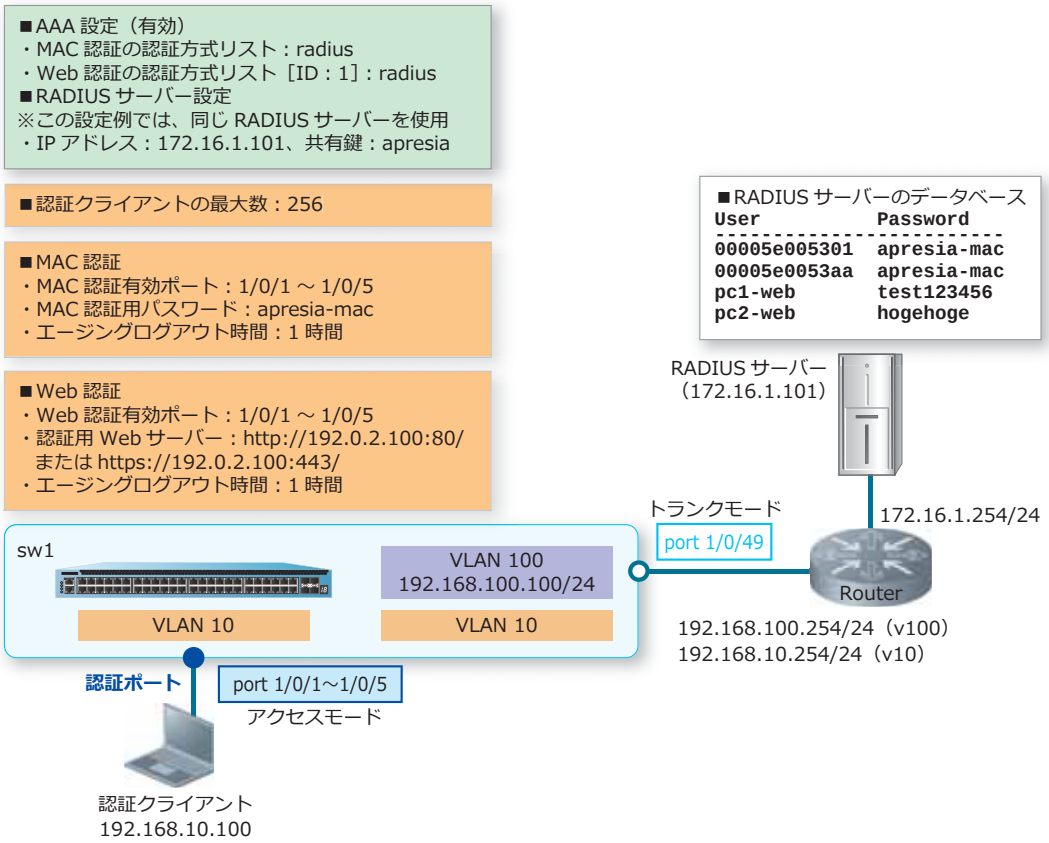
12.7.1 同一ポートで MAC 認証と Web 認証を使用する場合

同一ポートで MAC 認証と Web 認証を使用する場合の構成例と設定例を示します。この例では MAC 認証と Web 認証は以下のように設定しています。

表 12-17 同一ポートで MAC 認証と Web 認証を使用する場合の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia ※ この設定例では、MAC 認証も Web 認証も、同じ RADIUS サーバーを使用
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac
MAC 認証用エージングログアウト時間	1 時間
Web 認証有効ポート	ポート 1/0/1 からポート 1/0/5
認証用 Web サーバー	http://192.0.2.100:80/、または https://192.0.2.100:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
Web 認証用エージングログアウト時間	1 時間

図 12-14 同一ポートで MAC 認証と Web 認証を使用する場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に、Web 認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default group radius
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で MAC 認証と Web 認証を有効に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# authentication interface port 1/0/1-5 web
sw1(config-a-def)#
```

7. MAC 認証用パスワードを［apresia-mac］に設定します。また、MAC 認証用のエージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# logout aging-time 0 0 1 mac
sw1(config-a-def)#
```

8. 認証用 Web サーバーの IP アドレスを［192.0.2.100］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。また、Web 認証用のエージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
sw1(config-a-def)# logout aging-time 0 0 1 web
sw1(config-a-def)# exit
sw1(config)#
```

9. MAC 認証と Web 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)# web-authentication enable
sw1(config)# end
sw1#
```

10. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication mac-auth default group radius
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 mac
 logout aging-time 0 0 1 web

# WEB-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 web
 web-authentication http-ip ipv4 192.0.2.100
web-authentication enable

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable
```

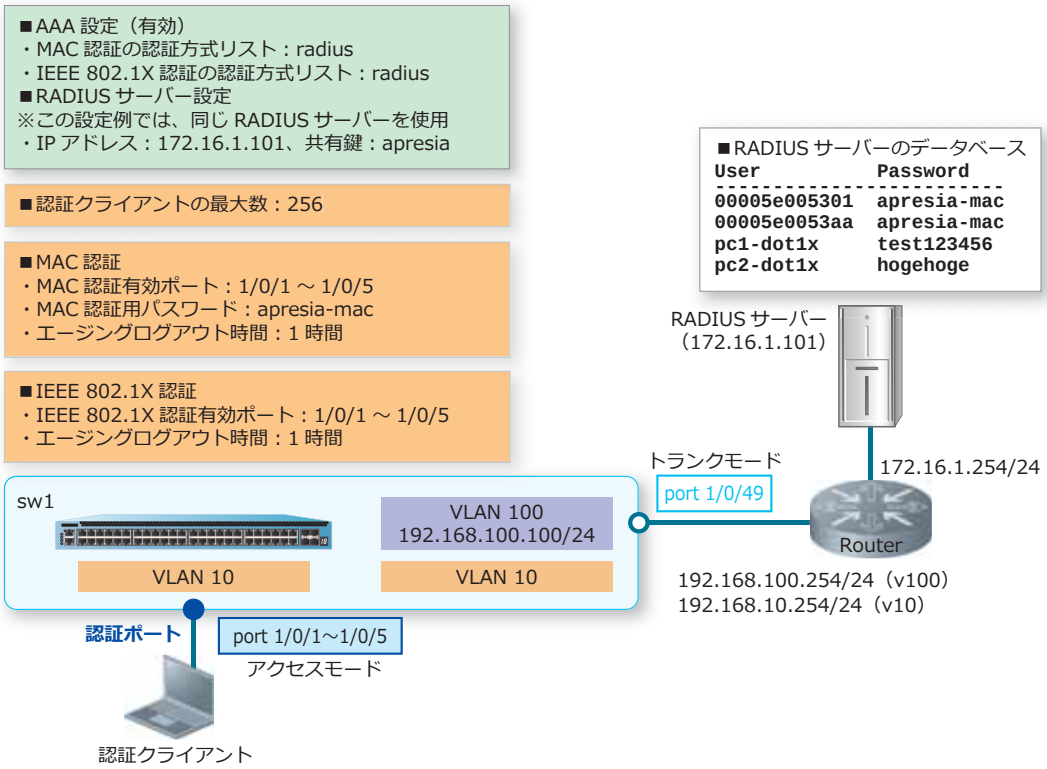
12.7.2 同一ポートで MAC 認証と IEEE 802.1X 認証を使用する場合

同一ポートで MAC 認証と IEEE 802.1X 認証を使用する場合の構成例と設定例を示します。この例では MAC 認証と IEEE 802.1X 認証は以下のように設定しています。

表 12-18 同一ポートで MAC 認証と IEEE 802.1X 認証を使用する場合の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia ※ この設定例では、MAC 認証も IEEE 802.1X 認証も、同じ RADIUS サーバーを使用
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac
MAC 認証用エージングログアウト時間	1 時間
IEEE 802.1X 認証有効ポート	ポート 1/0/1 からポート 1/0/5
IEEE 802.1X 認証用エージングログアウト時間	1 時間

図 12-15 同一ポートで MAC 認証と IEEE 802.1X 認証を使用する場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に、IEEE 802.1X 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default group radius
sw1(config)# aaa authentication dot1x default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で MAC 認証と IEEE 802.1X 認証を有効に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# authentication interface port 1/0/1-5 dot1x
sw1(config-a-def)#
```

7. MAC 認証用パスワードを［apresia-mac］に設定します。また、MAC 認証用のエージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# logout aging-time 0 0 1 mac
sw1(config-a-def)#
```

8. IEEE 802.1X 認証用のエージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# logout aging-time 0 0 1 dot1x
sw1(config-a-def)# exit
sw1(config)#
```

9. MAC 認証と IEEE 802.1X 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)# dot1x enable
sw1(config)# end
sw1#
```

10. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication dot1x default group radius
aaa authentication mac-auth default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 mac
 logout aging-time 0 0 1 dot1x

# DOT1X

access-defender
 authentication interface port 1/0/1-1/0/5 dot1x
dot1x enable

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable
```

12.8 AND 認証の構成例と設定例

AND 認証の構成例と設定例を示します。

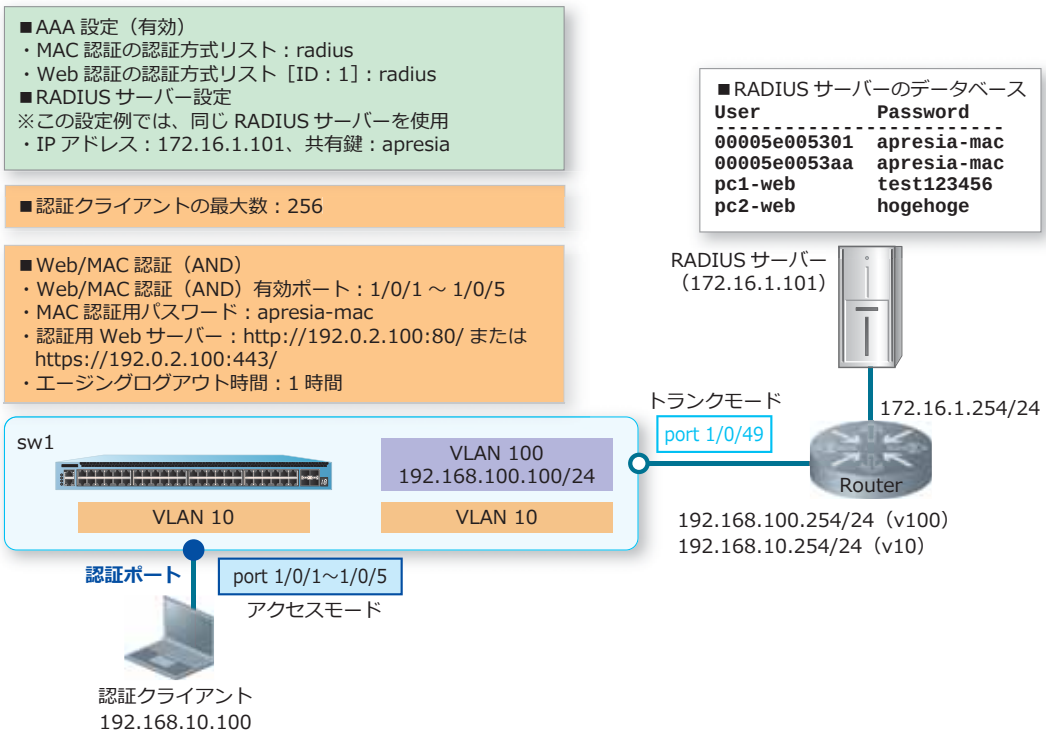
12.8.1 Web/MAC 認証（AND）の設定例

Web/MAC 認証（AND）の構成例と設定例を示します。この例では以下のように設定しています。

表 12-19 Web/MAC 認証（AND）の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia ※ この設定例では、MAC 認証も Web 認証も、同じ RADIUS サーバーを使用
認証クライアントの最大数	256
Web/MAC 認証（AND）有効ポート	ポート 1/0/1 からポート 1/0/5
Web/MAC 認証（AND）認証用パスワード	apresia-mac
認証用 Web サーバー	http://192.0.2.100:80/、または https://192.0.2.100:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
エージングログアウト時間	1 時間

図 12-16 Web/MAC 認証（AND）の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に、Web 認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default group radius
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で Web/MAC 認証（AND）を有効に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 web-mac
sw1(config-a-def)#
```

7. Web/MAC 認証（AND）の、MAC 認証用パスワードを［apresia-mac］に設定します。

```
sw1(config-a-def)# mac-authentication password apresia-mac web-mac
sw1(config-a-def)#
```

8. 認証用 Web サーバーの IP アドレスを［192.0.2.100］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。

```
sw1(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
sw1(config-a-def)#
```

9. Web/MAC 認証（AND）用のエージングログアウト時間を［1 時間］に設定します。Web/MAC 認証（AND）の場合は web パラメーターを指定して設定します。

```
sw1(config-a-def)# logout aging-time 0 0 1 web
sw1(config-a-def)# exit
sw1(config)#
```

10. MAC 認証と Web 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)# web-authentication enable
sw1(config)# end
sw1#
```

11. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication mac-auth default group radius
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 web
 authentication interface port 1/0/1-1/0/5 web-mac

# WEB-AUTHENTICATION

access-defender
 web-authentication http-ip ipv4 192.0.2.100
web-authentication enable

# MAC-AUTHENTICATION

access-defender
 mac-authentication password apresia-mac web-mac
mac-authentication enable
```

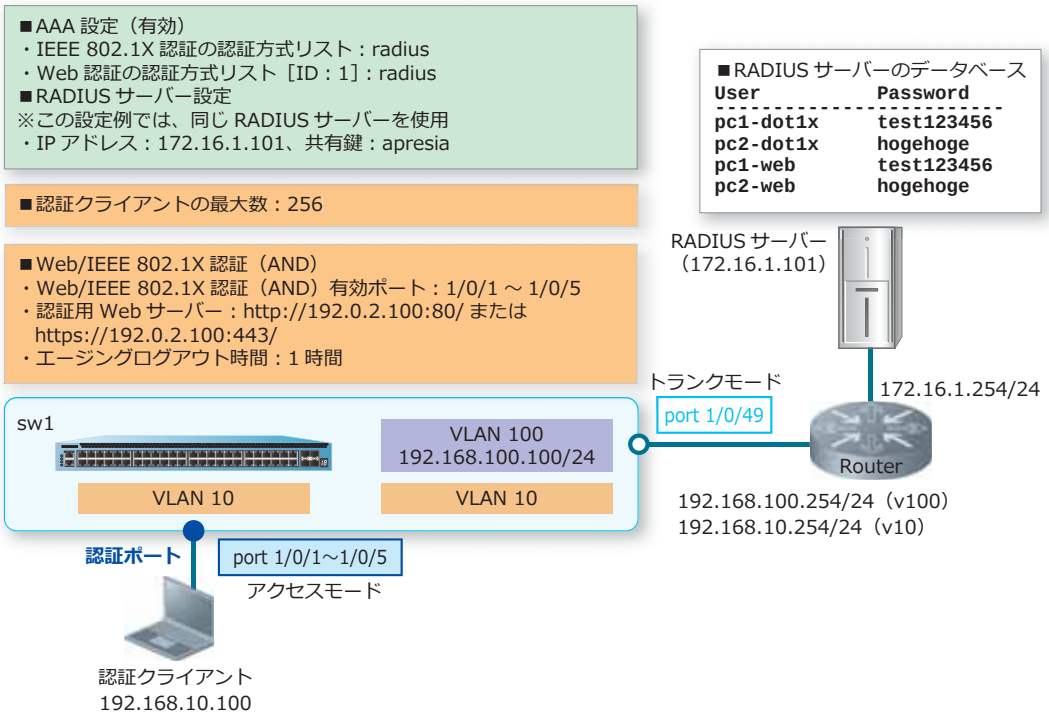
12.8.2 Web/IEEE 802.1X 認証（AND）の設定例

Web/IEEE 802.1X 認証（AND）の構成例と設定例を示します。この例では以下のように設定しています。

表 12-20 Web/IEEE 802.1X 認証（AND）の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia ※ この設定例では、IEEE 802.1X 認証も Web 認証も、同じ RADIUS サーバーを使用
認証クライアントの最大数	256
Web/IEEE 802.1X 認証（AND）有効ポート	ポート 1/0/1 からポート 1/0/5
認証用 Web サーバー	http://192.0.2.100:80/、または https://192.0.2.100:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
エージングログアウト時間	1 時間

図 12-17 Web/IEEE 802.1X 認証（AND）の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、IEEE 802.1X 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に、Web 認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication dot1x default group radius
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で Web/IEEE 802.1X 認証（AND）を有効に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 web-dot1x
sw1(config-a-def)#
```

7. 認証用 Web サーバーの IP アドレスを［192.0.2.100］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。

```
sw1(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
sw1(config-a-def)#
```

8. Web/IEEE 802.1X 認証（AND）用のエージングログアウト時間を［1 時間］に設定します。Web/IEEE 802.1X 認証（AND）の場合は web パラメーターを指定して設定します。

```
sw1(config-a-def)# logout aging-time 0 0 1 web
sw1(config-a-def)# exit
sw1(config)#
```

9. IEEE 802.1X 認証と Web 認証を有効にします。

```
sw1(config)# dot1x enable
sw1(config)# web-authentication enable
sw1(config)# end
sw1#
```

10. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication dot1x default group radius
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 web
 authentication interface port 1/0/1-1/0/5 web-dot1x

# DOT1X

dot1x enable

# WEB-AUTHENTICATION

access-defender
 web-authentication http-ip ipv4 192.0.2.100
web-authentication enable
```

12.9 AccessDefender の認証方式の構成例と設定例

AccessDefender の認証方式の構成例と設定例を示します。

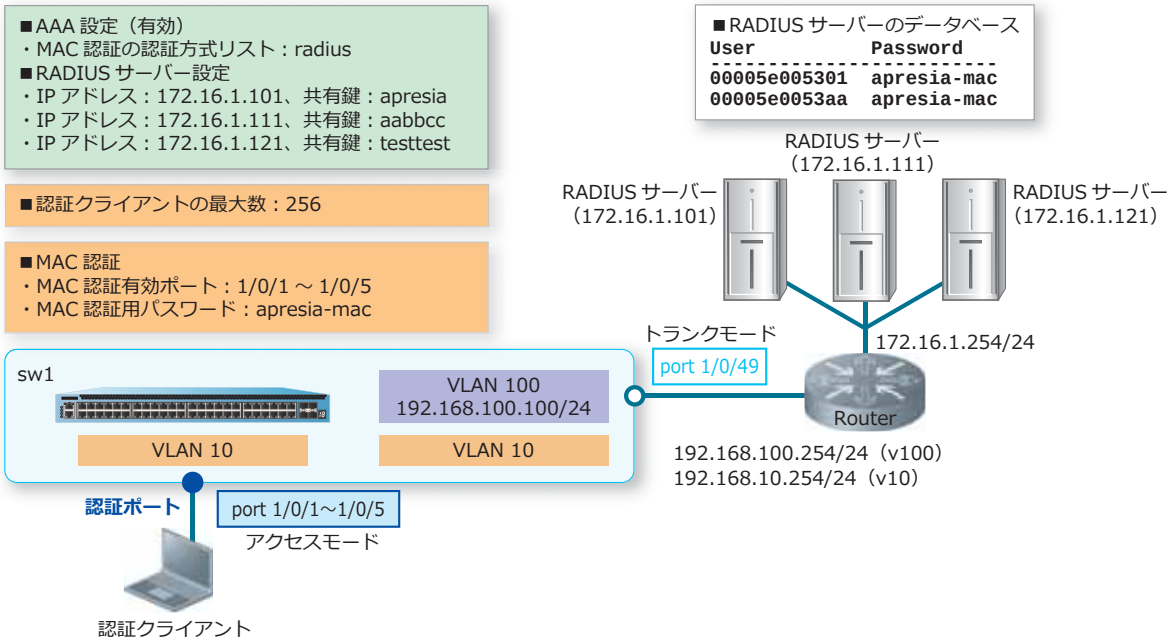
12.9.1 複数の RADIUS サーバーを使用する場合

複数の RADIUS サーバーを使用する場合の構成例と設定例を示します。所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に、設定した順番に登録されます。登録リストの先頭の RADIUS サーバーから問い合わせが行われ、タイムアウトなどで応答がない場合には次に登録された RADIUS サーバーに問い合わせます。

表 12-21 複数の RADIUS サーバーを使用する場合の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
RADIUS サーバー	• IP アドレス：172.16.1.111 • 共有鍵：aabbcc
RADIUS サーバー	• IP アドレス：172.16.1.121 • 共有鍵：testtest
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac

図 12-18 複数の RADIUS サーバーを使用する場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default group radius
sw1(config)#
```

4. 以下の RADIUS サーバーを設定します。所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

IP アドレス［172.16.1.101］、共有鍵［apresia］

IP アドレス［172.16.1.111］、共有鍵［aabbcc］

IP アドレス［172.16.1.121］、共有鍵［testtest］

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)# radius-server host 172.16.1.111 key aabbcc
sw1(config)# radius-server host 172.16.1.121 key testtest
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で MAC 認証を有効に、MAC 認証用パスワードを［apresia-mac］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# exit
sw1(config)#
```

7. MAC 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)# end
sw1#
```

8. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
radius-server host 172.16.1.111 key aabbcc
radius-server host 172.16.1.121 key testtest
aaa authentication mac-auth default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable
```

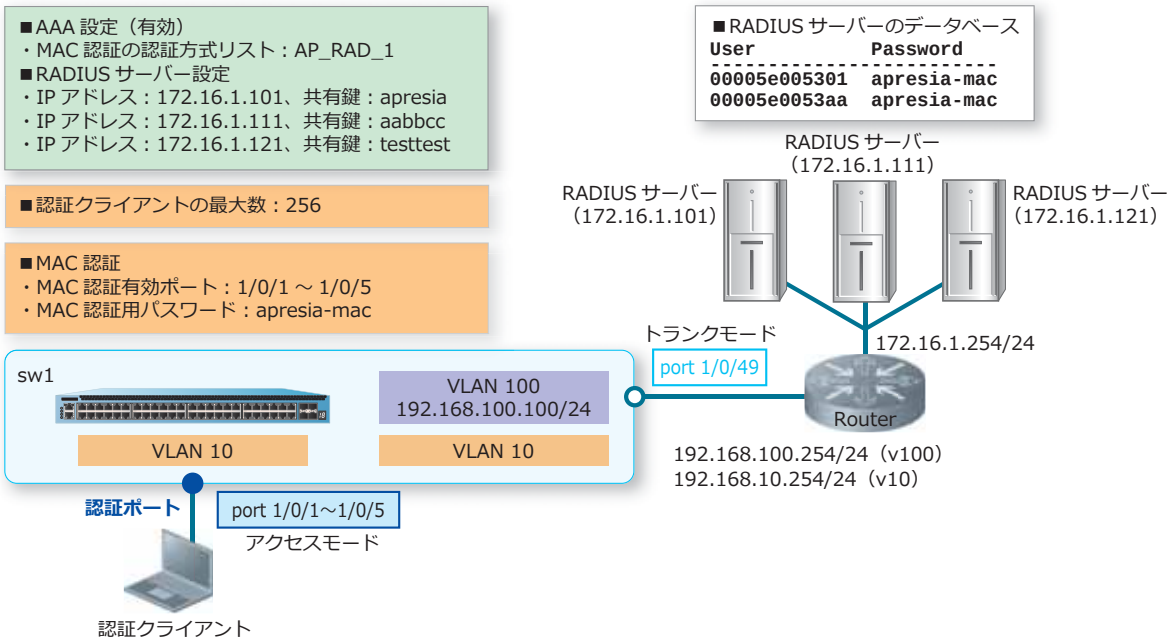
12.9.2 ユーザー設定グループで RADIUS を使用する場合

ユーザー設定グループで RADIUS を使用する場合の構成例と設定例を示します。この例では、ユーザーが設定した RADIUS サーバーグループ「AP_RAD_1」に RADIUS サーバーを登録して使用しています。登録リストの先頭の RADIUS サーバーから問い合わせが行われ、タイムアウトなどで応答がない場合には次に登録された RADIUS サーバーに問い合わせます。

表 12-22 ユーザー設定グループで RADIUS を使用する場合の設定例

項目	設定
RADIUS 認証	ユーザーが設定した RADIUS サーバーグループ「AP_RAD_1」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
RADIUS サーバー	• IP アドレス：172.16.1.111 • 共有鍵：aabbcc
RADIUS サーバー	• IP アドレス：172.16.1.121 • 共有鍵：testtest
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac

図 12-19 ユーザー設定グループで RADIUS を使用する場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。

```
sw1(config)# aaa new-model
sw1(config)#
```

4. 以下の RADIUS サーバーを設定します。所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

IP アドレス［172.16.1.101］、共有鍵［apresia］

IP アドレス［172.16.1.111］、共有鍵［aabbcc］

IP アドレス［172.16.1.121］、共有鍵［testtest］

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)# radius-server host 172.16.1.111 key aabbcc
sw1(config)# radius-server host 172.16.1.121 key testtest
sw1(config)#
```

5. RADIUS サーバーグループ「AP_RAD_1」を作成し、前の手順で設定した RADIUS サーバーを、このグループに所属するように設定します。

```
sw1(config)# aaa group server radius AP_RAD_1
sw1(config-sg-radius)# server 172.16.1.101
sw1(config-sg-radius)# server 172.16.1.111
sw1(config-sg-radius)# server 172.16.1.121
sw1(config-sg-radius)# exit
sw1(config)#
```

6. MAC 認証で使用する認証方式リストを、ユーザー設定の RADIUS サーバーグループ「AP_RAD_1」に指定します。

```
sw1(config)# aaa authentication mac-auth default group AP_RAD_1
sw1(config)#
```

7. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

8. ポート 1/0/1 からポート 1/0/5 で MAC 認証を有効に、MAC 認証用パスワードを［apresia-mac］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# exit
sw1(config)#
```

9. MAC 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)# end
sw1#
```

10. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
radius-server host 172.16.1.111 key aabbcc
radius-server host 172.16.1.121 key testtest
aaa group server radius AP_RAD_1
 server 172.16.1.101
 server 172.16.1.111
 server 172.16.1.121
aaa authentication mac-auth default group AP_RAD_1

# ACCESS-DEFENDER

access-defender
 total-client 256

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable
```

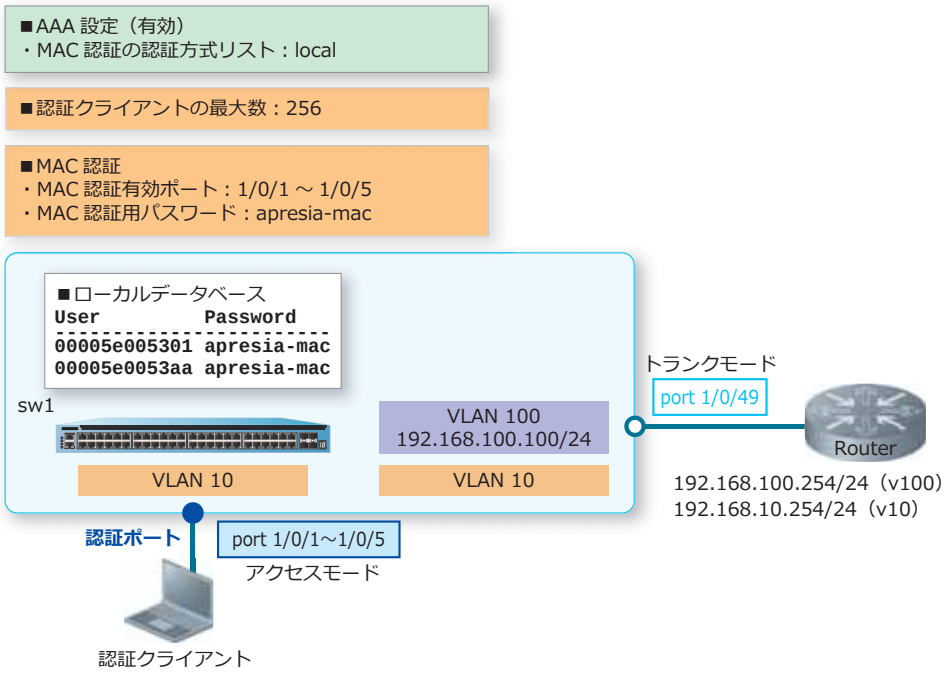
12.9.3 ローカルデータベースを使用する場合

ローカルデータベースを使用する場合の構成例と設定例を示します。この例では以下のように設定しています。

表 12-23 ローカルデータベースを使用する場合の設定例

項目	設定
MAC 認証	MAC 認証でローカルデータベースを使用（デフォルト設定）
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac

図 12-20 ローカルデータベースを使用する場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを「ローカルデータベース（デフォルト設定）」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default local
sw1(config)#
```

4. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

5. ポート 1/0/1 からポート 1/0/5 で MAC 認証を有効に、MAC 認証用パスワードを［apresia-mac］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# exit
sw1(config)#
```

6. MAC 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)#
```

7. ローカルデータベースに、以下のユーザー情報を登録します。

ユーザー名［00005e005301］、パスワード［apresia-mac］

ユーザー名［00005e0053aa］、パスワード［apresia-mac］

```
sw1(config)# access-defender
sw1(config-a-def)# aaa-local-db user 00005e005301 password apresia-mac
sw1(config-a-def)# aaa-local-db user 00005e0053aa password apresia-mac
sw1(config-a-def)# end
sw1#
```

8. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model

# ACCESS-DEFENDER

access-defender
 total-client 256
 aaa-local-db user 00005e005301 password apresia-mac
 aaa-local-db user 00005e0053aa password apresia-mac

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable
```

12.9.4 RADIUS とローカルデータベースを併用する場合

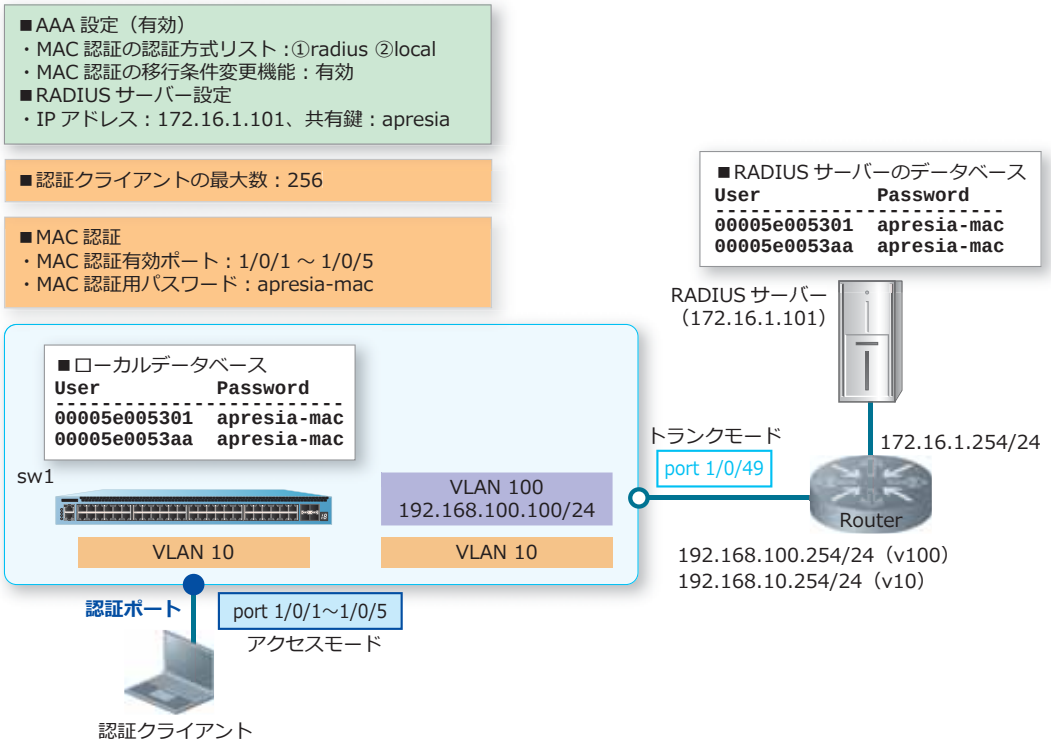
RADIUS とローカルデータベースを併用する場合の構成例と設定例を示します。この例では **aaa authentication control sufficient**コマンドでMAC認証の移行条件変更機能を有効に設定して、タイムアウトだけでなく明示的に認証拒否（Access-Reject）された場合でも、次の認証方法に問い合わせるようにしています。

CAUTION: IEEE 802.1X 認証では移行条件変更機能は使用できません。

表 12-24 RADIUS とローカルデータベースを併用する場合の設定例

項目	設定
MAC 認証の第 1 優先	MAC 認証の第 1 優先で、RADIUS 認証をデフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
MAC 認証の第 2 優先	MAC 認証の第 2 優先で、ローカルデータベースを使用
MAC 認証の移行条件変更機能	有効
認証クライアントの最大数	256
MAC 認証有効ポート	ポート 1/0/1 からポート 1/0/5
MAC 認証用パスワード	apresia-mac

図 12-21 RADIUS とローカルデータベースを併用する場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、MAC 認証で使用する認証方式リストを、第 1 優先をデフォルトの RADIUS サーバーグループ「radius」に、第 2 優先を「ローカルデータベース」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication mac-auth default group radius local
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. MAC 認証の移行条件変更機能を有効にします。

```
sw1(config)# aaa authentication control sufficient mac
sw1(config)#
```

6. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

7. ポート 1/0/1 からポート 1/0/5 で MAC 認証を有効に、MAC 認証用パスワードを［apresia-mac］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 mac
sw1(config-a-def)# mac-authentication password apresia-mac mac
sw1(config-a-def)# exit
sw1(config)#
```

8. MAC 認証を有効にします。

```
sw1(config)# mac-authentication enable
sw1(config)#
```

9. ローカルデータベースに、以下のユーザー情報を登録します。

ユーザー名［00005e005301］、パスワード［apresia-mac］

ユーザー名［00005e0053aa］、パスワード［apresia-mac］

```
sw1(config)# access-defender
sw1(config-a-def)# aaa-local-db user 00005e005301 password apresia-mac
sw1(config-a-def)# aaa-local-db user 00005e0053aa password apresia-mac
sw1(config-a-def)# end
sw1#
```

10. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication mac-auth default group radius local
aaa authentication control sufficient mac

# ACCESS-DEFENDER

access-defender
 total-client 256
 aaa-local-db user 00005e005301 password apresia-mac
 aaa-local-db user 00005e0053aa password apresia-mac

# MAC-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 mac
 mac-authentication password apresia-mac mac
mac-authentication enable
```

12.10 認証バイパスの構成例と設定例

認証バイパスの構成例と設定例を示します。

12.10.1 DHCP/DNS の認証バイパスの設定例

未認証クライアントからの DHCP パケットと DNS パケットを認証バイパスする場合の構成例と設定例を示します。なお、本設定例では VLAN や IP、AccessDefender 関連の設定は省略します。

- 拡張 IP アクセスリスト「Example-IPv4-EX-ACL」
- 宛先 UDP ポート番号［67］を認証バイパス
- 宛先 TCP/UDP ポート番号［53］を認証バイパス
- 認証バイパスを適用するポートは、ポート 1/0/1 からポート 1/0/5

1. 認証バイパス設定のために、拡張 IP アクセスリスト［Example-IPv4-EX-ACL］を作成し、以下のルールを設定します。

ルール 10（authentication-bypass）：宛先 UDP ポート番号［67］

ルール 20（authentication-bypass）：宛先 TCP ポート番号［53］

ルール 21（authentication-bypass）：宛先 UDP ポート番号［53］

```
sw1# configure terminal
sw1(config)# ip access-list extended Example-IPv4-EX-ACL
sw1(config-ip-ext-acl)# 10 permit authentication-bypass udp any any eq 67
sw1(config-ip-ext-acl)# 20 permit authentication-bypass tcp any any eq 53
sw1(config-ip-ext-acl)# 21 permit authentication-bypass udp any any eq 53
sw1(config-ip-ext-acl)# exit
sw1(config)#
```

2. 設定したアクセスリストを認証ポート（ポート 1/0/1 からポート 1/0/5）に適用します。

```
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# ip access-group Example-IPv4-EX-ACL in

The remaining applicable IP related access entries are 253
sw1(config-if-port-range)# end
sw1#
```

3. 実施後のアクセスリスト関連の設定を以下に抜粋します。

```
# ACL

ip access-list extended Example-IPv4-EX-ACL 3999
 10 permit authentication-bypass udp any any eq bootps
 20 permit authentication-bypass tcp any any eq domain
 21 permit authentication-bypass udp any any eq domain
interface port 1/0/1
 ip access-group Example-IPv4-EX-ACL in
interface port 1/0/2
 ip access-group Example-IPv4-EX-ACL in
interface port 1/0/3
 ip access-group Example-IPv4-EX-ACL in
interface port 1/0/4
 ip access-group Example-IPv4-EX-ACL in
interface port 1/0/5
 ip access-group Example-IPv4-EX-ACL in
```

12.10.2 VLAN の認証バイパスの設定例

特定の VLAN からの通信を認証バイパスする場合の構成例と設定例を示します。この例では、IP パケット対象化機能を有効にした拡張 MAC アクセスリストを使用しています。なお、本設定例では VLAN や IP、AccessDefender 関連の設定は省略します。

> ***NOTE:*** 拡張 MAC アクセスリストの IP パケット対象化機能は、NP7000 の 1.07.01 以降、NP5000 の 1.07.01 以降、NP4000 の 1.03.01 以降、NP2100 の 1.09.02 以降、NP2000 の 1.09.01 以降、NP2500 の 1.10.01 以降でサポートしています。
>
> ***NOTE:*** MAC 認証と関係なく CPU 宛てにコピーされるパケットは、認証バイパスにマッチしても CPU コピーされることに注意してください。

- IP パケット対象化機能を有効にした拡張 MAC アクセスリスト「Example-MAC-ACL」
- VLAN 50、VLAN 60 からの通信を認証バイパス
- 認証バイパスを適用するポートは、ポート 1/0/1 からポート 1/0/5

1. 拡張 MAC アクセスリストの IP パケット対象化機能を有効に設定します。

```
sw1# configure terminal
sw1(config)# mac access-list enable ip-packets
sw1(config)#
```

2. 認証バイパス設定のために、拡張 MAC アクセスリスト「Example-MAC-ACL」を作成し、以下のルールを設定します。

ルール 10（authentication-bypass）：VLAN［50］

ルール 20（authentication-bypass）：VLAN［60］

```
sw1(config)# mac access-list extended Example-MAC-ACL
sw1(config-mac-ext-acl)# 10 permit authentication-bypass any any vlan 50
sw1(config-mac-ext-acl)# 20 permit authentication-bypass any any vlan 60
sw1(config-mac-ext-acl)# exit
sw1(config)#
```

3. 設定したアクセスリストを認証ポート（ポート 1/0/1 からポート 1/0/5）に適用します。

```
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# mac access-group Example-MAC-ACL in

The remaining applicable MAC access entries are 1790
sw1(config-if-port-range)# end
sw1#
```

4. 実施後のアクセスリスト関連の設定を以下に抜粋します。

```
# ACL
mac access-list enable ip-packets
mac access-list extended Example-MAC-ACL 7999
 10 permit authentication-bypass any any vlan 50
 20 permit authentication-bypass any any vlan 60
interface port 1/0/1
 mac access-group Example-MAC-ACL in
interface port 1/0/2
 mac access-group Example-MAC-ACL in
interface port 1/0/3
 mac access-group Example-MAC-ACL in
interface port 1/0/4
 mac access-group Example-MAC-ACL in
interface port 1/0/5
 mac access-group Example-MAC-ACL in
```

12.11 ユーザーポリシーコントロールの構成例と設定例

ユーザーポリシーコントロールの構成例と設定例を示します。

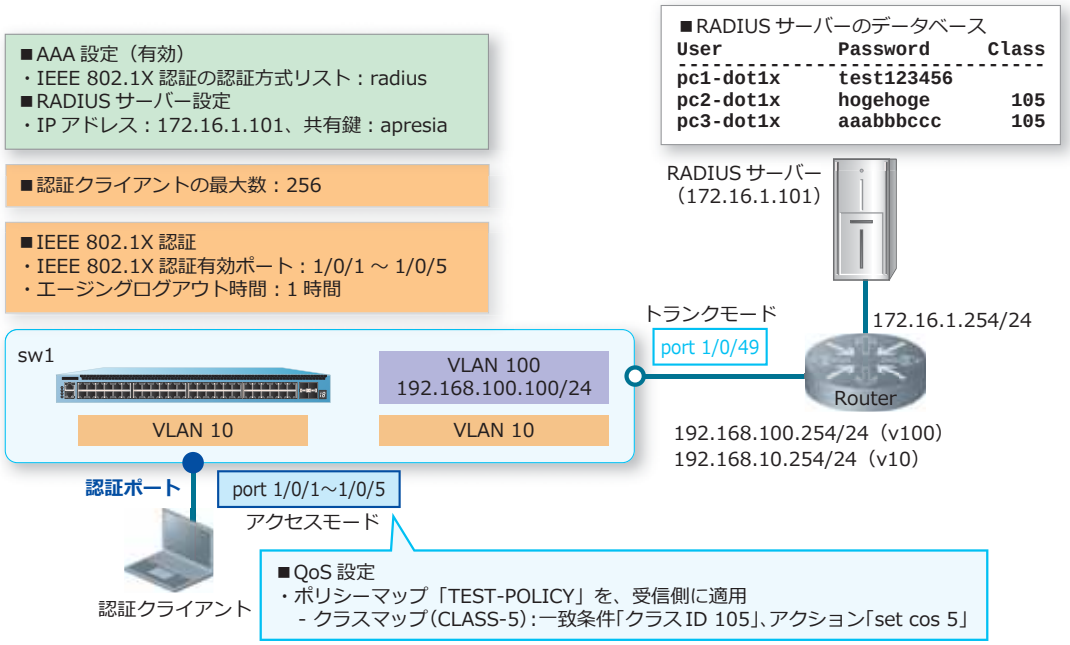
12.11.1 特定のユーザーグループだけ認証後に優先度を上げる場合

特定のユーザーグループだけ認証後に優先度を上げる場合の構成例と設定例を示します。この例では、クラス ID 105 に分類されたトラフィックの優先度を CoS 5 に変更しています。なお、この例では対象を IPv4 パケットと想定して拡張エキスパートアクセスリストを使用します。

表 12-25 特定のユーザーグループだけ認証後に優先度を上げる場合の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
IEEE 802.1X 認証有効ポート	ポート 1/0/1 からポート 1/0/5
IEEE 802.1X 認証のエージングログアウト時間	1 時間

図 12-22 特定のユーザーグループだけ認証後に優先度を上げる場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決しています。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、IEEE 802.1X 認証で使用する認証方式リストを、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication dot1x default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で IEEE 802.1X 認証を有効にします。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 dot1x
sw1(config-a-def)# logout aging-time 0 0 1 dot1x
sw1(config-a-def)# exit
sw1(config)#
```

7. IEEE 802.1X 認証を有効にします。

```
sw1(config)# dot1x enable
sw1(config)#
```

8. クラスマップ「CLASS-5」で使用する拡張エキスパートアクセスリスト［QOS-EX］を作成し、以下のルールを設定します。

ルール 10（許可）：クラス ID［105］

```
sw1(config)# expert access-list extended QOS-EX
sw1(config-exp-nacl)# 10 permit any any any any class 105
sw1(config-exp-nacl)# exit
sw1(config)#
```

9. クラスマップ［CLASS-5］を作成し、一致条件を［拡張エキスパートアクセスリスト：QOS-EX］に設定します。

```
sw1(config)# class-map CLASS-5
sw1(config-cmap)# match access-group name QOS-EX
sw1(config-cmap)# exit
sw1(config)#
```

10. ポリシーマップ［TEST-POLICY］を作成します。クラスマップ［CLASS-5］を関連付け、［CLASS-5］に分類されたトラフィックに対して CoS 値を 5 に変更するアクションを適用します。

```
sw1(config)# policy-map TEST-POLICY
sw1(config-pmap)# class CLASS-5
sw1(config-pmap-c)# set cos 5
sw1(config-pmap-c)# exit
sw1(config-pmap)# exit
sw1(config)#
```

11. 設定したポリシーマップを認証ポート（ポート 1/0/1 からポート 1/0/5）に適用します。

```
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# service-policy input TEST-POLICY
sw1(config-if-port-range)# end
sw1#
```

12. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication dot1x default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 dot1x

# DOT1X

access-defender
 authentication interface port 1/0/1-1/0/5 dot1x
dot1x enable
```

13. 実施後のポリシーマップ関連の設定を以下に抜粋します。

```
# ACL

expert access-list extended QOS-EX 9999
 10 permit any any any any class 105

# QOSPOLICY

class-map match-any CLASS-5
 match access-group name QOS-EX
policy-map TEST-POLICY
 class CLASS-5
 set cos 5
interface port 1/0/1
 service-policy input TEST-POLICY
interface port 1/0/2
 service-policy input TEST-POLICY
interface port 1/0/3
 service-policy input TEST-POLICY
interface port 1/0/4
 service-policy input TEST-POLICY
interface port 1/0/5
 service-policy input TEST-POLICY
```

12.11.2 スタティック認証クライアントを複数ポートで通信可能にする場合

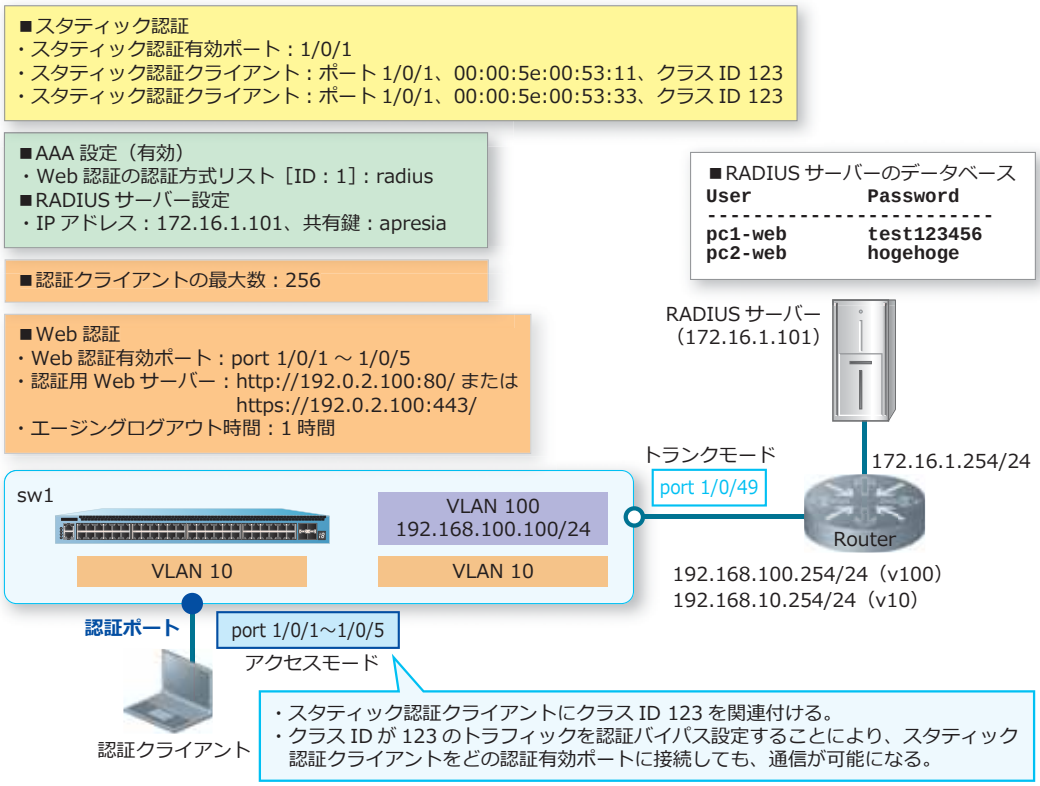
通常は、スタティック認証クライアントは接続インターフェースを指定して設定しますが、スタティック認証クライアントに関連付けたクラス ID を認証バイパスすることにより、スタティック認証クライアントを複数ポートで通信可能にする場合の構成例と設定例を示します。なお、この例では対象を IPv4 パケットと想定して拡張エキスパートアクセスリストを使用します。

> ***CAUTION:*** NP7000、NP5000、および NP3000 では、IP アクセスリストでクラス ID を使用できません。NP4000、NP2100、NP2000、および NP2500 では、IP アクセスリストでクラス ID を使用できます。

表 12-26 スタティック認証クライアントを複数ポートで通信可能にする場合の設定例

項目	設定
RADIUS 認証	デフォルトの RADIUS サーバーグループ「radius」で使用
RADIUS サーバー	• IP アドレス：172.16.1.101 • 共有鍵：apresia
認証クライアントの最大数	256
Web 認証有効ポート	ポート 1/0/1 からポート 1/0/5
認証用 Web サーバー	http://192.0.2.100:80/、または https://192.0.2.100:443/ ※HTTP プロトコル（80）と HTTPS プロトコル（443）はデフォルト有効
Web 認証のエージングログアウト時間	1 時間
スタティック認証有効ポート	ポート 1/0/1
スタティック認証端末	• ポート 1/0/1、00:00:5e:00:53:11、クラス ID 123 • ポート 1/0/1、00:00:5e:00:53:33、クラス ID 123

図 12-23 スタティック認証クライアントを複数ポートで通信可能にする場合の構成例



1. VLAN 10、VLAN 100 を作成し、構成例のように VLAN を割り当てます。

```
sw1# configure terminal
sw1(config)# vlan 10,100
sw1(config-vlan)# exit
sw1(config)#
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# switchport mode access
sw1(config-if-port-range)# switchport access vlan 10
sw1(config-if-port-range)# exit
sw1(config)#
sw1(config)# interface port 1/0/49
sw1(config-if-port)# switchport mode trunk
sw1(config-if-port)# switchport trunk allowed vlan 10,100
sw1(config-if-port)# exit
sw1(config)#
```

2. VLAN 100 インターフェースに管理用 IP アドレス［192.168.100.100/24］を設定します。また、本設定例ではデフォルトスタティックルートを［192.168.100.254］宛てに設定して、経路を解決するとします。

```
sw1(config)# interface vlan 100
sw1(config-if-vlan)# ip address 192.168.100.100/24
sw1(config-if-vlan)# exit
sw1(config)# ip route 0.0.0.0/0 192.168.100.254
sw1(config)#
```

3. 装置の AAA を有効化します。また、Web 認証で使用する認証方式リスト［ID：1］を、デフォルトの RADIUS サーバーグループ「radius」に指定します。

```
sw1(config)# aaa new-model
sw1(config)# aaa authentication web-auth 1 default group radius
sw1(config)#
```

4. RADIUS サーバーを、IP アドレス［172.16.1.101］、共有鍵［apresia］で設定します。設定した RADIUS サーバーは、所属する RADIUS グループを指定しない場合はデフォルトの RADIUS サーバーグループ「radius」に所属します。

```
sw1(config)# radius-server host 172.16.1.101 key apresia
sw1(config)#
```

5. AccessDefender 設定モードに遷移し、認証クライアントの最大数を［256］に設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# total-client 256
sw1(config-a-def)#
```

6. ポート 1/0/1 からポート 1/0/5 で Web 認証を有効に、認証用 Web サーバーの IP アドレスを［192.0.2.100］に設定します。装置の認証用 Web サーバーでは、HTTP プロトコル（TCP ポート番号 80）と HTTPS プロトコル（TCP ポート番号 443）はデフォルト有効になっています。また、エージングログアウト時間を［1 時間］に設定します。

```
sw1(config-a-def)# authentication interface port 1/0/1-5 web
sw1(config-a-def)# web-authentication http-ip ipv4 192.0.2.100
sw1(config-a-def)# logout aging-time 0 0 1 web
sw1(config-a-def)# exit
sw1(config)#
```

7. Web 認証を有効にします。

```
sw1(config)# web-authentication enable
sw1(config)#
```

8. ポート 1/0/1 でスタティック認証を有効に設定し、スタティックエントリー［ポート 1/0/1、00:00:5e:00:53:11、クラス ID 123］［ポート 1/0/1、00:00:5e:00:53:33、クラス ID 123］を設定します。

```
sw1(config)# access-defender
sw1(config-a-def)# authentication interface port 1/0/1 static
sw1(config-a-def)# exit
sw1(config)# access-defender static mac 0000.5e00.5311 class 123 interface port
1/0/1
sw1(config)# access-defender static mac 0000.5e00.5333 class 123 interface port
1/0/1
sw1(config)#
```

9. 認証バイパス設定のために、拡張エキスパートアクセスリスト［EXPERT-ACL］を作成し、以下のルールを設定します。

ルール 10（authentication-bypass）：クラス ID［123］

```
sw1(config)# expert access-list extended EXPERT-ACL
sw1(config-exp-nacl)# 10 permit authentication-bypass any any any any class 123
sw1(config-exp-nacl)# exit
sw1(config)#
```

10. 設定したアクセスリストを認証ポート（ポート 1/0/1 からポート 1/0/5）に適用します。

```
sw1(config)# interface range port 1/0/1-5
sw1(config-if-port-range)# expert access-group EXPERT-ACL in
sw1(config-if-port-range)# end
sw1#
```

11. 実施後の AccessDefender 関連の設定を以下に抜粋します。

```
# AAA

aaa new-model
radius-server host 172.16.1.101 key apresia
aaa authentication web-auth 1 default group radius

# ACCESS-DEFENDER

access-defender
 total-client 256
 logout aging-time 0 0 1 web
 authentication interface port 1/0/1 static
access-defender static mac 00-00-5E-00-53-11 class 123 interface port 1/0/1
access-defender static mac 00-00-5E-00-53-33 class 123 interface port 1/0/1

# WEB-AUTHENTICATION

access-defender
 authentication interface port 1/0/1-1/0/5 web
 web-authentication http-ip ipv4 192.0.2.100
web-authentication enable
```

12. 実施後のアクセスリスト関連の設定を以下に抜粋します。

```
# ACL

expert access-list extended EXPERT-ACL 9999
 10 permit authentication-bypass any any any any class 123
interface port 1/0/1
 expert access-group EXPERT-ACL in
interface port 1/0/2
 expert access-group EXPERT-ACL in
interface port 1/0/3
 expert access-group EXPERT-ACL in
interface port 1/0/4
 expert access-group EXPERT-ACL in
interface port 1/0/5
 expert access-group EXPERT-ACL in
```