10

セキュリティ

この章では、ポート、ユーザ、およびサーバに対するセキュリティ機能について説明します。

具体的な内容は、次のとおりです。

- 「RADIUS」
- 「パスワード強度」
- 「管理アクセス プロファイル ルール」
- 「認証方式」
- 「ストーム制御」
- 「ポート セキュリティ」
- 「802.1X」

RADIUS

スイッチは、Remote Authorization Dial-In User Service（RADIUS）クライアント機能をサポートします。RADIUS は、アクセス前にユーザを認証するため、広範囲にアクセス可能なネットワークの管理者によって選択されるプロトコルです。安全な方法でユーザを認証するために、RADIUS クライアントと RADIUS サーバは、同じ共有パスワードまたはシークレットで設定されます。このシークレットは、すべての RADIUS パケットに存在する 1 方向の暗号化認証を生成するために使用されます。シークレットが知られていなければ、悪意のあるユーザによってパケットをスプーフィングされる可能性が大幅に低くなります。

スイッチ上の RADIUS クライアントは、スイッチ管理アクセス認証と IEEE 802.1X（dot1X）ポート アクセス コントロールで使用されます（「管理アクセス プロファイル ルール」および「802.1X」を参照）。

[RADIUS] ページを使用して、グローバル RADIUS を設定し、RADIUS サーバを追加できます。

グローバル RADIUS の設定

グローバル設定を行うには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [RADIUS] の順にクリックします。

ステップ 2 パラメータを入力します。

- [リトライ回数] : RADIUS クライアントが要求を RADIUS サーバに再送信する最大回数。範囲は 1 ～ 10 です。デフォルトは 3 です。
- [応答タイムアウト] : スイッチが、別の要求を送信する前に、RADIUS サーバがサーバ要求に応答するのを待機する秒数。範囲は 1 ～ 30 です。デフォルトは 3 です。
- [デッドタイム] : スイッチが、RADIUS サーバを利用不可能と判別してから、その RADIUS サーバがバイパスされる時間。利用不可能なスイッチをバイパスすることで、スイッチの応答時間が向上します。範囲は 0 ～ 2000 です。デフォルトは 0 です。
- [RADIUS 属性 4(NAS-IP アドレス)] : 選択すると、スイッチは Access Request RADIUS サーバ パケットに Network Access Server（NAS; ネットワーク アクセス サーバ）属性を含むことができます。このオプションが無効な場合、RADIUS クライアントはスイッチ管理ポート アドレスを NAS-IP アドレスとして使用します。
- [NAS-IP アドレス] : Access Request パケットに含める IP アドレス。このフィールドは、RADIUS 属性 4 が有効な場合のみ、編集可能です。アドレスは、RADIUS サーバのスコープ内の NAS で一意である必要があります。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

RADIUS サーバの追加

複数の RADIUS サーバを設定でき、それらがアクセスされる順序を決定するプライオリティ レベルを設定できます。

注意 すべての管理ユーザは、読み取りおよび書き込み権限付きで作成されます。設定したすべての RADIUS サーバのユーザには同じ特権レベルがあることを確認してください。そうでない場合は、スイッチへのアクセスが認められません。

RADIUS サーバを [RADIUS テーブル] に追加するには、次の手順に従います。

ステップ 1 [追加] をクリックします

ステップ 2 パラメータを入力します。

- [RADIUS サーバ] : サーバの IP アドレスまたはホスト名。
- [プライオリティ] : プライオリティ数値が低いほど、サーバの実際のプライオリティは高くなります。たとえば、プライオリティ値 1 のサーバには、プライオリティ値 2 で設定されたサーバより高いプライオリティがあります。すべてのサーバが、同一またはデフォルトのプライオリティ値で設定されている場合、スイッチは、早いものから順に RADIUS サーバを処理します。範囲は 1 ～ 65535 です。デフォルトは 8 です。
- [キーストリング] : スイッチと RADIUS サーバの間のすべての RADIUS 通信の認証と暗号化に使用される共有シークレット テキスト文字列。このシークレットは、RADIUS サーバ側で設定されているシークレットと一致していなければなりません。シークレット キーは、エントリを削除し、対象のシークレット キーでエントリを再作成することで、編集できます。これは、32 ～ 176 文字の ASCII 英数文字である必要があります。
- [認証ポート] : RADIUS 認証要求および応答で使用されるポート番号。デフォルトポートである 1812 は、RADIUS 認証サーバ用の既知の IANA ポート番号です。範囲は 1025 ～ 65535 です。デフォルトは 1812 です。
- [メッセージオーセンティケータ] : このフィールドは、デフォルトで選択されます。有効な場合、メッセージ オーセンティケータ属性が、サーバへの RADIUS 要求メッセージに含まれます。この属性は、スプーフィングと不正改ざんから RADIUS メッセージを保護します。共有シークレットは、キーとして使用されます。RADIUS Message Authenticator 属性がパケットに存在する場合、サーバによって検証されます。検証に失敗した場合、サーバは要求パケットをドロップします。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

パスワード強度

[パスワード強度] ページを使用して、セキュアな管理ユーザ パスワードの属性を設定できます。

パスワード強度を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [パスワード強度] の順にクリックします。

ステップ 2 次のパラメータを入力します。

- [パスワードの長さ (最短)] : 管理ユーザ パスワードに必要な最小文字数。0 を指定して、パスワードの長さを 1 ～ 7 文字に設定するか、または、8 ～ 64 文字の値で特定のパスワード長を設定します。
- [パスワードエージングタイム] : チェックボックスをオンにして、パスワードの期限切れ後の期間を 1 ～ 365 日の間で入力します。パスワードの有効期限が切れた場合、ユーザは、続行する前に新しいパスワードを入力する必要があります。

ステップ 3 [強度チェック] フィールドで [有効] を選択して、実行するチェックのタイプを設定します。

- [パスワードの除外キーワードチェック] : [有効] を選択すると、ユーザがパスワードを作成または変更するときに、事前設定されたキーワードがパスワードで使用されているかどうかを、スイッチがチェックできるようになります。事前定義されたキーワードは、cisco と ocsic です。
- [パスワードのユーザ名チェック] : [有効] を選択すると、ユーザがパスワードを作成または変更するときに、パスワードにユーザ名を含めないようにできます。
- [文字は3回まで繰り返し可能] : [有効] を選択すると、パスワードで使用されている文字が、4 回以上連続して繰り返されているかどうか、スイッチがチェックできるようになります。
- [文字クラスの最小数] : チェックボックスをオンにして、パスワード文字列に含まなければならない文字クラスの最小数を入力します。文字クラスには、大文字、小文字、数字、および標準キーボードで利用可能な特殊文字の 4 つがあります。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

管理アクセス プロファイル ルール

[管理アクセスプロファイルルール] ページを使用して、管理目的でデバイスにアクセスするためのプロファイルとルールを定義できます。

特定のユーザ名、入力ポートまたは LAG、および送信元 IP アドレスへのアクセスを制限できます。

このページを表示するには、ナビゲーション ウィンドウで、[セキュリティ] > [管理アクセスプロファイルルール] の順にクリックします。

[アクセスプロファイルテーブル] には、現在設定されているプロファイル（存在する場合）のプロファイル名が表示されます。[プロファイルルールテーブル] には、プロファイルに対する既存のルールが表示されます。デフォルトでは、スイッチで設定されるアクセス プロファイルやルールはありません。1 つのプロファイルのみ作成および有効化でき、そのプロファイルに、作成するすべてのルールが割り当てられます。

アクセス プロファイルとルールの設定

アクセス プロファイルを作成し、ルールを割り当てるには、次の手順に従います。

ステップ 1 [アクセスプロファイルテーブル] で、[追加] をクリックします。

ステップ 2 アクセス プロファイル名を指定し、[有効] を選択します。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。

新しいプロファイルが [アクセスプロファイルテーブル] に表示されます。ここで、ルールをプロファイルに追加できます。

ステップ 4 [プロファイルルールテーブル] で、[追加] をクリックします。

ステップ 5 次のパラメータのいくつかを指定し、アクセスを制限または許可します。

- [ルールプライオリティ]：ルールは、着信管理要求に対して、プライオリティの昇順で検証されます。ルールが一致する場合、指定されたアクションが実行され、それ以降のルールは無視されます。たとえば、プライオリティ 1 の送信元 IP 10.10.10.10 を [許可] に設定し、プライオリティ 2 の送信元 IP 10.10.10.10 を [拒否] に設定した場合、プロファイルがアクティブであれば、この IP アドレスに対してアクセスが許可され、2 番目のルールは無視されます。範囲は 1 ～ 16 です。1 は最も高いプライオリティを示します。

- [管理方式]：スイッチ設定へのアクセスに使用する方式。デフォルトでは、すべてのユーザが Web ベースのスイッチ設定ユーティリティを使用できるように、HTTP アクセスが許可されます。指定したユーザのみを許可するには、たとえば、すべてのユーザに対して HTTP アクセスが拒否されるルールを作成してから、特定のユーザが許可される別のルールを作成します。特定のユーザを許可するルールには、すべてのユーザを拒否するルールより高い [ルールプライオリティ] が必要です。

  （注）：HTTP は唯一の管理アクセス方式であるため、[HTTP] オプションと [すべて] オプションは同じです。

- [アクション]：ルールの基準が一致した場合に実行されるアクションを選択します。
  - [許可]：指定したインターフェイス、ユーザ、または IP アドレスは、拒否ルールで明示的に禁止されているスイッチへのアクセスを許可されます。
  - [拒否]：指定したインターフェイス、ユーザ、または IP アドレスは、スイッチへのアクセスを拒否されます。
- [インターフェイスに適用]：[すべて] を選択して、このルールをすべてのインターフェイス（ポートおよび LAG）に適用します。または、[ユーザ定義] を選択して、ルールを適用するポートまたは LAG を選択します。
- [ユーザに適用]: このルールをすべてのシステム ユーザに適用する場合は [すべて] を選択します。または、[ユーザ定義] を選択して、ルールを適用するユーザを [ユーザ名] から選択します。
- [送信元 IP アドレスに適用]:[すべて] を選択して、あらゆる送信元 IP アドレスにルールを適用します。または、[ユーザ定義] を選択して、このルールを適用する送信元 IPv4 アドレスおよびマスクを指定します。

ステップ 6 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

新しいルールが [プロファイルルールテーブル] に表示されます。ルールを選択して、[編集] をクリックして編集したり、[削除] をクリックしてアクセス プロファイルからルールを削除したりできます。

（注） ユーザ cisco は、管理アクセスを拒否されません。

注意 現在 Web 管理セッションがアクティブなイントラネットまたはドメインへのアクセスを拒否するプロファイルがアクティブになった場合、セッションは、ログアウトまたはタイムアウトされるまでアクティブなままになります。それ以降のセッションは、プロファイルによってブロックされます。Internet Explorer 8 を使用するアクティブなセッションは、スイッチ管理 IP アドレスが Internet Explorer の [ローカル イントラネット サイト] リストに追加されていない場合、ただちに終了します。手順については、「Web ベースのスイッチ設定ユーティリティの開始」を参照してください。

アクセス プロファイルおよびルールの修正と削除

アクセス プロファイルを削除する、またはルールを修正する前に、プロファイルを無効にする必要があります。

アクセス プロファイルを無効にするには、次の手順に従います。

ステップ 1 [アクセスプロファイルテーブル] でプロファイルを選択して、[編集] をクリックします。

ステップ 2 [有効] チェックボックスをオフにします。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。

変更が完了したら、アクセス プロファイルを再び有効にします。

アクセス プロファイルを（無効にした後）削除するには、次の手順に従います。

ステップ 1 [アクセスプロファイルテーブル] で、プロファイルを選択します。

ステップ 2 [削除] をクリックします。

（アクセス プロファイルを無効にした後）プロファイル ルールを削除するには、次の手順に従います。

ステップ 1 [プロファイルルールテーブル] でルールを選択します。

ステップ 2 [削除] をクリックします。

（アクセス プロファイルを無効にした後）プロファイル ルールを修正するには、次の手順に従います。

ステップ 1 [プロファイルルールテーブル] でルールを選択して、[編集] をクリックします。

ステップ 2 新しい設定を入力します。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。

(すべての変更が完了した後) アクセス プロファイルを有効にするには、次の手順に従います。

ステップ 1 [アクセスプロファイルテーブル] でプロファイルを選択して、[編集] をクリックします。

ステップ 2 [有効] チェックボックスをオンにします。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。

認証方式

[認証方式] ページを使用して、ユーザがスイッチ ポートへのアクセスをどのように許可されるかを指定できます。

認証方式を選択するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [認証方式] の順にクリックします。

ステップ 2 [HTTP] リストで認証方法を選択します。

- [ローカル] : サプリカントからのユーザ ID とパスワードの組み合わせは、スイッチでローカルに保存されたユーザ データベースと比較されます。
- [なし] : ユーザ認証方式は使用されません。
- [RADIUS] : スイッチが認証要求を RADIUS サーバに渡し、RADIUS サーバが RADIUS の Access-Accept または Access-Reject フレームで応答します。
- [RADIUS、なし] : スイッチが認証要求を RADIUS サーバに渡します。サーバにアクセスできない場合、認証は使用されません。
- [RADIUS、ローカル] : スイッチが認証要求を RADIUS サーバに渡します。サーバにアクセスできない場合、ローカル ユーザ データベースが使用されます。

ステップ 3 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ストーム制御

トラフィック ストームは、過剰な数のブロードキャスト、マルチキャスト、または不明なユニキャスト メッセージが、単一ポートによってネットワーク全体で同時に送信された結果、発生します。転送されたメッセージ応答がネットワークのリソースに過負荷を与え、ネットワークをタイムアウトさせる可能性があります。

スイッチは、ポートあたりの着信ブロードキャスト/マルチキャスト/不明なユニキャストのパケット レートを測定し、レートが定義された値を超過した場合はパケットを破棄します。ストーム制御は、インターフェイスごとに有効または無効にできます。

[ストーム制御] ページを使用して、スイッチのインターフェイスでストーム制御を有効にし、設定できます。このページを表示するには、ナビゲーション ウィンドウで、[セキュリティ] > [ストーム制御] の順にクリックします。

ストーム制御は、デフォルトではすべてのパケット タイプに対してすべてのポートで無効です。ポートのストーム制御設定を編集するには、次の手順に従います。

ステップ 1 設定するポートを選択して、[編集] をクリックします。

ステップ 2 ブロードキャスト、マルチキャスト、およびユニキャストの各トラフィックに対して、選択したポートに次のパラメータを指定します。

- [モード]: [有効] を選択すると、そのトラフィック タイプに対してストーム制御保護が有効になります。
- [レートしきい値タイプ]: トラフィックがしきい値を超えたかどうかを、スイッチがどのように判別するかを選択します。
  - [パーセント]: リンクで容量の割合を超えた場合、トラフィックはドロップされます。
  - [pps]: 1 秒あたりのパケット。リンクで 1 秒あたりのパケットのしきい値を超過した場合、トラフィックはドロップされます。
- [レートしきい値]: パケットが転送される最大レートを指定します。[レートしきい値タイプ] が [パーセント] の場合は、全体のポート容量の割合を入力します（0% ～ 100%）。[レートしきい値タイプ] が [pps] の場合は、1 秒あたりのパケットのレートを入力します（0 ～ 14880000）。10Mpbs、100Mbps、および 1000Mbps で動作するポートの最大スループットは、それぞれ、1 秒あたり 14880、148800、1488000 パケットです。

（注）：ストーム制御をアクティブにするのに必要な入力トラフィックの実際のレートは、着信パケットのサイズと、ハードコーディングされた平均パケット サイズ（512 バイト）に基づきます。ハードウェアでは kbps での絶対レートに対する pps 値が必要とされるため、1 秒あたりのパケット レートが計算されます。たとえば、設定された制限が 10 パーセントの場合、これは約 25000 pps（100 M ポートに対して）に変換されます。

ステップ 3 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ポート セキュリティ

ポート単位でポートのセキュリティを有効にできます。ポートがセキュリティ保護されている（ロックされている）場合、スイッチは、送信元 MAC アドレスがポートでセキュリティ保護されているパケットのみを転送します。他のすべてのパケットは破棄されます。スイッチは、送信元 MAC アドレスが別のポートでセキュリティ保護されているポートからのパケットも破棄します。

セキュアな MAC アドレスは、静的に設定したり、動的に学習したりできます。セキュリティ保護されているポートでのセキュアな MAC アドレスの最大数は、256 です。スタティック セキュア MAC アドレスは、[スタティックアドレス] ページを使用して設定します。スタティック セキュア MAC アドレスおよびダイナミック セキュア MAC アドレスの両方にエージング制限があります（「ダイナミック アドレスのエージング タイムの設定」を参照）。

[ポートセキュリティ] ページを表示するには、ナビゲーション ウィンドウで、[セキュリティ] > [ポートセキュリティ] の順にクリックします。

[ポートセキュリティテーブル] には、各ポートの現在のセキュリティ設定が表示されます。LAG のデータのみを表示するには、[インターフェイスタイプ] リストから LAG を選択します。デフォルトでは、ポートのセキュリティは、グローバルおよび各インターフェイスで無効です。

ポート セキュリティの有効化

ポート セキュリティを設定するには、次の手順に従います。

ステップ 1 [ポートセキュリティ] ページで、[管理モード] で [有効] を選択して、[適用] をクリックします。

ステップ 2 ポートまたは LAG を選択し、[編集] をクリックします。

ステップ 3 次の設定を行います。

- [インターフェイスステータス]:[ロック] を選択すると、インターフェイスでポートセキュリティが有効になります。インターフェイスがロック解除状態からロック状態に移行した場合、そのポートのスイッチで動的に学習されたすべてのアドレスは、MAC アドレス リストから削除されます。
- [スタティック MAC アドレスの最大数]:ポートまたは LAG でのスタティック セキュア MAC アドレスの最大数を指定します。スタティック セキュア MAC アドレスは、[スタティックアドレス] ページで設定されます。セキュアなアドレスの合計数は、256 を超えることはできません。
- [ダイナミック MAC アドレスの最大数]:ポートまたは LAG から学習可能な、ダイナミック セキュア MAC アドレスの最大数を指定します。セキュアなアドレスの合計数は、256 を超えることはできません。

  ポート セキュリティがポートで有効で、スタティックおよびダイナミックな制限が新しい値に設定された場合、次のルールが適用されます。

  - 新しい値が、前の値より大きい場合は、ダイナミック アドレスまたはスタティック アドレスのどちらに対してもアクションは実行されません。
  - 新しい値が、前の値より小さい場合は、次のアクションが実行されます。

    ダイナミック アドレス:スイッチは、ポートで学習されたすべてのアドレスのフラッシュを開始します。

    スタティック アドレス:アドレスがセキュア、永続的、またはタイムアウトでの削除のいずれで設定されたかにかかわらず、スイッチは、スタティック アドレスを保持します（スタティック制限まで）。その後、MAC アドレス テーブルから残りのスタティック アドレスを削除します。

- [違反時アクション]：ロックされたポートで許可されていない着信パケットをスイッチが処理する方法を選択します。
  - [廃棄]：パケットはドロップされます。
  - [転送]：パケットは転送されますが、送信元 MAC アドレスは転送データベースに追加されません。
  - [シャットダウン]：パケットは廃棄され、ポートはシャットダウンされます。
- [ダイナミックアドレスをスタティックに変換]：[有効] を選択すると、すべてのダイナミック セキュア MAC アドレスがスタティック セキュア MAC アドレスに変換されます。
- [ポートのリセット]：選択すると、ポート セキュリティ機能によってポートがシャットダウンされた場合に、ポートがリセットされます。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

セキュア MAC アドレスの表示と設定

セキュア MAC アドレスの現在のリストと、関連付けられたポートおよび VLAN を表示するには、[ポートセキュリティ] ページで [セキュアアドレステーブル] をクリックします。

インターフェイスごとに、ポートのステータスがロックかロック解除かにかかわらず、[セキュアアドレステーブル] には、スタティックにセキュリティ保護された設定済みの各 MAC アドレスが表示されます。このテーブルには、ロックされたポートに対してダイナミックに学習された MAC アドレスも表示されます。ポートがロックからロック解除に変更された場合、またはリンクがダウンした場合、ポートのダイナミック エントリは、クリアされます。

[スタティックアドレステーブル] をクリックして、スタティック アドレスを設定するページを表示できます。「スタティック MAC アドレスの設定」を参照してください。エントリの [ステータス] フィールドは [セキュア] に設定するようにしてください。

[ポートセキュリティテーブル] をクリックして、[ポートセキュリティ] ページを再表示できます。

802.1X

Local Area Network（LAN; ローカルエリア ネットワーク）は、未承認デバイスが LAN インフラストラクチャに物理的に接続されることを許可する環境、または未承認ユーザがすでに接続された機器を経由して LAN にアクセスしようとすることを許可する環境で導入されている場合があります。そのような環境では、LAN で提供されるサービスへのアクセスを、それらのサービスの使用を許可されているユーザやデバイスに制限することが望ましい場合があります。

ポート ベースのアクセス制御では、接続されたポートで提供されるサービスにホストがアクセスできるかどうかをネットワークがコントロールすることができます。IEEE 802.1x プロトコルをベースにした、ポートベースのネットワーク アクセス制御を使用するようにスイッチを設定できます。

802.1x プロトコルでは、次の 3 種類のエンティティを定義します。

- サプリカント：リンクのリモート エンドでポートへのアクセスを要求するエンティティ。サプリカントは、ネットワーク上の別のノード、つまりオーセンティケータが、サーバからの認証を要求するために使用するネットワークに資格情報を提供します。
- オーセンティケータ：リンクのリモート エンドでサプリカントの認証を容易にするエンティティ。オーセンティケータは、認証が成功した場合、サプリカントにポートアクセスを許可します。
- 認証サーバ：オーセンティケータに代わって認証を実行するサーバ（RADIUS サーバなど）。サプリカントが認証中のポート経由で提供されるサービスへのアクセスを承認されているかどうかを示します。

認証プロセスでは、802.1X　は、サプリカントとオーセンティケータ間の　Extensible Authentication Protocol Over LAN（EAPOL）メッセージをサポートします。

スイッチ ポートは、オーセンティケータ、サプリカントのどちらにも設定できますが、両方には設定できません。

802.1X プロパティ値の設定

802.1X の [プロパティ] ページを使用して、グローバルな 802.1X 管理モードをスイッチで設定できます。

802.1X セキュリティをグローバルに有効にするには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [プロパティ] の順にクリックします。

ステップ 2 [ポートベース認証の状態] で [有効] を選択し、802.1X ポートベースの認証をスイッチでグローバルに許可します。

ステップ 3 [認証方式] リストから認証方式を選択します。

- [なし] : ユーザ認証方式は使用されません。
- [ローカル] : スイッチは、EAP-MD5 をベースにしたリモート サプリカントのローカル認証を実行します。サプリカント識別情報は、スイッチに設定された管理ユーザのいずれかである必要があります（「ユーザ アカウントの管理」を参照）。
- [RADIUS] : スイッチは、1 つまたは複数の外部 RADIUS サーバに依存して認証を実行します。サプリカントの ID と認証を、直接サーバに設定する必要があります （詳しくは、「RADIUS」を参照）。
- [RADIUS、なし] : スイッチは、1 つまたは複数の外部 RADIUS サーバに依存して認証を実行します （前述の [RADIUS] の説明を参照）。スイッチがどのサーバにもアクセスできない場合、どの認証も使用されません。
- [RADIUS、ローカル] : スイッチは、1 つまたは複数の外部 RADIUS サーバに依存して認証を実行します（前述の [RADIUS] の説明を参照）。スイッチがどのサーバにもアクセスできない場合、ローカルで認証を実行します（前述の [ローカル] の説明を参照）。

ステップ 4 [適用] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

（注） 個々のポートの役割を選択する手順については、「ポート PAE 機能の変更」を参照してください。また、個々のポートで認証を設定する手順については、「ポート認証の設定」を参照してください。

ポート PAE 機能の変更

[ポート PAE 機能] ページを使用して、各ポートの 802.1X 役割を表示したり、その役割をオーセンティケータまたはサプリカントとして設定したりできます。

オーセンティケータまたはサプリカントとしてポートの役割を変更するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [プロパティ] の順にクリックします。

ステップ 2 設定するポートを選択して、[編集] をクリックします。

ステップ 3 ポートの役割を選択します。

- [オーセンティケータ]：ローカル ポートへのアクセスを許可する前に、ポートがリモート サプリカントの認証を必要とする場合、このオプションを選択します。
- [サプリカント]：リモート ポートにアクセスする前に、ポートがリモート オーセンティケータから権限を求める必要がある場合、このオプションを選択します。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

ポート認証の設定

[ポート認証] ページを使用して、オーセンティケータとして動作するポートでのポート アクセス コントロールを設定できます。ポートをオーセンティケータとして有効にするには、「ポート PAE 機能の変更」を参照してください。

ポートのオーセンティケータ設定を編集するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [ポート認証] の順にクリックします。

[ポート認証テーブル] に、各ポートの現在の設定が表示されます。

ステップ 2 設定するポートを選択して、[編集] をクリックします。

ステップ 3 パラメータを入力します。

- [ローカルデータベースユーザ名]：右矢印および左矢印を使用して、設定された管理ユーザを [使用可能] または [選択済み] リストに移動します。[選択済み] リストのユーザのみがポートにアクセスでき、認証の対象になります。このリストは、認証がローカルの場合のみ適用され、RADIUS サーバが認証に使用される場合は適用されません。
- [現在のポート制御]：ポートの現在の認証ステータス（「許可」または「無許可」）。
- [管理ポート制御]：ポート認証モードを選択します。表示される値は次のとおりです。
  - [強制無許可]：ポートに接続されているサプリカントによるポート アクセスを常に拒否するには、このオプションを選択します。選択した場合、ポート制御ステータスは「無許可」になります。
  - [自動]：ポート制御が認証プロセスの結果に基づく場合は、このオプションを選択します。サプリカントが認証された場合、ポート制御ステータスは「許可」になり、サプリカントはポートへのアクセスを許可されます。サプリカントが認証されない場合、ポート制御ステータスが「無許可」になり、サプリカントはアクセスを拒否されます。
  - [強制許可]：リモート サプリカントの認証が必要ない場合に常にポート アクセスを許可するには、このオプションを選択します。選択した場合、ポート制御ステータスは「許可」になります。
- [定期再認証]：ポートがそのサプリカントを定期的に再認証する場合は、このオプションを選択します。認証された状態が維持される場合でも、ポートは、スケジュールされた間隔で再認証します。
- [再認証期間]：再認証試行の間隔。範囲は 300 ～ 4294967295 秒です。デフォルトは 3600 秒です。
- [即時再認証]：選択した場合、ただちにポートの再認証が強制的に実行されます。
- [認証状態]：現在のポート認証状態。示される状態には、初期化、接続解除、接続中、認証中、認証済み、打ち切り中、ホールド済み、強制認証、および強制非認証があります。
- [バックエンド状態]：バックエンドの認証ステート マシンの現在の状態。示される値には、要求、応答、成功、失敗、タイムアウト、アイドル、および初期化があります。

- [待機期間]：認証失敗情報交換後にスイッチが待機する時間。待機期間中、スイッチは認証要求の受け入れも開始も行いません。特定のクライアントと認証サーバに関する信頼できないリンクや特定の動作の問題など、一般的ではない事情に対応する場合にのみ、このコマンドのデフォルト値を変更してください。より迅速な応答時間をユーザに提供するには、デフォルト（60 秒）より小さい値を入力します。範囲は 0 ～ 65535 秒です。
- [EAP の再送信]：EAP 要求が再送信されるまでの時間。範囲は 1 ～ 65535 秒で、デフォルトは 30 秒です。
- [サプリカントタイムアウト]：EAP 要求がサプリカントに再送信されるまでの時間。特定のクライアントと認証サーバに関する信頼できないリンクや特定の動作の問題など、一般的ではない事情に対応する場合にのみ、このコマンドのデフォルト値（30 秒）を変更してください。より迅速な応答時間をユーザに提供するには、デフォルトより小さい値を入力します。範囲は、1 ～ 65535 秒です。
- [サーバタイムアウト]：スイッチが要求を認証サーバに再送信するまでの時間。範囲は 1 ～ 65535 秒で、デフォルトは 30 秒です。
- [最大 EAP 要求]：応答を受信しない場合、認証プロセスを再び開始する前に、スイッチが EAP 要求を送信できる、事前設定された最大回数。
- [終了原因]：終了の理由。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

サプリカント ポート認証の設定

[サプリカントポート認証] ページを使用して、サプリカント役割で設定されたポートでポート アクセス コントロールを設定できます。ポートをサプリカントとして有効にするには、「ポート PAE 機能の変更」を参照してください。

サプリカント ポート認証を設定するには、次の手順に従います。

ステップ 1 ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [サプリカントポート認証] の順にクリックします。

ステップ 2 設定するポートを選択して、[編集] をクリックします。

[現在のポート制御] フィールドに、ポートの現在の認証モードが表示されます。

ステップ 3 次の設定を行います。

- [管理ポート制御]：ポート認証モードを選択します。表示される値は次のとおりです。
  - [強制無許可]：インターフェイスを未承認状態に移行することにより、選択されたインターフェイスからのシステム アクセスを拒否します。
  - [自動]：サプリカント、オーセンティケータ、および認証サーバの間の認証交換の結果に基づいたインターフェイスのモードをスイッチが検出します。
  - [強制許可]：認証サーバでの認証を必要とせずに、ポートは承認済み状態になります。インターフェイスは、クライアントのポート ベースの認証なしに通常のトラフィックを送受信します。
- [ユーザ名]：サプリカントとして自身を特定するためにポートによって使用されるユーザを選択します。ユーザは、スイッチで設定されたスイッチ管理ユーザのいずれかである必要があります。ユーザに設定されたパスワードは、認証プロセスで使用されます。サプリカントとして、スイッチは EAP-MD5 認証方式をサポートします（ユーザの設定については、「ユーザ アカウントの管理」を参照）。

ステップ 4 [適用] をクリックしてから、[閉じる] をクリックします。変更内容が実行コンフィギュレーションに保存されます。

認証済みホストの表示

認証済みユーザが存在するポートを [認証済みホスト] ページで表示するには、ナビゲーション ウィンドウで、[セキュリティ] > [802.1X] > [認証済みホスト] の順にクリックします。

[認証済みホスト] に、各ホストの次の情報が表示されます。

- [ポート]：認証に使用されるポート。
- [ユーザ名]：ホストのユーザ名。
- [サプリカント MAC アドレス]：サプリカント デバイス MAC アドレス。
- [セッション時間]：サプリカントがログインしてからの時間（秒数）。
- [セッションタイムアウト]：指定のセッションが有効な時間。ポート認証で RADIUS サーバによって時間（秒数）が返されます。