



IEEE 802.1x ポートベースの認証の設定

この章では、IEEE 802.1x ポートベース認証を設定する方法について説明します。IEEE 802.1x 認証は、不正なデバイス（クライアント）によるネットワークアクセスを防止します。別途記載のないかぎり、スイッチという用語はスタンドアロンスイッチまたはスイッチスタックを意味します。

- [IEEE 802.1x ポートベース認証の制約事項 \(1 ページ\)](#)
- [IEEE 802.1x ポートベースの認証に関する情報 \(2 ページ\)](#)
- [802.1x ポートベース認証の設定方法 \(42 ページ\)](#)
- [IEEE 802.1x ポートベースの認証の設定例 \(89 ページ\)](#)
- [IEEE 802.1x ポートベースの認証統計情報とステータスのモニタリング \(91 ページ\)](#)
- [IEEE 802.1x ポートベースの認証の機能履歴 \(92 ページ\)](#)

IEEE 802.1x ポートベース認証の制約事項

- プライベート VLAN で使用する場合、スイッチポートは常に許可されません。認証、許可、およびアカウントिंग（AAA）サーバーからプッシュされるダイナミック VLAN は、プライベート VLAN ポートではサポートされません。データ クライアントセッションは、プライベート VLAN の dot1x ポートのセカンダリ VLAN で許可されることが期待されます。
- 通常のアクセス VLAN ポートでは、インターフェイスで設定されたプライベート VLAN ベースの許可とダイナミック VLAN だけがサポートされます。
- **dot1q tag vlan native** コマンドがグローバルレベルで設定されている場合、トランクポートでの dot1x 再認証は失敗します。
- 認証の失敗を引き起こす可能性があるため、音声 VLAN とアクセス VLAN の両方に同じ VLAN ID を同時に設定しないでください。
- 管理 VRF は、RADIUS の送信元インターフェイスとして使用できません。
- ダウンロード可能な ACL に重複するエントリが含まれている場合、エントリは自動的にマージされません。その結果、802.1Xセッション許可は失敗します。ダウンロード可能な

ACLが、同じポートのポートベースのエントリや名前ベースのエントリなど、重複するエントリなしで最適化されていることを確認します。

- ポートセキュリティは、IEEE 802.1x ポートベース認証ではサポートされていません。
- インターフェイスの実行中の設定を、フラッシュにロードされた設定ファイルで上書きすると、一部のポートがエンドポイントの認証に失敗する場合があります。

IEEE 802.1x ポートベースの認証に関する情報

802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント/サーバ型のアクセスコントロールおよび認証プロトコルを定めています。認証サーバーがスイッチポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。



(注) TACACS は、802.1x 認証ではサポートされていません。

802.1x アクセスコントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN (EAPOL)、Cisco Discovery Protocol、およびスパンニングツリープロトコル (STP) トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

次の表は、各クライアントがサポートするセッションの最大数を示しています。

| クライアントセッション | サポートされる最大セッション数 |
|--|-----------------|
| dot1x または MAB クライアントセッションの最大数 | 2000 |
| Web ベース認証セッションの最大数 | 2000 |
| クリティカル認証 VLAN を有効にしてサーバを再初期化した dot1x セッションの最大数 | 2000 |
| さまざまなセッション機能が適用される MAB セッションの最大数 | 2000 |
| サービス テンプレートまたはセッション機能が適用される dot1x セッションの最大数 | 2000 |

IEEE 802.1x ポートベースの認証の概要

802.1x 規格では、一般の人がアクセス可能なポートから不正なクライアントが LAN に接続しないように規制する（適切に認証されている場合を除く）、クライアント/サーバ型のアクセ

ス コントロールおよび認証プロトコルを定めています。認証サーバーがスイッチ ポートに接続する各クライアントを認証したうえで、スイッチまたは LAN が提供するサービスを利用できるようにします。



(注) TACACS は、802.1x 認証ではサポートされていません。

802.1x アクセスコントロールでは、クライアントを認証するまでの間、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN (EAPOL)、Cisco Discovery Protocol、およびスパニングツリープロトコル (STP) トラフィックしか許可されません。認証に成功すると、通常のトラフィックはポートを通過できるようになります。

ポートベース認証プロセス

IEEE 802.1X ポートベース認証を設定するには、認証、認可、およびアカウントिंग (AAA) を有効にし、認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

AAA プロセスは認証から始まります。802.1x ポートベース認証がイネーブルであり、クライアントが 802.1x 準拠のクライアント ソフトウェアをサポートしている場合、次のイベントが発生します。

- クライアント ID が有効で 802.1x 認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。
- EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアント MAC アドレスを認証用に使用します。このクライアント MAC アドレスが有効で認証に成功した場合、スイッチはクライアントにネットワークへのアクセスを許可します。クライアント MAC アドレスが無効で認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはクライアントに限定的なサービスを提供するゲスト VLAN を割り当てます。
- スイッチが 802.1x 対応クライアントから無効な ID を取得し、制限付き VLAN が指定されている場合、スイッチはクライアントに限定的なサービスを提供する制限付き VLAN を割り当てることができます。
- RADIUS 認証サーバーが使用できず (ダウンしていて) アクセスできない認証バイパスがイネーブルの場合、スイッチは、RADIUS 設定 VLAN またはユーザー指定アクセス VLAN で、ポートをクリティカル認証ステートにして、クライアントにネットワークのアクセスを許可します。

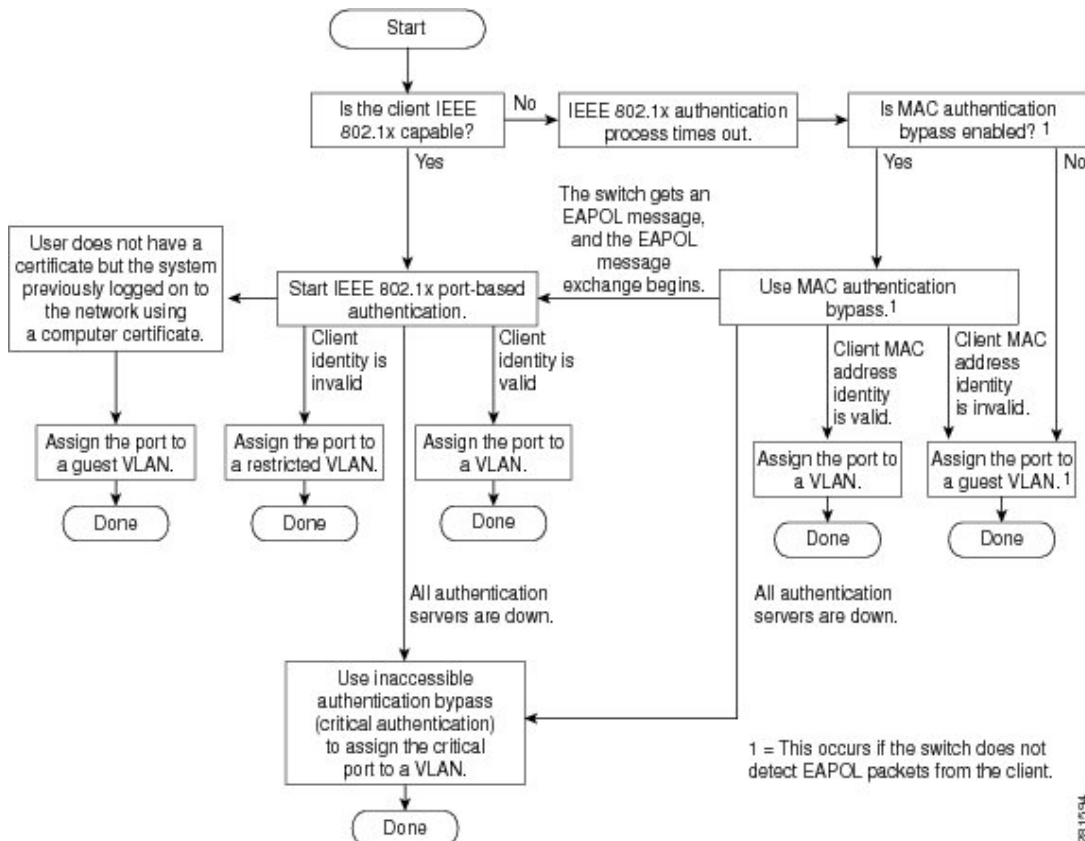


(注) アクセスできない認証バイパスは、クリティカル認証、または AAA 失敗ポリシーとも呼ばれます。

ポートで Multi Domain Authentication (MDA) が有効になっている場合、音声許可に該当する例外をいくつか伴ったフローを使用できます。

図 1: 認証フローチャート

次の図は認証プロセスを示します。



次の状況のいずれかが発生すると、スイッチはクライアントを再認証します。

- 定期的な再認証がイネーブルで、再認証タイマーの期限が切れている場合。

スイッチ固有の値を使用するか、RADIUS サーバーからの値に基づいて再認証タイマーを設定できます。

RADIUS サーバーを使用した 802.1x 認証の後で、スイッチは Session-Timeout RADIUS 属性 (Attribute[27])、および Termination-Action RADIUS 属性 (Attribute[29]) に基づいてタイマーを使用します。

Session-Timeout RADIUS 属性 (Attribute[27]) には再認証が行われるまでの時間を指定します。指定できる範囲は 1 ~ 65535 秒です。

Termination-Action RADIUS 属性 (Attribute[29]) には、再認証中に行われるアクションを指定します。アクションは *Initialize* および *ReAuthenticate* に設定できます。アクションに *Initialize* (属性値は *DEFAULT*) を設定した場合、802.1x セッションは終了し、認証中、接続は失われます。アクションに *ReAuthenticate* (属性値は *RADIUS-Request*) を設定した場合、セッションは再認証による影響を受けません。

- クライアントを手動で再認証するには、**dot1x re-authenticate interface interface-id** 特権 EXEC コマンドを入力します。

ポートベース認証の開始およびメッセージ交換

802.1x 認証中に、スイッチまたはクライアントは認証を開始できます。**authentication port-control auto** インターフェイス コンフィギュレーション コマンドを使用してポート上で認証をイネーブルにすると、スイッチは、リンクステータスがダウンからアップに移行したときに認証を開始し、ポートがアップしていて認証されていない場合は定期的に認証を開始します。スイッチはクライアントに EAP-Request/Identity フレームを送信し、その ID を要求します。クライアントはフレームを受信すると、EAP-Response/Identity フレームで応答します。

ただし、クライアントが起動時にスイッチからの EAP-Request/Identity フレームを受信しなかった場合、クライアントは EAPOL-Start フレームを送信して認証を開始できます。このフレームはスイッチに対し、クライアントの識別情報を要求するように指示します。



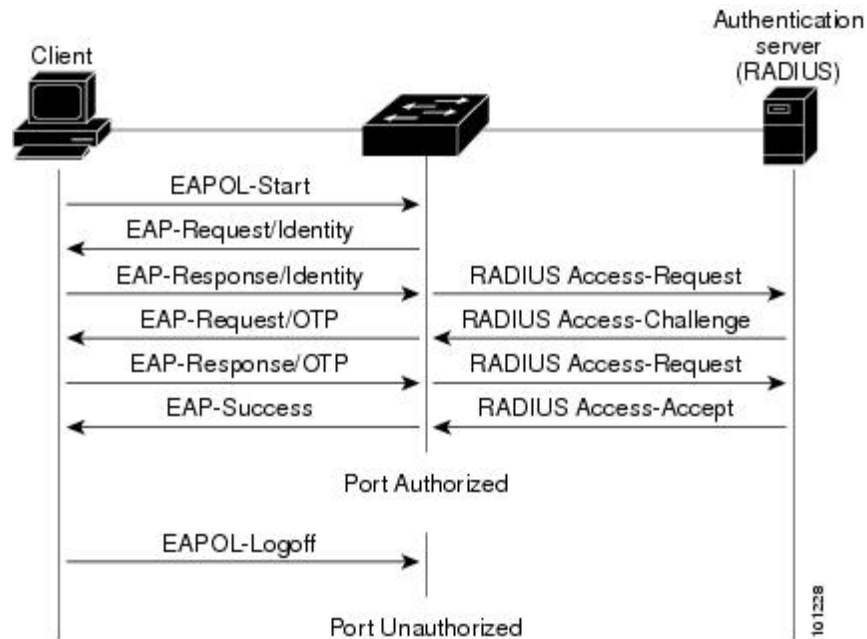
- (注) ネットワークアクセスデバイスで 802.1x 認証がイネーブルに設定されていない、またはサポートされていない場合には、クライアントからの EAPOL フレームはすべて廃棄されます。クライアントが認証の開始を 3 回試みても EAP-Request/Identity フレームを受信しなかった場合、クライアントはポートが許可ステータスであるものとしてフレームを送信します。ポートが許可ステータスであるということは、クライアントの認証が成功したことを実質的に意味します。

クライアントが自らの識別情報を提示すると、スイッチは仲介デバイスとしての役割を開始し、認証が成功または失敗するまで、クライアントと認証サーバーの間で EAP フレームを送受信します。認証が成功すると、スイッチポートは許可ステータスになります。認証に失敗した場合、認証が再試行されるか、ポートが限定的なサービスを提供する VLAN に割り当てられるか、あるいはネットワーク アクセスが許可されないかのいずれかになります。

実際に行われる EAP フレーム交換は、使用する認証方式によって異なります。

図 2: メッセージ交換

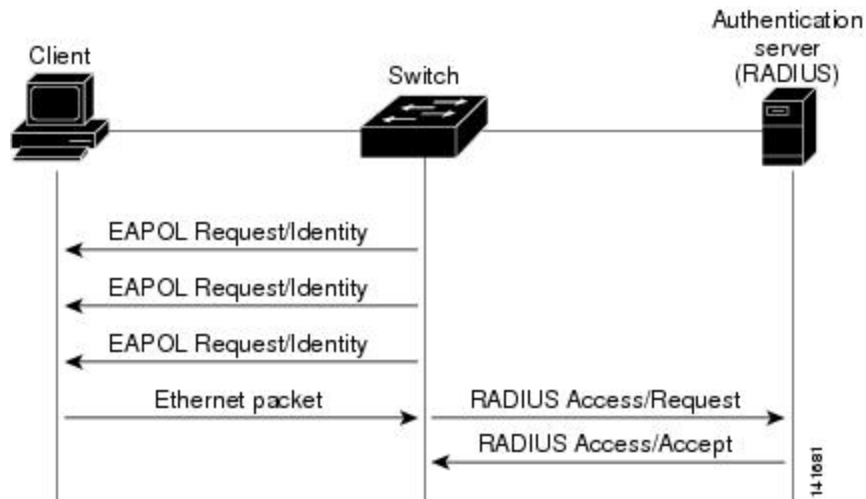
次の図に、クライアントが RADIUS サーバとの間で OTP（ワンタイムパスワード）認証方式を使用する際に行われるメッセージ交換を示します。



EAPOL メッセージ交換の待機中に 802.1x 認証がタイムアウトし、MAC 認証バイパスがイネーブルの場合、スイッチはクライアントからイーサネットパケットを検出するとそのクライアントを認証できません。スイッチは、クライアントの MAC アドレスを ID として使用し、RADIUS サーバーに送信される RADIUS Access/Request フレームにこの情報を保存します。サーバーがスイッチに RADIUS Access/Accept フレームを送信（認証が成功）すると、ポートが許可されます。認証に失敗してゲスト VLAN が指定されている場合、スイッチはポートをゲスト VLAN に割り当てます。イーサネットパケットの待機中にスイッチが EAPOL パケットを検出すると、スイッチは MAC 認証バイパスプロセスを停止して、802.1x 認証を開始します。

図 3: MAC 認証バイパス中のメッセージ交換

次の図に、MAC 認証バイパス中のメッセージ交換を示します。



ポートベース認証方法

表 1: 802.1x 機能

| 認証方法 | モード | | | |
|----------------|---|-----------|---|------------------------------------|
| | シングルホスト | マルチホスト | MDA | 複数 |
| 802.1x | VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL | VLAN 割り当て | VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL | VL ユー Filt ダウ AC リタ |
| MAC 認証バイパス | VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL | VLAN 割り当て | VLAN 割り当て ユーザ単位 ACL Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL | VL ユー Filt ダウ AC リタ |
| スタンドアロン Web 認証 | プロキシ ACL、Filter-ID 属性、ダウンロード可能な ACL | | | |

| 認証方法 | モード | | | |
|----------------------|---|---|---|-----------------------------------|
| | シングル ホスト | マルチ ホスト | MDA | 複数認 |
| NAC レイヤ 2 IP 検証 | Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL | Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL | Filter-ID 属性 ダウンロード可能 ACL リダイレクト URL | Filter-ID ダウンロード ACL リダイ |
| フォールバック方式としての Web 認証 | プロキシ ACL Filter-ID 属性 ダウンロード可能 ACL | プロキシ ACL Filter-ID 属性 ダウンロード可能 ACL | プロキシ ACL Filter-ID 属性 ダウンロード可能 ACL | プロキ Filter-I ダウ ACL |

¹ Cisco IOS リリース 12.2(50)SE 以降でサポートされています。

² 802.1x 認証をサポートしないクライアント用。

ユーザー単位 ACL とフィルタ ID



(注) フィルタ ID としてロールベース ACL を使用することは推奨されません。

MDA 対応ポートおよびマルチ認証ポートでは、複数のホストを認証できます。ホストに適用される ACL ポリシーは、別のホストのトラフィックには影響を与えません。マルチ ホストポートで認証されるホストが1つだけで、他のホストが認証なしでネットワークアクセスを取得する場合、発信元アドレスに any を指定することで、最初のホストの ACL ポリシーを他の接続ホストに適用できます。

許可状態および無許可状態のポート

802.1x 認証中に、スイッチのポート状態によって、スイッチはネットワークへのクライアントアクセスを許可します。ポートは最初、無許可状態です。この状態では、音声 VLAN ポートとして設定されていないポートは 802.1x 認証、Cisco Discovery Protocol、および STP パケットを除くすべての入力および出力トラフィックを禁止します。クライアントの認証が成功すると、ポートは許可状態に変更し、クライアントのトラフィック送受信を通常どおりに許可します。ポートが音声 VLAN ポートとして設定されている場合、VoIP トラフィックおよび 802.1x プロトコルパケットが許可された後クライアントが正常に認証されます。



(注) Cisco Discovery Protocol バイパスはサポートされていないため、ポートが err-disabled 状態になる場合があります。

802.1x をサポートしていないクライアントが、無許可ステートの 802.1x ポートに接続すると、スイッチはそのクライアントの識別情報を要求します。この状況では、クライアントは要求に応答せず、ポートは引き続き無許可ステートとなり、クライアントはネットワークアクセスを許可されません。

反対に、802.1x 対応のクライアントが、802.1x 標準が稼働していないポートに接続すると、クライアントは EAPOL-Start フレームを送信して認証プロセスを開始します。応答がなければ、クライアントは同じ要求を所定の回数だけ送信します。応答がないので、クライアントはポートが許可ステートであるものとしてフレーム送信を開始します。

authentication port-control インターフェイス コンフィギュレーション コマンド および 次のキーワードを使用して、ポートの許可ステートを制御できます。

- **force-authorized** : 802.1x 認証を無効にし、認証情報の交換を必要とせずに、ポートを許可ステートに変更します。ポートはクライアントとの 802.1x ベース認証を行わずに、通常のトラフィックを送受信します。これがデフォルト設定です。
- **force-unauthorized** : ポートが無許可ステートのままになり、クライアントからの認証の試みをすべて無視します。スイッチはポートを介してクライアントに認証サービスを提供できません。
- **auto** : 802.1x 認証をイネーブルにします。ポートは最初、無許可ステートであり、ポート経由で送受信できるのは EAPOL フレームだけです。ポートのリンクステートがダウンからアップに変更した際、または EAPOL-Start フレームを受信した際に、認証プロセスが開始されます。スイッチはクライアントの識別情報を要求し、クライアントと認証サーバとの間で認証メッセージのリレーを開始します。スイッチはクライアントの MAC アドレスを使用して、ネットワークアクセスを試みる各クライアントを一意に識別します。

クライアントが認証に成功すると（認証サーバから **Accept** フレームを受信すると）、ポートが許可ステートに変わり、認証されたクライアントからの全フレームがポート経由での送受信を許可されます。認証が失敗すると、ポートは無許可ステートのままですが、認証を再試行することはできません。認証サーバに到達できない場合、スイッチは要求を再送信します。所定の回数だけ試行してもサーバから応答が得られない場合には、認証が失敗し、ネットワークアクセスは許可されません。

クライアントはログオフするとき、EAPOL-Logoff メッセージを送信します。このメッセージによって、スイッチポートが無許可ステートになります。

ポートのリンクステートがアップからダウンに変更した場合、または EAPOL-Logoff フレームを受信した場合に、ポートは無許可ステートに戻ります。

802.1X のホストモード

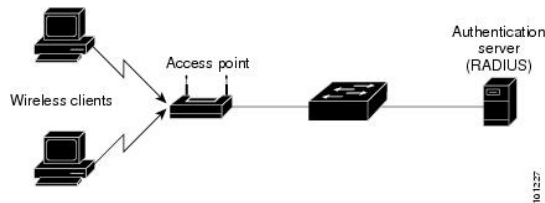
802.1x ポートは、シングルホストモードまたはマルチホストモードで設定できます。シングルホストモードでは、802.1x 対応のスイッチポートに接続できるのはクライアント 1 つだけです。スイッチは、ポートのリンクステートがアップに変化したときに、EAPOL フレームを送信することでクライアントを検出します。クライアントがログオフしたとき、または別のク

クライアントに代わったときには、スイッチはポートのリンクステートをダウンに変更し、ポートは無許可ステータスに戻ります。

マルチホストモードでは、複数のホストを単一の802.1x対応ポートに接続できます。このモードでは、接続されたクライアントのうち1つが許可されれば、クライアントすべてのネットワークアクセスが許可されます。ポートが無許可ステータスになると（再認証が失敗した場合、またはEAPOLログオフメッセージを受信した場合）、スイッチは接続されたすべてのクライアントのネットワークアクセスを拒否します。

このトポロジでは、ワイヤレスアクセスポイントが接続しているクライアントの認証を処理し、スイッチに対してクライアントとしての役割を果たします。

図 4: マルチホストモードの例



(注) すべてのホストモードで、ポートベース認証が設定されている場合、ラインプロトコルは許可の前にアップのままです。

スイッチはマルチドメイン認証 (MDA) をサポートしています。これにより、データ装置と IP Phone などの音声装置の両方を同じスイッチポートに接続できます。

アクセスセッション制限プロファイル

アクセスセッション制限プロファイルを使用すると、ポートに接続する音声ホストとデータホストの数を制限できます。アクセスセッション制限プロファイルは、どのホストモード設定よりも優先されます。アクセスセッション制限プロファイルが設定されている場合、ホストモードの設定は無視されます。

グローバルコンフィギュレーションモードで **access-session limit profile** コマンドを使用して、アクセスセッション制限プロファイルを作成できます。インターフェイスごとに許可されるデータおよび音声セッションの数を制限するようにプロファイルを設定できます。CDP バイパスがサポートされている場合、複数のホストを許可し、CDP パケットに基づいて認証をバイパスするようにプロファイルを設定できます。

アクセスセッション制限プロファイルは、インターフェイスレベルで適用する必要があります。

アクセスセッション制限プロファイルをインターフェイステンプレートに適用することもできます。

MAC 移動

あるスイッチポートでMACアドレスが認証されると、そのアドレスは同じスイッチの別の認証マネージャ対応ポートでは許可されません。スイッチが同じMACアドレスを別の認証マネージャ対応ポートで検出すると、そのアドレスは許可されなくなります。

場合によっては、MACアドレスを同じスイッチ上のポート間で移動する必要があります。たとえば、認証ホストとスイッチポート間に別のデバイス（ハブまたはIP Phoneなど）がある場合、ホストをデバイスから接続して、同じスイッチの別のポートに直接接続する必要があります。

デバイスが新しいポートで再認証されるように、MAC移動をグローバルにイネーブルにできます。ホストが別のポートに移動すると、最初のポートのセッションが削除され、ホストは新しいポートで再認証されます。MAC移動はすべてのホストモードでサポートされます（認証ホストは、ポートで有効にされているホストモードに関係なく、スイッチの任意のポートに移動できます）。MACアドレスがあるポートから別のポートに移動すると、スイッチは元のポートで認証済みセッションを終了し、新しいポートで新しい認証シーケンスを開始します。MAC移動の機能は、音声およびデータホストの両方に適用されます。



- (注) オープン認証モードでは、MACアドレスは、新しいポートでの許可を必要とせずに、元のポートから新しいポートへただちに移動します。

MAC 置換

MAC置換機能は、ホストが別のホストがすでに認証済みであるポートに接続しようとする発生する違反に対処するように設定できます。



- (注) 違反はマルチ認証モードでは発生しないため、マルチ認証モードのポートにこの機能は適用されません。マルチホストモードで認証が必要なのは最初のホストだけなので、この機能はこのモードのポートには適用されません。

replace キーワードを指定して **authentication violation** インターフェイス コンフィギュレーション コマンドを設定すると、マルチドメインモードのポートでの認証プロセスは、次のようになります。

- 既存の認証済みMACアドレスを使用するポートで新しいMACアドレスが受信されます。
- 認証マネージャは、ポート上の現在のデータホストのMACアドレスを、新しいMACアドレスで置き換えます。
- 認証マネージャは、新しいMACアドレスに対する認証プロセスを開始します。
- 認証マネージャによって新しいホストが音声ホストであると判断された場合、元の音声ホストは削除されます。

ポートがオープン認証モードになっている場合、MACアドレスはただちにMACアドレステーブルに追加されます。

802.1x アカウンティング

802.1x 標準では、ユーザの認証およびユーザのネットワークアクセスに対する許可方法を定義しています。ただし、ネットワークの使用法についてはトラッキングしません。802.1x アカウンティングは、デフォルトでディセーブルです。802.1x アカウンティングをイネーブルにすると、次の処理を 802.1x 対応のポート上でモニタできます。

- 正常にユーザを認証します。
- ユーザがログ オフします。
- リンクダウンが発生します。
- 再認証の正常な発生
- 再認証の失敗

スイッチは 802.1x アカウンティング情報を記録しません。その代わりに、スイッチはこの情報を RADIUS サーバに送信します。RADIUS サーバは、アカウンティングメッセージを記録するように設定する必要があります。

802.1x アカウンティング属性値ペア

RADIUS サーバに送信された情報は、属性値 (AV) ペアの形式で表示されます。これらの AV ペアのデータは、各種アプリケーションによって使用されます (たとえば課金アプリケーションの場合、RADIUS パケットの Acct-Input-Octets または Acct-Output-Octets 属性の情報が必要です)。

AV ペアは、802.1x アカウンティングが設定されているスイッチによって自動的に送信されます。次の種類の RADIUS アカウンティング パケットがスイッチによって送信されます。

- START : 新規ユーザー セッションが始まると送信されます。
- INTERIM : 既存のセッションが更新されると送信されます。
- STOP : セッションが終了すると送信されます。

次の表に、AV ペアおよびスイッチによって送信される AV ペアの条件を示します。

表 2: アカウンティング AV ペア

| 属性番号 | AV ペア名 | START | INTERIM | STOP |
|--------|----------------|-------|---------|------|
| 属性 [1] | User-Name | 送信 | 送信 | 送信 |
| 属性 [4] | NAS-IP-Address | 送信 | 送信 | 送信 |

| 属性番号 | AV ペア名 | START | INTERIM | STOP |
|---------|----------------------|-------|-----------------------|----------|
| 属性 [5] | NAS-Port | 送信 | 送信 | 送信 |
| 属性 [8] | Framed-IP-Address | 非送信 | 条件に応じて送信 ³ | 条件に応じて送信 |
| 属性 [30] | Called-Station-ID | 送信 | 送信 | 送信 |
| 属性 [31] | Calling-Station-ID | 送信 | 送信 | 送信 |
| 属性 [40] | Acct-Status-Type | 送信 | 送信 | 送信 |
| 属性 [41] | Acct-Delay-Time | 送信 | 送信 | 送信 |
| 属性 [42] | Acct-Input-Octets | 非送信 | 送信 | 送信 |
| 属性 [43] | Acct-Output-Octets | 非送信 | 送信 | 送信 |
| 属性 [47] | Acct-Input-Packets | 非送信 | 送信 | 送信 |
| 属性 [48] | Acct-Output-Packets | 非送信 | 送信 | 送信 |
| 属性 [44] | Acct-Session-ID | 送信 | 送信 | 送信 |
| 属性 [45] | Acct-Authentic | 送信 | 送信 | 送信 |
| 属性 [46] | Acct-Session-Time | 非送信 | 送信 | 送信 |
| 属性 [49] | Acct-Terminate-Cause | 非送信 | 非送信 | 送信 |
| 属性 [61] | NAS-Port-Type | 送信 | 送信 | 送信 |

³ 有効な静的 IP アドレスが設定されているか、ホストに対する Dynamic Host Control Protocol (DHCP) バインディングが DHCP スヌーピング バインディング テーブルに存在している場合に、Framed-IP-Address の AV ペアが送信されます。

802.1x 準備状態チェック

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1x をサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。802.1x 機能をサポートしていないデバイスでは、MAC 認証バイパスまたは Web 認証などの代替認証を使用します。

この機能が有用なのは、クライアントのサブリカントで NOTIFY EAP 通知パケットでのクエリーがサポートされている場合だけです。クライアントは、802.1x タイムアウト値内に応答しなければなりません。

スイッチと RADIUS サーバー間の通信

RADIUS セキュリティ サーバは、ホスト名または IP アドレス、ホスト名と特定の UDP ポート番号、または IP アドレスと特定の UDP ポート番号によって識別します。IP アドレスと UDP ポート番号の組み合わせによって、一意の ID が作成され、同一 IP アドレスのサーバ上にある複数の UDP ポートに RADIUS 要求を送信できるようになります。同じ RADIUS サーバ上の異なる 2 つのホストエントリに同じサービス（たとえば認証）を設定した場合、2 番めに設定されたホストエントリは、最初に設定されたホストエントリのフェールオーバーバックアップとして動作します。RADIUS ホスト エントリは、設定した順序に従って試行されます。

IEEE 802.1x 認証

802.1x 認証

802.1x 認証を設定する場合の注意事項は、次のとおりです。

- 802.1x 認証を使用するには、SISF ベースのデバイストラッキングを有効にする必要があります。デフォルトでは、SISF ベースのデバイストラッキングはスイッチで無効になっています。
- 802.1x 認証をイネーブルにすると、他のレイヤ 2 またはレイヤ 3 機能がイネーブルになる前に、ポートが認証されます。
- 802.1x 対応ポートが割り当てられている VLAN が変更された場合、この変更は透過的でスイッチには影響しません。たとえば、ポートが RADIUS サーバに割り当てられた VLAN に割り当てられ、再認証後に別の VLAN に割り当てられた場合に、この変更が発生します。

802.1x ポートが割り当てられている VLAN がシャットダウン、ディセーブル、または削除される場合、ポートは無許可になります。たとえば、ポートが割り当てられたアクセス VLAN がシャットダウンまたは削除された後、ポートは無許可になります。

- 802.1x プロトコルは、レイヤ 2 スタティックアクセス ポート、音声 VLAN ポート、およびレイヤ 3 ルーテッド ポートでサポートされますが、次のポートタイプではサポートされません。
 - **ダイナミック ポート**：ダイナミック モードのポートは、ネイバーとトランク ポートへの変更をネゴシエートする場合があります。ダイナミック ポートで 802.1x 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1x 認証はイネーブルになりません。802.1x 対応ポートのモードをダイナミックに変更しようとしても、エラーメッセージが表示され、ポート モードは変更されません。
 - **EtherChannel ポート**：アクティブまたはアクティブでない EtherChannel メンバを 802.1x ポートとして設定しないでください。EtherChannel ポートで 802.1x 認証をイネーブルにしようとする、エラーメッセージが表示され、802.1x 認証はイネーブルになりません。

- スイッチドポートアナライザ (SPAN) およびリモート SPAN (RSPAN) 宛先ポート : SPAN または RSPAN 宛先ポートであるポートの 802.1x 認証をイネーブルにすることができます。ただし、ポートを SPAN または RSPAN 宛先ポートとして削除するまでは、802.1x 認証はディセーブルになります。SPAN または RSPAN 送信元ポートでは 802.1x 認証をイネーブルにすることができます。
- スイッチ上で、**dot1x system-auth-control** グローバル コンフィギュレーション コマンドを入力して 802.1x 認証をグローバルにイネーブルにする前に、802.1x 認証と EtherChannel が設定されているインターフェイスから、EtherChannel の設定を削除してください。
- 802.1x 認証に関連するシステムメッセージをフィルタリングできます。



- (注) 802.1x に準拠したすべての CLI を同じインターフェイスまたは同じテンプレートで設定することを推奨します。

ポートベース認証マネージャ CLI コマンド

認証マネージャ インターフェイス コンフィギュレーション コマンドは、802.1x、MAC 認証バイパスおよび Web 認証など、すべての認証方法を制御します。認証マネージャ コマンドは、接続ホストに適用される認証方法のプライオリティと順序を決定します。

認証マネージャ コマンドは、ホスト モード、違反モードおよび認証タイマーなど、一般的な認証機能を制御します。一般的な認証コマンドには、**authentication host-mode**、**authentication violation**、および **authentication timer** インターフェイス コンフィギュレーション コマンドが含まれます。

802.1x 専用コマンドは、先頭に **dot1x** キーワードが付きます。たとえば、**authentication port-control auto** インターフェイス コンフィギュレーション コマンドは、インターフェイスでの認証をイネーブルにします。

スイッチでの **dot1x** を無効にするには、**no dot1x system-auth-control** を使用して、設定をグローバルに削除し、設定されているすべてのインターフェイスからも削除します。



- (注) 802.1x 認証がグローバルにディセーブル化されても、Web 認証など他の認証方法はそのポートでイネーブルのままです。

authentication manager コマンドは、以前の 802.1x コマンドと同じ機能を提供します。

認証マネージャが生成する冗長なシステムメッセージをフィルタリングすると、通常は、フィルタリングされた内容が認証の成功に結びつきます。802.1x 認証および MAB 認証の冗長なメッセージをフィルタリングすることもできます。認証方式ごとに異なるコマンドが用意されています。

- **no authentication logging verbose** グローバル コンフィギュレーション コマンドは、認証マネージャからの詳細メッセージをフィルタリングします。

- **no dot1x logging verbose** グローバル コンフィギュレーション コマンドは、802.1x 認証の詳細メッセージをフィルタリングします。
- **no mab logging verbose** グローバル コンフィギュレーション コマンドは、MAC 認証バイパス (MAB) の詳細メッセージをフィルタリングします。

802.1x 認証のデフォルト設定

表 3: 802.1x 認証のデフォルト設定

| 機能 | デフォルト設定 |
|--|--|
| スイッチの 802.1x イネーブル ステート | ディセーブル |
| ポート単位の 802.1x イネーブル ステート | ディセーブル (force-authorized) ポートはクライアントとの 802.1x ベース認証を行わずにラフィックを送受信します。 |
| AAA | ディセーブル |
| RADIUS サーバ <ul style="list-style-type: none"> • IP アドレス • UDP 認証ポート • デフォルトのアカウントング ポート • キー | <ul style="list-style-type: none"> • 指定なし • 1645 • 1646 • 指定なし |
| ホスト モード | シングル ホスト モード |
| 制御方向 | 双方向制御 |
| 定期的な再認証 | ディセーブル。 |
| 再認証の間隔 (秒) | 3600 秒 |
| 再認証回数 | 2 回 (ポートが無許可ステートになる前に、スイッチアクセスを再開する回数) |
| 待機時間 | 60 秒 (スイッチがクライアントとの認証情報の交換に失敗した場合、待機状態を続ける秒数) |
| 再送信時間 | 30 秒 (スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数) |
| 最大再送信回数 | 2 回 (スイッチが認証プロセスを再開する前に、EAP-Request/Identity フレームを送信する回数) |

| 機能 | デフォルト設定 |
|---------------------|---|
| クライアント タイムアウト時間 | 30 秒（認証サーバーからの要求をクライアントにリ スイッチが返答を待ち、クライアントに要求を再送 間） |
| 認証サーバー タイムアウト時間 | 30 秒（クライアントからの応答を認証サーバーにリ スイッチが応答を待ち、応答をサーバーに再送信す dot1x timeout server-timeout インターフェイス コンフ ン コマンドを使用して、このタイムアウト時間を変 |
| 無活動タイムアウト | ディセーブル |
| ゲスト VLAN | 指定なし |
| アクセス不能認証バイパス | ディセーブル |
| 制限付き VLAN | 指定なし |
| オーセンティケータ（スイッチ） モード | 指定なし |
| MAC 認証バイパス | ディセーブル |
| 音声認識セキュリティ | ディセーブル |

ポートベース認証とスイッチ スタック

スイッチが、スイッチ スタックに追加されるか、スイッチ スタックから削除される場合、RADIUS サーバーとスタックとの間の IP 接続が正常な場合、802.1x 認証は影響を受けません。これは、スタックのアクティブスイッチがスイッチスタックから削除される場合も、適用されます。アクティブスイッチに障害が発生した場合、スタック内のメンバスイッチは、選択プロセスを使用することによって新しいアクティブスイッチになり、802.1x 認証プロセスは通常どおり続行されます。

サーバーに接続されていたスイッチが削除されたか、そのスイッチに障害が発生したために、RADIUS サーバーへの IP 接続が中断された場合、これらのイベントが発生します。

- すでに認証済みで、定期的な再認証がイネーブルではないポートは、認証ステータスのままです。RADIUS サーバーとの通信は、必要ではありません。
- すでに認証済みで、（**dot1x re-authentication** グローバル コンフィギュレーション コマンドを使用して）定期的な再認証が有効になっているポートは、再認証の発生時に、認証プロセスに失敗します。ポートは、再認証プロセス中に、非認証ステータスに戻ります。RADIUS サーバーとの通信が必要です。

進行中の認証については、サーバー接続が行われていないため、認証はただちに失敗します。

障害が発生したスイッチが実行状態になり、スイッチスタックに再加入した場合、ブートアップの時刻と、認証の試行時までには RADIUS サーバーへの接続が再確立されたかどうかによって、認証は失敗する場合と、失敗しない場合があります。

RADIUS サーバーへの接続を失うことを避けるには、冗長接続を設定する必要があります。たとえば、アクティブスイッチへの冗長接続と、メンバスイッチへの別の接続を設定できます。アクティブスイッチに障害が発生した場合でも、スイッチスタックは、RADIUS サーバーに接続されたままです。

VLAN 割り当てを使用した 802.1x 認証

スイッチは、VLAN 割り当てを使用した 802.1x 認証をサポートしています。ポートの 802.1x 認証が成功すると、RADIUS サーバーは VLAN 割り当てを送信し、スイッチポートを設定します。RADIUS サーバーデータベースは、ユーザー名と VLAN のマッピングを維持し、スイッチポートに接続するクライアントのユーザー名に基づいて VLAN を割り当てます。この機能を使用して、特定のユーザーのネットワークアクセスを制限できます。

音声デバイスが許可されているときに、RADIUS サーバから許可された VLAN が返された場合、このポートの音声 VLAN は、割り当てられた音声 VLAN でパケットを送受信するように設定されています。音声 VLAN 割り当ては、マルチドメイン認証 (MDA) 対応のポートでのデータ VLAN 割り当てと同じように機能します。

スイッチと RADIUS サーバー上で設定された場合、VLAN 割り当てを使用した 802.1x 認証には次の特性があります。

- RADIUS サーバから VLAN が提供されない場合、または 802.1x 認証がディセーブルの場合、認証が成功するとポートはアクセス VLAN に設定されます。アクセス VLAN とは、アクセスポートに割り当てられた VLAN です。このポート上で送受信されるパケットはすべて、この VLAN に所属します。
- 802.1x 認証がイネーブルで、RADIUS サーバからの VLAN 情報が有効でない場合、認証に失敗して、設定済みの VLAN が引き続き使用されます。これにより、設定エラーによって不適切な VLAN に予期せぬポートが現れることを防ぎます。

設定エラーには、ルーテッドポートの VLAN、間違った VLAN ID、存在しないまたは内部 (ルーテッドポート) の VLAN ID、RSPAN VLAN、シャットダウンしている VLAN、あるいは一時停止している VLAN ID の指定などがあります。マルチドメインホストポートの場合、設定エラーには、設定済みまたは割り当て済み VLAN ID と一致するデータ VLAN の割り当て試行 (またはその逆) のために発生するものもあります。

- 802.1x 認証がイネーブルで、RADIUS サーバからのすべての情報が有効の場合、許可されたデバイスは認証後、指定した VLAN に配置されます。
- 802.1x ポートでマルチホストモードがイネーブルの場合、すべてのホストは最初に認証されたホストと同じ VLAN (RADIUS サーバにより指定) に配置されます。
- ポートセキュリティをイネーブル化しても、RADIUS サーバが割り当てられた VLAN の動作には影響しません。

- 802.1x 認証がポートでディセーブルの場合、設定済みのアクセス VLAN と設定済みの音声 VLAN に戻ります。
- 802.1x ポートが認証され、RADIUS サーバによって割り当てられた VLAN に配置されると、そのポートのアクセス VLAN 設定への変更は有効になりません。マルチドメインホストの場合、ポートが完全にこれらの例外で許可されている場合、同じことが音声デバイスに適用されます。
 - あるデバイスで VLAN 設定を変更したことにより、他のデバイスに設定済みまたは割り当て済みの VLAN と一致した場合、ポート上の全デバイスの認証が中断して、データおよび音声デバイスに設定済みの VLAN が一致しなくなるような有効な設定が復元されるまで、マルチドメインホストモードがディセーブルになります。
 - 音声デバイスが許可されて、ダウンロードされた音声 VLAN を使用している場合、音声 VLAN 設定を削除したり設定値を *dot1p* または *untagged* に修正したりすると、音声デバイスが未許可になり、マルチドメインホストモードが無効になります。

ポートが、強制許可 (force-authorized) ステート、強制無許可 (force-unauthorized) ステート、無許可ステート、またはシャットダウンステートの場合、ポートは設定済みのアクセス VLAN に配置されます。

VLAN 割り当てを設定するには、次の作業を実行する必要があります。

- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。(アクセスポートで 802.1x 認証を設定すると、VLAN 割り当て機能は自動的にイネーブルになります)。
- RADIUS サーバにベンダー固有のトンネル属性を割り当てます。RADIUS サーバーは次の属性をスイッチに返す必要があります。
 - [64] Tunnel-Type = VLAN
 - [65] Tunnel-Medium-Type = 802
 - [81] Tunnel-Private-Group-ID = VLAN 名または VLAN ID
 - [83] Tunnel-Preference

属性 [64] は、値 *VLAN* (タイプ 13) でなければなりません。属性 [65] は、値 *802* (タイプ 6) でなければなりません。属性 [81] は、IEEE 802.1x 認証ユーザに割り当てられた *VLAN* 名または *VLAN ID* を指定します。

ユーザー単位 ACL を使用した 802.1x 認証

ユーザー単位アクセスコントロールリスト (ACL) をイネーブルにして、異なるレベルのネットワーク アクセスおよびサービスを 802.1x 認証ユーザーに提供できます。RADIUS サーバーは、802.1x ポートに接続されるユーザーを認証する場合、ユーザー ID に基づいて ACL 属性を受け取り、これらをスイッチに送信します。スイッチは、ユーザーセッションの期間中、その

属性を 802.1x ポートに適用します。セッションが終了すると、認証が失敗した場合、またはリンクダウン状態の発生時に、ユーザー単位 ACL 設定が削除されます。スイッチは、RADIUS 指定の ACL を実行コンフィギュレーションには保存しません。ポートが無許可の場合、スイッチはそのポートから ACL を削除します。

ユーザーは同一のスイッチ上で、ルータ ACL および入力ポート ACL を使用できます。ただし、ポートの ACL はルータ ACL より優先されます。入力ポート ACL を VLAN に属するインターフェイスに適用する場合、ポート ACL は VLAN インターフェイスに適用する入力ルータ ACL よりも優先されます。ポート ACL が適用されたポート上で受信した着信パケットは、ポート ACL によってフィルタリングされます。その他のポートに着信したルーテッドパケットは、ルータ ACL によってフィルタリングされます。発信するルーテッドパケットには、ルータ ACL のフィルタが適用されます。コンフィギュレーションの矛盾を回避するには、RADIUS サーバーに保存するユーザー プロファイルを慎重に計画しなければなりません。

RADIUS は、ベンダー固有属性などのユーザー単位属性をサポートします。ベンダー固有属性 (VSA) は、オクテットストリング形式で、認証プロセス中にスイッチに渡されます。ユーザー単位 ACL に使用される VSA は、入力方向では `inacl#<n>` で、出力方向では `outacl#<n>` です。MAC ACL は、入力方向に限りサポートされます。VSA は入力方向に限りサポートされます。レイヤ 2 ポートの出力方向ではポート ACL をサポートしません。

拡張 ACL 構文形式だけを使用して、RADIUS サーバに保存するユーザー単位コンフィギュレーションを定義します。RADIUS サーバから定義が渡される場合、拡張命名規則を使用して作成されます。ただし、Filter-Id 属性を使用する場合、標準 ACL を示すことができます。

Filter-Id 属性を使用して、すでにスイッチに設定されているインバウンドまたはアウトバウンド ACL を指定できます。属性には、ACL 番号と、その後ろに入力フィルタリング、出力フィルタリングを示す `.in` または `.out` が含まれています。RADIUS サーバが `.in` または `.out` 構文を許可しない場合、アクセスリストはデフォルトで発信 ACL に適用されます。RADIUS サーバから送信された Filter-Id がデバイスで設定されていない場合、ユーザーは未承認としてマークされます。Filter-Id 属性は 1 ~ 199 (IP 標準 ACL) および 1300 ~ 2699 (IP 拡張 ACL) の範囲の IP ACL に対してだけサポートされます。

ユーザー単位 ACL の最大サイズは、4000 ASCII 文字ですが、RADIUS サーバのユーザー単位 ACL の最大サイズにより制限されます。

ユーザー単位の ACL を設定するには、次の前提条件を満たす必要があります。

- AAA 認証をイネーブルにします。
- **network** キーワードを使用して AAA 認証をイネーブルにし、RADIUS サーバからのインターフェイス設定を可能にします。
- 802.1x 認証をイネーブルにします。
- RADIUS サーバにユーザー プロファイルと VSA を設定します。
- 802.1x ポートをシングル ホスト モードに設定します。



(注) ユーザー単位 ACL がサポートされるのはシングル ホスト モードだけです。

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証

ACL およびリダイレクト URL は、ホストの 802.1x 認証または MAC 認証バイパス中に、RADIUS サーバーからスイッチにダウンロードできます。また、Web 認証中に ACL をダウンロードすることもできます。ダウンロード可能な ACL は *dACL* とも呼ばれます。

複数のホストが認証され、それらのホストがシングルホストモード、MDA モード、またはマルチ認証モードである場合、スイッチは ACL の送信元アドレスをホスト IP アドレスに変更します。

ACL およびリダイレクト URL は、802.1x 対応のポートに接続されるすべてのデバイスに適用できます。

ACL が 802.1x 認証中にダウンロードされない場合、スイッチは、ポートのスタティック デフォルト ACL をホストに適用します。マルチ認証モードまたは MDA モードで設定された音声 VLAN ポートでは、スイッチは ACL を認証ポリシーの一部として電話にだけ適用します。

スタック構成がある dACL の制限は、ポートベースの dACL あたり 64 ACE です。スタック構成なしの制限は、利用可能な TCAM エントリの数になり、これはアクティブな他の ACL 機能によって異なります。

同じタイプ (IPv4 または IPv6) の複数の dACL は、Cisco Identity Services Engine (ISE) ではサポートされません。一意の dACL のみが Cisco ISE から送信されるようにします。

802.1x および MAB 認証方式では、オープンおよびクローズの 2 つの認証方式がサポートされます。クローズ認証モードのポートにスタティック ACL がない場合、次のようになります。

- 最初のホスト認証では、許可ポリシーは IP アドレスを挿入せずに適用されます。
- 別のホストが検出されると、最初のホストのポリシーがリフレッシュされ、最初のセッションと後続セッションのポリシーが IP アドレスを挿入して実施されます。

オープン認証モードのポートにスタティック ACL がない場合、次のようになります。

- セキュリティ違反を防ぐために、IP アドレスを挿入してポリシーが実施されます。

許可ポリシーのないホストへのアクセスを制御するために、ディレクティブを設定することができます。サポートされているディレクティブの値は、*open* と *default* です。*open* ディレクティブを設定すると、すべてのトラフィックが許可されます。*default* ディレクティブは、ポートから提供されるアクセスにトラフィックを従わせます。ディレクティブは、AAA サーバー上のユーザープロファイル、またはスイッチ上のいずれかで設定できます。AAA サーバー上でディレクティブを設定するには、**authz-directive =<open/default>** グローバルコマンドを使用します。スイッチ上でディレクティブを設定するには、**epm access-control open** グローバルコンフィギュレーション コマンドを使用します。



(注) ディレクティブのデフォルト値は *default* です。

URL リダイレクト ACL の場合 :

- 許可アクセス コントロール エントリ (ACE) ルールに一致するパケットは、AAA サーバーに転送するために CPU に送信されます。
- 拒否 ACE ルールに一致するパケットは、スイッチを介して転送されます。
- 許可 ACE ルールにも拒否 ACE ルールにも一致しないパケットは、次の dACL によって処理されます。dACL がない場合、パケットは暗黙的拒否 ACL にヒットしてドロップされます。

VLAN ID ベース MAC 認証

ダウンロード可能な VLAN ではなくスタティック VLAN ID に基づいてホストを認証する場合、VLAN ID ベース MAC 認証を使用できます。スタティック VLAN ポリシーがスイッチで設定されている場合、認証用の各ホストの MAC アドレスとともに、VLAN 情報が IAS (Microsoft) RADIUS サーバーに送信されます。接続ポートに設定されている VLAN ID は MAC 認証に使用されます。VLAN ID ベース MAC 認証を IAS サーバーで使用することで、ネットワークで一定数の VLAN を使用できます。

機能は、STP によってモニターおよび処理される VLAN の数も制限します。ネットワークは固定 VLAN として管理できます。

MAC 認証バイパスを使用した IEEE 802.1x 認証

MAC 認証バイパス機能を使用し、クライアント MAC アドレスに基づいてクライアントを許可するようにスイッチを設定できます。たとえば、プリンタなどのデバイスに接続された IEEE 802.1x ポートでこの機能をイネーブルにできます。

クライアントからの EAPOL 応答の待機中に IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパスを使用してクライアントを許可しようとします。

MAC 認証バイパス機能が IEEE 802.1x ポートでイネーブルの場合、スイッチはクライアント ID として MAC アドレスを使用します。認証サーバーには、ネットワーク アクセスを許可されたクライアント MAC アドレスのデータベースがあります。スイッチは、IEEE 802.1x ポート上のクライアントを検出した後で、クライアントからのイーサネットパケットを待機します。スイッチは、MAC アドレスに基づいたユーザー名およびパスワードを持つ RADIUS-access/request フレームを認証サーバーに送信します。認証に成功すると、スイッチはクライアントにネットワークへのアクセスを許可します。許可が失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。このプロセスは、ほとんどのクライアントデバイスで動作します。ただし、代替の MAC アドレス形式を使用しているクライアントでは動作しません。標準の形式とは異なる MAC アドレスを持つクライアントに対して MAB 認証をどのように実行するかや、RADIUS の設定のどこでユーザ名とパスワードが異なることが要求されるかを設定できます。

リンクのライフタイム中に EAPOL パケットがインターフェイス上で検出された場合、スイッチは、そのインターフェイスに接続されているデバイスが 802.1x 対応サブリカントであることを確認し、（MAC 認証バイパス機能ではなく）802.1x 認証を使用してインターフェイスを認証します。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。

スイッチがすでに MAC 認証バイパスを使用してポートを許可し、IEEE 802.1x サブリカントを検出している場合、スイッチはポートに接続されているクライアントを許可します。再認証が発生するときに、Termination-Action RADIUS 属性値が DEFAULT であるために前のセッションが終了した場合、スイッチはポートに設定されている認証または再認証手法を使用します。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、IEEE 802.1x を使用して認証されたクライアントに対するプロセスと同じです。再認証中は、ポートは前に割り当てられた VLAN のままです。再認証に成功すると、スイッチはポートを同じ VLAN に保持します。再認証に失敗した場合、ゲスト VLAN が設定されていれば、スイッチはポートをゲスト VLAN に割り当てます。

再認証が Session-Timeout RADIUS 属性（Attribute[27]）、および Termination-Action RADIUS 属性（Attribute[29]）に基づいて行われるときに、Termination-Action RADIUS 属性（Attribute[29]）のアクションが *Initialize*（属性値は *DEFAULT*）である場合、MAC 認証バイパスセッションは終了し、再認証の間の接続は失われます。MAC 認証バイパス機能が IEEE 802.1x 認証がタイムアウトした場合、スイッチは MAC 認証バイパス機能を使用して再認証を開始します。これらの AV ペアの詳細については、RFC 3580 『IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines』を参照してください。

MAC 認証バイパスは、次の機能と相互に作用します。

- IEEE 802.1x 認証：802.1x 認証がポートでイネーブルの場合にのみ MAC 認証バイパスをイネーブルにできます。
- ゲスト VLAN：クライアントの MAC アドレス ID が無効な場合、ゲスト VLAN が設定されていれば、スイッチは VLAN にクライアントを割り当てます。
- 制限付き VLAN：IEEE 802.1x ポートに接続されているクライアントが MAC 認証バイパスで認証されている場合には、この機能はサポートされません。
- ポートセキュリティ
- 音声 VLAN
- プライベート VLAN：クライアントをプライベート VLAN に割り当てられます。
- Network Edge Access Topology (NEAT)：MAB と NEAT は相互に排他的です。インターフェイス上で NEAT が有効の場合は、MAB を有効にすることはできません。また、インターフェイス上で MAB が有効の場合は、NEAT を有効にすることはできません。

MAC 認証バイパス設定の注意事項

MAC 認証バイパス設定時の注意事項は次のとおりです。

- 特に明記していないかぎり、MAC 認証バイパスの注意事項は 802.1x 認証のものと同じです。
- ポートが MAC アドレスで許可された後に、ポートから MAC 認証バイパスをディセーブルにしても、ポート ステートに影響はありません。
- ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバデータベースにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレスがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポートを再認証できます。
- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MAC 認証バイパスにより接続されているが、非アクティブなホストのタイムアウト時間を設定できます。指定できる範囲は 1 ～ 65535 秒です。

802.1x マルチ認証モード

マルチ認証 (multiauth) モードでは、データ VLAN および音声 VLAN で複数のクライアントを認証できます。各ホストは個別に認証されます。マルチ認証ポートで認証できるデータデバイスまたは音声デバイスの数には制限はありません。

ハブまたはアクセス ポイントが 802.1x 対応ポートに接続されている場合、接続されている各クライアントを認証する必要があります。802.1x 以外のデバイスでは、MAC 認証バイパスまたは Web 認証をホスト単位認証フォールバック メソッドとして使用し、単一のポートで異なる方法で異なるホストを認証できます。

次の条件で、RADIUS サーバから提供された VLAN をマルチ認証モードで割り当てることができます。

- ホストがポートで最初に許可されたホストであり、RADIUS サーバが VLAN 情報を提供している。
- 後続のホストが、動作 VLAN に一致する VLAN を使用して許可される。
- ホストは VLAN が割り当てられていないポートで許可され、後続のホストでは VLAN 割り当てが設定されていないか、VLAN 情報が動作 VLAN と一致している。
- ポートで最初に許可されたホストにはグループ VLAN が割り当てられ、後続のホストでは VLAN 割り当てが設定されていないか、グループ VLAN がポート上のグループ VLAN と一致している。後続のホストが、最初のホストと同じ VLAN グループの VLAN を使用する必要がある。VLAN リストが使用されている場合、すべてのホストは VLAN リストで指定された条件に従う。
- VLAN がポート上のホストに割り当てられると、後続のホストは一致する VLAN 情報を持つ必要があり、この情報がなければポートへのアクセスを拒否される。
- クリティカル認証 VLAN の動作が、マルチ認証モード用に変更されない。ホストが認証を試みたときにサーバに到達できない場合、許可されたすべてのホストは、設定された VLAN で再初期化される。

ユーザーごとのマルチ認証 VLAN 割り当て

ユーザーごとのマルチ認証 VLAN 割り当て機能を使用すると、単一の設定済みアクセス VLAN を持つポート上のクライアントに割り当てられた VLAN に基づいて複数の運用アクセス VLAN を作成することができます。データドメインに関連付けられたすべての VLAN に対するトラフィックが dot1q とタグ付けされていないアクセスポートとして設定されているポートおよびこれらの VLAN は、ネイティブ VLAN として処理されます。

マルチ認証ポート 1 つあたりのホストの数は 8 ですが、さらに多くのホストが存在する場合があります。

次のシナリオは、ユーザーごとのマルチ認証 VLAN 割り当てに関連しています。

シナリオ 1

ハブがアクセスポートに接続されている場合、およびポートがアクセス VLAN (V0) で設定されている場合。

ホスト (H1) は、ハブを介して VLAN (V1) に割り当てられます。ポートの運用 VLAN は V1 に変更されます。この動作は、単一ホストポートまたはマルチドメイン認証ポートと同様です。

2 番目のホスト (H2) が接続され、VLAN (V2) に割り当てられる場合、ポートには 2 つの運用 VLAN があります (V1 および V2)。H1 と H2 がタグなし入力トラフィックを送信すると、H1 トラフィックは VLAN (V1) に、H2 トラフィックは VLAN (V2) にマッピングされ、VLAN (V1) および VLAN (V2) のポートからの出トラフィックはすべてタグなしになります。

両方のホスト H1 と H2 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN (V1) と VLAN (V2) がポートから削除され、設定された VLAN (V0) がポートに復元されます。

シナリオ 2

ハブがアクセスポートに接続されている場合、およびポートがアクセス VLAN (V0) で設定されている場合。ホスト (H1) は、ハブを介して VLAN (V1) に割り当てられます。ポートの運用 VLAN は V1 に変更されます。

2 番目のホスト (H2) が接続され明示的な VLAN ポリシーなしで承認されると、H2 はポート上で復元される設定済み VLAN (V0) を使用することを予期されます。2 つの運用 VLAN、VLAN (V0) および VLAN (V1) からの出トラフィックはすべてタグなしになります。

ホスト (H2) がログアウトするか、またはセッションがなんらかの理由で削除されると、設定された VLAN (V0) がポートから削除され、VLAN (V1) がそのポートでの唯一の運用 VLAN になります。

シナリオ 3

ハブがオープンモードでアクセスポートに接続されている場合、およびポートがアクセス VLAN (V0) で設定されている場合。

ホスト (H1) は、ハブを介して VLAN (V1) に割り当てられます。ポートの運用 VLAN は V1 に変更されます。2 番目のホスト (H2) が接続され無許可のままだと、オープンモードにより、運用 VLAN (V1) に引き続きアクセスできます。

ホスト H1 がログアウトするか、またはセッションがなんらかの理由で削除されると、VLAN (V1) はポートから削除され、ホスト (H2) は VLAN (V0) に割り当てられます。



(注) オープンモードと VLAN 割り当ての組み合わせは、ホスト (H2) に悪影響を与えます。そのホストは VLAN (V1) に対応するサブネット内に IP アドレスを含んでいるからです。

ユーザーごとのマルチ認証 VLAN 割り当ての制限

ユーザーごとのマルチ認証 VLAN 割り当て機能では、複数の VLAN からの出トラフィックは、ホストが自分宛てではないトラフィックを受信するポート上ではタグなしになります。これは、ブロードキャストおよびマルチキャストトラフィックで問題になる可能性があります。

- **IPv4 ARP** : ホストは他のサブネットからの ARP パケットを受信します。これは、IP アドレス範囲が重複する異なる仮想ルーティングおよび転送 (VRF) テーブルの 2 個のサブネットがポート上でアクティブな場合に問題となります。ホスト ARP キャッシュのエントリが無効になる可能性があります。

- **IPv6 制御パケット** : IPv6 の導入環境では、ルータアドバタイズメント (RA) は、その受信を想定されていないホストによって処理されます。ある VLAN からのホストが別の VLAN からの RA を受信すると、ホストはそれ自身に間違っただけの IPv6 アドレスを割り当てます。このようなホストは、ネットワークにアクセスできません。

回避策は、IPv6 ファーストホップセキュリティをイネーブルにして、ブロードキャスト ICMPv6 パケットがユニキャストに変換され、マルチ認証がイネーブルのポートから送信されるようにすることです。パケットは VLAN に属するマルチ認証ポートの各クライアント用に複製され、宛先 MAC が個々のクライアントに設定されます。1 つの VLAN を持つポートで、ICMPv6 パケットは正常にブロードキャストされます。

- **IP マルチキャスト** : 送信先のマルチキャストグループへのマルチキャストトラフィックは、異なる VLAN 上のホストがそのマルチキャストグループに参加している場合それらの VLAN 用に複製されます。異なる VLAN の 2 つのホストが (同じマルチ認証ポート上の) マルチキャストグループに参加している場合、各マルチキャストパケットのコピー 2 部がそのポートから送信されます。

ゲスト VLAN を使用した 802.1x 認証

スイッチ上の各 802.1x ポートにゲスト VLAN を設定し、クライアントに対して限定的なサービスを提供できます (802.1x クライアントのダウンロードなど)。これらのクライアントは 802.1x 認証用にシステムをアップグレードできる場合がありますが、一部のホスト (Windows 98 システムなど) は IEEE 802.1x 対応ではありません。

スイッチが EAP Request/Identity フレームに対する応答を受信していない場合、または EAPOL パケットがクライアントによって送信されない場合に、802.1x ポート上でゲスト VLAN をイネーブルにすると、スイッチはクライアントにゲスト VLAN を割り当てます。

スイッチは EAPOL パケット履歴を保持します。EAPOL パケットがリンクの存続時間中にインターフェイスで検出された場合、スイッチはそのインターフェイスに接続されているデバイスが IEEE 802.1x 対応のものであると判断します。インターフェイスはゲスト VLAN ステートにはなりません。インターフェイスのリンク ステータスがダウンした場合、EAPOL 履歴はクリアされます。EAPOL パケットがインターフェイスで検出されない場合、そのインターフェイスはゲスト VLAN のステートになります。

スイッチが 802.1x 対応の音声デバイスを許可しようとしたが、AAA サーバーが使用できない場合、許可は失敗します。ただし、EAPOL パケットの検出は EAPOL 履歴に保存されます。この音声デバイスは、AAA サーバーが使用可能になると許可されます。ただし、他のデバイスによるゲスト VLAN へのアクセスは許可されなくなります。この状況を防ぐには、次のいずれかのコマンドシーケンスを使用します。

- **authentication event no-response action authorize vlan *vlan-id*** インターフェイス コンフィギュレーション コマンドを入力し、ゲスト VLAN へのアクセスを許可します。
- **shutdown** インターフェイス コンフィギュレーション コマンドを入力し、さらに **no shutdown** インターフェイス コンフィギュレーション コマンドを入力してポートを再起動します。

リンクの存続時間中にデバイスが EAPOL パケットを送信した場合、スイッチはゲスト VLAN への認証アクセスに失敗したクライアントを許可しません。



- (注) インターフェイスがゲスト VLAN に変わってから EAPOL パケットが検出された場合、無許可ステートに戻って 802.1x 認証を再起動します。

スイッチ ポートがゲスト VLAN に変わると、802.1x 非対応クライアントはすべてアクセスを許可されます。ゲスト VLAN が設定されているポートに 802.1x 対応クライアントが加入すると、ポートは、ユーザ設定によるアクセス VLAN で無許可ステートになり、認証が再起動されます。

ゲスト VLAN は、単一のホスト、複数のホスト、複数認証、またはマルチドメインモードにおける 802.1x ポートでサポートされています。

RSPAN VLAN、プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN (ルーテッドポート) またはトランクポートではサポートされていません。アクセスポート上でだけサポートされます。

スイッチは MAC 認証バイパスをサポートします。MAC 認証バイパスが 802.1x ポートでイネーブルの場合、スイッチは、IEEE 802.1x 認証のタイムアウト時に EAPOL メッセージ交換を待機している間、クライアント MAC アドレスに基づいてクライアントを許可できます。スイッチは、802.1x ポート上のクライアントを検出したあとで、クライアントからのイーサネットパケットを待機します。スイッチは、MAC アドレスに基づいたユーザー名およびパスワードを持つ RADIUS-access/request フレームを認証サーバーに送信します。認証に成功すると、スイ

チはクライアントにネットワークへのアクセスを許可します。認証に失敗すると、スイッチはポートにゲスト VLAN を割り当てます（指定されていない場合）。

制限付き VLAN を使用した 802.1x 認証

ゲスト VLAN にアクセスできないクライアント向けに、限定されたサービスを提供するために、スイッチ スタックまたはスイッチの各 IEEE 802.1x ポートに対して制限付き VLAN（認証失敗 VLAN と呼ばれることもあります）を設定できます。これらのクライアントは、認証プロセスに失敗したため他の VLAN にアクセスできない 802.1x 対応クライアントです。制限付き VLAN を使用すると、認証サーバの有効なクレデンシアルを持っていないユーザ（通常、企業にアクセスするユーザ）に、サービスを制限したアクセスを提供できます。管理者は制限付き VLAN のサービスを制御できます。



(注) 両方のタイプのユーザに同じサービスを提供する場合、ゲスト VLAN と制限付き VLAN の両方を同じに設定できます。

この機能がないと、クライアントは認証失敗を永遠に繰り返すことになるため、スイッチポートがスパニングツリーのブロッキング状態から変わることができなくなります。制限付き VLAN の機能を使用することで、クライアントの認証試行回数を指定し（デフォルト値は 3 回）、一定回数後にスイッチポートを制限付き VLAN の状態に移行させることができます。

認証サーバはクライアントの認証試行回数をカウントします。このカウントが設定した認証試行回数を超えると、ポートが制限付き VLAN の状態に変わります。失敗した試行回数は、RADIUS サーバが *EAP failure* で応答したときや、EAP パケットなしの空の応答を返したときからカウントされます。ポートが制限付き VLAN に変わったら、このカウント数はリセットされます。

認証に失敗したユーザの VLAN は、もう一度認証を実行するまで制限された状態が続きます。VLAN 内のポートは設定された間隔に従って再認証を試みます（デフォルトは 60 秒）。再認証に失敗している間は、ポートの VLAN は制限された状態が続きます。再認証に成功した場合、ポートは設定された VLAN もしくは RADIUS サーバによって送信された VLAN に移行します。再認証はディセーブルにすることもできますが、ディセーブルにすると、*link down* または *EAP logoff* イベントを受信しない限り、ポートの認証プロセスを再起動できません。クライアントがハブを介して接続している場合、再認証機能はイネーブルにしておくことを推奨します。クライアントの接続をハブから切り離すと、ポートに *link down* や *EAP logoff* イベントが送信されない場合があります。

ポートが制限付き VLAN に移行すると、EAP 成功の疑似メッセージがクライアントに送信されます。このメッセージによって、繰り返し実行している再認証を停止させることができます。クライアントによっては（Windows XP が稼働しているデバイスなど）、EAP なしで DHCP を実装できません。

制限付き VLAN は、すべてのホストモードでの 802.1x ポート上、およびレイヤ 2 ポート上でサポートされます。

RSPAN VLAN、プライマリ プライベート VLAN、音声 VLAN を除いて、アクティブ VLAN を 802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN（ルーテッ

ドポート) またはトランクポートではサポートされていません。アクセスポート上でだけサポートされます。

ダイナミック ARP インスペクション、DHCP スヌーピング、IP 送信元ガードなどの他のセキュリティポート機能は、制限付き VLAN に対して個別に設定できます。

アクセス不能認証バイパスを使用した 802.1x 認証

スイッチが設定された RADIUS サーバーに到達できず、新しいホストを認証できない場合、アクセス不能認証バイパス機能を使用します。この機能は、クリティカル認証または AAA 失敗ポリシーとも呼ばれます。これらのホストをクリティカルポートに接続するようにスイッチを設定できます。

新しいホストがクリティカルポートに接続しようとする、そのホストはユーザ指定のアクセス VLAN、クリティカル VLAN に移動されます。管理者はこれらのホストに制限付き認証を付与します。

スイッチは、クリティカルポートに接続されているホストを認証しようとする場合、設定されている RADIUS サーバーのステータスをチェックします。利用可能なサーバーが 1 つあれば、スイッチはホストを認証できます。ただし、すべての RADIUS サーバーが利用不可能な場合は、スイッチはホストへのネットワークアクセスを許可して、ポートを認証ステートの特別なケースであるクリティカル認証ステートにします。



- (注) クリティカル認証をインターフェイスで設定する場合は、クリティカル承認 (クリティカル *vlan*) に使用する *vlan* をスイッチでアクティブにする必要があります。クリティカル *vlan* がアクティブまたはダウンしていると、クリティカル認証セッションは非アクティブな *vlan* の有効化を試行し続け、繰り返し失敗します。これは大量のメモリ保持の原因となる可能性があります。

複数認証ポートのアクセス不能認証バイパスのサポート

ポートが任意のホストモードで設定されていて、AAA サーバーを使用できない場合、ポートはマルチホストモードに設定され、クリティカル VLAN に移動されます。マルチ認証 (multiauth) ポートで、このアクセス不能バイパスをサポートするには、**authentication event server dead action reinitialize vlan *vlan-id*** コマンドを使用します。新しいホストがクリティカルポートに接続しようとする、そのポートは再初期化され、接続されているすべてのホストがユーザ指定のアクセス VLAN に移動されます。

このコマンドは、すべてのホストモードでサポートされます。

アクセス不能認証バイパスの認証結果

アクセス不能認証バイパス機能の動作は、ポートの許可ステートにより異なります。

- クリティカルポートに接続されているホストが認証しようとする際にポートが無許可ですべてのサーバーが利用できない場合、スイッチは RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN にあるポートをクリティカル認証ステートにします。

- ポートが許可済みで、再認証が行われた場合、スイッチは現在の VLAN（事前に RADIUS サーバーにより割り当てられた）でクリティカルポートをクリティカル認証ステートにします。
- 認証交換中に RADIUS サーバーが利用不可能となった場合、現在の交換はタイムアウトとなり、スイッチは次の認証試行の間にクリティカルポートをクリティカル認証ステートとします。

RADIUS サーバが再び使用可能になったときにホストを再初期化し、クリティカル VLAN から移動するように、クリティカルポートを設定できます。このように設定した場合、クリティカル認証ステートのすべてのクリティカルポートは自動的に再認証されます。

アクセス不能認証バイパス機能の相互作用

アクセス不能認証バイパスは、次の機能と相互に作用します。

- **ゲスト VLAN** : アクセス不能認証バイパスは、ゲスト VLAN と互換性があります。ゲスト VLAN が 802.1x ポートでイネーブルの場合、この機能は次のように相互に作用します。
 - スイッチが EAP Request/Identity フレームへの応答を受信しないとき、または EAPOL パケットがクライアントによって送信されないときに、少なくとも 1 つの RADIUS サーバーが使用できれば、スイッチはクライアントにゲスト VLAN を割り当てます。
 - すべての RADIUS サーバーが使用できず、クライアントがクリティカルポートに接続されている場合、スイッチはクライアントを認証して、クリティカルポートを RADIUS 認証済み VLAN またはユーザー指定のアクセス VLAN でクリティカル認証ステートにします。
 - すべての RADIUS サーバーが使用できず、クライアントがクリティカルポートに接続されていない場合、ゲスト VLAN が設定されていても、スイッチはクライアントにゲスト VLAN を割り当てられません。
 - すべての RADIUS サーバーが使用できず、クライアントがクリティカルポートに接続されていて、すでにゲスト VLAN が割り当てられている場合、スイッチはそのポートをゲスト VLAN に保持します。
- **制限付き VLAN** : ポートがすでに制限付き VLAN で許可されていて RADIUS サーバーが使用できない場合、スイッチはクリティカルポートを制限付き VLAN でクリティカル認証ステートにします。
- **802.1x アカウンティング** : RADIUS サーバーが使用できない場合、アカウンティングは影響を受けません。
- **プライベート VLAN** : プライベート VLAN ホストポートにアクセス不能認証バイパスを設定できます。アクセス VLAN は、セカンダリ VLAN でなければなりません。
- **音声 VLAN** : アクセス不能認証バイパスは音声 VLAN と互換性がありますが、RADIUS 設定済み VLAN またはユーザー指定のアクセス VLAN は、音声 VLAN と異ならなければなりません。

- **Remote Switched Port Analyzer (RSPAN)** : アクセス不能認証バイパスの RADIUS 設定済み VLAN またはユーザ指定のアクセス VLAN として RSPAN VLAN を指定しないでください。

スイッチ スタックで、次の動作が発生します。

- キープアライブパケットを送信することによって、スタックのアクティブスイッチにより、RADIUS サーバーのステータスがチェックされます。RADIUS サーバーのステータスが変更されると、アクティブスイッチからメンバスイッチへ、情報が送信されます。クリティカルポートの再認証時に、メンバスイッチにより、RADIUS サーバーのステータスがチェックされます。
- 新しいアクティブスイッチが選択されると、スイッチスタックと RADIUS サーバーとの間のリンクが変更される可能性があり、新しいアクティブスイッチにより、キープアライブパケットがただちに送信され、RADIUS サーバーのステータスがアップデートされます。サーバーのステータスが *dead* から *alive* に変化すると、スイッチはクリティカル認証ステートの状態にあるすべてのスイッチ ポートを再認証します。

メンバスイッチがスタックに追加されると、アクティブスイッチからメンバスイッチへサーバーステータスが送信されます。

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、アクセス不能認証バイパス

VLAN 割り当て、ゲスト VLAN、制限付き VLAN、およびアクセス不能認証バイパス設定時の注意事項は、次のとおりです。

- 802.1x 認証をポート上でイネーブルにすると、音声 VLAN の機能を持つポート VLAN は設定できません。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x ゲスト VLAN として設定できます。ゲスト VLAN 機能は、内部 VLAN (ルーテッドポート) またはトランクポートではサポートされていません。アクセス ポート上でだけサポートされます。
- DHCP クライアントが接続されている 802.1x ポートのゲスト VLAN を設定した後、DHCP サーバからホスト IP アドレスを取得する必要があります。クライアント上の DHCP プロセスが時間切れとなり DHCP サーバーからホスト IP アドレスを取得しようとする前に、スイッチ上の 802.1x 認証プロセスを再起動する設定を変更できます。802.1x 認証プロセスの設定を減らします (**authentication timer inactivity** および **authentication timer reauthentication** インターフェイス コンフィギュレーション コマンド)。設定の減少量は、接続された 802.1x クライアントのタイプによって異なります。
- アクセス不能認証バイパス機能を設定する際には、次の注意事項に従ってください。
 - この機能はシングル ホスト モードおよびマルチホスト モードの 802.1x ポートでサポートされます。
 - Windows XP を稼働しているクライアントに接続されたポートがクリティカル認証ステートの場合、Windows XP はインターフェイスが認証されないと報告する場合があります。

- Windows XP クライアントで DHCP が設定され、DHCP サーバーからの IP アドレスがある場合、クリティカル ポートで EAP 認証成功メッセージを受信しても DHCP 設定プロセスを再初期化しません。
- アクセス不能認証バイパス機能および制限 VLAN を 802.1x ポート上に設定できます。スイッチが制限付き VLAN 内でクリティカル ポートを再認証しようとし、すべての RADIUS サーバーが利用不可能な場合、スイッチはポートステートをクリティカル認証ステートに変更し、制限付き VLAN に残ります。
- RSPAN VLAN または音声 VLAN を除くあらゆる VLAN を、802.1x 制限付き VLAN として設定できます。制限付き VLAN 機能は、内部 VLAN (ルーテッドポート) またはトランクポートではサポートされていません。アクセスポート上でだけサポートされます。

802.1x クリティカル音声 VLAN

ポートに接続されている IP フォンが Cisco Identity Services Engine (ISE) によって認証される際、その IP フォンは音声ドメインに参加します。ISE が到達不能である場合、スイッチはデバイスが音声デバイスなのかどうかを判断できません。サーバーが使用できない場合、電話機は音声ネットワークにアクセスできないため、動作できません。

データトラフィックの場合、アクセス不能認証バイパス (クリティカル認証) を設定し、サーバーが使用できない場合にトラフィックがネイティブ VLAN を通過できるようにすることができます。RADIUS 認証サーバーが使用できず (ダウンしていて)、アクセスできない認証バイパスがイネーブルの場合、スイッチは、クライアントにネットワークのアクセスを許可し、RADIUS 設定 VLAN またはユーザー指定アクセス VLAN でポートをクリティカル認証ステートにします。設定された RADIUS サーバーにスイッチが到達できず、新しいホストを認証できない場合、スイッチはこれらのホストをクリティカルポートに接続します。クリティカルポートに接続を試行している新しいホストは、ユーザー指定のアクセス VLAN (クリティカル VLAN) に移動され、制限付き認証を許可されます。



(注) クリティカル音声 VLAN のダイナミック割り当ては、ネストされたサービスプレートではサポートされません。そのため、デバイスはループ内で VLAN を連続的に切り替えます。

authentication event server dead action authorize voice インターフェイス コンフィギュレーション コマンドを使用して、クリティカル音声 VLAN 機能を設定できます。ISE が応答しない場合、ポートはクリティカル認証モードになります。ホストからのトラフィックが音声 VLAN でタグ付けされると、接続デバイス (電話機) は、ポートに対して設定された音声 VLAN に配置されます。IP フォンは Cisco Discovery Protocol (シスコデバイス) や LLDP または DHCP を介して音声 VLAN ID を学習します。

switchport voice vlan vlan-id インターフェイス コンフィギュレーション コマンドを入力して、ポートの音声 VLAN を設定できます。

この機能は、マルチドメイン モードおよびマルチ認証ホスト モードでサポートされます。スイッチがシングルホスト モードまたはマルチホスト モードの場合にコマンドを入力できます

が、デバイスがマルチドメインまたはマルチ認証ホストモードに変わらない限りコマンドは有効になりません。

音声 VLAN ポートを使用した IEEE 802.1x 認証

音声 VLAN ポートは特殊なアクセス ポートで、次の 2 つの VLAN ID が対応付けられています。

- IP Phone との間で音声トラフィックを伝送する VVID。VVID は、ポートに接続された IP Phone を設定するために使用されます。
- IP Phone を通じて、スイッチと接続しているワークステーションとの間でデータトラフィックを伝送する PVID。PVID は、ポートのネイティブ VLAN です。

ポートの許可ステートにかかわらず、IP Phone は音声トラフィックに対して VVID を使用します。これにより、IP Phone は IEEE 802.1x 認証とは独立して動作できます。

シングルホストモードでは、IP Phone だけが音声 VLAN で許可されます。マルチホストモードでは、サブリカントが PVID で認証された後、追加のクライアントがトラフィックを音声 VLAN 上で送信できます。マルチホストモードがイネーブルの場合、サブリカント認証は PVID と VVID の両方に影響します。

リンクがあるとき、音声 VLAN ポートはアクティブになり、IP Phone からの最初の Cisco Discovery Protocol メッセージを受け取るとデバイスの MAC アドレスが表示されます。Cisco IP Phone は、他のデバイスから受け取った Cisco Discovery Protocol メッセージをリレーしません。その結果、複数の IP Phone が直列に接続されている場合、スイッチは直接接続されている 1 台の IP Phone のみを認識します。音声 VLAN ポートで IEEE 802.1x 認証がイネーブルの場合、スイッチは 2 ホップ以上離れた認識されない IP Phone からのパケットをドロップします。

IEEE 802.1x 認証をスイッチポート上でイネーブルにすると、音声 VLAN でもあるアクセスポート VLAN を設定できます。

IP 電話がシングルホストモードで 802.1x 対応のスイッチポートに接続されている場合、スイッチは認証を行わずに電話ネットワークアクセスを承認します。ポートで Multidomain Authentication (MDA) を使用して、データデバイスと IP フォンなどの音声デバイスの両方を認証することを推奨します。



- (注) 音声 VLAN が設定され、Cisco IP Phone が接続されているアクセスポートで IEEE 802.1x 認証をイネーブルにした場合、Cisco IP Phone のスイッチへの接続が最大 30 秒間失われます。

WoL 機能を使用した IEEE 802.1x 認証

IEEE 802.1x 認証の Wake-on-LAN (WoL) 機能を使用すると、スイッチにマジックパケットと呼ばれる特定のイーサネットフレームを受信させて、休止状態の PC を起動させることができます。この機能は、管理者が休止状態のシステムへ接続しなければならない場合に役立ちます。

WoL を使用するホストが IEEE 802.1x ポートを通じて接続され、ホストの電源がオフになると、IEEE 802.1x ポートは無許可になります。無許可になったポートはEAPOL パケットしか送受信できないため、WoL マジック パケットはホストに届きません。さらに PC が休止状態になると、PC が認証されなくなるため、スイッチ ポートは閉じたままになります。

スイッチが WoL 機能を有効にした IEEE 802.1x 認証を使用している場合、スイッチはマジック パケットを含むトラフィックを無許可の IEEE 802.1x ポートに転送します。ポートが無許可の間、スイッチは EAPOL パケット以外の入力トラフィックをブロックし続けます。ホストはパケットを受信できますが、パケットをネットワーク内にある他のデバイスに送信できません。



(注) PortFast がポートでイネーブルになっていないと、そのポートは強制的に双方向ステートになります。

authentication control-direction in インターフェイス コンフィギュレーション コマンドを使用してポートを単方向として設定すると、ポートはスパンニングツリーフォワーディングステートに変更されます。ポートは、ホストにパケットを送信できますが、受信はできません。

authentication control-direction both インターフェイス コンフィギュレーション コマンドを使用してポートを双方向として設定すると、ポートは、両方向でアクセスコントロールされます。ポートは、ホストとの間でパケットを送受信しません。

柔軟な認証の順序設定

柔軟な認証の順序設定を使用して、ポートが新しいホストを認証するとき使用するの方法の順序を設定できます。The IEEE 802.1X の柔軟な認証機能では、以下の 3 つの認証方法をサポートしています。

- dot1X : IEEE 802.1X 認証はレイヤ 2 の認証方式です。
- mab : MAC 認証バイパスはレイヤ 2 の認証方式です。
- webauth : Web 認証はレイヤ 3 の認証方式です。

この機能を使用すると、各ポートでどの認証方式を使用するかを制御できます。また、そのポートの方式についてフェールオーバー順も制御できます。たとえば、MAC 認証バイパスおよび 802.1x は、プライマリまたはセカンダリ認証方法として使用し、Web 認証は、これらの認証のいずれか、または両方が失敗した場合のフォールバック方法として使用できます。

The IEEE 802.1X の柔軟な認証機能では、以下のホスト モードをサポートしています。

- multi-auth : マルチ認証では、音声 VLAN に 1 つの認証、データ VLAN に複数の認証を使用できます。
- multi-domain : マルチドメイン認証では、音声 VLAN に 1 つ、データ VLAN に 1 つ、計 2 つの認証を使用できます。

Open1x 認証

Open1x 認証によって、デバイスが認証される前に、そのデバイスがポートにアクセスできるようになります。オープン認証が設定されている場合、新しいホストはポートに定義されているアクセス コントロール リスト (ACL) に基づいてトラフィックを渡します。ホストが認証されると、RADIUS サーバに設定されているポリシーがそのホストに適用されます。

オープン認証を次の状況で設定できます。

- シングルホストモードでのオープン認証：1人のユーザーだけが認証の前後にネットワークにアクセスできます。
- MDA モードでのオープン認証：音声ドメインの1人のユーザーだけ、およびデータドメインの1人のユーザーだけが許可されます。
- マルチホストモードでのオープン認証：任意のホストがネットワークにアクセスできます。
- 複数認証モードでのオープン認証：MDAの場合と似ていますが、複数のホストを認証できます。



(注) オープン認証が設定されている場合は、他の認証制御よりも優先されます。これは、**authentication open** インターフェイス コンフィギュレーション コマンドを使用した場合、**authentication port-control** インターフェイス コンフィギュレーション コマンドに関係なく、ポートがホストにアクセス権を付与することを意味します。

マルチドメイン認証

スイッチはマルチドメイン認証 (MDA) をサポートしています。これにより、データ装置と IP Phone などの音声装置の両方を同じスイッチポート上で認証できます。ポートはデータドメインと音声ドメインに分割されます。



(注) すべてのホストモードで、ポートベース認証が設定されている場合、ラインプロトコルは許可の前にアップのままです。

MDA では、デバイス認証の順序が指定されません。ただし、最適な結果を得るには、MDA 対応のポート上のデータ デバイスよりも前に音声デバイスを認証することを推奨します。

MDA を設定するときには、次の注意事項に従ってください。

- MDA のスイッチ ポートを設定する必要があります。
- ホストモードがマルチドメインに設定されている場合、IP Phone の音声 VLAN を設定する必要があります。

- MDA 対応ポートでの音声 VLAN の割り当てはサポートされています。
- 音声デバイスを認可するには、値を *device-traffic-class=voice* に設定した Cisco 属性値 (AV) ペア属性を送信するように AAA サーバーを設定する必要があります。この値を使用しない場合、音声デバイスはデータ デバイスとして扱われます。



(注) *traffic-class=voice* が AAA サーバーから *service-template* としてダウンロードされると、音声ドメインではなくデータドメインでセッションが作成されます。

- ゲスト VLAN および制限付き VLAN 機能は、MDA 対応のポートのデータ デバイスだけに適用されます。許可に失敗した音声デバイスは、データ デバイスとして扱われます。
- 複数のデバイスでポートの音声またはデータドメインの許可を行おうとすると、*errordisable* になります。
- デバイスが許可されるまで、ポートはそのトラフィックをドロップします。他社製 IP Phone または音声デバイスはデータおよび音声 VLAN の両方に許可されます。データ VLAN では、音声デバイスを DHCP サーバーに接続して IP アドレスおよび音声 VLAN 情報を取得することができます。音声デバイスが音声 VLAN で送信を開始すると、データ VLAN へのアクセスはブロックされます。
- データ VLAN とバインドしている音声デバイス MAC アドレスは、ポートセキュリティ MAC アドレス制限にカウントされません。
- MDA では、IEEE 802.1x 認証をサポートしていないデバイスへのスイッチポートの接続を許可するフォールバック メカニズムとして、MAC 認証バイパスを使用できます。
- データまたは音声デバイスがポートで検出されると、認証に成功するまでその MAC アドレスがブロックされます。許可に失敗した場合、MAC アドレスが 5 分間ブロックされたままになります。
- ポートが未認証中に 6 つ以上のデバイスがデータ VLAN で検出された場合や、複数の音声デバイスが音声 VLAN で検出された場合、ポートは *errdisable* になります。
- ポートのホストモードをシングルホストモードまたはマルチホストモードからマルチドメインモードに変更すると、ポートでは許可されたデータ デバイスは許可されたままになります。ただし、ポートの音声 VLAN で許可されている Cisco IP Phone は自動的に削除されるので、そのポートでは再認証を行う必要があります。
- ゲスト VLAN や制限付き VLAN などのアクティブ フォールバック メカニズムは、ポートをシングルモードまたはマルチホストモードからマルチドメインモードに変更したあとも設定されたままになります。
- ポートのホストモードをマルチドメインモードからシングルモードまたはマルチホストモードに変更すると、許可されているすべてのデバイスがポートから削除されます。

- まずデータ ドメインを許可してゲスト VLAN に参加させる場合、IEEE 802.1x 非対応の音声デバイスは、音声 VLAN のパケットをタグ付けして、認証を開始する必要があります。
- MDA 対応ポートでは、ユーザー単位 ACL を推奨しません。ユーザー単位 ACL ポリシーを備えた、許可されたデバイスは、ポートの音声 VLAN とデータ VLAN の両方のトラフィックに影響を与えることがあります。このようなデバイスを使用する場合は、ポートでユーザー単位 ACL を適用するデバイスは 1 台だけにしてください。

Network Edge Access Topology を使用した 802.1x サプリカントおよびオーセンティケータスイッチ

Network Edge Access Topology (NEAT) 機能は、ワイヤリング クローゼット (会議室など) 外の領域まで識別を拡張します。これにより、任意のタイプのデバイスをポートで認証できます。

- 802.1x スイッチ サプリカント : 802.1x サプリカント機能を使用することで、別のスイッチの サプリカントとして機能するようにスイッチを設定できます。この設定は、たとえば、スイッチがワイヤリング クローゼット外にあり、トランクポートを介してアップストリーム スイッチに接続される場合に役に立ちます。802.1x スイッチ サプリカント機能を使用して設定されたスイッチは、セキュアな接続のためにアップストリーム スイッチで認証します。サプリカント スイッチが認証に成功すると、オーセンティケータ スイッチでポートモードがアクセスからトランクに変更されます。サプリカント スイッチでは、CISP を有効にするときに手動でトランクを設定する必要があります。
- アクセス VLAN は、オーセンティケータ スイッチで設定されている場合、認証が成功した後にトランク ポートのネイティブ VLAN になります。

デフォルトでは、BPDU ガードが有効にされたオーセンティケータ スイッチにサプリカントのスイッチを接続する場合、オーセンティケータのポートはサプリカント スイッチが認証する前に Spanning Tree Protocol (STP) のブリッジ プロトコル データ ユニット (BPDU) を受信した場合、errdisable 状態になる可能性があります。認証中にサプリカントのポートから送信されるトラフィックを制御できます。**dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証が完了する前にオーセンティケータ ポートがシャットダウンすることがないように、認証中に一時的にサプリカントのポートをブロックします。認証に失敗すると、サプリカントのポートが開きます。**no dot1x supplicant controlled transient** グローバル コンフィギュレーション コマンドを入力すると、認証期間中にサプリカント ポートが開きます。これはデフォルトの動作です。

BPDU ガードが **spanning-tree bpduguard enable** インターフェイス コンフィギュレーション コマンドによりオーセンティケータのスイッチ ポートで有効になっている場合、サプリカント スイッチで **dot1x supplicant controlled transient** コマンドを使用することを強く推奨します。



- (注) **spanning-tree portfast bpduguard default** グローバル コンフィギュレーション コマンドを使用して、グローバルにオーセンティケータ スイッチで BPDU ガードを有効にした場合、**dot1x supplicant controlled transient** コマンドを入力すると、BPDU の違反が避けられなくなります。

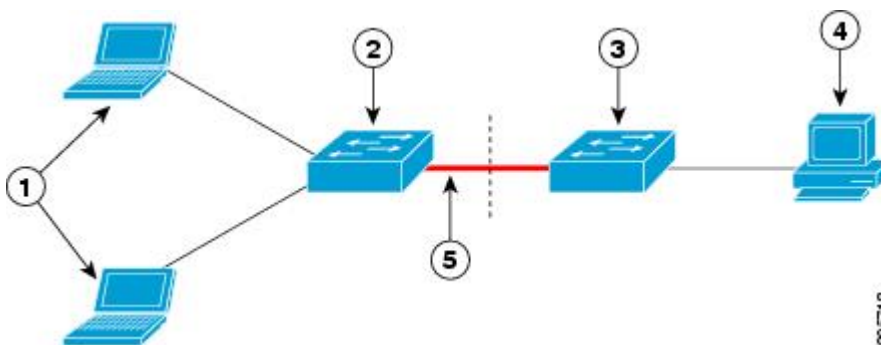
1 つ以上のサプリカントスイッチに接続するオーセンティケータ スイッチ インターフェイスでMDAまたはmultiauthモードをイネーブルにできます。マルチホストモードはオーセンティケータ スイッチ インターフェイスではサポートされていません。

インターフェイスで有効になっているシングルホストモードでオーセンティケータ スイッチをリブートすると、インターフェイスが認証前にerr-disabled状態に移行する場合があります。err-disabled 状態から回復するには、オーセンティケータ ポートをフラップしてインターフェイスを再度アクティブにし、認証を開始します。

すべてのホストモードで機能するように **dot1x supplicant force-multicast** グローバル コンフィギュレーション コマンドを Network Edge Access Topology (NEAT) のサプリカントスイッチで使用します。

- ホスト許可：許可済み（サプリカントでスイッチに接続する）ホストからのトラフィックだけがネットワークで許可されます。これらのスイッチは、Client Information Signalling Protocol (CISP) を使用して、サプリカントスイッチに接続する MAC アドレスをオーセンティケータ スイッチに送信します。
- 自動有効化：オーセンティケータ スイッチでのトランク コンフィギュレーションを自動的に有効化します。これにより、サプリカントスイッチから着信する複数のVLANのユーザートラフィックが許可されます。ISE で `cisco-av-pair` を `device-traffic-class=switch` として設定します（この設定は `group` または `user` 設定で行うことができます）。

図 5: CISP を使用したオーセンティケータまたはサプリカントスイッチ



| | | | |
|---|--------------------|---|----------------------------|
| 1 | ワークステーション (クライアント) | 2 | サプリカントスイッチ (ワイヤリングクローゼット外) |
| 3 | オーセンティケータ スイッチ | 4 | Cisco ISE |
| 5 | トランク ポート | | |



- (注) **switchport nonegotiate** コマンドは、NEAT を使用したサブリカントおよびオーセンティケータスイッチではサポートされません。このコマンドは、トポロジのサブリカント側で設定しないでください。オーセンティケータサーバ側で設定した場合は、内部マクロによってポートからこのコマンドが自動的に削除されます。

802.1x ユーザ ディストリビューション

802.1x ユーザ ディストリビューションを設定すると、複数の異なる VLAN で同じグループ名のユーザのロード バランシングを行うことができます。

VLAN は、RADIUS サーバにより提供されるか、VLAN グループ名でスイッチ CLI を介して設定します。

- RADIUS サーバを設定して、ユーザの複数の VLAN 名を送信します。複数の VLAN 名は、ユーザへの応答の一部として送信できます。802.1x ユーザ ディストリビューションは、特定の VLAN のすべてのユーザを追跡し、許可されたユーザをユーザ数が最も少ない VLAN に移動することでロード バランシングを行います。
- RADIUS サーバを設定してユーザの VLAN グループ名を送信します。VLAN グループ名は、ユーザへの応答の一部として送信できます。スイッチ CLI を使用して設定した VLAN グループ名で、選択された VLAN グループ名を検索できます。VLAN グループ名が検出されると、この VLAN グループ名で対応する VLAN を検索して、ユーザ数が最も少ない VLAN が検出されます。ロード バランシングは、対応する許可済みユーザをその VLAN に移動することで行われます。

RADIUS サーバが、承認の結果として属性の VLAN グループ名を送信するたびに、グループの中で最もユーザー数の少ない VLAN がエンドユーザーに割り当てられます。再認証の場合（認証セッションが存在する）、および CoA の場合（セッションアライブ）、グループ内で最もユーザー数の少ない VLAN でなくても、同じ VLAN が維持されます。



- (注) RADIUS サーバは、VLAN-ID、VLAN 名または VLAN グループを任意に組み合わせて VLAN 情報を送信できます。

802.1x ユーザ ディストリビューションの設定時の注意事項

- 少なくとも1つの VLAN が VLAN グループにマッピングされることを確認してください。
- 複数の VLAN を VLAN グループにマッピングできます。
- VLAN を追加または削除することで、VLAN グループを変更できます。
- 既存の VLAN を VLAN グループ名からクリアする場合、VLAN の認証済みポートはクリアされませんが、既存の VLAN グループからマッピングが削除されます。

- 最後の VLAN を VLAN グループ名からクリアすると、VLAN グループがクリアされます。
- アクティブ VLAN がグループにマッピングされても VLAN グループをクリアできます。VLAN グループをクリアすると、グループ内で任意の VLAN の認証ステートであるポートまたはユーザはクリアされませんが、VLAN の VLAN グループへのマッピングはクリアされます。

Network Admission Control レイヤ 2 IEEE 802.1x 検証

スイッチは、デバイスのネットワーク アクセスを許可する前にエンドポイント システムやクライアントのウイルス対策の状態またはポストチャを調べる Network Admission Control (NAC) レイヤ 2 IEEE 802.1x 検証をサポートしています。NAC レイヤ 2 IEEE 802.1x 検証を使用すると、以下の作業を実行できます。

- Session-Timeout RADIUS 属性（属性 [27]）と Termination-Action RADIUS 属性（属性 [29]）を認証サーバーからダウンロードします。
- Session-Timeout RADIUS 属性（属性 [27]）の値として再認証試行間の秒数を指定し、RADIUS サーバーからクライアントのアクセス ポリシーを取得します。
- スイッチが Termination-Action RADIUS 属性（属性 [29]）を使用してクライアントを再認証する際のアクションを設定します。値が *DEFAULT* であるか、値が設定されていない場合、セッションは終了します。値が RADIUS 要求の場合、再認証プロセスが開始します。
- VLAN の番号や名前、または VLAN グループ名のリストを Tunnel Group Private ID（属性 [81]）の値として設定し、VLAN の番号や名前、または VLAN グループ名のプリファレンスを Tunnel Preference（属性 [83]）の値として設定します。Tunnel Preference を設定しない場合、最初の Tunnel Group Private ID（属性 [81]）属性がリストから選択されます。
- NAC ポスチャトークンを表示します。これは、**show authentication** 特権 EXEC コマンドを使用して、クライアントのポストチャを示します。
- ゲスト VLAN としてセカンダリ プライベート VLAN を設定します。

NAC レイヤ 2 IEEE 802.1x 検証の設定は、RADIUS サーバーにポストチャ トークンを設定する必要があることを除いて、IEEE 802.1x ポートベース認証と似ています。

音声認識 802.1x セキュリティ



- (注) 音声認識 IEEE 802.1x 認証を使用するには、スイッチが LAN Base イメージを実行している必要があります。

音声認識 802.1x セキュリティ機能を使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにするようにスイッチを設定します。以

前のリリースでは、セキュリティ違反の原因であるデータ クライアントを認証しようとする
と、ポート全体がシャットダウンし、接続が完全に切断されます。

この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN で
セキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN
のトラフィックは中断することなくスイッチで送受信されます。

コモンセッション ID

認証マネージャは、使用された認証方式が何であれ、クライアントの単一のセッション ID（共
通セッション ID）を使用します。この ID は、表示コマンドや MIB などのすべてのレポートに
使用されます。セッション ID は、セッション単位のすべての Syslog メッセージに表示されま
す。

セッション ID には、次の情報が含まれます。

- ネットワーク アクセス デバイス (NAD) の IP アドレス
- 一意の 32 ビット整数（機械的に増加します）
- セッション開始タイム スタンプ（32 ビット整数）

次に、`show authentication` コマンドの出力に表示されたセッション ID の例を示します。この例
では、セッション ID は `160000050000000B288508E5` です。

```
Device# show authentication sessions
Interface  MAC Address      Method  Domain  Status      Session ID
Fa4/0/4    0000.0000.0203  mab     DATA   Authz Success 160000050000000B288508E5
```

次に、Syslog 出力にセッション ID が表示される例を示します。この例でも、セッション ID は
`160000050000000B288508E5` です。

```
1w0d: %AUTHMGR-5-START: Starting 'mab' for client (0000.0000.0203) on Interface Fa4/0/4
AuditSessionID 160000050000000B288508E5
1w0d: %MAB-5-SUCCESS: Authentication successful for client (0000.0000.0203) on Interface
Fa4/0/4 AuditSessionID 160000050000000B288508E5
1w0d: %AUTHMGR-7-RESULT: Authentication result 'success' from 'mab' for client
(0000.0000.0203) on Interface Fa4/0/4 AuditSessionID 160000050000000B288508E5
```

セッション ID は、NAD、AAA サーバー、その他のレポート分析アプリケーションでクライア
ントを識別するために使用されます。ID は自動的に表示されます。設定は必要ありません。

ポートあたりのデバイスの最大数

802.1x 対応のポートに接続できるデバイスの最大数です。

- シングル ホスト モードの場合、アクセス VLAN で接続できるデバイスは 1 台だけです。
ポートが音声 VLAN でも設定されている場合、音声 VLAN を介して送受信できる Cisco IP
Phone の数には制限はありません。

- マルチドメイン認証 (MDA) モードの場合、アクセス VLAN で 1 台のデバイス、音声 VLAN で 1 台の IP Phone が許可されます。
- マルチホストモードでは、1つの 802.1x サブリカントだけがポートで許可されますが、非 802.1x ホストは数に制限なく、アクセス VLAN で許可されます。音声 VLAN で許可されるデバイスの数には制限はありません。

802.1x ポートベース認証の設定方法

802.1X 認証の設定

ユーザー単位 ACL または VLAN 割り当てを可能にするには、AAA 許可をイネーブルにしてネットワーク関連のすべてのサービス要求に対してスイッチを設定する必要があります。

次に、802.1x の AAA プロセスを示します。

始める前に

802.1x ポートベース認証を設定するには、認証、許可、アカウンティング (AAA) をイネーブルにして認証方式リストを指定する必要があります。方式リストは、ユーザ認証のためにクエリー送信を行う手順と認証方式を記述したものです。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|----|
| ステップ 1 | ユーザーがスイッチのポートに接続します。 | |
| ステップ 2 | 認証が実行されます。 | |
| ステップ 3 | RADIUS サーバ設定に基づいて、VLAN 割り当てが適宜イネーブルになります。 | |
| ステップ 4 | スイッチが開始メッセージをアカウンティング サーバーに送信します。 | |
| ステップ 5 | 必要に応じて、再認証が実行されます。 | |
| ステップ 6 | スイッチが仮のアカウンティング アップデートを、再認証結果に基づいたアカウンティング サーバーに送信します。 | |
| ステップ 7 | ユーザーがポートから切断します。 | |
| ステップ 8 | スイッチが停止メッセージをアカウンティング サーバーに送信します。 | |

802.1x ポートベース認証の設定

802.1x ポートベースの認証を設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | aaa new-model 例： Device(config)# aaa new-model | AAA をイネーブルにします。 |
| ステップ 4 | aaa authentication dot1x{ default } method1 例： Device(config)# aaa authentication dot1x default group radius | 802.1x 認証方式リストを作成します。 authentication コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、 default キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方式リストは、自動的にすべてのポートに適用されます。 method1 には、 group radius キーワードを入力して、認証用のすべての RADIUS サーバリストを使用できるようにします。 (注) コマンドラインのヘルプストリングには他のキーワードも表示されますが、サポートされるのは group radius キーワードのみです。 |

| | コマンドまたはアクション | 目的 |
|---------|---|---|
| ステップ 5 | dot1x system-auth-control 例 : Device(config)# dot1x system-auth-control | スイッチで 802.1x 認証をグローバルに有効にします。 |
| ステップ 6 | aaa authorization network {default} group radius 例 : Device(config)# aaa authorization network default group radius | (任意) ユーザー単位 ACL や VLAN 割り当てなど、ネットワーク関連のすべてのサービス要求に対するユーザー RADIUS 許可をスイッチに設定します。 |
| ステップ 7 | radius server server name 例 : Device(config)# radius server rsim address ipv4 124.2.2.12 | (任意) RADIUS サーバーの IP アドレスを指定します。 |
| ステップ 8 | address {ipv4 ipv6} ip address 例 : Device(config-radius-server)# address ipv4 10.0.1.12 | RADIUS サーバーの IP アドレスを設定します。 |
| ステップ 9 | key string 例 : Device(config-radius-server)# key rad123 | (任意) RADIUS サーバー上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 |
| ステップ 10 | exit 例 : Device(config-radius-server)# exit | RADIUS サーバーモードを終了して、グローバル コンフィギュレーションモードを開始します。 |
| ステップ 11 | interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/2 | IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイスコンフィギュレーションモードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---------|---|---|
| ステップ 12 | switchport mode access 例： Device (config-if) # switchport mode access | (任意) ステップ 6 および 7 で RADIUS サーバを設定した場合のみ、ポートをアクセスモードに設定します。 |
| ステップ 13 | authentication port-control auto 例： Device (config-if) # authentication port-control auto | ポートでの 802.1x 認証を有効にします。 |
| ステップ 14 | dot1x pae authenticator 例： Device (config-if) # dot1x pae authenticator | インターフェイスのポートアクセスエンティティを、オーセンティケータとしてのみ動作し、サブリカント用のメッセージは無視するように設定します。 |
| ステップ 15 | end 例： Device (config-if) # end | インターフェイス コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

定期的な再認証の設定

802.1x クライアントの定期的な再認証をイネーブルにし、再認証の間隔を指定できます。再認証を行う間隔を指定しない場合、3600 秒おきに再認証が試みられます。

クライアントの定期的な再認証を有効にし、再認証が行われるまでの間隔 (秒) を設定するには、次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。 |
| ステップ 2 | configure terminal 例： | グローバル コンフィギュレーションモードを開始します。 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| | Device# configure terminal | |
| ステップ 3 | interface interface-id 例 : Device(config)# interface gigabitethernet 2/0/1 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | authentication periodic 例 : Device(config-if)# authentication periodic | クライアントの定期的な再認証（デフォルトではディセーブル）をイネーブルにします。 (注) デフォルト値は 3600 秒です。再認証タイマーの値を変更するか、スイッチに RADIUS-provided セッションタイムアウトを使用させるには、 authentication timer reauthenticate コマンドを入力します。 |
| ステップ 5 | authentication timer {[inactivity reauthenticate restart unauthorized]} {value}} 例 : Device(config-if)# authentication timer reauthenticate 180 | 再認証の試行の間隔（秒）を設定します。 authentication timer キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> • inactivity : クライアントからのアクティビティがなくなり無許可になるまでの間隔（秒） • reauthenticate : 自動再認証試行が開始されるまでの時間（秒） • restart value : 無許可ポートの認証の試行が行われるまでの間隔（秒） • unauthorized value : 不正セッションが削除されるまでの間隔（秒） このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 6 | end 例 : Device(config-if) # end | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

802.1x 違反モードの設定

次に示す状況で、シャットダウン、Syslogエラーを生成、または新しいデバイスからのパケットを廃棄するように 802.1x ポートを設定できます。

- デバイスが 802.1x 対応のポートに接続した
- ポートで認証されるデバイスの最大数に達した

スイッチ上にセキュリティ違反アクションを設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | aaa new-model 例 : Device(config)# aaa new-model | AAA をイネーブルにします。 |
| ステップ 4 | aaa authentication dot1x { default } method1 例 : Device(config)# aaa authentication dot1x default group radius | 802.1x 認証方式リストを作成します。 authentication コマンドにリストが指定されていない場合に使用するデフォルトのリストを作成するには、 default キーワードの後ろにデフォルト状況で使用される方式を指定します。デフォルトの方 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| | | <p>式リストは、自動的にすべてのポートに適用されます。</p> <p><i>method1</i> には、group radius キーワードを入力して、認証用のすべてのRADIUSサーバリストを使用できるようにします。</p> |
| ステップ 5 | interface interface-type interface-number 例： <pre>Device(config)# interface gigabitethernet 1/0/4</pre> | IEEE 802.1x 認証をイネーブルにするクライアントに接続しているポートを指定し、インターフェイスコンフィギュレーションモードを開始します。 |
| ステップ 6 | switchport mode access 例： <pre>Device(config-if)# switchport mode access</pre> | ポートをアクセスモードに設定します。 |
| ステップ 7 | authentication violation {shutdown restrict protect replace} 例： <pre>Device(config-if)# authentication violation restrict</pre> | <p>違反モードを設定します。キーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> • shutdown : エラーによってポートがディセーブルになります。 • restrict : Syslog エラーを生成します。 • protect : トラフィックをポートに送信するすべての新しいデバイスからパケットをドロップします。 • replace : 現在のセッションを削除し、新しいホストで認証します。 |
| ステップ 8 | end 例： <pre>Device(config-if)# end</pre> | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

待機時間の変更

スイッチはクライアントを認証できなかった場合に、所定の時間だけアイドル状態を続け、その後再び認証を試みます。**authentication timer restart** インターフェイス コンフィギュレーション コマンドは、アイドル状態の期間を制御します。認証が失敗する理由としては、クライアントが無効なパスワードを提示した場合などが考えられます。デフォルトよりも小さい値を入力することによって、ユーザへの応答時間を短縮できます。

待機時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet 2/0/1 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | authentication timer restart seconds 例： Device(config-if)# authentication timer restart 30 | クライアントとの認証のやり取りに失敗した場合に、スイッチが待機状態のままでの秒数を設定します。 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 60 秒です。 |
| ステップ 5 | end 例： Device(config-if)# end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 6 | show authentication sessions interface interface-id 例： | 入力を確認します。 |

| | コマンドまたはアクション | 目的 |
|--------|--|---------------------------------|
| | Device# show authentication sessions interface gigabitethernet2/0/1 | |
| ステップ 7 | copy running-config startup-config 例： Device# copy running-config startup-config | (任意) コンフィギュレーション ファイルに設定を保存します。 |

スイッチからクライアントへの再送信時間の変更

クライアントはスイッチからの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。スイッチがこの応答を受信できなかった場合、所定の時間（再送信時間）だけ待機し、その後フレームを再送信します。



- (注) このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバーの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチがクライアントからの通知を待機する時間を変更するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| | <code>gigabitethernet2/0/1</code> | |
| ステップ 4 | authentication timer reauthenticate <i>seconds</i> 例 : Device (config-if) # authentication timer reauthenticate 60 | スイッチが EAP-Request/Identity フレームに対するクライアントからの応答を待ち、要求を再送信するまでの秒数を設定します。 指定できる範囲は 1 ~ 65535 秒です。デフォルトは 5 秒です。 |
| ステップ 5 | end 例 : Device (config-if) # end | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 6 | show authentication sessions interface <i>interface-id</i> 例 : Device# show authentication sessions interface gigabitethernet 2/0/1 | 入力を確認します。 |
| ステップ 7 | copy running-config startup-config 例 : Device# copy running-config startup-config | (任意) コンフィギュレーションファイルに設定を保存します。 |

スイッチからクライアントへのフレーム再送信回数の設定

スイッチからクライアントへの再送信時間を変更できるだけでなく、(クライアントから応答が得られなかった場合に) スイッチが認証プロセスを再起動する前に、クライアントに EAP-Request/Identity フレームを送信する回数を変更できます。



- (注) このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバーの動作に問題がある場合など、異常な状況に対する調整を行う必要があるときに限って変更してください。

スイッチからクライアントへのフレーム再送信回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例： Device># enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet2/0/1 | 設定するポートを指定し、インターフェイス コンフィギュレーションモードを開始します。 |
| ステップ 4 | dot1x max-reauth-req count 例： Device(config-if)# dot1x max-reauth-req 5 | スイッチが認証処理を再開するまでに、クライアントへ EAP 要求/アイデンティティフレームを送信する回数を変更できます。指定できる範囲は 1～10 です。デフォルトは 2 です。 |
| ステップ 5 | end 例： Device(config-if)# end | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

ホストモードの設定

authentication port-control インターフェイス コンフィギュレーション コマンドが **auto** に設定されている IEEE 802.1x 許可ポート上で、複数のホスト（クライアント）を許可するには、特権 EXEC モードで次の手順を実行します。マルチドメイン認証（MDA）を設定してイネーブルにするには、**multi-domain** キーワードを使用します。これにより、ホストデバイス、および IP Phone（シスコ製または他社製）など音声デバイスの両方が同じスイッチポートで許可されます。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet 2/0/1 | 複数ホストが間接的に接続されているポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | authentication host-mode[multi-auth multi-domain multi-host single-host] 例： Device(config-if)# authentication host-mode multi-host | 単一の 802.1x 許可ポートで複数のホスト（クライアント）を許可することができます。 キーワードの意味は次のとおりです。 <ul style="list-style-type: none"> multi-auth : 音声 VLAN とデータ VLAN の両方で複数の認証クライアントを許可します。 (注) multi-auth キーワードは、authentication host-mode コマンドでのみ使用できます。 multi-host : シングルホストの認証後に 802.1x 許可ポートで複数のホスト（クライアント）の接続を許可します。 multi-domain : ホストデバイスと IP Phone（シスコ製または他社製）など音声デバイスの両方が、IEEE 802.1x 許可ポートで認証されるようにします。 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| | | <p>(注) ホストモードが multi-domain に設定されている場合、IP Phone の音声 VLAN を設定する必要があります。</p> <p>指定のインターフェイスに対し authentication port-control インターフェイス コンフィギュレーション コマンドが auto に設定されていることを確認してください。</p> |
| ステップ 5 | end 例 : Device(config-if)# end | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

MAC 移動のイネーブル化

MAC 移動を使用すると、認証されたホストをデバイスのポート間で移動できます。

デバイスで MAC 移動をグローバルに有効にするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | authentication mac-move permit 例 : Device(config)# authentication mac-move | デバイスで MAC 移動を有効にします。デフォルトは deny です。 セッション認識型ネットワークモードでは、デフォルト CLI は access-session |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | <code>permit</code> | mac-move deny です。セッション認識型ネットワークでMAC移動をイネーブルにするには、 no access-session mac-move グローバル コンフィギュレーション コマンドを使用します。 mac-move のデフォルト値は、レガシーモード (IBNS 1.0) の場合は deny で、C3PL モード (IBNS 2.0) の場合は permit です。 |
| ステップ 4 | end 例： Device(config)# end | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

MAC 置換のイネーブル化

MAC 置換を使用すると、ホストはポート上の認証ホストを置換できます。

インターフェイス上で MAC 置換をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Devic(config)# interface gigabitethernet2/0/2 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 4 | authentication violation {protect replace restrict shutdown} 例： <pre>Device(config-if)# authentication violation replace</pre> | インターフェイス上で MAC 置換をイネーブルにするには、 replace キーワードを使用します。ポートが現在のセッションを削除し、新しいホストを使用して認証を開始します。 他のキーワードは、次のような機能があります。 <ul style="list-style-type: none"> • protect : ポートは、システムメッセージを生成せずに、予期しない MAC を使用するパケットをドロップします。 • restrict : 違反パケットが CPU によってドロップされ、システムメッセージが生成されます。 • shutdown : ポートは、予期しない MAC アドレスを受信すると error disabled になります。 |
| ステップ 5 | end 例： <pre>Device(config-if)# end</pre> | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

802.1x アカウンティングの設定

802.1x アカウンティングを使用して、AAA システム アカウンティングをイネーブルにすると、ロギングのためにシステム リロード イベントをアカウンティング RADIUS サーバに送信できます。サーバは、アクティブな 802.1x セッションすべてが終了したものと判断します。



- (注) Cisco IOS XE Everest 16.6.x では、定期的な AAA アカウンティングのアップデートはサポートされていません。スイッチは、定期的な中間アカウンティングレコードをアカウンティングサーバに送信しません。定期的な AAA アカウンティングのアップデートは、Cisco IOS XE Fuji 16.9.x 以降のリリースで利用できます。

RADIUS は信頼性の低い UDP トランスポートプロトコルを使用するため、ネットワーク状態が良好でないと、アカウンティングメッセージが失われることがあります。設定した回数のアカウンティング要求の再送信後、スイッチが RADIUS サーバからアカウンティング応答メッセージを受信しない場合、次のメッセージが表示されます。

Accounting message %s for session %s failed to receive Accounting Response.

このストップメッセージが正常に送信されない場合、次のメッセージが表示されます。

00:09:55: %RADIUS-4-RADIUS_DEAD: RADIUS server 172.20.246.201:1645,1646 is not responding.



- (注) ログイングの開始、停止、仮のアップデートメッセージ、タイムスタンプなどのアカウンティングタスクを実行するように、RADIUSサーバを設定する必要があります。これらの機能をオンにするには、RADIUSサーバの [Network Configuration] タブの [Update/Watchdog packets from this AAA client] のログイングをイネーブルにします。次に、RADIUSサーバの [System Configuration] タブの [CVS RADIUS Accounting] をイネーブルにします。

AAA がスイッチでイネーブルになった後、802.1x アカウンティングを設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet 1/0/3 | 設定するポートを指定し、インターフェイス コンフィギュレーションモードを開始します。 |
| ステップ 4 | aaa accounting dot1x default start-stop group radius 例： Device(config-if)# aaa accounting dot1x default start-stop group radius | すべての RADIUS サーバのリストを使用して 802.1x アカウンティングをイネーブルにします。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 5 | aaa accounting system default start-stop group radius 例： <pre>Device(config-if)# aaa accounting system default start-stop group radius</pre> | (任意) システム アカウンティングをイネーブルにし (すべてのRADIUSサーバーのリストを使用)、スイッチがリロードするときにシステムアカウンティングリロードイベントメッセージを生成します。 |
| ステップ 6 | end 例： <pre>Device(config-if)# end</pre> | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

802.1x 準備状態チェックの設定

802.1x 準備状態チェックは、すべてのスイッチ ポートの 802.1x アクティビティをモニタリングし、802.1xをサポートするポートに接続されているデバイスの情報を表示します。この機能を使用して、スイッチ ポートに接続されているデバイスが 802.1x に対応できるかどうかを判別できます。

802.1x 準備状態チェックは、802.1x で設定できるすべてのポートで使用できます。準備状態チェックは、**dot1x force-unauthorized** として設定されるポートでは使用できません。

802.1x 準備状態チェックをスイッチでイネーブルにする場合には、次の手順に従ってください。

始める前に

準備状態チェックをスイッチでイネーブルにする場合、次の注意事項に従ってください。

- 準備状態チェックは通常、802.1x がスイッチでイネーブルにされる前に使用されます。
- インターフェイスを指定せずに **dot1x test eapol-capable** 特権 EXEC コマンドを使用すると、スイッチ スタックのすべてのポートがテストされます。
- **dot1x test eapol-capable** コマンドを 802.1x 対応のポートで設定し、リンクがアップになると、ポートは、802.1x に対応するかどうか、接続クライアントでクエリーを実行します。クライアントが通知パケットに応答すると、802.1x 対応です。クライアントがタイムアウト時間内に応答すると Syslog メッセージが生成されます。クライアントがクエリーに応答しない場合、クライアントは 802.1x 対応ではありません。Syslog メッセージは生成されません。
- 準備状態チェックは、複数のホスト (たとえば、IP Phone に接続される PC) を扱うポートに送信できます。Syslog メッセージは、タイマー時間内に準備状態チェックに応答する各クライアントに生成されます。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | dot1x test eapol-capable [interface interface-id] 例： Device# dot1x test eapol-capable interface gigabitethernet1/0/13 DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL capable | スイッチ上で 802.1x 準備状態チェックをイネーブルにします。 （任意） <i>interface-id</i> では、IEEE 802.1x の準備状態をチェックするポートを指定します。 （注） オプションの interface キーワードを省略した場合、スイッチのすべてのインターフェイスがテストされます。 |
| ステップ 3 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 4 | dot1x test timeout timeout 例： Device(config)# dot1x test timeout 54 | （任意）EAPOL 応答の待機に使用するタイムアウトを設定します。範囲は1～65535秒です。デフォルトは10秒です。 |
| ステップ 5 | end 例： Device(config)# end | グローバル コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

スイッチ/RADIUS サーバー間通信の設定

RADIUS サーバーのパラメータを設定するには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | ip radius source-interface vlan vlan interface number 例： Device(config)# ip radius source-interface vlan 80 | RADIUS パケットが、指定されたインターフェイスの IP アドレスを含むように指定します。 |
| ステップ 4 | radius server server name 例： Device(config)# radius server rsim address ipv4 172.16.0.1 | (任意) RADIUS サーバーの IP アドレスを指定します。 |
| ステップ 5 | address {ipv4 ipv6} ip address 例： Device(config-radius-server)# address ipv4 10.0.1.2 auth-port 1550 acct-port 1560 | RADIUS サーバーの IP アドレスを設定します。 |
| ステップ 6 | key string 例： Device(config-radius-server)# key rad123 | (任意) RADIUS サーバー上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 |
| ステップ 7 | exit 例： Device(config-radius-server)# exit | RADIUS サーバーモードを終了して、グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 8 | radius-server dead-criteria tries <i>num-tries</i> 例： Device(config)# radius-server dead-criteria tries 30 | RADIUS サーバーに送信されたメッセージへの応答がない場合に、このサーバーが非アクティブであると見なすまでの送信回数を指定します。指定できる <i>num-tries</i> の範囲は 1 ~ 100 です。 |
| ステップ 9 | end 例： Device(config)# end | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

再認証回数の設定

ポートが無許可ステートに変わる前に、デバイスが認証プロセスを再開する回数を変更することもできます。



- (注) このコマンドのデフォルト値は、リンクの信頼性が低下した場合や、特定のクライアントおよび認証サーバの動作に問題がある場合など、異常な状況に対する調整を行う必要がある際に限って変更してください。

再認証回数を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 3 | interface interface-id 例： Device# interface gigabitethernet2/0/1 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | switchport mode access 例： Device(config-if)# switchport mode access | RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。 |
| ステップ 5 | dot1x max-req count 例： Device(config-if)# dot1x max-req 4 | ポートが無許可ステートに変わる前に、デバイスが認証プロセスを再開する回数を設定します。指定できる範囲は 0 ~ 10 です。デフォルトは 2 です。 |
| ステップ 6 | end 例： Device(config-if)# end | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

ゲスト VLAN の設定

サーバが EAP Request/Identity フレームに対する応答を受信しない場合、ゲスト VLAN を設定すると、802.1x 対応でないクライアントはゲスト VLAN に配置されます。802.1x 対応であっても、認証に失敗したクライアントは、ネットワークへのアクセスが許可されません。スイッチは、シングルホストモードまたはマルチホストモードでゲスト VLAN をサポートします。

ゲスト VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet 2/0/2 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | dot1x port-control auto 例： Device(config-if)# dot1x port-control auto | ポートでの 802.1x 認証をイネーブルにします。 |
| ステップ 5 | authentication event no-response action authorize vlan vlan-id 例： Device(config-if)# authentication event no-response action authorize vlan 2 | アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッドポート)、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。 |
| ステップ 6 | end 例： Device(config-if)# end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

制限付き VLAN の設定

デバイスに制限付き VLAN を設定すると、認証サーバが有効なユーザ名とパスワードを受信しなかった場合、IEEE 802.1x 準拠のクライアントが制限付き VLAN に移動します。デバイスは、シングルホストモードでのみ制限付き VLAN をサポートします。

制限付き VLAN を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet 2/0/2 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | authentication port-control auto 例： Device(config-if)# authentication port-control auto | ポートでの 802.1x 認証をイネーブルにします。 |
| ステップ 5 | authentication event fail action authorize vlan vlan-id 例： Device(config-if)# authentication event fail action authorize vlan 2 | アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN（ルーテッドポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。 |
| ステップ 6 | end 例： Device(config-if)# end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

制限付き VLAN の認証試行回数の設定

ユーザーに制限付き VLAN を割り当てる前に、**authentication event fail retry retry count** インターフェイス コンフィギュレーション コマンドを使用して、認証試行回数を最大に設定できます。指定できる試行回数は 1 ~ 3 です。デフォルトは 3 回に設定されています。

認証試行回数を最大に設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none">パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet 2/0/3 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | authentication port-control auto 例： Device(config-if)# authentication port-control auto | ポートでの 802.1x 認証をイネーブルにします。 |
| ステップ 5 | authentication event fail action authorize vlan vlan-id 例： Device(config-if)# authentication event fail action authorize vlan 8 | アクティブ VLAN を 802.1x 制限付き VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN（ルーテッドポート）、RSPAN VLAN または音声 VLAN を除き、任意のアクティブ VLAN を 802.1x 制限 VLAN として設定できます。 |
| ステップ 6 | authentication event fail retry retry count 例： Device(config-if)# authentication event fail retry 2 | |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 7 | end 例 : Device(config-if) # end | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

クリティカル音声 VLAN を使用した 802.1x アクセス不能認証バイパスの設定

ポートにクリティカル音声 VLAN を設定し、アクセス不能認証バイパス機能をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | aaa new-model 例 : Device(config) # aaa new-model | AAA をイネーブルにします。 |
| ステップ 4 | radius-server dead-criteria {time seconds} [tries number] 例 : Device(config) # radius-server dead-criteria time 20 tries 10 | RADIUS サーバーが使用不可またはダウン（切断）と見なされる条件を設定します。 <ul style="list-style-type: none"> time : 1 ~ 120 秒。スイッチは、デフォルトの <i>seconds</i> 値を 10 ~ 60 の間で動的に決定します。 number : 1 ~ 100 の試行回数。スイッチは、デフォルトの <i>triesnumber</i> を 10 ~ 100 の間で動的に決定します。 |

| | コマンドまたはアクション | 目的 |
|---------|--|---|
| ステップ 5 | radius-serverdeadtime 分 例 : Device (config) # radius-server deadtime 60 | (任意) RADIUS サーバに要求が送信されない分数を設定します。指定できる範囲は 0 ~ 1440 分 (24 時間) です。デフォルト値は 0 分です。 |
| ステップ 6 | radius server <i>server name</i> 例 : Device (config) # radius server rsim address ipv4 124.2.2.12 | (任意) RADIUS サーバーの IP アドレスを指定します。 |
| ステップ 7 | address {ipv4 ipv6} ip address auth-port port_number acct-port port_number 例 : Device (config-radius-server) # address ipv4 10.0.1.2 auth-port 1550 acct-port 1560 | RADIUS サーバーの IP アドレスを設定します。 |
| ステップ 8 | key string 例 : Device (config-radius-server) # key rad123 | (任意) RADIUS サーバー上で動作する RADIUS デーモンとスイッチの間で使用する認証および暗号キーを指定します。 |
| ステップ 9 | exit 例 : Device (config-radius-server) # exit | RADIUS サーバーモードを終了して、グローバル コンフィギュレーションモードを開始します。 |
| ステップ 10 | dot1x critical {eapol recovery delay milliseconds} 例 : Device (config) # dot1x critical eapol Device (config) # dot1x critical recovery delay 2000 | (任意) アクセス不能認証バイパスのパラメータを設定します。 <ul style="list-style-type: none"> • eapol : スイッチがクリティカルポートを正常に認証すると、スイッチが EAPOL 成功メッセージを送信するように指定します。 • recovery delay milliseconds : 使用できない RADIUS サーバーが使用できるようになったときに、スイッチがクリティカルポートを再初期化するために待機する回復遅延期 |

| | コマンドまたはアクション | 目的 |
|---------|--|---|
| | | 間を設定します。指定できる範囲は 1 ～ 10000 ミリ秒です。デフォルトは 1000 ミリ秒です（ポートは毎秒再初期化できます）。 |
| ステップ 11 | interface <i>interface-id</i> 例： <pre>Device(config)# interface gigabitethernet 1/0/1</pre> | 設定するポートを指定し、インターフェイスコンフィギュレーションモードを開始します。 |
| ステップ 12 | authentication event server dead action {authorize reinitialize} vlan <i>vlan-id</i> 例： <pre>Device(config-if)# authentication event server dead action reinitialicze vlan 20</pre> | これらのキーワードを使用して、RADIUS サーバが到達不能な場合にポートでホストを移動します。 <ul style="list-style-type: none"> • authorize : 認証しようとする新しいホストをユーザー指定のクリティカル VLAN に移動します。 • reinitialize : ポートのすべての許可済みホストをユーザー指定のクリティカル VLAN に移動します。 |
| ステップ 13 | switchport voice vlan <i>vlan-id</i> 例： <pre>Device(config-if)# switchport voice vlan</pre> | ポートの音声 VLAN を指定します。音声 VLAN はステップ 6 で設定されたクリティカルデータ VLAN と同じにはできません。 |
| ステップ 14 | authentication event server dead action authorize voice 例： <pre>Device(config-if)# authentication event server dead action authorize voice</pre> | RADIUS サーバが到達不能な場合、ポートのデータトラフィックを音声 VLAN に移動するために、クリティカル音声 VLAN を設定します。 |
| ステップ 15 | end 例： <pre>Device(config-if)# end</pre> | インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 16 | show authentication interface <i>interface-id</i> 例： | (任意) 設定を確認します。 |

| | コマンドまたはアクション | 目的 |
|--|---|----|
| | Device(config-if)# show authentication interface gigabitethernet 1/0/1 | |

例

RADIUS サーバーのデフォルト設定に戻すには、**no radius-server dead-criteria**、**no radius-server deadtime**、および **no radius-server** グローバル コンフィギュレーション コマンドを使用します。アクセス不能な認証バイパスをディセーブルにするには、**no authentication event server dead action** インターフェイス コンフィギュレーション コマンドを使用します。クリティカル音声 VLAN をディセーブルにするには、**authentication event server dead action authorize voice** インターフェイス コンフィギュレーション コマンドを使用します。

WoL を使用した 802.1x 認証の設定

WoL を使用した 802.1x 認証をイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet2/0/3 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | authentication control-direction {both in} 例： | ポートで WoL を使用して 802.1x 認証をイネーブルにし、次のキーワードを使用 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| | <pre>Device(config-if)# authentication control-direction both</pre> | <p>してポートを双方向または単方向に設定します。</p> <ul style="list-style-type: none"> • both : ポートを双方向に設定します。ポートは、ホストにパケットを送受信できません。デフォルトでは、ポートは双方向です。 • in : ポートを単方向に設定します。ポートは、ホストにパケットを送信できますが、受信はできません。 |
| ステップ 5 | <p>end</p> <p>例 :</p> <pre>Device(config-if)# end</pre> | <p>インターフェイスコンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。</p> |
| ステップ 6 | <p>show authentication sessions interface interface-id</p> <p>例 :</p> <pre>Device# show authentication sessions interface gigabitethernet2/0/3</pre> | <p>インターフェイスの現在の認証マネージャセッションに関する情報を表示します。</p> |

MAC 認証バイパスの設定

MAC 認証バイパスをイネーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | <p>enable</p> <p>例 :</p> <pre>Device> enable</pre> | <p>特権 EXEC モードを有効にします。</p> <ul style="list-style-type: none"> • パスワードを入力します (要求された場合)。 |
| ステップ 2 | <p>configure terminal</p> <p>例 :</p> <pre>Device# configure terminal</pre> | <p>グローバル コンフィギュレーションモードを開始します。</p> |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 3 | interface interface-id 例 : Device(config)# interface gigabitethernet 2/0/1 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | authentication port-control auto 例 : Device(config-if) # authentication port-control auto | ポートでの 802.1x 認証をイネーブルにします。 |
| ステップ 5 | mab [eap] 例 : Device(config-if) # mab | MAC 認証バイパスをイネーブルにします。 (任意) eap キーワードを使用して、許可に EAP を使用できるようにデバイスを設定します。 |
| ステップ 6 | end 例 : Device(config-if) # end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

802.1x ユーザー ディストリビューションの設定

VLAN グループを設定して、VLAN をそのグループにマッピングするには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 3 | vlan group <i>vlan-group-name</i> vlan-list vlan-list 例 : Device(config)# vlan group eng-dept vlan-list 10 | VLAN グループを設定し、単一の VLAN または VLAN の範囲をそのグループにマッピングします。 |
| ステップ 4 | no vlan group <i>vlan-group-name</i> vlan-list vlan-list 例 : Device(config)# no vlan group eng-dept vlan-list 10 | VLAN グループ コンフィギュレーションまたは VLAN グループ コンフィギュレーションの要素をクリアします。 |
| ステップ 5 | end 例 : Device(config)# end | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

NAC レイヤ 2 802.1x 検証の設定

NAC レイヤ 2 802.1x 検証を設定できます。これは、RADIUS サーバーを使用した 802.1x 認証とも呼ばれます。

NAC レイヤ 2 802.1x 検証を設定するには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例 : Device> enable | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none"> パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 3 | interface interface-id 例 : Device(config)# interface gigabitethernet2/0/3 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | switchport mode access 例 : Device(config-if)# switchport mode access | RADIUS サーバを設定した場合に限り、ポートをアクセスモードに設定します。 |
| ステップ 5 | authentication event no-response action authorize vlan vlan-id 例 : Device(config-if)# authentication event no-response action authorize vlan 8 | アクティブ VLAN を 802.1x ゲスト VLAN として指定します。指定できる範囲は 1 ~ 4094 です。 内部 VLAN (ルーテッドポート)、RSPAN VLAN、音声 VLAN を除くあらゆるアクティブ VLAN を 802.1x ゲスト VLAN として設定できます。 |
| ステップ 6 | authentication periodic 例 : Device(config-if)# authentication periodic | クライアントの定期的な再認証 (デフォルトではディセーブル) をイネーブルにします。 |
| ステップ 7 | authentication timer reauthenticate 例 : Device(config-if)# authentication timer reauthenticate | クライアントに対する再認証試行を設定します (1 時間に設定)。 このコマンドがスイッチの動作に影響するのは、定期的な再認証をイネーブルに設定した場合だけです。 |
| ステップ 8 | end 例 : Device(config-if)# end | インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 9 | show authentication sessions interface interface-id 例 : Device# show authentication sessions | インターフェイスの現在の認証マネージャセッションに関する情報を表示します。 |

| | コマンドまたはアクション | 目的 |
|--|---|----|
| | <code>interface gigabitethernet2/0/3</code> | |

NEAT を使用したオーセンティケータ スイッチの設定

この機能を設定するには、ワイヤリングクローゼット外の1つのスイッチがサブリカントとして設定され、オーセンティケータ スイッチに接続されている必要があります。



- (注)
- CISP または NEAT セッションがアクティブなときにラインカードを取り外してシャーシに挿入する場合は、オーセンティケータ スイッチ インターフェイスの設定を明示的にフラッピングすることによって、アクセスモードに復元する必要があります。
 - `cisco-av-pairs` は、ISE で `device-traffic-class=switch` として設定されている必要があります。これにより、サブリカントが正常に認証された後でトランクとしてインターフェイスが設定されます。

スイッチをオーセンティケータに設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例： <code>Device> enable</code> | 特権 EXEC モードを有効にします。 <ul style="list-style-type: none">• パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： <code>Device# configure terminal</code> | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | cisp enable 例： <code>Device(config)# cisp enable</code> | CISP をイネーブルにします。 |
| ステップ 4 | interface interface-id 例： <code>Device(config)# interface</code> | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| | <code>gigabitethernet 2/0/1</code> | |
| ステップ 5 | switchport mode access 例： Device(config-if)# switchport mode access | ポートモードを access に設定します。 |
| ステップ 6 | authentication port-control auto 例： Device(config-if)# authentication port-control auto | ポート認証モードを auto に設定します。 |
| ステップ 7 | dot1x pae authenticator 例： Device(config-if)# dot1x pae authenticator | インターフェイスをポート アクセス エンティティ (PAE) オーセンティケータとして設定します。 |
| ステップ 8 | spanning-tree portfast 例： Device(config-if)# spanning-tree portfast trunk | 単一ワーク ステーションまたはサーバに接続されたアクセス ポート上で Port Fast をイネーブルにします。 |
| ステップ 9 | end 例： Device(config-if)# end | インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

NEAT を使用したサブリカント スイッチの設定

スイッチをサブリカントに設定するには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---------------------|--|
| ステップ 1 | enable 例： | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | Device> enable | |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | cisp enable 例： Device(config)# cisp enable | CISP をイネーブルにします。 |
| ステップ 4 | dot1x credentials profile 例： Device(config)# dot1x credentials test | 802.1x クレデンシャルプロファイルを作成します。これは、サブリカントとして設定されるポートに接続する必要があります。 |
| ステップ 5 | username suppswitch 例： Device(config)# username suppswitch | ユーザ名を作成します。 |
| ステップ 6 | password password 例： Device(config)# password myswitch | 新しいユーザ名のパスワードを作成します。 |
| ステップ 7 | dot1x supplicant force-multicast 例： Device(config)# dot1x supplicant force-multicast | ユニキャストまたはマルチキャストパケットのいずれかを受信した場合にスイッチに強制的にマルチキャスト EAPOL だけを送信させます。 これにより、NEAT がすべてのホストモードでのサブリカントスイッチで機能できるようにもなります。 |
| ステップ 8 | interface interface-id 例： Device(config)# interface gigabitethernet1/0/1 | 設定するポートを指定し、インターフェイスコンフィギュレーションモードを開始します。 |

| | コマンドまたはアクション | 目的 |
|---------|--|--|
| ステップ 9 | switchport trunk encapsulation dot1q 例 : Device (config-if) # switchport trunk encapsulation dot1q | ポートをトランク モードに設定します。 |
| ステップ 10 | switchport mode trunk 例 : Device (config-if) # switchport mode trunk | インターフェイスを VLAN トランク ポートとして設定します。 |
| ステップ 11 | dot1x pae supplicant 例 : Device (config-if) # dot1x pae supplicant | インターフェイスをポートアクセスエンティティ (PAE) サプリカントとして設定します。 |
| ステップ 12 | dot1x credentials profile-name 例 : Device (config-if) # dot1x credentials test | 802.1x クレデンシャルプロファイルをインターフェイスに対応付けます。 |
| ステップ 13 | end 例 : Device (config-if) # end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

ダウンロード可能 ACL およびリダイレクト URL を使用した 802.1x 認証の設定



(注) スイッチにダウンロードする前に、ダウンロード可能な ACL を ACS で設定する必要があります。

ポートでの認証後、**show ip access-list** 特権 EXEC コマンドを使用して、ポートにダウンロードした ACL を表示できます。



- (注) **show ip access-lists interface** コマンドの出力には、dACL フィルタ ID や ACL フィルタ ID は表示されません。これは、物理インターフェイスではなく、各認証セッションのマルチドメイン認証によって作成された仮想ポートに ACL が接続されるためです。dACL フィルタ ID や ACL フィルタ ID を表示するには、**show ip access-lists access-list-name** コマンドを使用します。**access-list-name** は、**show access-session interface interface-name detail** コマンドの出力から取得する必要があります。**access-list-name** では大文字と小文字が区別されます。

ダウンロード可能な ACL の設定

これらのポリシーは、クライアントが認証され、クライアント IP アドレスが IP デバイストラッキングテーブルに追加された後で有効になります。その後スイッチがダウンロード可能な ACL をポートに適用します。

特権 EXEC モードで次の手順を実行します。

始める前に

SISF ベースのデバイストラッキングは、802.1x 認証を設定するための前提条件です。デバイストラッキングをプログラムまたは手動で有効にしていることを確認します。詳細については、「SISF ベースのトラッキングの設定」の章を参照してください。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | aaa new-model 例： Device(config)# aaa new-model | AAA をイネーブルにします。 |
| ステップ 4 | aaa authorization network default local group radius 例： | 許可の方法をローカルに設定します。認可方式を削除するには、 no aaa |

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| | Device(config)# aaa authorization network default local group radius | authorization network default local group radius コマンドを使用します。 |
| ステップ 5 | radius-server vsa send authentication 例： Device(config)# radius-server vsa send authentication | RADIUS VSA 送信認証を設定します。 |
| ステップ 6 | interface interface-id 例： Device(config)# interface gigabitethernet2/0/4 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 7 | ip access-group acl-id in 例： Device(config-if)# ip access-group default_acl in | ポートの入力方向のデフォルト ACL を設定します。 (注) <i>acl-id</i> はアクセスリストの名前または番号です。 |
| ステップ 8 | end 例： Device(config-if)# end | インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

ダウンロードポリシーの設定

始める前に

SISF ベースのデバイストラッキングは、802.1x 認証を設定するための前提条件です。デバイストラッキングをプログラムまたは手動で有効にしていることを確認します。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|--------|---|---|
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | access-list access-list-number { deny permit } { hostname any host } log 例 : Device(config)# access-list 1 deny any log | デフォルトポートACLを定義します。 access-list-number には、1 ~ 99 または 1300 ~ 1999 の 10 進数を指定します。 条件が一致した場合にアクセスを拒否する場合は deny を指定し、許可する場合は permit を指定します。 source は、次のようなパケットを送信するネットワークまたはホストの送信元アドレスです。 <ul style="list-style-type: none"> • hostname : ドット付き 10 進表記による 32 ビット長の値。 • any : source および source-wildcard の値 0.0.0.0 255.255.255.255 の省略形を意味するキーワード any。source-wildcard 値を入力する必要はありません。 • host : source および source-wildcard の値 source 0.0.0.0 の省略形を意味するキーワード host。 (任意) source-wildcard ビットを送信元アドレスに適用します。 (任意) ログを入力して、エントリと一致するパケットに関する情報ロギングメッセージをコンソールに送信します。 |
| ステップ 4 | interface interface-id 例 : Device(config)# interface gigabitethernet 2/0/2 | インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 5 | ip access-group acl-id in 例 : | ポートの入力方向のデフォルト ACL を設定します。 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| | Device(config-if)# ip access-group default_acl in | (注) <i>acl-id</i> はアクセスリストの名前または番号です。 |
| ステップ6 | exit 例： Device(config-if)# exit | インターフェイス コンフィギュレーションモードを終了し、グローバルコンフィギュレーションモードに戻ります。 |
| ステップ7 | aaa new-model 例： Device(config)# aaa new-model | AAA をイネーブルにします。 |
| ステップ8 | aaa authorization network default group radius 例： Device(config)# aaa authorization network default group radius | 許可の方法をローカルに設定します。認可方式を削除するには、 no aaa authorization network default group radius コマンドを使用します。 |
| ステップ9 | radius-server vsa send authentication 例： Device(config)# radius-server vsa send authentication | ベンダー固有属性を認識し使用するために、ネットワークアクセスサーバーを設定します。 (注) ダウンロード可能な ACL が機能する必要があります。 |
| ステップ10 | end 例： Device(config)# end | グローバル コンフィギュレーションモードを終了し、特権 EXEC モードに戻ります。 |

VLAN ID ベース MAC 認証の設定

特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | mab request format attribute 32 vlan access-vlan 例： Device(config)# mab request format attribute 32 vlan access-vlan | VLAN ID ベース MAC 認証をイネーブルにします。 |
| ステップ 4 | end 例： Device(config)# end | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

柔軟な認証順序の設定

下の手順で使用される例は、MAB が IEEE 802.1x 認証 (dot1x) の前に試行されるように柔軟な認証の順序設定の順序を変更します。MAB は最初の認証方式として設定されているため、MAB は他のすべての認証方式よりも優先されます。

特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |

| | コマンドまたはアクション | 目的 |
|--------|--|--|
| ステップ 2 | configure terminal 例 : Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例 : Device(config)# interface gigabitethernet 1/0/1 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | switchport mode access 例 : Device(config-if)# switchport mode access | RADIUS サーバを事前に設定した場合に限り、ポートをアクセス モードに設定します。 |
| ステップ 5 | authentication order [dot1x mab] {webauth} 例 : Device(config-if)# authentication order mab dot1x | (任意) ポート上で使用される認証方式の順序を設定します。 |
| ステップ 6 | authentication priority [dot1x mab] {webauth} 例 : Device(config-if)# authentication priority mab dot1x | (任意) 認証方式をポート プライオリティ リストに追加します。 |
| ステップ 7 | end 例 : Device(config-if)# end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

Open1x の設定

ポートの許可ステータスの手動制御をイネーブルにするには、特権 EXEC モードで次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーションモードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet 1/0/1 | 設定するポートを指定し、インターフェイスコンフィギュレーションモードを開始します。 |
| ステップ 4 | switchport mode access 例： Device(config-if)# switchport mode access | RADIUS サーバを設定した場合に限り、ポートをアクセスモードに設定します。 |
| ステップ 5 | authentication control-direction {both in} 例： Device(config-if)# authentication control-direction both | (任意) ポート制御を単一方方向モードまたは双方向モードに設定します。 |
| ステップ 6 | authentication fallback name 例： Device(config-if)# authentication fallback profile1 | (任意) 802.1x 認証をサポートしないクライアント用のフォールバック方法として Web 認証を使用するようポートを設定します。 |
| ステップ 7 | authentication host-mode[multi-auth multi-domain multi-host single-host] 例： Device(config-if)# authentication | (任意) ポート上で認証マネージャモードを設定します。 |

| | コマンドまたはアクション | 目的 |
|---------|--|--|
| | <code>host-mode multi-auth</code> | |
| ステップ 8 | authentication open 例： <pre>Device(config-if)# authentication open</pre> | (任意) ポート上でオープンアクセスをイネーブルまたはディセーブルにします。 |
| ステップ 9 | authentication order [dot1x mab] {webauth} 例： <pre>Device(config-if)# authentication order dot1x webauth</pre> | (任意) ポート上で使用される認証方式の順序を設定します。 |
| ステップ 10 | authentication periodic 例： <pre>Device(config-if)# authentication periodic</pre> | (任意) ポート上で再認証をイネーブルまたはディセーブルにします。 |
| ステップ 11 | authentication port-control {auto force-authorized force-un authorized} 例： <pre>Device(config-if)# authentication port-control auto</pre> | (任意) ポートの許可状態の手動制御をイネーブルにします。 |
| ステップ 12 | end 例： <pre>Device(config-if)# end</pre> | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

ポート上での 802.1x 認証の無効化

802.1x 認証をポートでディセーブルにするには、**no dot1x pae** インターフェイス コンフィギュレーション コマンドを使用します。

ポートで 802.1x 認証をディセーブルにするには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet 2/0/1 | 設定するポートを指定し、インターフェイス コンフィギュレーション モードを開始します。 |
| ステップ 4 | switchport mode access 例： Device(config-if)# switchport mode access | (任意) RADIUS サーバを設定した場合に限り、ポートをアクセス モードに設定します。 |
| ステップ 5 | no dot1x pae authenticator 例： Device(config-if)# no dot1x pae authenticator | ポートでの 802.1x 認証をディセーブルにします。 |
| ステップ 6 | end 例： Device(config-if)# end | インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

802.1x 認証設定のデフォルト値へのリセット

802.1x 認証設定をデフォルト値に戻すには、特権 EXEC モードで次の手順を実行します。この手順は任意です。

手順

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | interface interface-id 例： Device(config)# interface gigabitethernet 1/0/2 | インターフェイスコンフィギュレーション モードを開始し、設定するポートを指定します。 |
| ステップ 4 | dot1x default 例： Device(config-if)# dot1x default | 設定可能な 802.1x のパラメータをデフォルト値へ戻します。 |
| ステップ 5 | end 例： Device(config-if)# end | インターフェイスコンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |

音声認識 802.1x セキュリティの設定

音声認識 802.1x セキュリティ機能をデバイスで使用して、セキュリティ違反が発生した場合にデータまたは音声 VLAN に関係なく VLAN だけをディセーブルにします。この機能は、PC が IP Phone に接続されている IP Phone 環境で使用できます。データ VLAN でセキュリティ違反が検出されると、データ VLAN だけがシャットダウンされます。音声 VLAN のトラフィックは中断することなくデバイスで送受信されます。

デバイスで音声認識 802.1x 音声セキュリティを設定する場合、次の注意事項に従ってください。

- 音声認識 802.1x セキュリティをイネーブルにするには、**errdisable detect cause security-violation shutdown vlan** グローバル コンフィギュレーション コマンドを入力します。音声認識 802.1x セキュリティをディセーブルにするには、このコマンドの **no** バー

ジョンを入力します。このコマンドは、デバイスの 802.1x 設定ポートのすべてに適用されます。



(注) **shutdown vlan** キーワードを指定しない場合、**error-disabled** ステータスになった際にポート全体がシャットダウンされます。

- **errdisable recovery cause security-violation** グローバル コンフィギュレーション コマンドを使用して、**error-disabled** リカバリを設定すると、ポートは自動的に再びイネーブルにされます。**error-disabled** リカバリがポートで設定されていない場合、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドを使用してポートを再びイネーブルにします。
- 個々の VLAN を再びイネーブルにするには、**clear errdisable interface interface-id vlan [vlan-list]** 特権 EXEC コマンドを使用します。範囲を指定しない場合、ポートのすべての VLAN がイネーブルにされます。

音声認識 802.1x セキュリティを有効にするには、次の手順を実行します。

手順

| | コマンドまたはアクション | 目的 |
|--------|--|---|
| ステップ 1 | enable 例： Device> enable | 特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。 |
| ステップ 2 | configure terminal 例： Device# configure terminal | グローバル コンフィギュレーション モードを開始します。 |
| ステップ 3 | errdisable detect cause security-violation shutdown vlan 例： Device(config)# errdisable detect cause security-violation shutdown vlan | セキュリティ違反エラーが発生したすべての VLAN をシャットダウンします。 (注) shutdown vlan キーワードを指定しない場合、すべてのポートが errdisable ステータスになり、シャットダウンされます。 |
| ステップ 4 | errdisable recovery cause security-violation 例： | 802.1X セキュリティ違反により無効になったポートの自動回復を有効にします。 |

| | コマンドまたはアクション | 目的 |
|--------|---|--|
| | Device(config)# errdisable recovery cause security-violation | |
| ステップ 5 | 次を入力します。 <ul style="list-style-type: none"> • shutdown • no shutdown 例： Device(config)# no shutdown | (任意) errdisable の VLAN を再びイネーブルにして、すべての errdisable 指示をクリアします。 |
| ステップ 6 | exit 例： Device(config)# exit | グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。 |
| ステップ 7 | clear errdisable interface interface-id vlan [vlan-list] 例： Device# clear errdisable interface gigabitethernet 0/1/1 vlan vlan_list | (任意) errdisable になっている個々の VLAN を再びイネーブルにします。 <ul style="list-style-type: none"> • <i>interface-id</i> 引数の場合、個々の VLAN を再び有効にするポートを指定します。 • (任意) <i>vlan-list</i> 引数の場合、再び有効にする VLAN のリストを指定します。<i>vlan-list</i> を指定しない場合は、すべての VLAN が再びイネーブルになります。 |
| ステップ 8 | show errdisable detect 例： Device# show errdisable detect | error-disabled 検出ステータスを表示します。 |

IEEE 802.1x ポートベースの認証の設定例

次に IEEE 802.1x ポートベースの認証の設定例を示します。

例：アクセス不能認証バイパスの設定

次に、アクセス不能認証バイパス機能を設定する例を示します。

例：VLAN グループの設定

```

Device> enable
Device# configure terminal
Device(config)# radius-server dead-criteria time 30 tries 20
Device(config)# radius-server deadtime 60
Device(config)# radius server server1
Device(config-radius-server)# address ipv4 172.29.36.49 acct-port 1618 auth-port 1612
Device(config-radius-server)# key abc1234
Device(config-radius-server)# exit
Device(config)# dot1x critical eapol
Device(config)# dot1x critical recovery delay 2000
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# dot1x critical
Device(config-if)# dot1x critical recovery action reinitialize
Device(config-if)# dot1x critical vlan 20
Device(config-if)# end

```

例：VLAN グループの設定

次に、VLAN グループを設定し、そのグループに VLAN をマッピングし、VLAN グループ コンフィギュレーションおよび指定 VLAN とのマッピングを確認する例を示します。

```

Device> enable
Device(config)# vlan group eng-dept vlan-list 10
Device(config)# exit
Device# show vlan group group-name eng-dept

```

| Group Name | Vlans Mapped |
|------------|--------------|
| eng-dept | 10 |

```
Device# show dot1x vlan-group all
```

| Group Name | Vlans Mapped |
|------------|--------------|
| eng-dept | 10 |
| hr-dept | 20 |

次に、VLAN を既存の VLAN グループに追加し、VLAN が追加されたことを確認する例を示します。

```

Device> enable
Device(config)# vlan group eng-dept vlan-list 30
Device(config)# exit
Device(config)# show vlan group eng-dept

```

| Group Name | Vlans Mapped |
|------------|--------------|
| eng-dept | 10,30 |

次に、VLAN を VLAN グループから削除する例を示します。

```

Device> enable
Device# no vlan group eng-dept vlan-list 10

```

次に、すべての VLAN が VLAN グループからクリアされたときに、その VLAN グループもクリアされる例を示します。

```
Device> enable
Device(config)# no vlan group eng-dept vlan-list 30
Vlan 30 is successfully cleared from vlan group eng-dept.
Device(config)# exit
Device# show vlan group group-name eng-dept
```

次の例では、すべての VLAN グループをクリアする方法を示します。

```
Device> enable
Device(config)# no vlan group end-dept vlan-list all
Device(config)# exit
Device# show vlan-group all
```

IEEE 802.1x ポートベースの認証統計情報とステータスのモニタリング

ここでは、IEEE 802.1x ポートベース認証の統計情報とステータスをモニターするコマンドを示します。

表 4: 特権 EXEC 表示コマンド

| コマンド | 目的 |
|--|---|
| show dot1x all statistics | すべてのポートの 802.1x 統計情報を表示します。 |
| show dot1x interface interface-id statistics | 指定されたポートの 802.1x 統計情報を表示します。 |
| show dot1x all[count details statistics summary] | スイッチの 802.1x 管理ステータスおよび動作ステータスを表示します。 |
| show dot1x interface interface-id | 指定されたポートの 802.1x 管理ステータスおよび動作ステータスを表示します。 |

表 5: グローバルコンフィギュレーションコマンド

| コマンド | 目的 |
|---------------------------------|--------------------------------|
| no dot1x logging verbose | 詳細な 802.1x 認証メッセージをフィルタリングします。 |

IEEE 802.1x ポートベースの認証の機能履歴

| リリース | 機能 | 機能情報 |
|----------------------------------|---|---|
| Cisco IOS XE Everest 16.5.1a | IEEE 802.1x ポートベースの認証 | IEEE 802.1x 認証は、不正なデバイス（クライアント）によるネットワークアクセスを防止します。 |
| Cisco IOS XE Amsterdam 17.2.1 | セッション制限： MAC アドレスフラッ ディング DOS 攻撃を 防ぎます | access-session limit profile コマンドは、ポートに接続する音声およびデータホストの数を制限するために導入されました。 |

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェアイメージのサポート情報を検索できます。Cisco Feature Navigator には、<http://www.cisco.com/go/cfn> [英語] からアクセスします。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。