802.1X の設定

この章では、Cisco NX-OS デバイス上で IEEE 802.1X ポートベースの認証を設定する手順について説明します。

この章は、次の項で構成されています。

802.1X について

802.1X では、クライアント サーバ ベースのアクセス コントロールと認証プロトコルを定義し、許可されていないクライアントが公にアクセス可能なポートを経由して LAN に接続するのを規制します。認証サーバは、Cisco NX-OS デバイスのポートに接続されるクライアントを個々に認証します。

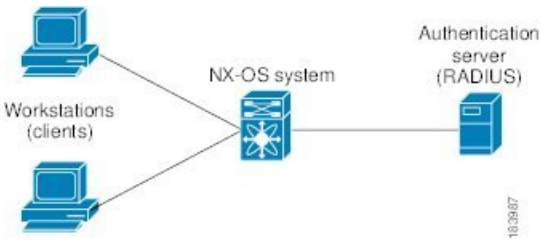
802.1X アクセス コントロールでは、クライアントが認証されるまで、そのクライアントが接続しているポート経由では Extensible Authentication Protocol over LAN（EAPOL）トラフィック

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。

デバイスのロール

802.1X ポート ベースの認証では、ネットワーク上のデバイスにそれぞれ特定のロールがあります。

***Figure 1: 802.1X* デバイスのロール**



特定のロールは次のとおりです。

サプリカント

LAN および Cisco NX-OS デバイス サービスへのアクセスを要求し、Cisco NX-OS デバイスからの要求に応答するクライアント デバイスです。ワークステーションでは、Microsoft Windows XP が動作するデバイスで提供されるような、802.1X 準拠のクライアント ソフトウェアが稼働している必要があります。

認証サーバ

サプリカントの実際の認証を行います。認証サーバはサプリカントの識別情報を確認し、LAN および Cisco NX-OS デバイスのサービスへのアクセスをサプリカントに許可すべきかどうかを Cisco NX-OS デバイスに通知します。Cisco NX-OS デバイスはプロキシとして動作するので、認証サービスはサプリカントに対しては透過的に行われます。認証サーバとして、拡張認証プロトコル（EAP）拡張機能を備えた Remote Authentication Dial-In User Service（RADIUS）セキュリティ デバイスだけがサポートされています。この認証サーバは、Cisco Secure Access Control Server バージョン 3.0 で使用可能です。RADIUS はサプリカント サーバ モデルを使用し、RADIUS サーバと 1 つまたは複数の RADIUS クライアントとの間でセキュア認証情報を交換します。

オーセンティケータ

サプリカントの認証ステータスに基づいて、ネットワークへの物理アクセスを制御します。オーセンティケータは、サプリカントと認証サーバとの仲介デバイス（プロキシ）として動作し、サプリカントから識別情報を要求し、得られた識別情報を認証サーバに確認し、サプリカントに応答をリレーします。オーセンティケータには、EAP フレームのカプセル化/カプセル化解除、および認証サーバとの対話を処理する、RADIUS クライアントが含まれています。

オーセンティケータが EAPOL フレームを受信して認証サーバにリレーする際は、イーサネット ヘッダーを取り除き、残りの EAP フレームを RADIUS 形式にカプセル化します。このカプセル化のプロセスでは EAP フレームの変更または確認が行われないため、認証サーバはネイティブ フレーム フォーマットの EAP をサポートする必要があります。オーセンティケータは

認証サーバからフレームを受信すると、サーバのフレーム ヘッダーを削除し、残りの EAP フレームをイーサネット用にカプセル化してサプリカントに送信します。

Note Cisco NX-OS デバイスがなれるのは、802.1X オーセンティケータだけです。

認証の開始およびメッセージ交換

オーセンティケータ（Cisco NX-OS デバイス）とサプリカント（クライアント）のどちらも認証を開始できます。ポート上で認証をイネーブルにした場合、オーセンティケータはポートのリンク ステートがダウンからアップに移行した時点で、認証を開始する必要があります。続いて、オーセンティケータは EAP-Request/Identity フレームをサプリカントに送信して識別情報を要求します（通常、オーセンティケータは1つまたは複数の識別情報の要求のあとに、最初の Identity/Request フレームを送信します）。サプリカ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。

サプリカントがブートアップ時にオーセンティケータから EAP-Request/Identity フレームを受信しなかった場合、サプリカントは EAPOL 開始フレームを送信することにより認証を開始することができます。この開始フレームにより、オーセンティケータはサプリカントの識別情報を要求します。

Note ネットワーク アクセス デバイスで 802.1X がイネーブルになっていない場合、またはサポートされていない場合、Cisco NX-OS デバイスはサプリカントからの EAPOL フレームをすべてドロップします。サプリカントが、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、サプリカントはポートが許可ステートにあるものとしてデータを送信します。ポートが許可ステートになっている場合は、サプリカントの認証が成功したことを意味します。

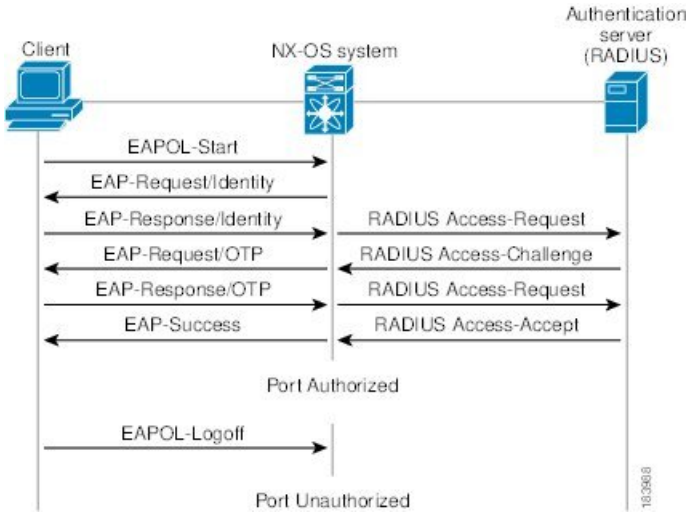
サプリカントが自己の識別情報を提示すると、オーセンティケータは仲介装置としてのロールを開始し、認証が成功または失敗するまで、サプリカントと認証サーバの間で EAP フレームを送受信します。認証が成功すると、オーセンティケータのポートは許可ステートになります。

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。

Figure 2: **メッセージ交換**

次の図に、サプリカントが RADIUS サーバにワンタイム パスワード（OTP）認証方式を使用して開始するメッセージ交換を示します。OTP 認証デバイスは、シークレット パスフレーズ

を使用して、一連のワンタイム（使い捨て）パスワードを生成します。



ユーザのシークレットパスフレーズは、認証時やパスフレーズの変更時などにネットワークを通過することはありません。

インターフェイスのオーセンティケータ PAE ステータス

インターフェイスで 802.1X をイネーブルにすると、Cisco NX-OS ソフトウェアにより、オーセンティケータ Port Access Entity（PAE）インスタンスが作成されます。オーセンティケータ PAE は、インターフェイスでの認証をサポートするプロトコル エンティティです。インターフェイスで 802.1X をディセーブルにしても、オーセンティケータ PAE インスタンスは自動的にクリアされません。必要に応じ、オーセンティケータ PAE をインターフェイスから明示的に削除し、再度適用することができます。

許可ステートおよび無許可ステートのポート

サプリカントのネットワークへのアクセスが許可されるかどうかは、オーセンティケータのポートステートで決まります。ポートは、無許可ステートで開始します。このステートにあるポートは、802.1X プロトコル パケットを除いたすべての入トラフィックおよび出トラフィックを禁止します。サプリカントの認証に成功すると、ポートは許可ステートに移行し、サプリカントのすべてのトラフィック送受信を通常どおりに許可します。

802.1X 認証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 ポートに接続した場合、オーセンティケータは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 プロトコルの稼働していないポートに接続すると、クライアントは EAPOL 開始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。

ポートには次の許可ステートがあります。

Force authorized
802.1X ポートベースの認証をディセーブルにし、認証情報の交換を必要としないで許可ステートに移行します。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。この許可ステートはデフォルトです。

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。オーセンティケータは、インターフェイスを経由してクライアントに認証サービスを提供することができません。

Auto
802.1X ポートベースの認証をイネーブルにします。ポートは無許可ステートで開始し、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移行したとき、またはサプリカントから EAPOL 開始フレームを受信したときに、認証プロセスが開始します。オーセンティケータは、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。オーセンティケータはサプリカントの 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サプリカントを一意に識別します。

サプリカントの認証に成功すると（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、認証されたサプリカ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す。認証サーバに到達できない場合、オーセンティケータは要求を再送信できます。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、サプリカントのネットワーク アクセスは認可されません。

サプリカントはログオフするとき、EAPOL ログオフ メッセージを送信します。このメッセージによって、オーセンティケータのポートは無許可ステートに移行します。

ポートのリンク ステートがアップからダウンに移行した場合、または EAPOL ログオフ フレームを受信した場合、ポートは無許可ステートに戻ります。

MAC 認証バイパス

MAC 認証バイパス機能を使用して、サプリカントの MAC アドレスに基づいてサプリカントを認証するように、Cisco NX-OS デバイスを設定できます。たとえば、プリンタなどのデバイスに接続されている 802.1X 機能を設定したインターフェイスで、この機能をイネーブルにすることができます。

サプリカントからの EAPOL 応答を待機している間に 802.1X 認証がタイムアウトした場合は、MAC 認証バイパスを使用して Cisco NX-OS デバイスはクライアントの許可を試みます。

インターフェイスで MAC 認証バイパス機能をイネーブルにすると、Cisco NX-OS デバイスは MAC アドレスをサプリカント ID として使用します。認証サーバには、ネットワーク アクセスが許可されたサプリカントの MAC アドレスのデータベースがあります。Cisco NX-OS デバイスは、インターフェイスでクライアントを検出した後、クライアントからのイーサネット パケットを待ちます。Cisco NX-OS デバイスは、MAC アドレスに基づいてユーザ名とパスワー

ドを含んだRADIUSアクセス/要求フレームを認証サーバに送信します。許可に成功した場合、Cisco NX-OS デバイス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。

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で検出される場合、このインターフェイスに接続されているデバイスが 802.1X 対応サプリカントであることを Cisco NX-OS デバイスが判別し、（MAC 認証バイパスではなく）802.1X 認証を使用してインターフェイスを許可します。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。

Cisco NX-OS デバイスがすでに MAC 認証バイパスを使用してインターフェイスを許可していて、802.1X サプリカントを検出した場合、Cisco NX-OS デバイスはインターフェイスに接続されているクライアントを無許可にしません。再認証を実行する際に、Cisco NX-OS デバイスは 802.1X 認証を優先再認証プロセスとして使用します。

MAC 認証バイパスで許可されたクライアントを再認証することができます。再認証プロセスは、802.1X で認証されたクライアントと同様です。再認証中に、ポートは前に割り当てられた VLAN に残ります。再認証に成功した場合、スイッチはポートを同じ VLAN 内に保持します。

再認証が Session-Timeout RADIUS 属性（Attribute [27]）と Termination-Action RADIUS 属性（Attribute [29]）に基づいていて、Termination-Action RADIUS 属性（Attribute [29]）アクションが初期化の場合、（属性値は DEFAULT）、MAC 認証バイパス セッションが終了して、再認証中に接続が失われます。MAC 認証バイパスがイネーブルで 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許可を開始します。これらの AV ペアの詳細については、RFC 3580「*IEEE 802.1X* リモート認証ダイヤル イン ユーザ サービス（RADIUS）使用ガイドライン」を参照してください。

MAC 認証バイパスは、次の機能と相互作用します。

- 802.1X 認証：802.1X 認証がポートでイネーブルの場合にだけ、MAC 認証バイパスをイネーブルにできます。
- ポート セキュリティ：同じレイヤ 2 ポート上で 802.1X 認証とポート セキュリティを構成することはできません。
- Network Admission Control（NAC）レイヤ 2 IP 検証：例外リスト内のホストを含む 802.1X ポートが MAC 認証バイパスで認証されたあとに、この機能が有効になります。

MAC-Based Authentication（MAB）に基づくダイナミック VLAN 割り当て

Cisco Nexus 9000 シリーズ スイッチはダイナミック VLAN 割り当てをサポートします。802.1X 認証またはMABが完了した後。ポートを起動する前に、認証の結果としてピア/ホストを特定のVLANに配置できるようにすることができます（許可の一部として）。RADIUSサーバは、一般的に Access-Accept 内にトンネル属性を含めることによって目的の VLAN を示します。VLAN をポートにバインドするこの手順は、ダイナミック VLAN 割り当てを構成します。

RADIUS からの VLAN 割り当て

802.1X または MAB によって認証が完了すると、RADIUS サーバからの応答にダイナミック VLAN 情報を含めることができるようになり、これをポートに割り当てることができます。この情報は、トンネル属性の形式の受け入れアクセス メッセージの RADIUS サーバからの応答に存在します。VLAN 割り当てのために、次のトンネル属性が送信されます。

- Tunnel-type=VLAN(13)
- Tunnel-Medium-Type=802
- Tunnel-Private-Group-ID=VLANID

アクセス VLAN の設定のために、3 つのパラメータをすべて受け取る必要があります。

シングル ホストおよびマルチ ホストのサポート

802.1X 機能では、1 つのポートのトラフィックを 1 台のエンドポイント装置に限定することも（シングル ホスト モード）、1 つのポートのトラフィックを複数のエンドポイント装置に許可することも（マルチ ホスト モード）できます。

シングル ホスト モードでは、802.1X ポートで 1 台のエンドポイント装置のみからのトラフィックが許可されます。エンドポイント装置が認証されると、Cisco NX-OS デバイスはポートを許可ステートにします。エンドポイント装置がログオフすると、Cisco NX-OS デバイスはポートを無許可ステートに戻します。802.1X のセキュリティ違反とは、認証に成功して許可された単一の MAC アドレスとは異なる MAC アドレスをソースとするフレームが検出された場合をいいます。このような場合、このセキュリティ アソシエーション（SA）違反（他の MAC アドレスからの EAPOL フレーム）が検出されたインターフェイスはディセーブルにされます。シングル ホスト モードは、ホストツースイッチ型トポロジで 1 台のホストが Cisco NX-OS デバイスのレイヤ 2 ポート（イーサネット アクセス ポート）またはレイヤ 3 ポート（ルーテッド ポート）に接続されている場合にだけ適用できます。

マルチ ホスト モードに設定されている 802.1X ポートで、認証が必要になるのは最初のホストだけです。最初のホストの許可に成功すると、ポートは許可ステートに移行します。ポートが許可ステートになると、後続のホストがネットワーク アクセスの許可を受ける必要はありません。再認証に失敗したり、または EAPOL ログオフ メッセージを受信して、ポートが無許可ステートになった場合には、接続しているすべてのクライアントはネットワーク アクセスを拒否されます。マルチ ホスト モードでは、SA 違反の発生時にインターフェイスをシャットダウンする機能がディセーブルになります。マルチ ホスト モードは、スイッチツースイッチ型トポロジおよびホストツースイッチ型トポロジの両方に適用できます。

サポートされるトポロジ

802.1X ポートベースの認証は、ポイントツーポイント トポロジをサポートします。

この設定では、802.1X 対応のオーセンティケータ（Cisco NX-OS デバイス）ポートにサプリカント（クライアント）を 1 台だけ接続することができます。オーセンティケータは、ポートのリンク ステートがアップ ステートに移行したときにサプリカントを検出します。サプリカン

トがログオフしたとき、または別のサプリカントに代わったときには、オーセンティケータはポートのリンク ステートをダウンに変更し、ポートは無許可ステートに戻ります。

ユーザ単位の DACL について

Cisco NX-OS リリース 10.2(1)以降、IEEE 802.1X を使用した認証後のポリシー適用として、Cisco ISE サーバからユーザ単位のダイナミック アクセス コントロール リスト（DACL）をダウンロードできます。

ユーザ単位の DACL を設定して、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 認証ユーザに提供できます。RADIUS サーバは、802.1X ポートに接続されるユーザを認証する場合、ユーザ 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。スイッチは、セッションが終了するたびに、または認証が失敗した場合に、ユーザ単位の DACL 設定を削除します。

RADIUS は、ベンダー固有属性などのユーザ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。ユーザ単位 DACL に使用される VSA は、入力方向の `inacl#<n>` であり、その場合、`n` は 1 から 32 です。構文は次のとおりです。

```
ip:inacl#<n>=permit | deny [protocol] [source_subnet] [dest_subnet] [operator][port]
```

例1：`ip:inacl#1=permit udp any any eq 5555`

例2：`ip:inacl#2=deny udp any any eq 6666`

VSA は入力方向に限りサポートされます。

クリティカル認証

Cisco NX-OS リリース 10.1(1) から、ポートの 802.1X クリティカル認証は、ISP ドメイン内の RADIUS サーバに到達できなかったときに認証に失敗した 802.1X ユーザに対応します。クリティカル認証機能は、802.1X 認証が RADIUS または ISE サーバを介してのみ実行される場合にサポートされます。802.1X ユーザが RADIUS 認証に失敗した場合でも、ネットワークへのアクセスは許可されます。これを行うには、**dot1x authentication event server dead action authorize** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

Cisco NX-OS リリース 10.5（2）F 以降、802.1x 機能とクリティカル認証機能はマルチドメインポートでサポートされています。

音声 VLAN 向け 802.1X について

音声 VLAN 向け 802.1X の概要

IEEE 802.1X の音声 VLAN 機能は、単一のポートでマルチドメイン 802.1X認証を可能にし、VoIP 電話とそれらに接続されているデータクライアントの両方の認証をサポートします。この機能を使用すると、1 つの特別なアクセスポートを構成して、2 つの VLAN 識別子に関連付けることができます。1つは音声トラフィック専用、もう1つはデータトラフィック専用です。このセットアップでは、同じポートで 1 つの音声クライアントと 1 つのデータクライアントに対応する、マルチドメインホストモードのサポートが必要です。

ユーザーはこの機能を活用し、単一のアクセスポートを介して接続された音声デバイスとデータデバイスの両方の安全で効率的なネットワーク トラフィック管理を保証できます。音声トラフィックとデータ トラフィックを別々の VLAN に分離することで、ネットワーク管理者は両方のタイプのデバイスの堅牢なセキュリティと認証を維持しながら、高品質の VoIP 通信を確保できます。

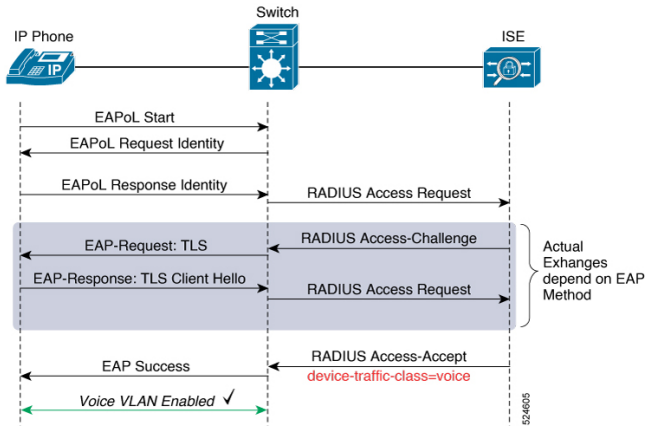
音声 VLAN 用 802.1X の機能

- 単一のポートでのマルチドメイン 802.1X 認証を有効にします。
- 新しいホストモード（マルチドメイン）は、1 つのポートで 1 つの音声デバイス（通常は IP 電話）と 1 つのデータデバイス（通常は PC）をサポートします。
- アイデンティティに基づいてユーザーを区別できるポートで単一のオーセンティケータを実行し、ユーザーを適切なドメイン（データと音声用に異なる VLAN）に配置します。
- 同じポートでデータトラフィックと音声トラフィックの分離を維持します。

音声VLAN の 802.1X のメッセージ交換

- **VoIP 電話接続**：802.1X が構成されているスイッチに VoIP 電話が接続されています。
- **VoIP 電話認証**：VoIP 電話は、EAP または MAB のいずれかを使用して認証できます。
- **音声デバイスの認識**：VoIP 電話は RADIUS サーバによって音声デバイスとして認識され、802.1X は音声 VLAN 内の電話をセキュア化します。
- **データデバイス接続**：データデバイス（ラップトップなど）は、VoIP 電話を使用してスイッチに接続されます。

- **データデバイス認証**：データデバイスは 802.1X 認証をトリガーし、データ VLAN の RADIUS サーバによって承認されます。



DACL について

ダイナミック ACL（DACL）は、ユーザおよびグループがアクセスできる権限を含む単一の ACL です。dot1x MAB クライアントへのアクセスを制限します。DACL ポリシーが Cisco ISE サーバからプッシュされ、MAC アドレスがブラックリストに登録されます。これにより、ブラックリストに登録された MAC に ACL が適用され、MAB へのアクセスが制限されます。単一の DACL は、すべてのブラックリスト MAB クライアントをサポートします。

Cisco NX-OS Release 9.3(5) では、DACL は Cisco Nexus スイッチで事前設定されています。

802.1X の前提条件

- Cisco Nexus リリース 7.0(3)I7(1) ソフトウェア。

EAP-TLS プロファイルを使用した 802.1X ポートベース認証には、次の前提条件が必要です。

- PKI インフラは、EAP-TLS の証明書管理を提供します。特例を申請する必要があります。
  - RSA キーペアの生成
  - 証明書トラストポイントの作成
  - CA の認証
- 802.1X では、EAP-TLS を提供するために、デバイス上の ISE などのリモート EAP サーバが必要です。ローカル認証サーバはサポートされていません。
- 両方の参加デバイス（CA サーバーと Cisco Identity Services Engine（ISE））が Network Time Protocol（NTP）を使用して同期されていることを確認します。時間がすべてのデバイスで同期されていないと、証明書は検証されません。

- AAA サーバーの到達可能性：スイッチが相互に認証するためです。
- スイッチは相互認証を行うため、両方のスイッチに適切な AAA 設定と AAA 接続が必要です。

802.1X のガイドラインと制約事項

802.1X ポートベースの認証には、次の設定に関する注意事項と制約事項があります。

- （中断あり/中断なしの）インサービス ソフトウェア アップグレード（ISSU）を使用して Cisco Nexus シリーズ スイッチを Cisco NX-OS リリース 9.2(1) にアップグレードする場合は、まず **no feature dot1x** コマンドを使用して 802.1x を無効にします。機能を有効にするには、**feature dot1x** コマンドを使用してマルチ認証を機能させます。
- Cisco NX-OS リリース 9.2(1) 以降では、802.1X ポートでマルチ認証モードが有効になります。ダイナミック VLAN の割り当ては、最初の認証済みホストに対し行われます。ユーザ クレデンシャルに基づいてその後に許可されたデータ ホストは、正しく認証されたと見なされます。ただし、まだ VLAN が割り当てられていないか、ポートで最初に正しく認証されたホストと一致する VLAN 割り当てがなされていることを条件とします。これにより、ポートで正常に認証されたすべてのホストは、確実に同じ VLAN メンバになります。ダイナミック VLAN 割り当ての柔軟性は、最初に認証されたホストだけに当てはまります。
- Cisco NX-OS リリース 9.2(3) 以降、802.1X ポートベース認証は FEX-ST およびホスト インターフェイス（HIF）ポートでサポートされます。IEEE 802.1X ポートベース認証のサポートは、ストレートおよびデュアルホーム FEX の両方に適用されます。
- Cisco Nexus 9000 シリーズ スイッチは、以下のものについては、802.1X をサポートしていません。
  - トランジット トポロジの設定
  - vPC ポート
  - PVLAN ポート
  - L3（ルーテッド）ポート
  - ポート セキュリティ
  - CTS および MACsec PSK が有効になっているポート。
  - LACP ポートチャネルを使用した 802.1X。

（注） 802.1X は、スタティック ポートチャネルをサポートします。

（注） vPCポートおよびサポートされていないすべての機能では、802.1X は無効になります。

- Cisco NX-OS ソフトウェアが 802.1X 認証をサポートするのは、物理ポート上だけです。
- ダイナミック VLAN 割り当ては、Cisco Nexus 9300-FX/EX/FX2 プラットフォーム スイッチでのみサポートされます。
- Cisco NX-OSソフトウェアは、CTS または MACsec PSK 機能については動作しません。グローバルな「mac-learn disable」と 802.1X 機能は相互に排他的であり、同時に設定することはできません。
- 802.1X は IP ソース ガードおよび uRPF 機能とは相互に排他的であり、同時に設定することはできません。Cisco Nexus シリーズ スイッチを Cisco NX-OS リリース9.2(3) にアップグレードする場合は、これらの機能のいずれかを無効にする必要があります。
- スイッチのリロード中、802.1X は RADIUS アカウンティングの停止を生じさせません。
- Cisco NX-OS ソフトウェアは、次の 802.1X プロトコル拡張機能をサポートしません。
  - 論理 VLAN 名から ID への 1 対多のマッピング
  - Web 許可
  - ダイナミック ドメイン ブリッジ割り当て
  - IP テレフォニー
  - ゲスト VLAN
- 非アクティブなセッションの再認証を防ぐには、authentication timer inactivity コマンドを使用して、非アクティブタイマーを、authentication timer reauthenticateコマンドで設定された再認証間隔よりも短い間隔に設定します。
- インターフェイスで 802.1X が有効になっている異なる VLAN で、同じ MAC が学習されると、セキュリティ違反が発生します。
- DME 対応プラットフォームで 802.1X を有効にした状態で MAC の学習を無効に設定しても、エラー メッセージは表示されません。
- Cisco Nexusリリース9.2(1) では、VLAN がインターフェイスで設定されていなくても、タグ付き EAPOL フレームは処理され、クライアントのインターフェイスで認証は成功します。
- 孤立ポートで学習されたセキュア MAC は、vPCピアで同期されません。
- Cisco NX-OS リリース 9.2(1) 以降、MAC 認証バイパスは Cisco Nexus 9300-FX/FX2 TOR スイッチでサポートされます。

- Cisco NX-OSリリース 9.3(5) 以降、802.1X は Cisco Nexus 9300-FX3 プラットフォーム スイッチでサポートされます。
- Cisco NX-OSリリース 10.1(2) 以降、802.1X は Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- Cisco NX-OS リリース 10.2(1)F 以降、802.1X は N9K-C9364D-GX2A および N9K-C9332D-GX2B スイッチでサポートされます。
- Cisco NX-OS リリース 10.3(2)F 以降、MAC 認証バイパスとマルチ認証は、N9K-X9788TC-FX および N9K-X97160YC-EX ラインカードを備えた Cisco Nexus 9508 スイッチでサポートされています。
- N9K-X9788TC-FX および N9K-X97160YC-EX ライン カードを備えた Cisco Nexus C9508 スイッチは、802.1Xを使用した次の機能をサポートしていません。
  - dVLAN
  - DACL
  - FEX-AA
  - VXLAN と mac-move
  - CoA
  - 認証方式として MAB のみがサポートされ、EAP はサポートされません
  - サポートは、単一のアクセス VLAN を持つアクセス ポートに対するものです。
- NX-OS リリース 10.3(3)F 以降、IPv6 アンダーレイは、Cisco Nexus 9300-FX/FX2/FX3/GX/GX2 スイッチ、および X97160YC-EX、9700-FX/GX ライン カードを搭載したCisco Nexus 9500 スイッチにおいて、VXLAN EVPN の 802.1X でサポートされます。
- Cisco NX-OS リリース 10.4(1)F 以降、Cisco Nexus 9336C-FX2、93180YC-FX3、93108TC-FX3P スイッチ、および X9716D-GX ライン カードを搭載した Cisco Nexus 9500 スイッチは、MACSec を必要とするアップリンクポートで（証明書を伝送するために）EAP/EAP-TLS を使用する 802.1X ポートベース認証をサポートします。次の制限があります。
  - EAP-TLS でサポートされる TLS バージョンは 1.2 です。
  - スイッチごとに単一の EAP プロファイルをサポートし、複数のインターフェイスで同じ EAP プロファイルを使用できます。
  - サプリカントの MAC 移動プロファイルはサポートされません。
  - オーセンティケータ プロファイルは、L3 ポート、トランクポート、vPC で、MACsec EAP-TLS に対してのみ有効になります。

（注） MAB/EAP クライアントの 802.1X オーセンティケータ機能は、L3 またはトランクおよび vPC ポートではサポートされません。

- EAP-TLS は、MACsec が構成されたインターフェイスの EAP でのみサポートされます。
- EAP-TLS は、マルチホスト モードでのみサポートされます。
- 802.1X MACsec 対応インターフェイスでの DACL/クリティカル AUTH/FEX-AA およびその他の 802.1X 機能はサポートされていません。
- EAP-TLS はリモート認証（ISE/RADIUS：ISE 3.0 以降）でのみサポートされ、ローカル認証ではサポートされません。
- EAP-TLS 構成が正しく機能するには、次の順序に従う必要があります。
  - 最初に **macsec eap policy** コマンドを設定してから、**dot1x supplicant eap profile TLS** コマンドを設定する必要があります。
  - EAP profile コマンドの **no** 形式の場合は、まず **dot1x supplicant eap profile TLS** コマンドを削除してから **macsec eap policy** コマンドを削除する必要があります。
  - **no feature** コマンドについては、DME DB の不整合を回避するために、最初に 802.1X 機能を削除してから MACsec 機能を削除することを推奨します。
- スイッチ全体に構成されている単一の EAP プロファイルは、異なるインターフェイスに適用できます。
- **macsec eap policy** がインターフェイスで構成されている場合、通常の 802.1X 認証者機能またはコマンドはサポートされません。
- ピアツーピア MACsec 対応スイッチには、同じ 802.1X または MACsec 設定が必要です。
- コマンドが異なる場合（一方が should-secure、もう一方が must-secure など）、動作は未定義になり、回復には shut/no-shut のトリガーが必要になります。
- トラストポイントを使用して MACsec セキュアセッションが作成され、EAP プロファイルがインターフェイスに追加されると、次のようになります。
  - トラストポイント構成を削除しても、MACsec セッションは削除されません。
  - 802.1X サプリカント コマンドを削除しても、MACsec セッションは削除されません。
  - MACsec セッションは、MACsec インターフェイス固有のコマンドを削除した場合にのみ削除されます。
- MACsec PKI は、中間スイッチまたはホップのないスイッチでサポートされるので、直接接続する必要があります。
- MACsec PKI（802.1X EAP-TLS）モードは、EoR ステートフル スイッチ オーバー（SSO）をサポートしていません。
- EAP-TLS は、次のインターフェイス タイプでのみサポートされます。

- L2/L3 ポート、ポートチャネル メンバー ポート、トランク ポート、およびブレークアウト ポート
- サポートされていないインターフェイスタイプ：コマンドレベルの制限はありません。

- サポートされる MACsec セッションの数は、物理インターフェイスの規模によって異なります。

- Cisco NX-OS リリース 10.4(3)F 以降、EAP-TLS は Cisco Nexus スイッチで Transport Layer Security バージョン 1.3 および 1.2 をサポートします。

（注） RADIUS サーバーが TLS v1.3 に対応していない場合は、サポートされる最小バージョンである TLS v1.2 が使用されます。

音声 VLAN に関連した 802.1X のガイドラインと制限事項

- Cisco NX-OS リリース 10.5(2)F 以降において、802.1X 音声 VLAN機能は、次の Cisco Nexus スイッチでサポートされます。
  - N9K-C9348GC-FXP
  - N9K-C93108TC-FX3P
  - N9K-C9348GC-FX3
  - N9K-C9348GC-FX3PH
- 音声 VLAN 構成では、L2 スイッチポートモードアクセスのみがサポートされます。
- 1 つの音声 VLAN と 1 つのデータVLAN のみがサポートされます。
- ダイナミックアクセス制御リスト（DACL）およびダイナミック VLAN（DVLAN）は、マルチドメイン認証（MDA）ポートではサポートされません。
- 次のコマンドは、802.1X で構成されたポートの音声 VLAN 構成ではサポートされません。
  - **switchport voice vlan untagged**
  - **switchport voice vlan dot1p**

  これらの構成が 802.1Xポートに存在する場合、電話機機能は許可されません。したがって、マルチドメインポートには特定の音声 VLAN ID を構成する必要があります。
- アクセス VLAN と音声 VLAN の両方に同じ値を設定することはサポートされません。同じ値で構成していた場合は、値を変更し、ポートをフラップしてください。

802.1X向け事前ユーザDACLサポートのガイドラインと制約事項

- 次のスイッチ プラットフォームは、この機能をサポートしています。
  - Cisco Nexus 9300-FX プラットフォーム スイッチ
  - Cisco Nexus 9300-FX2 プラットフォーム スイッチ
- ユーザー単位の DACL は、IPv4 TCP、UDP、および ICMP ACL ルールをサポートしますが、IPv6 ACL ルールはサポートしません。
- ユーザー単位の DACL は、4 KB 未満の単一の RADIUS 応答に制限され、サポートされる ACE の最大数は 32 です。
- この機能は、スイッチポートの標準 ACL をサポートしていません。
- ポートごとに 1 つの DACL のみがサポートされます。スイッチ全体でサポートされる DACL の最大数は、そのスイッチのポート数と同じです。
- DACL とダイナミック VLAN は、同じポートで同時にサポートされません。
- ISE からの DACL コンテンツの動的な変更はサポートされていません。これを実現するには、 **clear dot1x interface** コマンドを使用して以前に適用した DACL をポートからクリアし、ISE からの新しい DACL を適用します。これにより、このポート上のすべてのクライアントで一時的なトラフィックの中断が発生します。
- AA FEX モードの Cisco Nexus 9000 シリーズ スイッチは、ユーザー単位の DACL をサポートしていません。
- ユーザー単位の DACL は、MAB およびマルチ認証ホスト モードのみをサポートします。
- 他のすべての Nexus 9000 802.1x 機能と同様に、ユーザごとの DACL は物理ポート、つまり通常の L2 アクセス ポートでのみサポートされ、トランク、vPC、ポートチャネルとそのメンバー、およびサブインターフェイスではサポートされません。
- スイッチに適用される他のすべての Nexus 9000 ACL と同様に、ユーザごとの DACL の最大制限は 4000 ASCII 文字です。
- ユーザーごとの DACL 機能の MAC 移動プロファイルはサポートされていません。
- Cisco NX-OS リリース 10.2(1) 以降、この機能は Cisco Nexus 9300-FX/FX2/ TOR スイッチでサポートされます。
- Cisco NX-OS リリース 10.5(2)F 以降、DACL 機能は Cisco Nexus 9300-FX3、GX、GX2、H2R、H1 シリーズ スイッチでサポートされています。

クリティカル認証のガイドラインと制限事項

- クリティカル認証は、基本的なMABクライアントのみをサポートし、FEX-AAやVxLANなどのトポロジではサポートされません。
- 不正なクライアント トラフィックはすべて許可されるため、**authentication event server dead action authorize** コマンドを常に有効にすると、セキュリティ上のリスクが生じます。
- Cisco NX-OS リリース 10.1(2) 以降、クリティカル認証機能は Cisco Nexus 9300-FX/FX2/FX3/GX TOR スイッチでサポートされています。
- Cisco NX-OS リリース 10.2(1)F 以降、クリティカル認証機能は N9K-C9364D-GX2A および N9K-C9332D-GX2B スイッチでサポートされます。
- Cisco NX-OS リリース 10.3(2)F 以降、重要な認証機能は、N9K-X9788TC-FX および N9K-X97160YC-EX ラインカードを備えた Cisco Nexus 9508 スイッチでサポートされています。

802.1X のデフォルト設定

次の表に、802.1X パラメータのデフォルト設定を示します。

***Table 1: 802.1X* のデフォルト パラメータ**

パラメータ	デフォルト
802.1X 機能	ディセーブル
AAA 802.1X 認証方式	設定なし
インターフェイス単位の 802.1x プロトコル イネーブル ステート	ディセーブル（**force-authorized**） **Note** ポートはサプリカントとの 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。
定期的な再認証	ディセーブル
再認証の間隔（秒）	3600 秒
待機タイムアウト時間	60 秒（Cisco NX-OS デバイスがサプリカントとの認証情報の交換に失敗した後、待機状態を続ける秒数）
再送信タイムアウト時間	30 秒（Cisco NX-OS デバイスが EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求を再送信するまでの秒数）

パラメータ	デフォルト
最大再送信回数	2 回（Cisco NX-OS デバイスが認証プロセスを再開するまでに、EAP-Request/Identity フレームを送信する回数）
ホスト モード	シングル ホスト
サプリカント タイムアウト時間	30 秒（認証サーバからの要求をサプリカントにリレーするとき、Cisco NX-OS デバイスがサプリカントに要求を再送信するまでに、サプリカントの応答を待つ時間）
認証サーバ タイムアウト時間	30 秒（サプリカントからの応答を認証サーバにリレーするとき、Cisco NX-OS デバイスがサーバに応答を再送信するまでに、サーバからの応答を待つ時間）

802.1X の設定

ここでは、802.1X 機能の設定方法について説明します。

802.1X の設定プロセス

ここでは、802.1X を設定するプロセスについて説明します。

Procedure

ステップ 1 802.1X 機能をイネーブルにします。
ステップ 2 リモート RADIUS サーバへの接続を設定します。
ステップ 3 イーサネット インターフェイスで 802.1X 機能をイネーブルにします。

802.1X 機能のイネーブル化

サプリカント デバイスを認証する前に、Cisco NX-OS デバイス上で 802.1X 機能をイネーブルにする必要があります。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:**	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

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	
ステップ 2	**feature dot1x** **Example:** `switch(config)# feature dot1x`	802.1X 機能をイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **show dot1x** **Example:** `switch# show dot1x`	802.1X機能のステータスを表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X の AAA 認証方式の設定

802.1X 認証にリモート RADIUS サーバを使用できます。RADIUS サーバおよび RADIUS サーバ グループを設定し、デフォルト AAA 認証方式を指定したあとに、Cisco NX-OS デバイスは 802.1X 認証を実行します。

Before you begin

リモート RADIUS サーバ グループの名前またはアドレスを取得します。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 2	**aaa authentication dot1x default group** *group-list* **Example:**	802.1X 認証に使用する RADIUS サーバ グループを指定します。

	Command or Action	Purpose
	`switch(config)# aaa authentication dot1x default group rad2`	*Group-list* 引数は、スペースで区切られたグループ名のリストで構成されます。グループ名は、次のように指定します。 • **radius**RADIUS サーバのグローバル プールを使用して認証を行います。 • *named-group* ：認証に RADIUS サーバのグローバル プールを使用します。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **show radius-server** **Example:** `switch# show radius-server`	RADIUS サーバの設定を表示します。
ステップ 5	(Optional) **show radius-server group** [*group-name*] **Example:** `switch# show radius-server group rad2`	RADIUS サーバ グループの設定を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでの 802.1X 認証の制御

インターフェイス上で実行される 802.1X 認証を制御できます。インターフェイスの 802.1X 認証ステートは、次のとおりです。

自動（Auto）
インターフェイス上で、802.1X 認証を有効にします。

強制認証
インターフェイス上の 802.1X 認証を無効にし、認証を行わずにインターフェイス上のすべてのトラフィックを許可します。このステートがデフォルトです。

Force-unauthorized
インターフェイス上のすべてのトラフィックを禁止します。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet** *slot* / *port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、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 3	**dot1x port-control** {**auto** | **force-authorized** | **forced-unauthorized**} **Example:** `switch(config-if)# dot1x port-control auto`	インターフェイスの 802.1X 認証ステートを変更します。デフォルトの設定は force-authorized です。

ステップ 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 5	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	(Optional) **show dot1x interface ethernet** *slot* / *port* **Example:** `switch# show dot1x interface ethernet 2/1`	インターフェイスの 802.1X 機能のステータスおよび設定情報を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

音声 VLAN 向け 802.1X の構成

Cisco NX-OSリリース 10.5(2)F 以降では、単一ポートでマルチドメイン 802.1X 認証を有効にできます。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet** *slot* / *port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、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 3	**dot1x host-mode multi-domain** 例： `switch(config-if)# dot1x host-mode multi-domain`	インターフェイスレベルでマルチドメインホストモードを有効化または無効化します。 インターフェイスレベルでマルチドメインホストモードを無効化にするには、このコマンドの **no** 形式を使用します。 （注） 音声クライアントは、ホストモードマルチドメインのポートでのみ正常に認証されます。ホストモードがそれ以外の場合、音声クライアントは認証に失敗し、無効になります。

ステップ 4	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		コンフィグレーション モードを終了します。

EAP-TLS の設定

Cisco NX-OS リリース 10.4(1)F 以降では、802.1X 認証に EAP-TLS プロファイルを使用できます。

始める前に

- Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。
- インターフェイスで、MACsec EAP ポリシーを構成し、**dot1x supplicant eap profile** にアタッチします。MACsec EAP ポリシーの構成については、「MACsec EAP の構成」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	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**[no] eap profile TLS**
	例：
	`switch(config)# eap profile TLS`
	`switch(config-eap-profile)#`
		802.1X EAP プロファイル モードを構成します。
		コマンドの **no** フォームは、eap プロファイルを無効にするために使用されます。

ステップ 3	**pki-trustpoint** *trustpoint name*
	例：
	`switch(config-eap-profile)#`
	`pki-trustpoint tp1`
	`switch(config-eap-profile)#`
		使用するトラストポイントを指定します。

ステップ 4	**method** *type*
	例：
	`switch(config-eap-profile)# method TLS`
	`switch(config-eap-profile)#`
		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。
		使用する EAP 方式を指定します。

ステップ 5	**interface ethernet** *slot/port*
	例：
	`switch(config-eap-profile)# interface ethernet 1/30`
	`switch(config-if)#`
		設定するインターフェイスを選択し、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	**[no] dot1x supplicant eap profile** *eap profile name* 例： `switch(config-if)# dot1x supplicant eap profile`	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。 802.1X サプリカントを EAP プロファイルに構成します。

インターフェイスでのオーセンティケータ PAE の作成または削除

インターフェイスで 802.1X オーセンティケータ Port Access Entity（PAE）インスタンスを作成または削除できます。

（注） デフォルトでは、インターフェイスで 802.1X をイネーブルにしたときに、Cisco NX-OS ソフトウェアによってインターフェイスでオーセンティケータ PAE インスタンスが作成されます。

始める前に

802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	（任意） **show dot1x interface ethernet** *slot/port* 例： `switch# show do1x interface ethernet 2/1`	インターフェイス上の 802.1X の設定を表示します。

ステップ 3	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、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	[**no**] **dot1x pae authenticator** 例： `switch(config-if)# dot1x pae authenticator`	インターフェイスでオーセンティケータ PAE インスタンスを作成します。インターフェイスから PAE インスタンスを削除するには、**no** 形式を使用します。 （注） オーセンティケータ PAE がインターフェイスにすでに存在している場合は、**dot1x pae authentication** コマンドを実行してもインターフェイス上の設定は変更されません。

	コマンドまたはアクション	目的
ステップ 5	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

クリティカル認証を有効にする

始める前に

- RADIUS のモニタリングを有効にします。
- グループ内のすべてのサーバが RADIUS サーバであ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	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**radius-server test idle-time** *minutes* 例： `switch(config)# radius-server test idle-time 1`	グローバルなサーバモニタリング用のパラメータを指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 （注） RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。グループに複数のサーバがある場合は、各サーバのアイドル タイマーを 1に設定します。
ステップ 3	**radius-server deadtime** 分 例： `switch(config)# radius-server deadtime 1`	以前に応答の遅かった RADIUS サーバを Cisco NX-OS デバイスがチェックを始めるまでの分数を指定します。デフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 （注）

	コマンドまたはアクション	目的
		デッドタイムを0より大きい値に設定して、モニタリングを有効にします。
ステップ 4	**radius-server host** *ipv4-address* **key**[**0** |**6** |**7**] *key-value* 例： `switch(config)# radius-server host 10.105.222.183 key 7 "fewhg" authentication accounting`	すべての RADIUS サーバ用の RADIUS キーを指定します。key-value がクリアテキスト（**0**）の形式か、タイプ 6 暗号化（**6**）形式か、タイプ 7 暗号化（**7**）形式かを指定できます。Cisco NX-OS ソフトウェアでは、実行コンフィギュレーションに保存する前にクリアテキストのキーを暗号化します。デフォルトの形式はクリアテキストです。最大で 63 文字です。デフォルトでは、RADIUS キーは設定されません。 （注） **generate type7_encrypted_secret** コマンドを使用して共有秘密をすでに設定している場合、2 番目の例のように引用符で囲んで入力してください。詳細については、RADIUS または TACACS+ の共有秘密の設定を参照してください。
ステップ 5	**radius-server host** *ipv4-address* **test idle-time** *minutes* 例： `switch(config)# radius-server host 10.105.222.183 test idle-time 1`	サーバモニタリング用のパラメータを個別に指定します。デフォルトのユーザ名は test、デフォルトのパスワードは test です。アイドル タイマーのデフォルト値は 0 分です。有効な範囲は 0 ～ 1440 分です。 （注） RADIUS サーバの定期的なモニタリングを行うには、アイドル タイマーに 0 より大きな値を設定する必要があります。

ステップ 6	**aaa group server radius** *group-name*
	例：
	`switch(config)# aaa group server radius ISE_2.4`
	`switch(config-radius)#`
		RADIUS サーバ グループを作成し、そのグループの RADIUS サーバ グループ コンフィギュレーション サブモードを開始します。*group-name* 引数は、最大 127 文字の長さの英数字のストリングで、大文字小文字が区別されます。

	コマンドまたはアクション	目的
		RADIUS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。 （注） デフォルトのシステム生成デフォルト グループ（RADIUS）は削除できません。
ステップ 7	**server** {*ipv4-address* | *ipv6-address* | *hostname*} 例： `switch(config-radius)# server 10.105.222.183`	RADIUS サーバを、RADIUS サーバ グループのメンバーとして設定します。指定した RADIUS サーバが見つからなかった場合は、**radius-server host** コマンドを使用してサーバを設定し、このコマンドをもう一度実行します。
ステップ 8	**use-vrf** *vrf-name* 例： `switch(config-radius)# use-vrf management`	サーバ グループ内のサーバとの接続に使用する VRF を指定します。
ステップ 9	**source-interface** *interface* 例： `switch(config-radius)# source-interface mgmt 0`	このデバイスで設定されているすべての RADIUS サーバ グループ用のグローバル発信元インターフェイスを設定します。

ステップ 10	**exit**
	例：
	`switch(config-radius)# exit`
	`switch(config)#`
		RADIUS サーバ グループ コンフィギュレーション サブモードを終了します。

ステップ 11	**authentication event server dead action authorize** 例： `switch(config)# authentication event server dead action authorize`	RADIUS サーバに到達できない場合に、すべてのクライアントを認可します。

インターフェイスの定期再認証のイネーブル化

インターフェイスの 802.1X 定期再認証をイネーブルにし、再認証を実行する頻度を指定します。期間を指定しないで再認証をイネーブルにした場合、再認証を行う間隔はグローバル値にデフォルト設定されます。

Note 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、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 3	**dot1x re-authentication** **Example:** `switch(config-if)# dot1x re-authentication`	インターフェイスに接続されているサプリカントの定期再認証をイネーブルにします。デフォルトでは、定期再認証はディセーブルです。
ステップ 4	(Optional) **dot1x timeout re-authperiod** *seconds* **Example:** `switch(config-if)# dot1x timeout re-authperiod 3300`	再認証の間隔（秒）を設定します。デフォルトは 3600 秒です。値の範囲は 1 ～ 65535 です。 **Note** インターフェイス上の定期再認証をイネーブルにする場合だけ、このコマンドは Cisco NX-OS デバイスの動作に影響します。

ステップ 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		コンフィギュレーション モードを終了します。

ステップ 6	(Optional) **show dot1x all** **Example:** `switch(config)# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。

	Command or Action	Purpose
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

手動によるサプリカントの再認証

Cisco NX-OS デバイス全体のサプリカントまたはインターフェイスのサプリカントを手動で再認証できます。

Note 再認証プロセス中、すでに認証されているサプリカントのステータスは影響を受けません。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose
ステップ 1	**dot1x re-authenticate** [**interface** *slot*/*port*] **Example:** `switch# dot1x re-authenticate interface 2/1`	Cisco NX-OS デバイスまたはインターフェイス上のサプリカントを再認証します。

インターフェイスの 802.1X 認証タイマーの変更

Cisco NX-OS デバイスのインターフェイス上で変更できる 802.1X 認証タイマーは、次のとおりです。

待機時間タイマー
Cisco NX-OS デバイスがサプリカントを認証できない場合、スイッチは所定の時間アイドル状態になり、その後再試行します。待機時間タイマーの値でアイドルの時間が決まります。認証が失敗する原因には、サプリカントが無効なパスワードを提供した場合があります。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。デフォルトは、グローバル待機時間タイマーの値です。範囲は 1 ～ 65535 秒です。

レート制限タイマー
レート制限時間中、サプリカントから過剰に送信されている EAPOL-Start パケットを抑制します。オーセンティケータはレート制限時間中、認証に成功したサプリカントからの EAPOL-Start パケットを無視します。デフォルト値は 0 秒で、オーセンティケータはすべての EAPOL-Start パケットを処理します。範囲は 1 ～ 65535 秒です。

レイヤ 4 パケットに対するスイッチと認証サーバ間の再送信タイマー
認証サーバは、レイヤ4パケットを受信するたびにスイッチに通知します。スイッチがパケット送信後に通知を受信できない場合、Cisco NX-OS デバイスは所定の時間だけ待機した後、パケットを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

EAP 応答フレームに対するスイッチとサプリカント間の再送信タイマー
サプリカントは、Cisco NX-OS デバイスの EAP-Request/Identity フレームに対し、EAP-Response/Identity フレームで応答します。Cisco NX-OS デバイス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）だけ待機した後、フレームを再送信します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。

EAP 要求フレームに対するスイッチとサプリカント間の再送信タイマー
サプリカントは、EAP 要求フレームを受信したことを Cisco NX-OS デバイスに通知します。オーセンティケータがこの通知を受信できなかった場合、オーセンティケータは所定の時間だけ待機した後、フレームを再送信します。デフォルトは、グローバル再送信時間タイマーの値です。範囲は 1 ～ 65535 秒です。

Inactive period timeout
Cisco NX-OS デバイスが設定された期間にわたって非アクティブのままである場合。timeout inactivity-period 値は、非アクティブ期間を決定します。最小推奨値は 1800 秒です。値が再認証時間の値よりも小さいことを確認する必要があります。

Note このデフォルト値は、リンクの信頼性が低下した場合や、特定のサプリカ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場合にだけ変更してください。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、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 3	(Optional) **dot1x timeout quiet-period** *seconds* **Example:**	オーセンティケータが EAP-Request/Identity フレームに対するサプリカントからの応答を待ち、要求

	Command or Action	Purpose
	`switch(config-if)# dot1x timeout quiet-period 25`	を再送信するまでの時間を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。
ステップ 4	(Optional) **dot1x timeout ratelimit-period** *seconds* **Example:** `switch(config-if)# dot1x timeout ratelimit-period 10`	認証に成功したサプリカントからの EAPOL-Start パケットを無視する時間を秒数で設定します。デフォルト値は 0 秒です。範囲は 1 ～ 65535 秒です。
ステップ 5	(Optional) **dot1x timeout server-timeout** *seconds* **Example:** `switch(config-if)# dot1x timeout server-timeout 60`	Cisco NX-OS デバイスが認証サーバにパケットを送信する前に待機する時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。
ステップ 6	(Optional) **dot1x timeout supp-timeout** *seconds* **Example:** `switch(config-if)# dot1x timeout supp-timeout 20`	Cisco NX-OS デバイスが EAP 要求フレームを再送信する前に、サプリカントが EAP 要求フレームに応答してくるのを待機する時間を秒数で設定します。デフォルトは 30 秒です。範囲は 1 ～ 65535 秒です。
ステップ 7	(Optional) **dot1x timeout tx-period** *seconds* **Example:** `switch(config-if)# dot1x timeout tx-period 40`	サプリカントから EAP 要求フレームを受信した通知が送信されない場合に、EAP 要求フレームを再送信する間隔を秒数で設定します。デフォルトはすべてのインターフェイスに設定されるグローバル秒数です。範囲は 1 ～ 65535 秒です。
ステップ 8	(Optional) **dot1x timeout inactivity-period** *seconds* **Example:** `switch(config-if)# dot1x timeout inactivity-period 1800`	スイッチが非アクティブ状態を維持できる秒数を設定します。最小推奨値は 1800 秒です。

ステップ 9	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーションモードを終了します。

ステップ 10	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	802.1X の設定を表示します。

	Command or Action	Purpose
ステップ 11	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップコンフィギュレーションにコピーします。

MAC 認証バイパスのイネーブル化

サプリカントの接続されていないインターフェイス上で、MAC 認証バイパスをイネーブルにすることができます。

始める前に

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、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 3	**dot1x mac-auth-bypass** [**eap**] 例： `switch(config-if)# dot1x mac-auth-bypass`	MAC 認証バイパスをイネーブルにします。デフォルトはバイパスのディセーブルです。**eap** キーワードを使用して、許可に EAP を使用するように Cisco NX-OS デバイスを設定します。

ステップ 4	**exit**
	例：
	`switch(config-if)# exit`
	`switch(config)#`
		コンフィギュレーション モードを終了します。

ステップ 5	（任意） **show dot1x all** 例： `switch# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。

	コマンドまたはアクション	目的
ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

デフォルトの 802.1X 認証方法の構成 - MAB

Cisco NX-OS リリース 9.3(5) 以降では、802.1X 対応ポートで受信されるすべてのトラフィックは、MAC認証バイパス（MAB）によってのみ認証できます。Cisco NX-OS リリース 9.3(5) よりも前では、すべてのトラフィックは最初に EAPOL によって認証され、MAB による認証は EAPOL 認証セッションがタイムアウトした後にのみ行われました。

始める前に

Cisco NX-OS デバイスで MAB 機能をイネーブルにします。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet** *slot/port*
	例：
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		インターフェイスを選択し、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 3	**dot1x mac-auth-bypass** 例： `switch(config-if)# dot1x mac-auth-bypass`	MAC 認証バイパスをイネーブルにします。デフォルトはバイパスのディセーブルです。
ステップ 4	[**no**] **dot1x authentication order mab** 例： `switch(config-if)# dot1x authentication order mab`	RADIUS サーバでデータ トラフィックの認証に対して MABをイネーブルにします。このコマンドの no 形式を使用すると、デフォルトの認証方式を EAPOL に変更します。
ステップ 5	**exit** 例：	コンフィグレーション モードを終了します。

	コマンドまたはアクション	目的
	`switch(config-if)# exit` `switch(config)#`	
ステップ 6	（任意） **show dot1x all** 例： `switch# show dot1x all`	802.1X 機能のすべてのステータスおよびコンフィギュレーション情報を表示します。
ステップ 7	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ダイナミック アクセス リストの作成

始める前に

次の状態を確認してください。

- 802.1X MAB クライアントの特定のトラフィック クラスを許可またはブロックするように、すべての ACE で ACL 名（acl-name）を事前にプログラムします。デバイスに設定されている ACL 名（acl-name）は、ISE サーバから受信する acl-name と一致する必要があります。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**hardware access-list tcam region ing-dacl** *tcam size*
	例：
	`switch(config)# hardware access-list tcam region ing-dacl 256`
	`switch(config)#`
		TCAM サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。

ステップ 3	**ip access-list** *blacklist* 例： `switch(config)# ip access-list creative_blacklist`	定義済みのブラックリストを設定し、設定された TCAM サイズに基づいて適用します。

	コマンドまたはアクション	目的
ステップ 4	（任意） **show ip access-list** 例： `switch(config)# ip access-list creative_blacklist1`	設定済みの IP アクセス リストを表示します。

ステップ 5	（任意） **show ip access-list dynamic**
	例：
	`switch(config)# ip access-list creative_blacklist1_new_Ethernet1/1 statistics per-entry`
	`10 permit udp 0000.1b40.ff13 0000.0000.0000 any range bootps bootpc vlan 100 [match=123]`
	`20 permit udp 0000.1b40.ff13 0000.0000.0000 any eq domain vlan 100 [match=456]`
	`30 deny 0000.1b40.ff13 0000.0000.0000 any [match=789]`
		設定済みの IP アクセス リストを表示します。

ステップ 6	（任意） **copy running-config startup-config** 例： `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

ユーザ単位の DACL 設定

Cisco ISE サーバでユーザごとの DACL を設定できます。その後、さまざまなユーザおよびユーザ グループがネットワークにアクセスする方法を制御するために、これを許可ポリシーに実装できます。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`switch# configure terminal`
	`switch(config)#`
		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 2	**hardware access-list tcam region ing-dacl** 例： `switch(config)# hardware access-list tcam region ing-dacl`	新しい DACL-TCA Mリージョンを作成するようにスイッチで TCAM を設定します。

	コマンドまたはアクション	目的

ステップ 3	**exit**
	例：
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	**reload** 例： `switch# reload`	Cisco NX-OS デバイスをリロードします。

次のタスク

ISE のブロックリストされたクライアントの DACL を設定します。

（注） ISE の ACE には、すべての DACL クライアントに対して暗黙的な拒否が内部的に追加されるため、IP の拒否ルールを設定しないでください。

ブロックリスト クライアントは 802.1X ポートに接続し、radius access-accept メッセージの一部として ACL AV-Pair をダウンロードします。受信した ACL は、特定のクライアントのポートに適用されます。

DACL の設定方法の詳細については、『*Cisco ID* サービス エンジン管理者ガイド、リリース *3.0*』の「セグメント」の章にある「ダウンロード可能な *ACL* の権限を設定する」の項を参照してください。

シングル ホスト モードまたはマルチ ホスト モードのイネーブル化

インターフェイス上でシングル ホスト モードまたはマルチ ホスト モードをイネーブルにすることができます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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。

	Command or Action	Purpose

ステップ 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、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 3	**dot1x host-mode** {**multi-host** | **single-host**} **Example:** `switch(config-if)# dot1x host-mode multi-host`	ホスト モードを設定します。デフォルトは、single-host です。 **Note** 指定したインターフェイスで **dot1x port-control** インターフェイス設定コマンドが **auto** に設定されていることを確認してください。
ステップ 4	**dot1x host-mode multi-auth** **Example:** `switch(config-if)# dot1x host-mode multi-auth`	複数認証モードを設定します。ポートは、EAP または MAB のいずれか、または両方の組み合わせが正常に認証された場合にのみ許可されます。認証に失敗すると、ネットワーク アクセスが制限されます。 EAP または MAB の認証

ステップ 5	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		コンフィギュレーション モードを終了します。

ステップ 6	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 7	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Cisco NX-OS デバイスでの 802.1X 認証の無効化

Cisco NX-OS デバイス上の 802.1X 認証を無効にできます。デフォルトでは、802.1X 機能を有効にすると、Cisco NX-OS ソフトウェアが 802.1X 認証を有効にします。ただし、802.1X 機能を無効にした場合、設定は Cisco NX-OS デバイスから削除されます。Cisco NX-OS ソフトウェアでは、802.1X の設定を失わずに 802.1X 認証を無効にできます。

Note 802.1X認証を無効にすると、設定されているポートモードに関係なく、すべてのインターフェイスのポート モードがデフォルトの force-authorized になります。802.1X 認証を再び有効にすると、Cisco NX-OS ソフトウェアはインターフェイス上に設定したポート モードを復元します。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 2	**no dot1x system-auth-control** **Example:** `switch(config)# no dot1x system-auth-control`	Cisco NX-OS デバイス上の 802.1X 認証を無効にします。デフォルトでは有効になっています。 **Note** Cisco NX-OS デバイス上の 802.1X 認証を有効にするには、**dot1x system-auth-control** コマンドを使用します。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **show dot1x** **Example:** `switch# show dot1x`	802.1X機能のステータスを表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 機能のディセーブル化

Cisco NX-OS デバイス上の 802.1X 機能をディセーブルにできます。

802.1Xをディセーブルにすると、関連するすべての設定が自動的に廃棄されます。CiscoNX-OSソフトウェアは、802.1Xを再度イネーブルにして設定を回復する場合に使用できる自動チェックポイントを作成します。詳細については、ご使用のプラットフォームの『*Cisco NX-OS* システム管理設定ガイド』を参照してください。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 2	**no feature dot1x** **Example:** `switch(config)# no feature dot1x`	802.1X 機能をディセーブルにします。 **Caution** 802.1X 機能をディセーブルにすると、802.1X のすべての設定が削除されます。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		設定モードを終了します。

ステップ 4	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X インターフェイス設定のデフォルト値へのリセット

インターフェイスの 802.1X 設定をデフォルト値にリセットすることができます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能を有効にします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)`
		設定するインターフェイスを選択し、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 3	**dot1x default** **Example:** `switch(config-if)# dot1x default`	インターフェイスの 802.1X 設定をデフォルト値に戻します。

ステップ 4	**exit**
	Example:
	`switch(config-if)# exit`
	`switch(config)#`
		コンフィグレーション モードを終了します。

ステップ 5	(Optional) **show dot1x all** **Example:** `switch(config)# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

インターフェイスでのオーセンティケータとサプリカント間のフレームの最大数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサプリカントに認証要求を再送信する最大回数を設定できます。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、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 3	**dot1x max-req** *count* **Example:** `switch(config-if)# dot1x max-req 3`	最大認証要求リトライ回数を変更します。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。 **Note** 指定したインターフェイスで **dot1x port-control** インターフェイス設定コマンドが **auto** に設定されていることを確認してください。

ステップ 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		インターフェイス コンフィギュレーション モードを終了します。

ステップ 5	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 認証の RADIUS アカウンティングのイネーブル化

802.1X 認証のアクティビティに対する RADIUS アカウンティングをイネーブルにできます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose

ステップ 1	**configure terminal**
	Example:
	`switch# configure terminal`
	`switch(config)#`
		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 2	**dot1x radius-accounting** **Example:** `switch(config)# dot1x radius-accounting`	802.1X に対する RADIUS アカウンティングをイネーブルにします。デフォルトではディセーブルになっています。

ステップ 3	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		コンフィギュレーション モードを終了します。

ステップ 4	(Optional) **show dot1x** **Example:** `switch# show dot1x`	802.1X の設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config** **Example:** `switch# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X の AAA アカウンティング方式の設定

802.1X 機能に対する AAA アカウンティング方式をイネーブルにできます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	**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 2	**aaa accounting dot1x default group** *group-list*	802.1X に対する AAA アカウンティングをイネーブルにします。デフォルトではディセーブルになっています。

	Command or Action	Purpose
		group-list 引数には、グループ名をスペースで区切ったリストを指定します。グループ名は、次のように指定します。 • **radius**：設定済みのすべての RADIUS サーバ • *named-group*：設定済みの任意の RADIUS サーバ グループ名
ステップ 3	**exit**	コンフィギュレーション モードを終了します。
ステップ 4	(Optional) **show aaa accounting**	AAA アカウンティングの設定を表示します。
ステップ 5	(Optional) **copy running-config startup-config**	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

Example

次に、802.1X 機能を有効にする例を示します。

```
switch# configure terminal
switch(config)# aaa accounting dot1x default group radius
switch(config)# exit
switch# show aaa accounting
switch# copy running-config startup-config
```

インターフェイスでの再認証最大リトライ回数の設定

セッションがタイムアウトするまでに、Cisco NX-OS デバイスがインターフェイス上でサプリカントに再認証要求を再送信する最大回数を設定できます。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	**configure terminal** **Example:**	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。

	Command or Action	Purpose
	`switch# configure terminal` `switch(config)#`	

ステップ 2	**interface ethernet** *slot/port*
	Example:
	`switch(config)# interface ethernet 2/1`
	`switch(config-if)#`
		設定するインターフェイスを選択し、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 3	**dot1x max-reauth-req** *retry-count* **Example:** `switch(config-if)# dot1x max-reauth-req 3`	最大再認証要求リトライ回数を変更します。デフォルトは2回です。有効な範囲は 1 ～ 10 回です。

ステップ 4	**exit**
	Example:
	`switch(config)# exit`
	`switch#`
		インターフェイスコンフィギュレーション モードを終了します。

ステップ 5	(Optional) **show dot1x all** **Example:** `switch# show dot1x all`	802.1X 機能のすべてのステータスおよび設定情報を表示します。
ステップ 6	(Optional) **copy running-config startup-config** **Example:** `switch(config)# copy running-config startup-config`	実行コンフィギュレーションを、スタートアップ コンフィギュレーションにコピーします。

802.1X 設定の確認

802.1X 情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
show dot1x	802.1X 機能のステータスを表示します。
show dot1x all [**details** | **statistics** | **summary**]	802.1X機能のすべてのステータスおよび設定情報を表示します。
show dot1x interface ethernet *slot/port* [**details** | **statistics** | **summary**]	イーサネットインターフェイスの802.1X機能のステータスおよび設定情報を表示します。
show running-config dot1x [**all**]	実行コンフィギュレーション内の 802.1X 機能の設定を表示します。

コマンド	目的
show startup-config dot1x	スタートアップ コンフィギュレーション内の 802.1X 機能の設定を表示します。

これらのコマンドの出力フィールドの詳細については、ご使用のプラットフォームの『*Cisco NX-OS* セキュリティ コマンド リファレンス』を参照してください。

次に、認証された状態のオーセンティケータとサプリカントの両方としてのポートのEAP-TLS設定に関する情報を表示する例を示します。

```
switch(config)# show dot1x int eth 5/6 details

Dot1x Info for Ethernet5/6
-----------------------------------
                      PAE = AUTHENTICATOR
              PortControl = AUTO
                 HostMode = MULTI HOST
         ReAuthentication = Disabled
              QuietPeriod = 60
           ServerTimeout = 30
              SuppTimeout = 30
            ReAuthPeriod = 3600 (Locally configured)
               ReAuthMax = 2
                  MaxReq = 2
                 TxPeriod = 30
          RateLimitPeriod = 0
         InactivityPeriod = 0
          Mac-Auth-Bypass = Disabled

Dot1x Info for Ethernet5/6
-----------------------------------
                      PAE = SUPPLICANT
               StartPeriod = 30
                AuthPeriod = 30
                HeldPeriod = 60
                  MaxStart = 3

Dot1x Authenticator Client List
-------------------------------
               Supplicant = C4:B2:39:2C:EE:50
                   Domain = DATA
            Auth SM State = AUTHENTICATED
       Auth BEND SM State = IDLE
              Port Status = AUTHORIZED
    Authentication Method = EAP
         Authenticated By = Remote Server
                Auth-Vlan = 0
             DACL-Applied = False

Dot1x Supplicant Client List
-------------------------------
            Authenticator = C4:B2:39:2C:EE:50
        Supp SM State = AUTHENTICATED
        Supp Bend SM State = IDLE
              Port Status = AUTHORIZED
```

VXLAN EVPN の 802.1X サポート

このセクションでは、VXLAN EVPN の 802.1X 機能の構成方法について説明します。

VXLAN EVPN の 802.1X サポートに関する注意事項と制約事項

VXLAN EVPN の 802.1X サポートに関する注意事項と制約事項を次に示します。

- Cisco NX-OS リリース 9.3(7) 以降では、VXLAN EVPN 機能の 802.1X サポートが Cisco Nexus 9300-GX プラットフォーム スイッチでサポートされます。
- ポート チャネル インターフェイスまたはポート チャネルのメンバー ポートはサポートされません。
- vPC ポートはサポートされません。
- この機能の現在のサポートでは、802.1X セキュア MAC 更新のために BGP-EVPN コントロール プレーンで定期的および動的な EVPN 更新を使用します。そのため、グローバル ポリシーが「dot1x mac-move deny」であっても、EVPN をまたいで移動することはできません。
- 「dot1x mac-move」ポリシーがファブリック全体で同じに設定されていることを確認します。ノード間で設定の検証は行われないため、設定ポリシーが同期していない場合は予期しない動作が発生する可能性があります。
- 拒否モードと許可モードのローカルからリモートへの MAC 移動動作は許可されます。したがって、拒否モードが有効になっていても、MAC 移動は許可されます。
- 802.1X とポート セキュリティ ポートが異なる VLAN を使用していることを確認します。同じ VLAN を両方のポートに割り当てることはできません。
- 802.1X は VLAN を認識しないため、2 つの異なる VLAN で同じ MAC を使用することはできません。選択された MAC 移動モードに応じて、MAC は新しい VLAN に移動されるか、拒否されます。
- スタティック MAC とセキュア MAC を同時に設定することはできません。
- -R ライン カードを搭載した Cisco Nexus 9504 および Cisco Nexus 9508 プラットフォーム スイッチは、VXLAN でのマルチ認証およびマルチ認証をサポートしていません。
- RADIUS の認可変更は VXLAN EVPN によりサポートされています。
- スケール設定の推奨再認証時間間隔はデフォルト値で、3600 秒です。
- 802.1X はファブリック ピアリングではサポートされていません。

VXLAN EVPN の 802.1X サポートの設定

この手順では、VXLAN EVPN の 802.1X を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `switch# 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 2	**feature dot1x** 例： `switch(config)# feature dot1x`	802.1X 機能をイネーブルにします。デフォルトではディセーブルになっています。
ステップ 3	**dot1x mac-move {permit | deny}** 例： `switch(config)# dot1x mac-move permit`	**deny** パラメータは MAC 移動を拒否します。**permit** パラメータは MAC 移動を許可します。

ステップ 4	（任意） **show running-config dot1x all**
	例：
	`switch(config)# show running-config dot1x all`
	
	`!Command: show running-config dot1x all`
	`!No configuration change since last restart`
	`!Time: Thu Sep 20 10:22:58 2018`
	
	`version 9.2(2) Bios:version 07.64`
	`feature dot1x`
	
	`dot1x system-auth-control`
	`dot1x mac-move deny`
	
	`interface Ethernet1/1`
	`  dot1x host-mode multi-auth`
	`  dot1x pae authenticator`
	`  dot1x port-control auto`
	`  no dot1x re-authentication`
	`  dot1x max-req 1`
	`  dot1x max-reauth-req 2`
	`  dot1x timeout quiet-period 60`
	`  dot1x timeout re-authperiod 3600`
	`  dot1x timeout tx-period 1`
	`  dot1x timeout server-timeout 30`
	`  dot1x timeout ratelimit-period 0`
	`  dot1x timeout supp-timeout 30`
	`  dot1x timeout inactivity-period 0`
	`  dot1x mac-auth-bypass`
	
	`interface Ethernet1/33`
		802.1X の設定を表示します。

	コマンドまたはアクション	目的
	dot1x host-mode multi-auth dot1x pae authenticator dot1x port-control auto no dot1x re-authentication dot1x max-req 1 dot1x max-reauth-req 2 dot1x timeout quiet-period 60 dot1x timeout re-authperiod 3600 dot1x timeout tx-period 1 dot1x timeout server-timeout 30 dot1x timeout ratelimit-period 0 dot1x timeout supp-timeout 30 dot1x timeout inactivity-period 0 dot1x mac-auth-bypass	

VXLAN EVPNの 802.1X サポートの確認

VXLAN EVPN の構成情報での 802.1X サポートを表示するには、次のいずれかのコマンドを入力します。

コマンド	目的
show running-config dot1x all	802.1X の実行構成を表示します。
show dot1x all summary	インターフェイスのステータスを表示します。
show dot1x	デフォルト設定を表示します。
show dot1x all	インターフェイスの詳細を表示します。

show running-config dot1x all コマンドの例

```
switch# show running-config dot1x all
!Command: show running-config dot1x all
!No configuration change since last restart
!Time: Thu Sep 20 10:22:58 2018

version 9.2(2) Bios:version 07.64
feature dot1x

dot1x system-auth-control
dot1x mac-move deny


interface Ethernet1/1
  dot1x host-mode multi-auth
  dot1x pae authenticator
  dot1x port-control auto
  no dot1x re-authentication
  dot1x max-req 1
  dot1x max-reauth-req 2
  dot1x timeout quiet-period 60
  dot1x timeout re-authperiod 3600
  dot1x timeout tx-period 1
  dot1x timeout server-timeout 30
  dot1x timeout ratelimit-period 0
```

```
  dot1x timeout supp-timeout 30
  dot1x timeout inactivity-period 0
  dot1x mac-auth-bypass

interface Ethernet1/33
  dot1x host-mode multi-auth
  dot1x pae authenticator
  dot1x port-control auto
  no dot1x re-authentication
  dot1x max-req 1
  dot1x max-reauth-req 2
  dot1x timeout quiet-period 60
  dot1x timeout re-authperiod 3600
  dot1x timeout tx-period 1
  dot1x timeout server-timeout 30
  dot1x timeout ratelimit-period 0
  dot1x timeout supp-timeout 30
  dot1x timeout inactivity-period 0
  dot1x mac-auth-bypass
```

show dot1x all summary コマンドの例

```
switch# show dot1x all summary

           Interface     PAE              Client          Status
-----------------------------------------------------------------
         Ethernet1/1    AUTH               none    UNAUTHORIZED

           Interface     PAE              Client          Status
-----------------------------------------------------------------
        Ethernet1/33    AUTH   00:16:5A:4C:00:07      AUTHORIZED
                               00:16:5A:4C:00:06      AUTHORIZED
                               00:16:5A:4C:00:05      AUTHORIZED
                               00:16:5A:4C:00:04      AUTHORIZED
switch#
switch# show mac address-table vlan 10
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
*   10     0016.5a4c.0004   secure   -         T      F    Eth1/33
*   10     0016.5a4c.0005   secure   -         T      F    Eth1/33
*   10     0016.5a4c.0006   secure   -         T      F    Eth1/33
*   10     0016.5a4c.0007   secure   -         T      F    Eth1/33

switch#
switch# show mac address-table vlan 10 (VPC-PEER)
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
*   10     0016.5a4c.0004   secure   -         T      F    vPC Peer-Link
*   10     0016.5a4c.0005   secure   -         T      F    vPC Peer-Link
*   10     0016.5a4c.0006   secure   -         T      F    vPC Peer-Link
*   10     0016.5a4c.0007   secure   -         T      F    vPC Peer-Link

switch#
switch# show mac address-table vlan 10 (RVTEP)
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, O - Overlay MAC
```

```
        age - seconds since last seen,+ - primary entry using vPC Peer-Link,
        (T) - True, (F) - False, C - ControlPlane MAC, ~ - vsan
   VLAN     MAC Address      Type      age     Secure NTFY Ports
---------+-----------------+--------+---------+------+----+------------------
C   10     0016.5a4c.0004   dynamic  0         F      F    nve1(67.67.67.67)
C   10     0016.5a4c.0005   dynamic  0         F      F    nve1(67.67.67.67)
C   10     0016.5a4c.0006   dynamic  0         F      F    nve1(67.67.67.67)
C   10     0016.5a4c.0007   dynamic  0         F      F    nve1(67.67.67.67)
```

show dot1x コマンドの例

```
switch# show dot1x
          Sysauthcontrol Enabled
   Dot1x Protocol Version 2
                Mac-Move Deny
```

show dot1x all コマンドの例

```
switch# show dot1x  all
          Sysauthcontrol Enabled
   Dot1x Protocol Version 2
                Mac-Move Deny

Dot1x Info for Ethernet1/1
-----------------------------------
                     PAE = AUTHENTICATOR
             PortControl = AUTO
                HostMode = MULTI AUTH
         ReAuthentication = Disabled
              QuietPeriod = 60
           ServerTimeout = 30
             SuppTimeout = 30
            ReAuthPeriod = 3600 (Locally configured)
               ReAuthMax = 2
                  MaxReq = 1
                TxPeriod = 1
          RateLimitPeriod = 0
         InactivityPeriod = 0
          Mac-Auth-Bypass = Enabled

Dot1x Info for Ethernet1/33
-----------------------------------
                     PAE = AUTHENTICATOR
             PortControl = AUTO
                HostMode = MULTI AUTH
         ReAuthentication = Disabled
              QuietPeriod = 60
           ServerTimeout = 30
             SuppTimeout = 30
            ReAuthPeriod = 3600 (Locally configured)
               ReAuthMax = 2
                  MaxReq = 1
                TxPeriod = 1
          RateLimitPeriod = 0
         InactivityPeriod = 0
          Mac-Auth-Bypass = Enabled
```

クリティカル認証の確認

次の例は、クリティカル認証機能が有効になっているかどうかを表示する方法を示しています。

```
switch(config)# show dot1x
                Sysauthcontrol Enabled
        Dot1x Protocol Version 2
                      Mac-Move Permit
  Server-Dead-Action-Authorize Enabled
```

Server-Dead-Action-Authorize パラメータの値が **Enabled** の場合、クリティカル認証機能が有効になります。

802.1X のモニタリング

Cisco NX-OS デバイスが保持している 802.1X のアクティビティに関する統計情報を表示できます。

Before you begin

Cisco NX-OS デバイスで 802.1X 機能をイネーブルにします。

Procedure

	Command or Action	Purpose
ステップ 1	**show dot1x** {**all** | **interface ethernet** *slot*/*port*} **statistics** **Example:** `switch# show dot1x all statistics`	802.1X 統計情報を表示します。

802.1X の設定例

次に、アクセス ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae authenticator
dot1x port-control auto
```

次に、トランク ポートに 802.1X を設定する例を示します。

```
feature dot1x
aaa authentication dot1x default group rad2
interface Ethernet2/1
dot1x pae authenticator
```

```
dot1x port-control auto
dot1x host-mode multi-host
```

Note 802.1X 認証が必要なすべてのインターフェイスに対して、**dot1x pae authenticator** コマンドおよび **dot1x port-control auto** コマンドを繰り返してください。

ユーザ 1 人あたりの DACL の設定例

次の例は、ポートの 1 つで設定されたユーザごとの DACL を示しています。DACL が適用されると、ブロックリスト トラフィックは除外されます。DACL-Applied パラメータの値が true の場合、クライアントは ISE から ACL を受信したブロックリスト クライアントです。

```
switch# show dot1x all summary
Interface      PAE        Client               Status
Ethernet1/1    AUTH       36:12:61:51:21:52    AUTHORIZED
                          36:12:61:51:21:53    AUTHORIZED

switch# show dot1x all details
----------------------------

Supplicant = 36:12:61:51:21:52
Domain = DATA
Auth SM State = AUTHENTICATED
DACL-Applied = False
------------------------------
Supplicant = 36:12:61:51:21:53
Domain = DATA
Auth SM State = AUTHENTICATED
DACL-Applied = True
```

次に、ブロックリストされたトラフィックを表示する例を示します。

```
switch# show ip access-list dynamic
IP access list DOT1X_Restricted_base_acl_Ethernet1/1_new statistics per-entry fragments
 deny-all
10 permit udp any 3612.6151.2153 0000.0000.0000 any eq 5555 vlan 100 [match=0]
20 permit udp any 3612.6151.2153 0000.0000.0000 any eq 6666 vlan 100 [match=0]
30 deny ip any 3612.6151.2153 0000.0000.0000 any vlan 100 [match=0]
```

802.1X に関する追加情報

ここでは、802.1X の実装に関する追加情報について説明します。

標準

標準	タイトル
IEEE Std 802.1X- 2004（IEEE Std 802.1X-2001 の改訂版）	『*802.1X IEEE Standard for Local and Metropolitan Area Networks Port-Based Network Access Control*』

標準	タイトル
RFC 2284	『*PPP Extensible Authentication Protocol (EAP)*』
RFC 3580	『*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*』

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。