IEEE 802.1X VLAN 割り当て

IEEE 802.1X VLAN 割り当て機能は、アクセスポートに IEEE 802.1X 認証が設定されている場合に自動的に有効になります。これにより、RADIUS サーバーは VLAN 割り当てをデバイスポートに送信できます。この割り当てにより、特定のユーザーのネットワークアクセスを制限できるようにデバイスポートが構成されます。

IEEE 802.1X VLAN 割り当てに関する前提条件

次のタスクは、IEEE 802.1X VLAN 割り当て機能を実装する前に完了する必要があります。

- IEEE 802.1X をデバイス ポートで有効にする必要があります。
- デバイスが RADIUS 設定されていること、および Cisco Secure アクセス コントロール サーバ（ACS）に接続されていることが必要です。RADIUS プロトコルの概念とアクセス コントロール リスト（ACL）の作成および適用方法を理解しておく必要があります。
- EAP サポートを RADIUS サーバで有効にする必要があります。
- ユーザーがログオフしたときに EAP-Logoff（Stop）メッセージがスイッチに送信されるよう、IEEE 802.1X サプリカントを設定する必要があります。IEEE 802.1X サプリカントをこのように設定しないと、EAP-Logoff メッセージはスイッチに送信されず、付随するアカウンティング Stop メッセージが認証サーバーに送信されません。http://support.microsoft.com の Microsoft Knowledge Base の記事を参照し、SupplicantMode レジストリを 3 に設定し、AuthMode レジストリを 1 に設定します。
- すべてのネットワーク関連のサービス要求について、ポートで認証、許可、およびアカウンティング（AAA）を設定する必要があります。認証方式リストを有効化および指定する

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送信を行う手順と認証方式を記述したものです。詳細については、IEEE 802.1X Authenticator 機能モジュールを参照してください。

- ポートの認証に成功する必要があります。

IEEE 802.1X VLAN 割り当て機能は、スイッチポートをサポートする Cisco 89x および 88x シリーズ統合スイッチングルータ（ISR）でのみ使用できます。

次の ISR-G2 ルータがサポートされています。

- 1900
- 2900
- 3900
- 3900e

次のカードまたはモジュールはスイッチ ポートをサポートします。

- ACL をサポートする拡張高速 WAN インターフェイスカード（EHWIC）：
  - EHWIC-4ESG-P
  - EHWIC-9ESG-P
  - EHWIC-4ESG
  - EHWIC-9ESG
- ACL をサポートしない高速 WAN インターフェイスカード（HWIC）：
  - HWIC-4ESW-P
  - HWIC-9ESW-P
  - HWIC-4ESW
  - HWIC-9ES

IEEE 802.1X VLAN 割り当てに関する制約事項

- IEEE 802.1X VLAN 割り当て機能は、スイッチポートでのみ使用できます。
- 次のいずれかの条件が発生すると、デバイスポートは常に設定済みアクセス VLAN に割り当てられます。
  - RADIUS サーバから VLAN が指定されなかった場合。
  - RADIUS サーバからの VLAN 情報が無効だった場合。
  - ポートで IEEE 802.1X 認証が無効になっています。

- ポートのステートが、force authorized、force unauthorized、unauthorized、または shutdown のいずれかだった場合。

（注） アクセス VLAN 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。

- 設定されたアクセス VLAN に割り当てることで、設定エラーが原因でポートが不適切な VLAN に予期せず表示されるのを防ぎます。構成エラーの例には、次のものがあります。
  - 存在しない、または不正な VLAN ID
  - 音声 VLAN ID への割り当てを試みました
- IEEE 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。
- IEEE 802.1X ポートで multihost 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 サーバーにより指定）に配置されます。
- IEEE 802.1X ポートが認証され、RADIUS サーバーによって割り当てられた VLAN に配置された場合、ポートのアクセス VLAN 設定への変更は反映されません。
- この機能は、スイッチポートの標準 ACL をサポートしません。

IEEE 802.1X VLAN 割り当てに関する情報

認可の設定

AAA 許可機能は、ユーザーが実行できることと実行できないことを決定するために使用されます。AAA 許可が有効になっている場合、ネットワーク アクセス サーバーは、ローカル ユーザー データベースまたはセキュリティ サーバーのいずれかにあるユーザー プロファイルから取得した情報を使用して、ユーザーのセッションを設定します。ユーザは、ユーザ プロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

IEEE 802.1X 認証と VLAN の割り当て

デバイスポートは、VLAN 割り当てに使用した IEEE802.1X 認証をサポートします。ポートの IEEE 802.1X 認証が成功すると、RADIUS サーバーは VLAN 割り当てを送信してデバイス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、デバイスポートに接続するサプリカントのユーザー名に基づいて VLAN を割り当てます。

IEEE 802.1X VLAN 割り当てを構成する方法

VLAN 割り当てのための AAA 許可のイネーブル化

AAA 許可によってユーザが使用できるサービスが制限されます。AAA 許可が有効になっていると、デバイスはユーザーのプロファイルから取得した情報を使用します。このプロファイルは、ローカルのユーザーデータベースまたはセキュリティサーバ上にあり、ユーザーのセッションを設定します。ユーザは、ユーザプロファイル内の情報で認められている場合に限り、要求したサービスのアクセスが認可されます。

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。 • 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 radius if-authenticated** 例： `Device(config)# aaa authorization network radius if-authenticated`	ネットワーク関連のすべてのサービス要求に対して、ユーザが RADIUS 許可を受けるように device を設定します。ユーザーが承認されている場合、RADIUS 許可は成功します。
ステップ 5	**aaa authorization exec radius if-authenticated** 例： `Device(config)# aaa authorization exec radius if-authenticated`	ユーザに特権 EXEC のアクセス権限がある場合、ユーザが RADIUS 許可を受けるように device を設定します。ユーザーが承認されている場合、RADIUS 許可は成功します。
ステップ 6	**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。

IEEE 802.1X 認証および承認のイネーブル化

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 authentication dot1x** {**default** | *listname*} *method1* [*method2...*] 例： `Device(config)# aaa authentication dot1x default group radius`	デバイスが AAA サーバと通信できるように、特権コマンド レベルにアクセスするユーザ権限の決定に使用される一連の認証方式を作成します。
ステップ 5	**dot1x system-auth-control** 例： `Device(config)# dot1x system-auth-control`	802.1x ポートベースの認証をグローバルにイネーブルにします。
ステップ 6	**identity profile default** 例： `Device(config)# identity profile default`	アイデンティティ プロファイルを作成し、dot1x プロファイル コンフィギュレーション モードを開始します。
ステップ 7	**exit** 例： `Device(config-identity-prof)# exit`	dot1x プロファイル 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 8	**interface** *type slot/port* 例： `Device(config)# interface Gigabitethernet 1/0/1`	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、802.1X 認証をイネーブルにするインターフェイスを指定します。

	コマンドまたはアクション	目的
ステップ 9	**access-session port-control** {**auto** | **force-authorized** | **force-unauthorized**} 例： `Device(config-if)# access-session port-control auto`	インターフェイス上で 802.1x ポートベースの認証をイネーブルにします。 • **auto**：IEE 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とき、または EAPOL-Start フレームを受信したときに、認証プロセスが開始されます。デバイスはサプリカントの識別を要求し、サプリカントと認証サーバ間で認証メッセージのリレーを開始します。デバイスはサプリカントの 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。 • **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、クライアントの IEEE 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、サプリカントからの認証の試みをすべて無視します。デバイスは、このポートを介してサプリカントに認証サービスを提供することはできません。
ステップ 10	**dot1x pae**[**supplicant** |**authenticator** |**both**] 例： `Device(config-if)# dot1x pae authenticator`	ポートアクセスエンティティ（PAE）のタイプを設定します。 • **supplicant**：インターフェイスはサプリカントとしてだけ機能し、オーセンティケータ向けのメッセージに応答しません。

	コマンドまたはアクション	目的
		• **authenticator**：インターフェイスはオーセンティケータとしてだけ動作し、サプリカント向けのメッセージに応答しません。 • **both**：インターフェイスは、サプリカントおよびオーセンティケータとして動作するため、すべての dot1x メッセージに応答します。
ステップ 11	**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 モードを開始します。
ステップ 12	**show dot1x** 例： `Device# show dot1x`	デバイスで 802.1x 認証が設定されているかどうかを表示します。

RADIUS サーバーデータベースでの許可 VLAN の指定

Internet Engineering Task Force（IETF）ドラフト規格に、ベンダー固有の属性（属性 26）を使用して、デバイスと RADIUS サーバ間でベンダー固有の情報を通信するための方式が定められています。各ベンダーは、Vendor-Specific Attribute（VSA）を使用することによって、一般的な用途には適さない独自の拡張属性をサポートできます。シスコが実装する RADIUS では、この仕様で推奨されるフォーマットを使用して、ベンダー固有のオプションを 1 つサポートしています。

- RADIUS サーバーデータベースで、次のベンダー固有のトンネル属性を割り当てる必要があります。RADIUS サーバは次の属性をデバイス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

属性 [64] は、値 VLAN（タイプ 13）である必要があります。属性 [65] は、値 802（タイプ 6）である必要があります。属性 [81] は、IEEE 802.1X 認証ユーザーに割り当てられた VLAN 名または VLAN ID を指定します。

IEEE 802.1X VLAN 割り当ての設定例

例：VLAN 割り当てのための AAA 許可のイネーブル化

次の例は、VLAN 割り当てに対して AAA 許可を有効にする方法を示しています。

```
Device> enable
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authorization network radius if-authenticated
Device(config)# aaa authorization exec radius if-authenticated
Device(config)# end
```

例：802.1X 認証のイネーブル化

次の例は、デバイスで 802.1X 認証を有効にする方法を示しています。

```
Device# configure terminal
Device(config)# aaa new-model
Device(config)# aaa authentication dot1x default group radius group radius
Device(config)# dot1x system-auth-control
Device(config)# interface gigabitethernet 1/0/1
Device(config-if)# dot1x port-control auto
```

次は、 **show dot1x** コマンドのサンプル出力で、デバイスで設定した 802.1X 認証を示しています。

```
Device# show dot1x all

Sysauthcontrol              Enabled
Dot1x Protocol Version            2
Dot1x Info for GigabitEthernet 1/0/1
-----------------------------------
PAE                       = AUTHENTICATOR
PortControl               = AUTO
ControlDirection          = Both
HostMode                  = MULTI_HOST
ReAuthentication          = Enabled
QuietPeriod               = 600
ServerTimeout             = 60
SuppTimeout               = 30
ReAuthPeriod              = 1800 (Locally configured)
ReAuthMax                 = 2
MaxReq                    = 3
TxPeriod                  = 60
RateLimitPeriod           = 60
```

IEEE 802.1X ポートベース認証に関するその他の参考資料

標準および RFC

標準/RFC	タイトル
IEEE 802.1X	「*Port Based Network Access Control*」
RFC 3580	『*IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines*』

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

IEEE 802.1X VLAN 割り当ての機能履歴

次の表に、このモジュールで説明する機能のリリースおよび関連情報を示します。

これらの機能は、特に明記されていない限り、導入されたリリース以降のすべてのリリースで使用できます。

リリース	機能	機能情報
Cisco IOS XE Gibraltar 16.11.1	IEEE 802.1X VLAN 割り当て	IEEE 802.1X VLAN 割り当て機能は、アクセスポートに IEEE 802.1X 認証が設定されている場合に自動的に有効になります。これにより、RADIUS サーバーは VLAN 割り当てをデバイスポートに送信できます。この割り当てにより、特定のユーザーのネットワークアクセスを制限できるようにデバイスポートが構成されます。

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。