CLIによるスイッチのグローバル802.1xプロパティの設定

概要

IEEE 802.1xは、クライアントとサーバ間のアクセス制御を容易にする標準です。ローカルアクセスネットワーク(LAN)またはスイッチによってクライアントにサービスを提供するには、スイッチポートに接続されたクライアントが、リモート認証ダイヤルインユーザサービス(RADIUS)を実行する認証サーバによって認証される必要があります。

802.1x認証は、不正なクライアントがパブリックにアクセス可能なポートを介してLANに接続するのを制限します。802.1x認証は、クライアントサーバモデルです。このモデルでは、ネットワークデバイスには次の役割があります。

- クライアントまたはサプリカント：クライアントまたはサプリカントは、LANへのアクセスを要求するネットワークデバイスです。クライアントはオーセンティケータに接続されています。
- オーセンティケータ：オーセンティケータは、ネットワークサービスを提供し、サプリカントポートが接続されているネットワークデバイスです。次の認証方式がサポートされています。

  - 802.1x-based：すべての認証モードでサポートされます。802.1xベースの認証では、オーセンティケータは802.1xメッセージまたはEAP over LAN(EAPoL)パケットからExtensible Authentication Protocol(EAP)メッセージを抽出し、RADIUSプロトコルを使用して認証サーバに渡します。

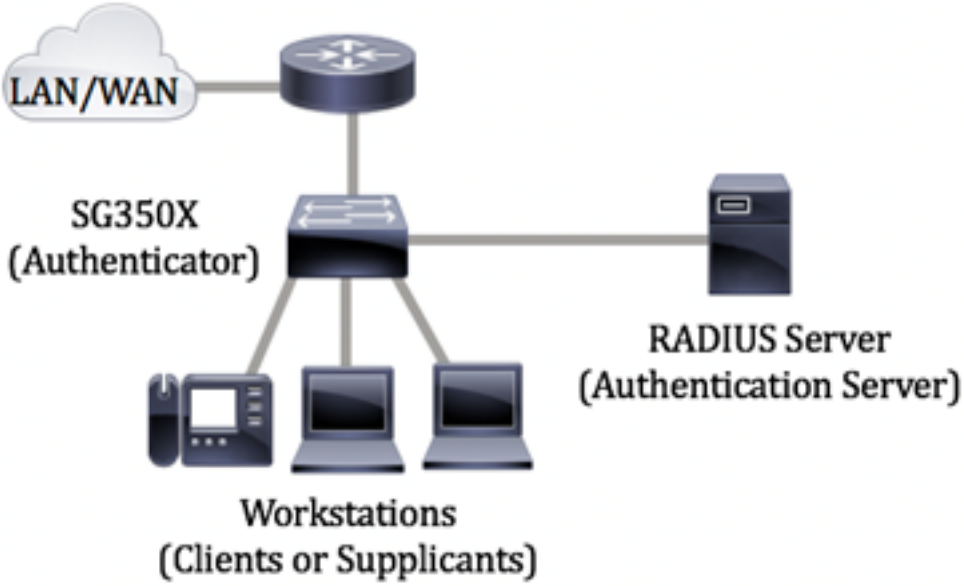
  - MACベース：すべての認証モードでサポートされます。メディアアクセス制御(MAC)ベースでは、オーセンティケータ自体が、ネットワークアクセスを求めるクライアントに代わってソフトウェアのEAPクライアント部分を実行します。

  - Webベース：マルチセッションモードでのみサポートされます。Webベース認証では、オーセンティケータ自体が、ネットワークアクセスを求めるクライアントに代わってソフトウェアのEAPクライアント部分を実行します。

- 認証サーバ：認証サーバは、クライアントの実際の認証を実行します。デバイスの認証サーバは、EAP拡張を備えたRADIUS認証サーバです。

  注：ネットワークデバイスは、クライアントまたはサプリカント、オーセンティケータ、または両方のポートを使用できます。

  次の図は、特定のロールに従ってデバイスを設定したネットワークを示しています。この例では、SG350Xスイッチが使用されています。



ガイドライン イン 802.1xの設定:

1. RADIUS サーバを設定します。スイッチのRADIUSサーバーの設定方法については、ここをクリックしてください。
2. 仮想ローカルエリアネットワーク(VLAN)を設定します。 スイッチのWebベースのユーティリティを使用してVLANを作成するには、ここをクリックします。CLIベースの手順については、ここをクリックします。
3. スイッチのポートからVLANへの設定を行います。Webベースのユーティリティを使用して設定するには、ここをクリックします。CLIを使用するには、ここをクリックします。
4. スイッチのグローバル802.1xプロパティを設定します。スイッチのWebベースのユーティリティを使用してグローバル802.1xプロパティを設定する方法については、ここをクリックしてください。
5. （オプション）スイッチで時間範囲を設定します。スイッチで時間範囲を設定する方法については、ここをクリックしてください。
6. 802.1xポート認証を設定します。スイッチのWebベースのユーティリティを使用するには、ここをクリックします。

目的

この記事では、認証およびゲストVLANプロパティを含む、スイッチのコマンドラインインターフェイス(CLI)を使用してグローバル802.1xプロパティを設定する方法について説明します。ゲストVLANは、加入しているデバイスやポートを802.1x、MACベース、またはWebベースの認証を介して認証および許可する必要のないサービスにアクセスできるようにします。

該当するデバイス

- Sx300シリーズ
- Sx350シリーズ
- SG350Xシリーズ
- Sx500シリーズ
- Sx550Xシリーズ

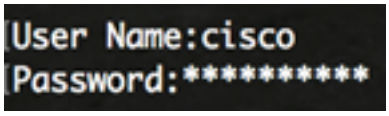
[Software Version]

- 1.4.7.06 — Sx300、Sx500
- 2.2.8.04 — Sx350、SG350X、Sx550X

CLIによるスイッチの802.1xプロパティの設定

802.1xの設定

ステップ1：スイッチコンソールにログインします。デフォルトのユーザ名とパスワードはcisco/ciscoです。新しいユーザ名またはパスワードを設定している場合は、クレデンシャルを入力します。



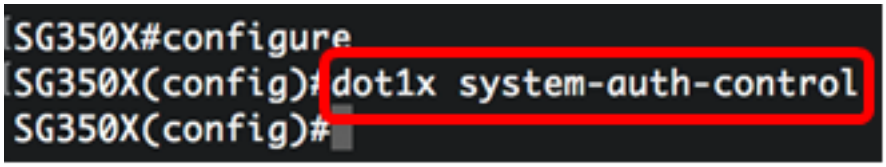
注：コマンドは、スイッチの正確なモデルによって異なる場合があります。この例では、SG350Xスイッチにtelnetでアクセスします。

ステップ2：スイッチの特権EXECモードから、次のように入力してグローバルコンフィギュレーションモードに入ります。

```
SG350X#configure
```

ステップ3：スイッチで802.1x認証をグローバルに有効にするには、グローバルコンフィギュレーションモードで**dot1x system-auth-control**コマンドを使用します。

```
SG350x(config)#dotx1 system-auth-control
```



ステップ4: (オプション) スイッチで802.1x認証をグローバルに無効にするには、次のように入力します。

```
SG350x(config)#no dotx1 system-auth-control
```

注：これが無効になっている場合、802.1X、MACベース、およびWebベースの認証は無効になります。

ステップ5:802.1x認証が有効な場合に、認証に使用するサーバを指定するには、次のように入力します。

```
SG350x(config)#aaa authentication dot1x default [radius none | radius |]
```

次のオプションがあります。

- radius none:RADIUSサーバを使用して、最初にポート認証を実行します。サーバがダウンしたときなど、サーバからの応答がない場合、認証は行われず、セッションは許可されます。サーバが使用可能で、ユーザクレデンシャルが正しくない場合、アクセスが拒否され、セッションが終了します。

- radius:RADIUSサーバに基づいてポート認証を実行します。認証が実行されない場合、セッションは終了します。これはデフォルトの認証です。
- none：ユーザを認証せず、セッションを許可します。

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#
```

注：この例では、デフォルトの802.1x認証サーバはRADIUSです。

ステップ6:（オプション）デフォルト認証を復元するには、次のように入力します。

```
SG350X(config)#no aaa authentication dot1x default
```

ステップ7：グローバルコンフィギュレーションモードで、次のように入力してVLANインターフェイスコンフィギュレーションコンテキストを入力します。

```
SG350X(config)#interface vlan [vlan-id]
```

- vlan-id：設定するVLAN IDを指定します。

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#
```

ステップ8：権限のないポートに対してゲストVLANを使用できるようにするには、次のように入力します。

```
SG350X(config-if)#dot1x guest-vlan
```

注：ゲストVLANが有効になっている場合、すべての不正ポートがゲストVLANで選択されたVLANに自動的に参加します。ポートが後で承認されると、ゲストVLANから削除されます。

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#dot1x guest-vlan
SG350X(config-if)#
```

ステップ9：インターフェイス設定コンテキストを終了するには、次のように入力します。

```
SG350X(config-if)#exit
```

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#dot1x guest-vlan
SG350X(config-if)#exit
SG350X(config)#
```

ステップ10:802.1X（またはポートアップ）を有効にしてからゲストVLANにポートを追加するまでの時間遅延を設定するには、次のように入力します。

```
SG350X(config)#dot1x guest-vlan timeout [timeout]
```

- timeout:802.1X（またはポートアップ）を有効にしてからゲストVLANにポートを追加するまでの遅延時間（秒）を指定します。範囲は30 ~ 180秒です。

注：リンクアップ後、ソフトウェアが802.1xサプリカントを検出しない場合、またはポート認証が失敗した場合、そのポートはゲストVLANタイムアウト期間が経過した後にのみゲストVLANに追加されます。ポートが[Authorized]から[Not Authorized]に変更された場合、そのポートは[Guest VLAN Timeout]期間が経過した後にのみゲストVLANに追加されます。VLAN認証を有効または無効にするには、VLAN認証を使用します。

```
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#
```

注：この例では、使用されるゲストVLANタイムアウトは60秒です。

ステップ11：トラップを有効にするには、次のオプションの1つ以上をチェックします。

```
SG350X(config)# dot1x traps authentication [failure | | quiet] [802.1x | mac | web]
```

次のオプションがあります。

- 802.1x authentication failure traps:802.1x認証が失敗した場合にトラップを送信します。
- 802.1x authentication success traps:802.1x認証が成功した場合にトラップを送信します。
- mac authentication failure traps:MAC認証が失敗した場合にトラップを送信します。
- mac authentication success traps:MAC認証が成功した場合にトラップを送信します。
- web authentication failure traps:Web認証が失敗した場合にトラップを送信します。
- web authentication success traps:Web認証が成功した場合にトラップを送信します。
- web authentication quiet traps：クワイエット期間が始まったらトラップを送信します。

注：この例では、802.1x認証失敗と成功トラップが入力されています。

```
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#dot1x traps authentication success 802.1x
SG350X(config)#dot1x traps authentication failure 802.1x
SG350X(config)#
```

ステップ12：インターフェイス設定コンテキストを終了するには、次のように入力します。

```
SG350X(config)#exit
```

```
SG350X#configure
SG350X(config)#dot1x system-auth-control
SG350X(config)#aaa authentication dot1x default radius
SG350X(config)#interface vlan 10
SG350X(config-if)#dot1x guest-vlan
SG350X(config-if)#exit
SG350X(config)#dot1x guest-vlan timeout 60
SG350X(config)#dot1x traps authentication success 802.1x
SG350X(config)#dot1x traps authentication failure 802.1x
SG350X(config)#exit
SG350X#
```

ステップ13: (オプション) スイッチに設定されているグローバル802.1xプロパティを表示するには、次のように入力します。

```
SG350X#show dot1x
```

```
SG350X(config)#exit
SG350X#show dot1x

Authentication is enabled
Authenticating Servers: Radius
Unauthenticated VLANs: 20
Guest VLAN: VLAN 10, timeout 60 sec
Authentication failure traps are enabled for 802.1x
Authentication success traps are enabled for 802.1x
Authentication quiet traps are disabled
```

これで、スイッチの802.1xプロパティが正しく設定されました。

VLAN認証の設定

802.1xが有効な場合、不正なポートまたはデバイスは、ゲストVLANまたは非認証VLANの一部でない限り、VLANにアクセスできません。ポートをVLANに手動で追加する必要があります。

VLANで認証を無効にするには、次の手順を実行します。

ステップ1：スイッチの特権EXECモードから、次のように入力してグローバルコンフィギュレーションモードに入ります。

```
SG350X#configure
```

ステップ2：グローバルコンフィギュレーションモードで、次のように入力してVLANインターフェイスコンフィギュレーションコンテキストを入力します。

```
KSG350x(config)# interface vlan [vlan-id]
```

- vlan-id：設定するVLAN IDを指定します。

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#
```

注：この例では、VLAN 20が選択されています。

ステップ3:VLANで802.1x認証を無効にするには、次のように入力します。

SG350X(config-if)#dot1x auth-not-req

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#dot1x auth-not-req
SG350X(config-if)#
```

ステップ4:（オプション）VLANで802.1x認証を有効にするには、次のように入力します。

SG350X(config-if)#no dot1x auth-not-req

ステップ5：インターフェイス設定コンテキストを終了するには、次のように入力します。

```
SG350X#configure
SG350X(config)#interface vlan 20
SG350X(config-if)#dot1x auth-not-req
SG350X(config-if)#end
SG350X#
```

ステップ6:（オプション）スイッチの802.1xグローバル認証設定を表示するには、次のように入力します。

```
SG350X(config-if)#end
SG350X#show dot1x

Authentication is enabled
Authenticating Servers: Radius
Unauthenticated VLANs: 20
Guest VLAN: VLAN 10, timeout 60 sec
Authentication failure traps are enabled for 802.1x
Authentication success traps are enabled for 802.1x
Authentication quiet traps are disabled
```

注：この例では、VLAN 20が非認証VLANとして示されています。

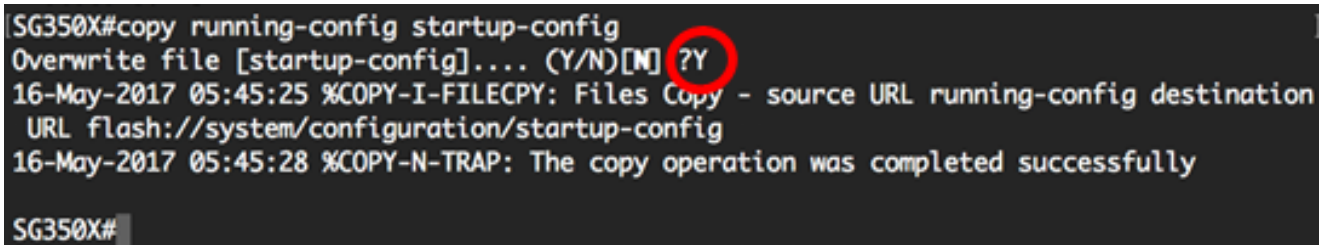
ステップ7:（オプション）スイッチの特権EXECモードで、次のように入力して、設定した設定をスタートアップコンフィギュレーションファイルに保存します。

```
SG350X#copy running-config startup-config
```

```
SG350X#copy running-config startup-config
Overwrite file [startup-config].... (Y/N)[N] ?
```

ステップ8:（オプション）Overwrite file [startup-config]..プロンプトが表示されたら、キー

ボードで**Y**（はい）を押し、No（いいえ）を押します。



これで、スイッチのVLANで802.1x認証設定が正常に設定されたはずです。

重要：スイッチの802.1xポート認証設定の設定に進むには、上記のガイドラインに従ってください。