Catalyst 3550 シリーズ スイッチ上の 802.1x 有線認証と ACS バージョン 4.2 の設定例

目次

概要

このドキュメントでは、Cisco Access Control Server（ACS）バージョン 4.2 と有線認証用の Remote Access Dial In User Service（RADIUS）プロトコルを使用した基本的な IEEE 802.1x 設定例を示します。

前提条件

要件

シスコでは次を推奨しています。

- ACS とスイッチの間の IP 到達可能性を確認する。
- ACS とスイッチの間で User Datagram Protocol（UDP）ポート 1645 および 1646 が開いていることを確認する。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Catalyst 3550シリーズスイッチ
- Cisco Secure ACS バージョン 4.2

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中

のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

設定

スイッチの設定例

1. RADIUS サーバと事前共有キーを定義するために、次のコマンドを入力します。

```
Switch(config)# radius-server host 192.168.1.3  key  cisco123
```

2. 802.1x 機能を有効にするために、次のコマンドを入力します。

```
Switch(config)# dot1x system-auth-control
```

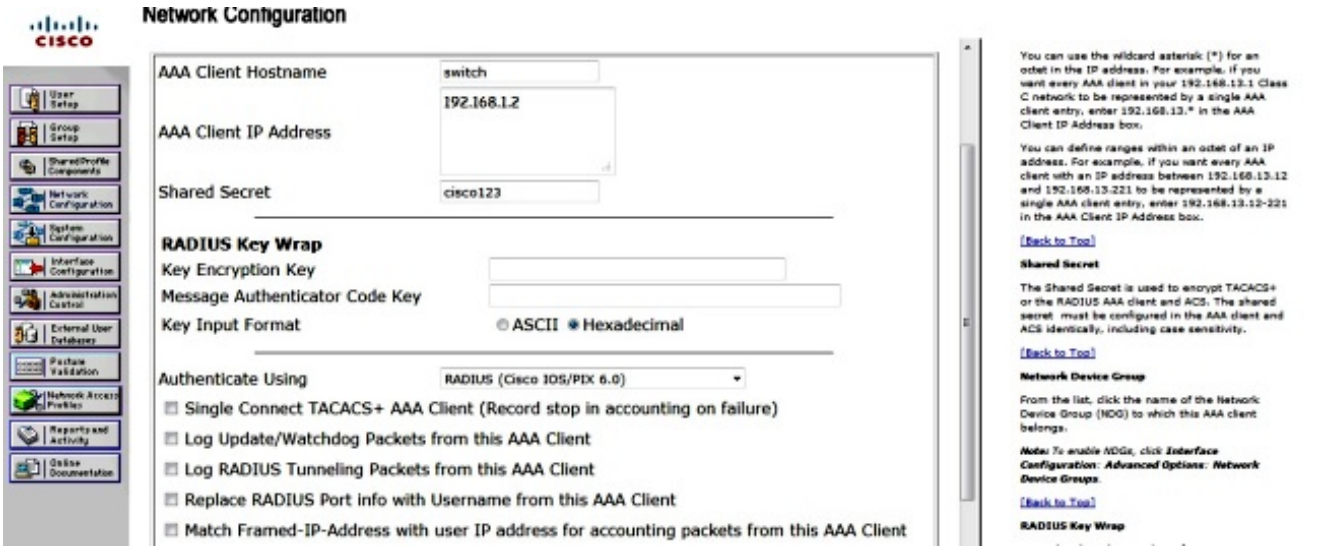
3. 認証、認可、およびアカウンティング（AAA）と RADIUS の認証および認可をグローバルに有効にするために、次のコマンドを入力します。
注: この手順は、RADIUS サーバから属性を渡す必要がある場合には必須です。 それ以外の場合は省略できます。

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
awitch(Config)# aaa authorization network default group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
```

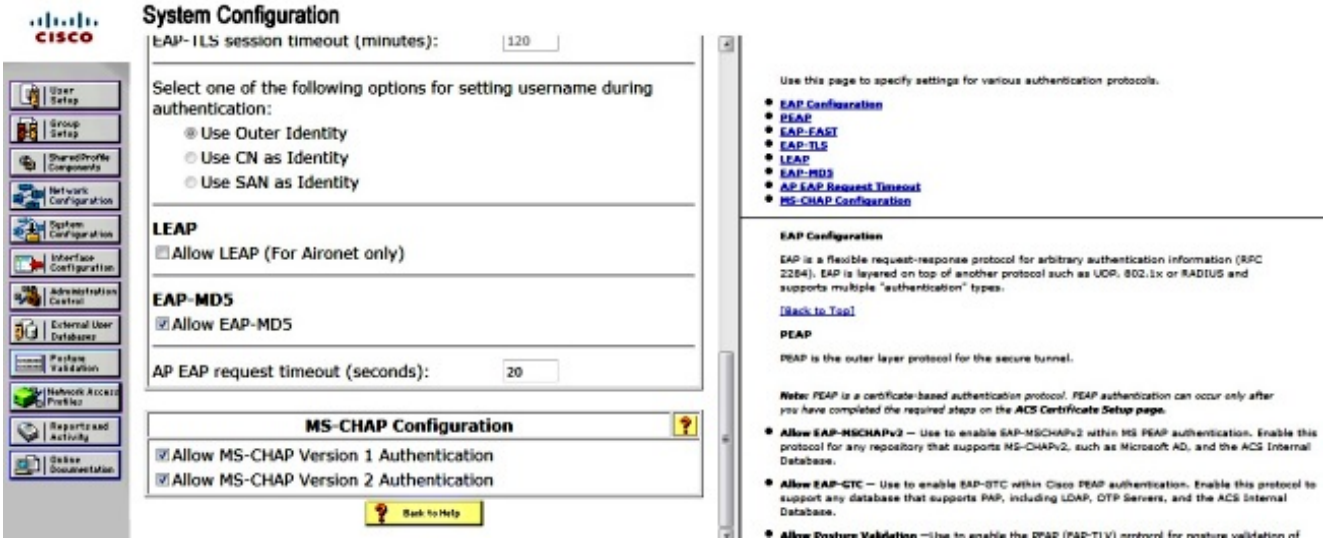
```
Switch(config-if)# switchport mode acces
Switch(config-if)# switchport access vlan <vlan>
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
Switch(config-if)# dot1x timeout quiet-period <seconds to wait after failed attempt>
Switch(config-if)# dot1x timeout tx-period <time to resubmit request>
```

ACS 設定

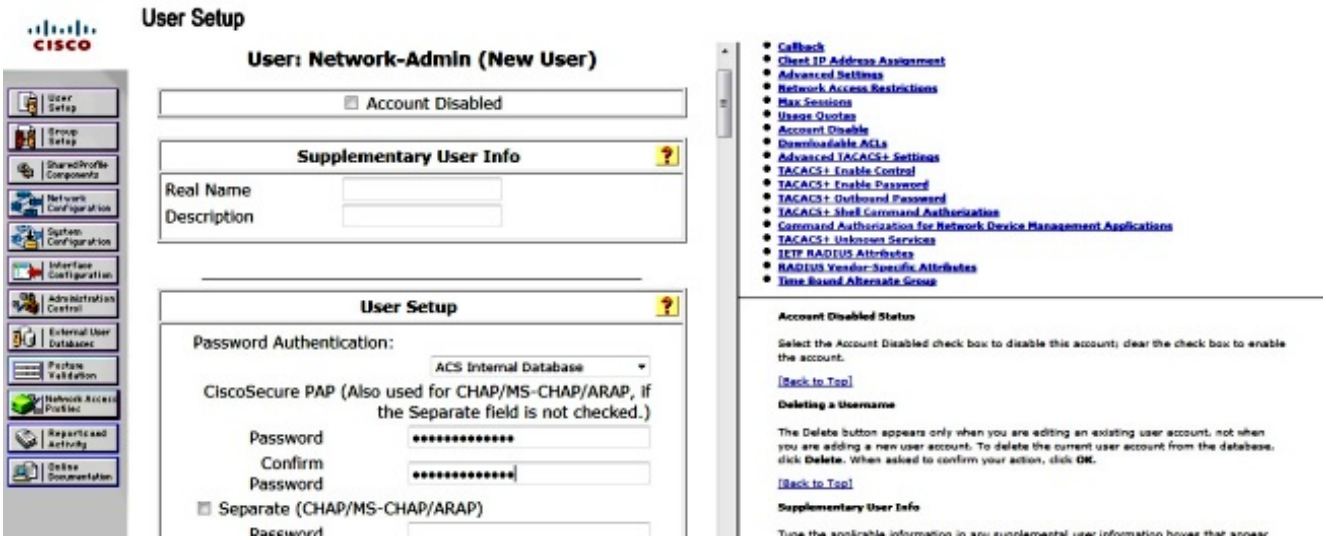
1. ACS にスイッチを AAA クライアントとして追加するために、[Network Configuration] > [Add entry AAA client] に移動し、次の情報を入力します。
IP アドレス： *<IP>*共有秘密： *<key>*認証方法： Radius (Cisco IOS®/PIX 6.0)



2. 認証設定を指定するために、[System Configuration] > [Global Authentication Setup] に移動し、[Allow MS-CHAP Version 2 Authentication] チェックボックスがオンになっていることを確認します。



3. ユーザを設定するために、メニューの [User Setup] をクリックし、次の手順を実行します。次の**ユーザ情報**を入力します： Network-Admin *<username>*。**[Add/Edit]** をクリックします。**[Real Name]** に次のように入力します： Network-Admin *<descriptive name>*.[Description] に次のように入力します： *<your choice>*。**[Password Authentication]** から次の選択します： ACS Internal Database。**[Password]** に次のように入力します： ..... *<password>*.**パスワードを確認します**： *<password>*.[Submit] をクリックします。



確認

特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

設定が正常に機能していることを確認するには、次のコマンドを入力します。

- **show dot1x**
- **show dot1x summary**
- **show dot1x interface**
- **show authentication sessions interface *<interface>***
- **show authentication interface *<interface>***

```
Switch(config)# show dot1x
_____________________________________________________
Sysauthcontrol Enabled
Dot1x Protocol Version 3
_____________________________________________________
Switch(config)# show dot1x summary
_____________________________________________________
Interface PAE Client Status
_____________________________________________________
Fa0/4 AUTH
_____________________________________________________
Switch(config)# show dot1x interface fa0/4 detail
_____________________________________________________
Dot1x Info for FastEthernet0/4
_____________________________________________________
PAE = AUTHENTICATOR
PortControl = FORCE_AUTHORIZED
ControlDirection = Both
HostMode = SINGLE_HOST
QuietPeriod = 5
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

トラブルシューティング

ここでは、設定をトラブルシューティングするために使用できる debug コマンドを示します。

> **注:** debug コマンドを使用する前に、『**debug コマンドの重要な情報**』を参照してください。

- debug dot1x all
- debug authentication all
- debug radius (**デバッグ レベルで** RADIUS **の情報を提供**)
- debug aaa authentication (**認証のデバッグ**)
- debug aaa authorization (**認可のデバッグ**)