Exemple de configuration de l'authentification câblée 802.1x sur un commutateur de la gamme Catalyst 3550 et un ACS version 4.2

Table des matières

Introduction

Ce document fournit un exemple de configuration de base IEEE 802.1x avec Cisco Access Control Server (ACS) Version 4.2 et le protocole RADIUS (Remote Access Dial In User Service) pour l'authentification filaire.

Conditions préalables

Exigences

Cisco vous recommande de :

- Confirmez l'accessibilité IP entre ACS et le commutateur.
- Assurez-vous que les ports UDP (User Datagram Protocol) 1645 et 1646 sont ouverts entre ACS et le commutateur.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Commutateurs Cisco Catalyst, série 3550

- Cisco Secure ACS version 4.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurer

Exemple de configuration de commutateur

1. Afin de définir le serveur RADIUS et la clé pré-partagée, entrez cette commande :

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

2. Afin d'activer la fonctionnalité 802.1x, entrez cette commande :

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

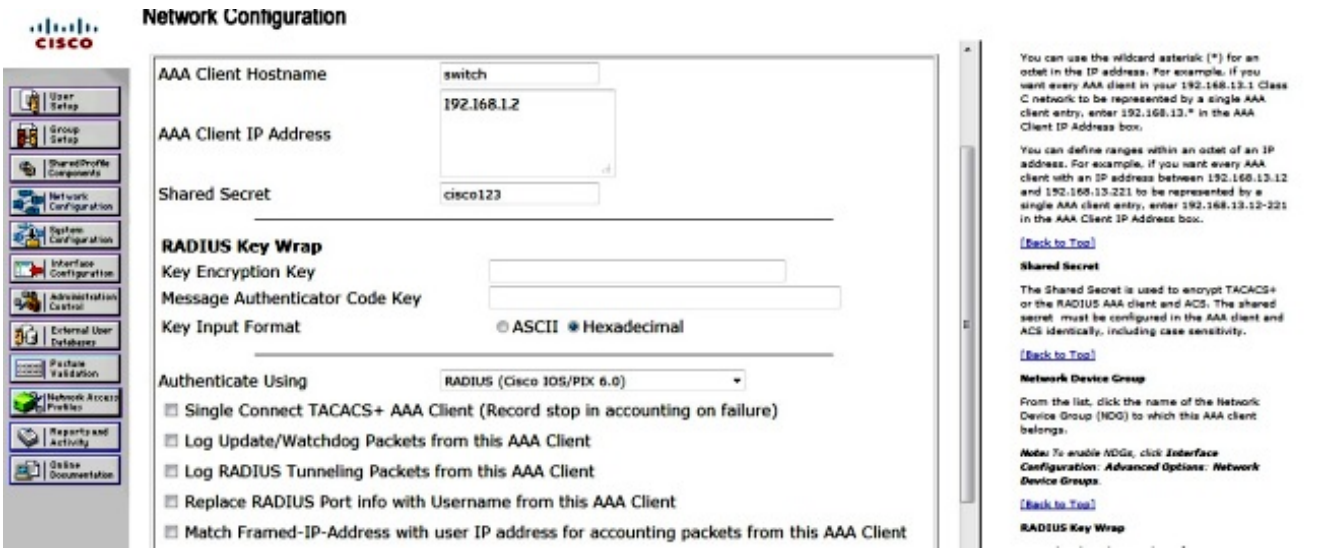
3. Afin d'activer globalement l'authentification AAA (Authentication, Authorization, and Accounting) et l'authentification et l'autorisation RADIUS, entrez ces commandes :
Remarque : ceci est nécessaire si vous devez passer des attributs à partir du serveur RADIUS ; sinon, vous pouvez l'ignorer.

```
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
```

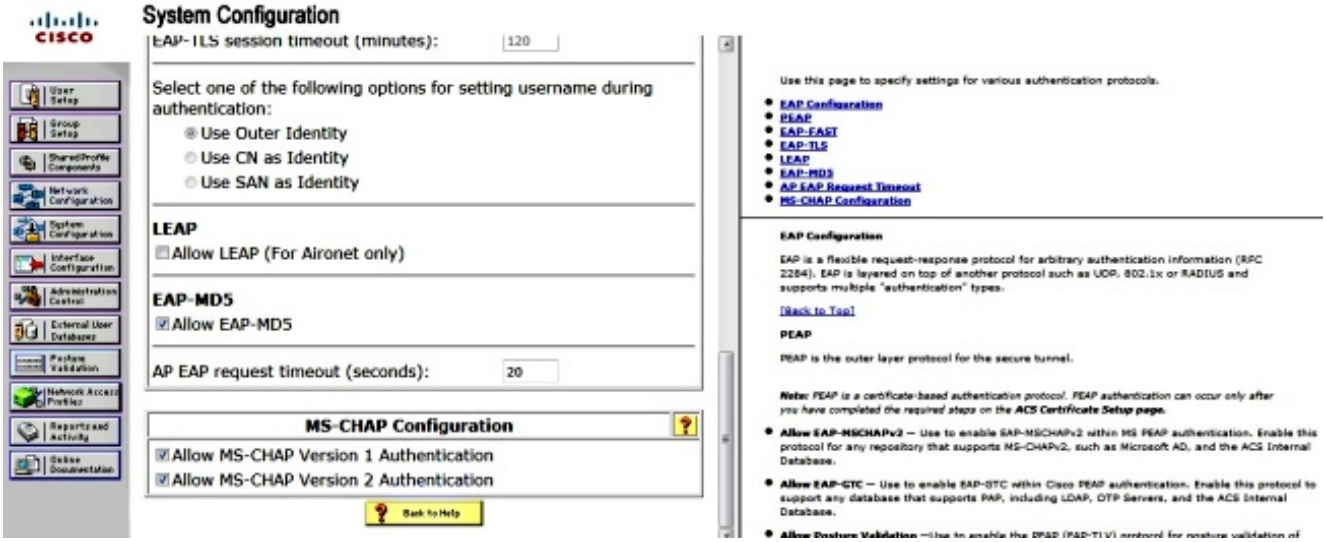
```
Switch(config-if)# switchport mode acces
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
Switch(config-if)# dot1x timeout quiet-period
Switch(config-if)# dot1x timeout tx-period
```

Configuration ACS

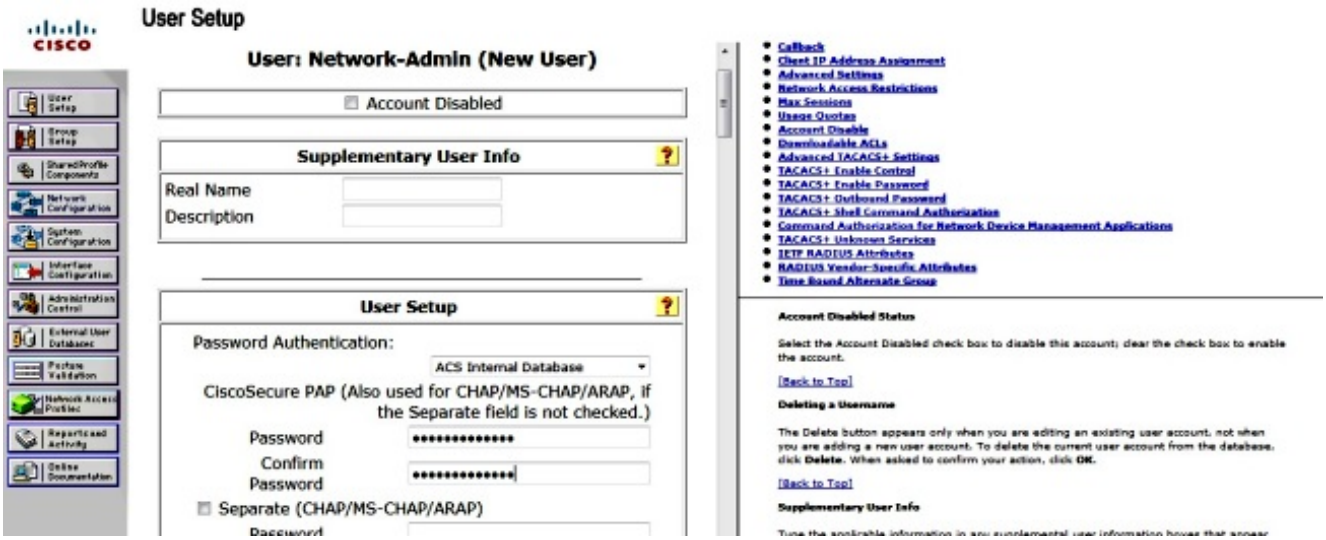
1. Afin d'ajouter le commutateur en tant que client AAA dans ACS, naviguez à **Configuration du réseau > Ajouter l'entrée client AAA**, et entrez ces informations :
Adresse IP : *<IP>*Secret partagé : *<key>*Authentification à l'aide de : Radius (Cisco IOS®/PIX 6.0)



2. Afin de configurer la configuration de l'authentification, naviguez vers **System Configuration > Global Authentication Setup**, et vérifiez que la case à cocher **Allow MS-CHAP Version 2 Authentication** est activée :



3. Afin de configurer un utilisateur, cliquez sur **User Setup** dans le menu, et complétez ces étapes :
   Entrez les informations **utilisateur** : Network-Admin *<username>*.Cliquez sur **Add/Edit.**Entrez le **nom réel** : Network-Admin *<nom descriptif>*.Ajoutez une **description** : *<votre choix>*.Sélectionnez **Authentification par mot de passe** : Base de données interne ACS.Saisissez le **mot de passe** : ..... *<mot de passe>*Confirmez le **mot de passe** : *<password>*.Cliquez sur Submit.



Vérifier

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Entrez ces commandes afin de confirmer que votre configuration fonctionne correctement :

- **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
```

Dépannage

Cette section fournit des commandes debug que vous pouvez utiliser afin de dépanner votre configuration.

> **Remarque : Consulter les renseignements importants sur les commandes de débogage avant d'utiliser les commandes de débogage.**

- **debug dot1x all**
- **debug authentication all**
- **debug radius (fournit les informations de radius au niveau du débogage)**
- **debug aaa authentication (debug for authentication)**
- **debug aaa authorization (debug for authorization)**

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.