le 802.1x a câblé l'authentification sur un commutateur de gamme Catalyst 3550 et un exemple de configuration de version 4.2 ACS

Contenu

Introduction

Ce document fournit à un exemple de base de configuration de 802.1x d'IEEE la version 4.2 du serveur de contrôle d'accès de Cisco (ACS) et l'Accès à distance se connectent le protocole de service d'utilisateur (RAYON) pour l'authentification de câble.

Conditions préalables

Conditions requises

Cisco recommande que vous :

- Confirmez l'accessibilité par IP entre ACS et le commutateur.
- Assurez-vous que les ports 1645 et 1646 de Protocole UDP (User Datagram Protocol) 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 de la gamme Cisco Catalyst 3550

- Version 4.2 de Cisco Secure ACS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Configuration de commutateur d'exemple

1. Afin de définir le serveur de RAYON et la clé pré-partagée, sélectionnez cette commande :
   ```
   Switch(config)# radius-server host 192.168.1.3  key  cisco123
   ```

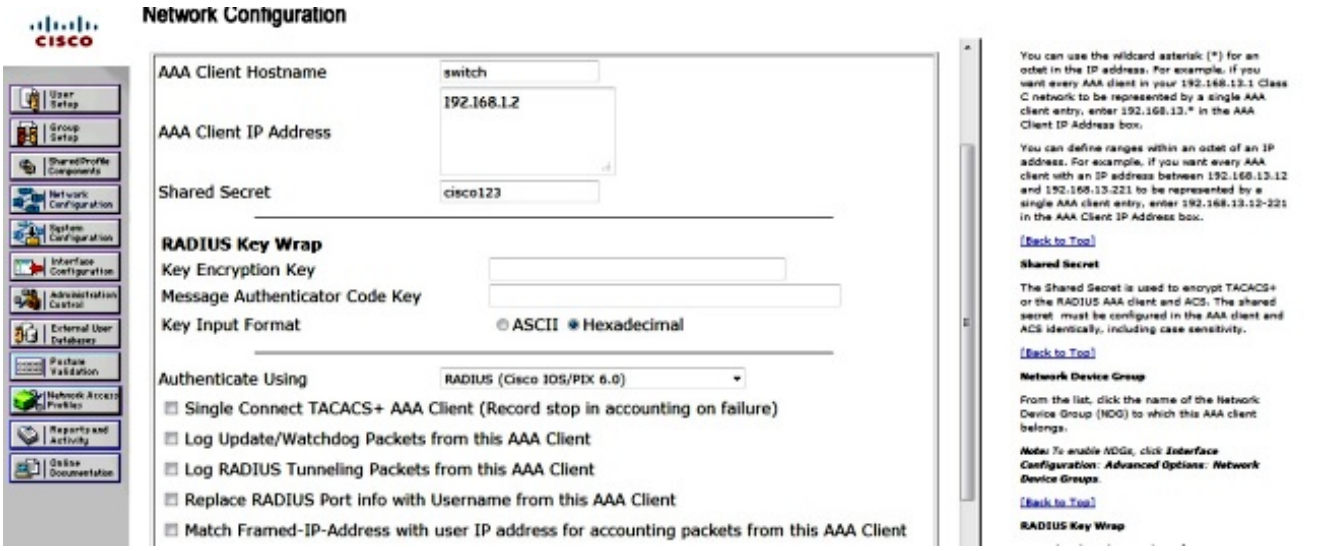
2. Afin d'activer la fonctionnalité de 802.1x, sélectionnez cette commande :
   ```
   Switch(config)# dot1x system-auth-control
   ```

3. L'Authentification, autorisation et comptabilité (AAA) de global-enable et l'authentification et l'autorisation de RAYON, sélectionnent ces commandes :
   Remarque: C'est nécessaire si vous devez passer des attributs du serveur de RAYON ; autrement, vous pouvez l'ignorer.

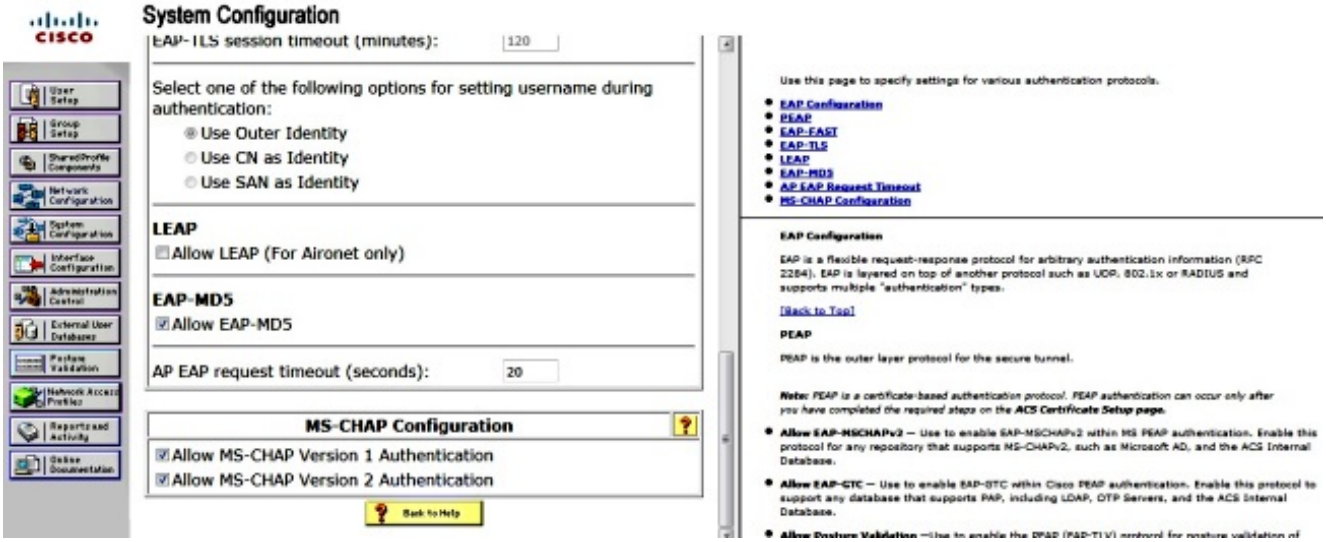
   ```
   Switch(config)# aaa new-model
   Switch(config)# aaa authentication dot1x default group radius
   awitch(Config)# aaa authorization network default group radius
   Switch(Config)# aaa accounting dot1x default start-stop group radius

   Switch(config-if)# switchport mode acces
   Switch(config-if)# switchport access vlan <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>
   ```

Configuration ACS

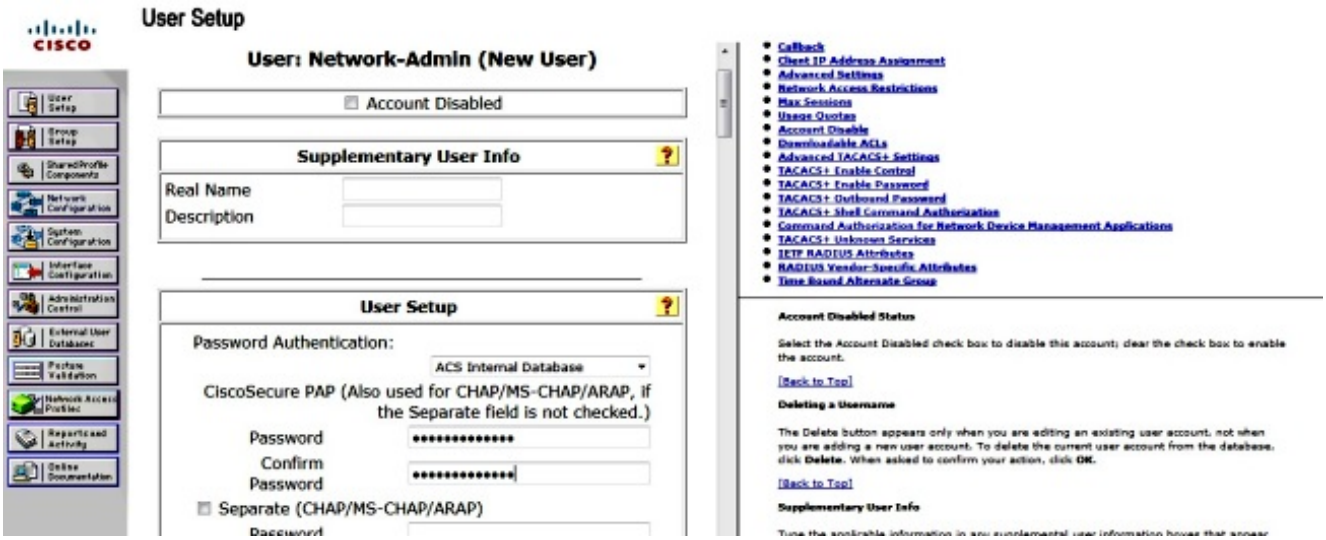
1. Afin d'ajouter le commutateur en tant que client d'AAA dans ACS, naviguez vers la **configuration réseau > ajoutent le client d'AAA d'entrée**, et écrivent ces informations : Adresse IP : *<IP>*Secret partagé : *<key>*Authentifiez utilisant : Rayon (Cisco IOS ®/PIX 6.0)



2. Afin de configurer l'authentification installer, naviguez vers la **configuration de système > installation globale d'authentification**, et vérifiez que la case d'**authentification de version 2 de l'autoriser MS-CHAP** est cochée :



3. Afin de configurer un utilisateur, cliquez sur User Setup sur le menu, et terminez-vous ces étapes :
   Écrivez les **informations utilisateur** : *<username> de Réseau*-admin.Cliquez sur Add**/éditez.**Écrivez le **nom réel** : *Name> <descriptive de Réseau*-admin.Ajoutez une **description** : *choice> de <your*.Sélectionnez l'**authentification de mot de passe** : ACS Internal Database.Entrez le **mot de passe** : ..... *<password>*.Confirmez le **mot de passe** : *<password>*.Cliquez sur **Submit**.



Vérifiez

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

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

- **show dot1x**
- **résumé de show dot1x**
- **interface de show dot1x**
- ***<interface> d'*interface de show authentication sessions**
- ***<interface> de* show authentication 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
```

Dépannez

Cette section fournit les commandes de débogage que vous pouvez employer afin de dépanner votre configuration.

> Remarque: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- **debug dot1x tout**
- **debug authentication tout**
- **debug radius (fournit les informations du rayon à met au point de niveau)**
- **debug aaa authentication (mettez au point pour l'authentification)**
- **autorisation de debug aaa (mettez au point pour l'autorisation)**