802.1x Kabelgebundene Authentifizierung auf einem Catalyst Switch der Serie 3550 und einem ACS Version 4.2 Konfigurationsbeispiel

Inhalt

Einleitung

Dieses Dokument enthält ein einfaches IEEE 802.1x-Konfigurationsbeispiel mit Cisco Access Control Server (ACS) Version 4.2 und dem RADIUS-Protokoll (Remote Access Dial In User Service) für die kabelgebundene Authentifizierung.

Voraussetzungen

Anforderungen

Cisco empfiehlt Folgendes:

- Bestätigen Sie die IP-Verfügbarkeit zwischen ACS und dem Switch.
- Stellen Sie sicher, dass die UDP-Ports 1645 und 1646 zwischen ACS und dem Switch offen sind.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Catalyst Switches der Serie 3550

- Cisco Secure ACS Version 4.2

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

Beispielkonfiguration eines Switches

1. Geben Sie den folgenden Befehl ein, um den RADIUS-Server und den vorinstallierten Schlüssel zu definieren:

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

2. Um die 802.1x-Funktionalität zu aktivieren, geben Sie den folgenden Befehl ein:

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

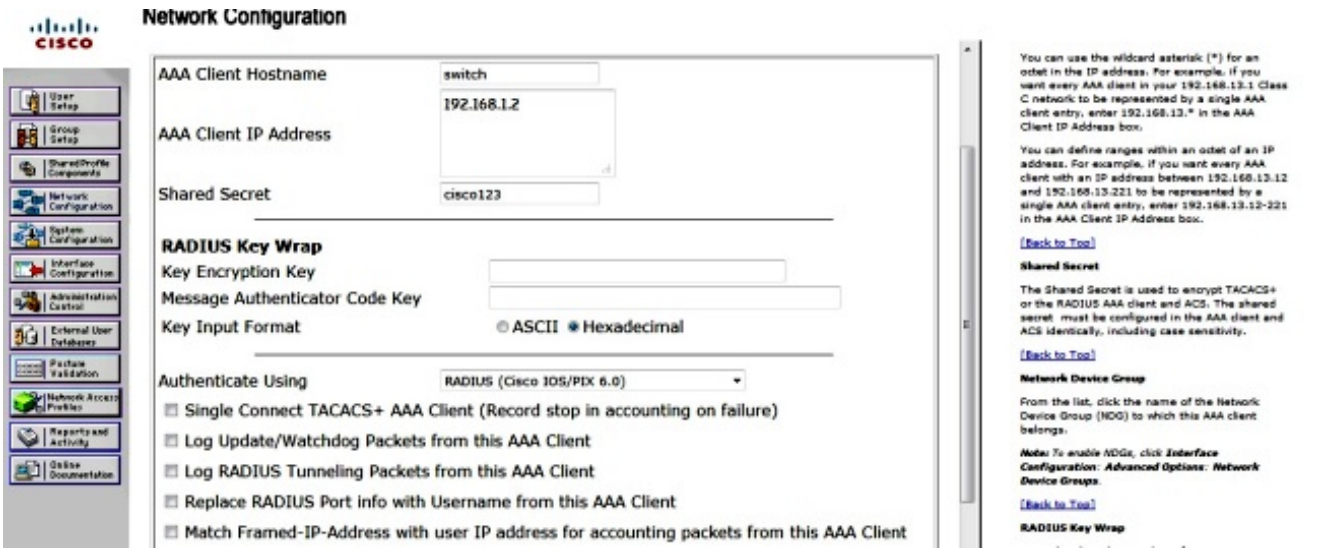
3. Geben Sie die folgenden Befehle ein, um AAA (Authentication, Authorization, and Accounting) und RADIUS-Authentifizierung und -Autorisierung global zu aktivieren: **Hinweis**: Dies ist erforderlich, wenn Attribute vom RADIUS-Server übergeben werden müssen. Andernfalls können Sie sie überspringen.

```
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
```

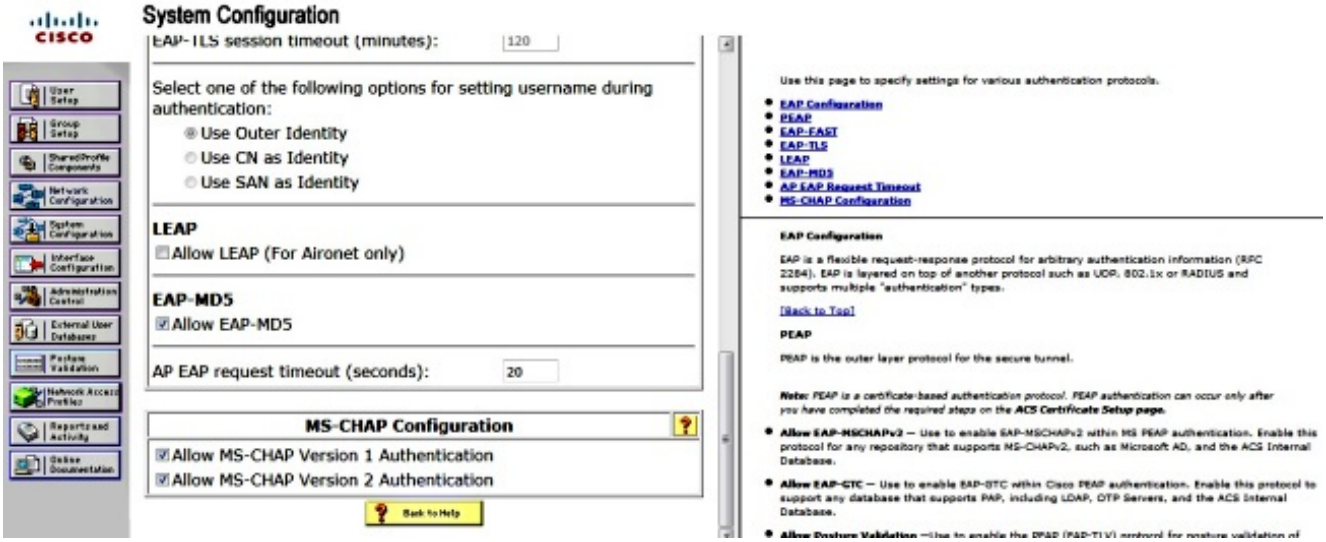
```
Switch(config-if)# switchport mode acces
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)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

ACS-Konfiguration

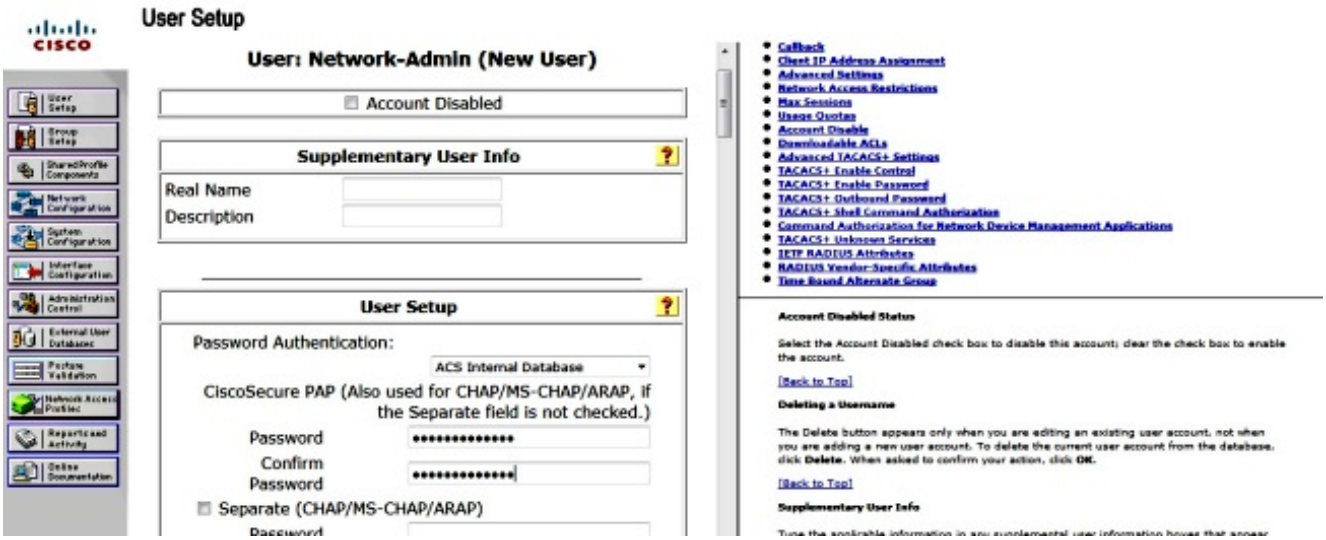
1. Um den Switch als AAA-Client in ACS hinzuzufügen, navigieren Sie zu **Network Configuration > Add entry AAA client,** und geben Sie die folgenden Informationen ein: IP-Adresse: *<IP>*Gemeinsamer geheimer Schlüssel: *<Schlüssel>*Authentifizierung über Radius (Cisco IOS®/PIX 6.0)



2. Um das Authentifizierungs-Setup zu konfigurieren, navigieren Sie zu **System Configuration > Global Authentication Setup,** und überprüfen Sie, ob das Kontrollkästchen **Allow MS-CHAP Version 2 Authentication (MS-CHAP-Authentifizierung Version 2 zulassen)** aktiviert ist:



3. Um einen Benutzer zu konfigurieren, klicken Sie im Menü auf **User Setup** (Benutzereinrichtung), und führen Sie die folgenden Schritte aus:
Geben Sie die **Benutzerinformationen** ein: Network-Admin *<Benutzername>*.Klicken Sie auf **Hinzufügen/Bearbeiten.**Geben Sie den **richtigen Namen ein**: Network-Admin *<beschreibender Name>*.Fügen Sie eine **Beschreibung hinzu**: *<Ihre Wahl>*.Wählen Sie **Kennwortauthentifizierung:** Interne ACS-Datenbank.Geben Sie das **Kennwort ein**: ..... *<Kennwort>*.Bestätigen Sie das **Kennwort**: *<Kennwort>*.Klicken Sie auf **Senden**.



Überprüfung

Das Output Interpreter-Tool (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Geben Sie die folgenden Befehle ein, um sicherzustellen, dass Ihre Konfiguration ordnungsgemäß funktioniert:

- **Punkt 1x anzeigen**
- **dot1x-Zusammenfassung anzeigen**
- **show dot1x-Schnittstelle**
- **show authentication sessions interface *<Schnittstelle>***
- **show authentication interface *<Schnittstelle>***

```
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
```

Fehlerbehebung

In diesem Abschnitt finden Sie Debugbefehle, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

> **Hinweis**: Lesen Sie Wichtige Informationen zu Debug-Befehlen, bevor Sie **Debug-**Befehle verwenden.

- **debug dot1x all**
- **debug authentication all**
- **Debug-Radius (liefert die Informationen zum Radius auf Debugebene)**
- **debug aaa authentication (debug für Authentifizierung)**
- **debug aaa Authorization (debug for Authorization)**

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.