Autenticação com Fio 802.1x em um Catalyst 3550 Series Switch e um Exemplo de Configuração ACS Versão 4.2

Contents

Introduction

Este documento fornece um exemplo de configuração básica do IEEE 802.1x com o Cisco Access Control Server (ACS) Versão 4.2 e o protocolo Remote Access Dial In User Service (RADIUS) para autenticação com fio.

Prerequisites

Requirements

A Cisco recomenda:

- Confirme a alcançabilidade de IP entre o ACS e o switch.
- Certifique-se de que as portas 1645 e 1646 do User Datagram Protocol (UDP) estejam abertas entre o ACS e o switch.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Catalyst 3550 Series Switches
- Cisco Secure ACS versão 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.

Configurar

Configuração de switches de exemplo

1. Para definir o servidor RADIUS e a chave pré-compartilhada, insira este comando:

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

2. Para habilitar a funcionalidade 802.1x, insira este comando:

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

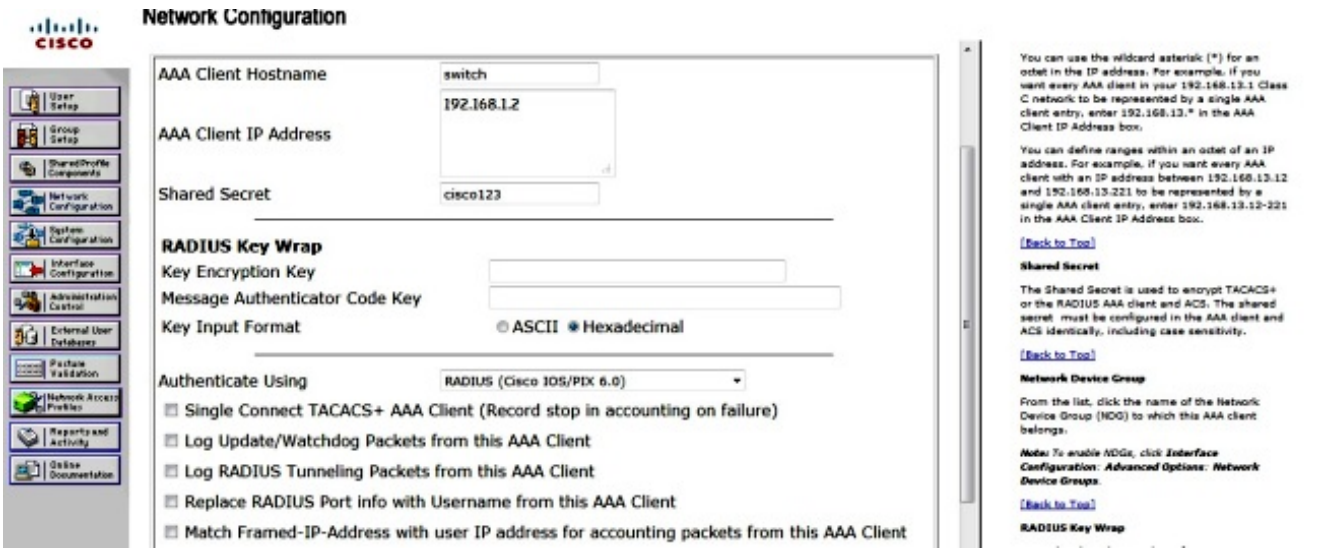
3. Para habilitar globalmente a autenticação e a autorização AAA (Authentication, Authorization, and Accounting) e RADIUS, insira estes comandos:
   Observação: isso será necessário se você precisar passar atributos do servidor RADIUS; caso contrário, você poderá ignorá-los.

```
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
```

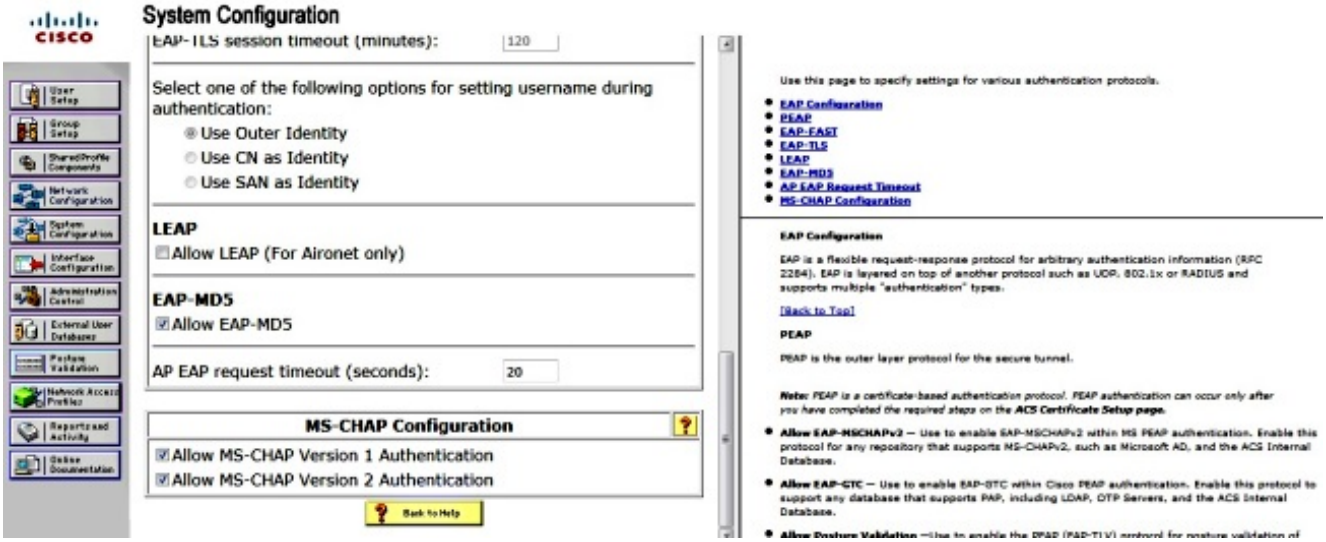
```
Switch(config-if)# switchport mode acces
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)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

Configuração do ACS

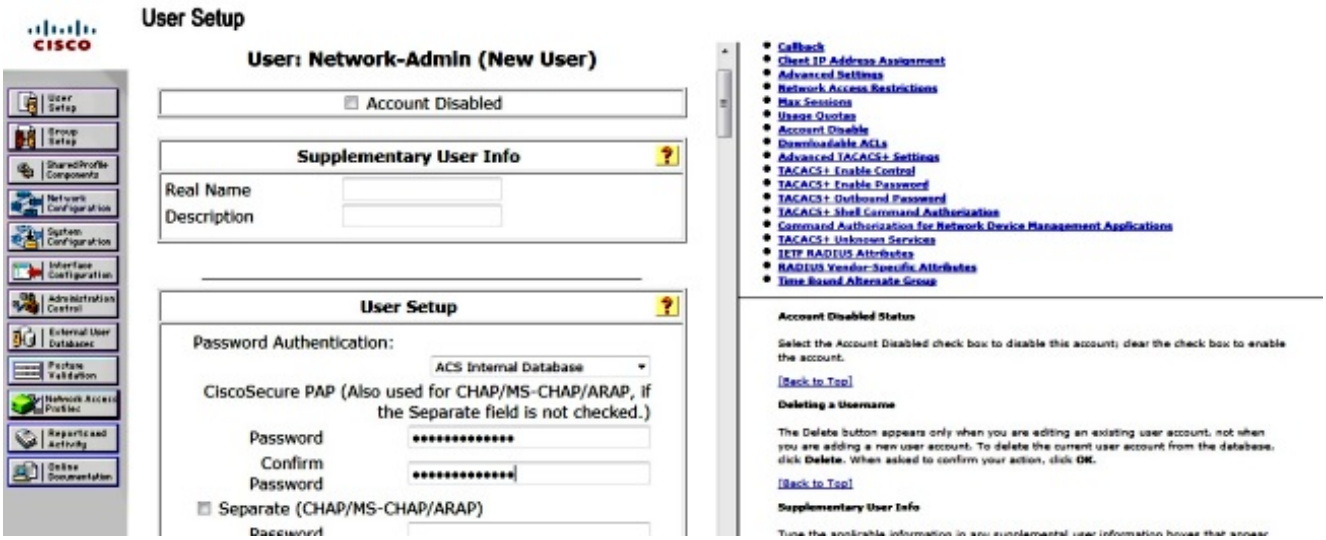
1. Para adicionar o switch como um cliente AAA no ACS, navegue para **Network Configuration > Add entry AAA client** e insira estas informações:
   Endereço IP: *<IP>*Segredo compartilhado: *<key>*Autenticar usando: Radius (Cisco IOS®/PIX 6.0)



2. Para configurar a autenticação, navegue até **System Configuration > Global Authentication Setup** e verifique se a caixa de seleção **Allow MS-CHAP Version 2 Authentication** está marcada:



3. Para configurar um usuário, clique em **User Setup** no menu e conclua estas etapas: Insira as informações de **usuário**: Network-Admin *<username>*.Clique em **Add/Edit.**Insira o **nome real**: Network-Admin *<nome descritivo>*.Adicione uma **Descrição**: *<sua escolha>*.Selecione a opção **Password Authentication**: ACS Internal Database.Insira a **senha**: ..... *<password>*.Confirme a **senha**: *<password>*.Clique em Submit.



Verificar

A ferramenta Output Interpreter (exclusiva para clientes registrados) é compatível com alguns comandos de exibição.. Use a ferramenta Output Interpreter para visualizar uma análise do resultado gerado pelo comando show..

Insira estes comandos para confirmar se sua configuração funciona corretamente:

- **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
```

Troubleshoot

Esta seção fornece comandos de depuração que você pode usar para solucionar problemas de configuração.

> **Nota:Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos debug.**

- **debug dot1x all**
- **debug authentication all**
- **debug radius (fornece as informações de radius no nível de depuração)**
- **debug aaa authentication (debug for authentication)**
- **debug aaa authorization (debug para autorização)**

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.