Catalyst 3550系列交换机和ACS版本4.2上的802.1x有线身份验证配置示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[配置](#)
[交换机配置示例](#)
[ACS配置](#)
[验证](#)
[故障排除](#)

简介

本文档提供了使用思科访问控制服务器(ACS)版本4.2和远程访问拨入用户服务(RADIUS)协议进行有线身份验证的基本IEEE 802.1x配置示例。

先决条件

要求

Cisco推荐您：

- 确认ACS和交换机之间的IP连通性。
- 确保ACS和交换机之间的用户数据报协议(UDP)端口1645和1646处于打开状态。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Cisco Catalyst 3550 系列交换机
- 思科安全ACS版本4.2

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

配置

交换机配置示例

1. 要定义RADIUS服务器和预共享密钥，请输入以下命令：

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

2. 要启用802.1x功能，请输入以下命令：

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

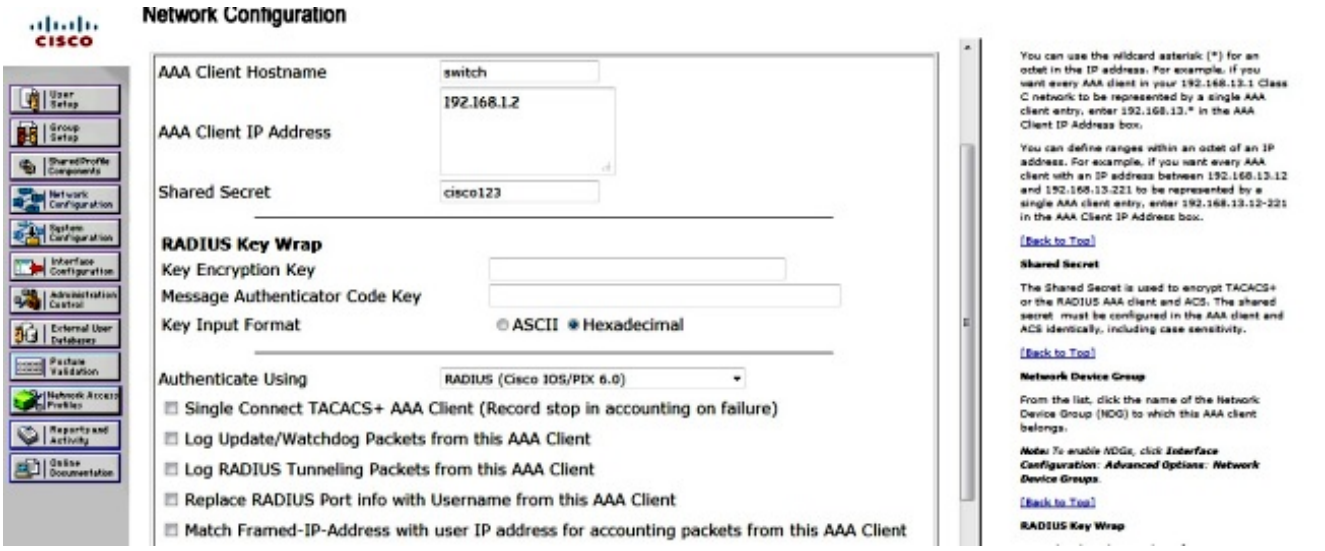
3. 要全局启用身份验证、授权和记帐(AAA)以及RADIUS身份验证和授权，请输入以下命令：
   注意：如果需要从RADIUS服务器传递属性，则必须执行此操作；否则，您可以跳过它。

```
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
```

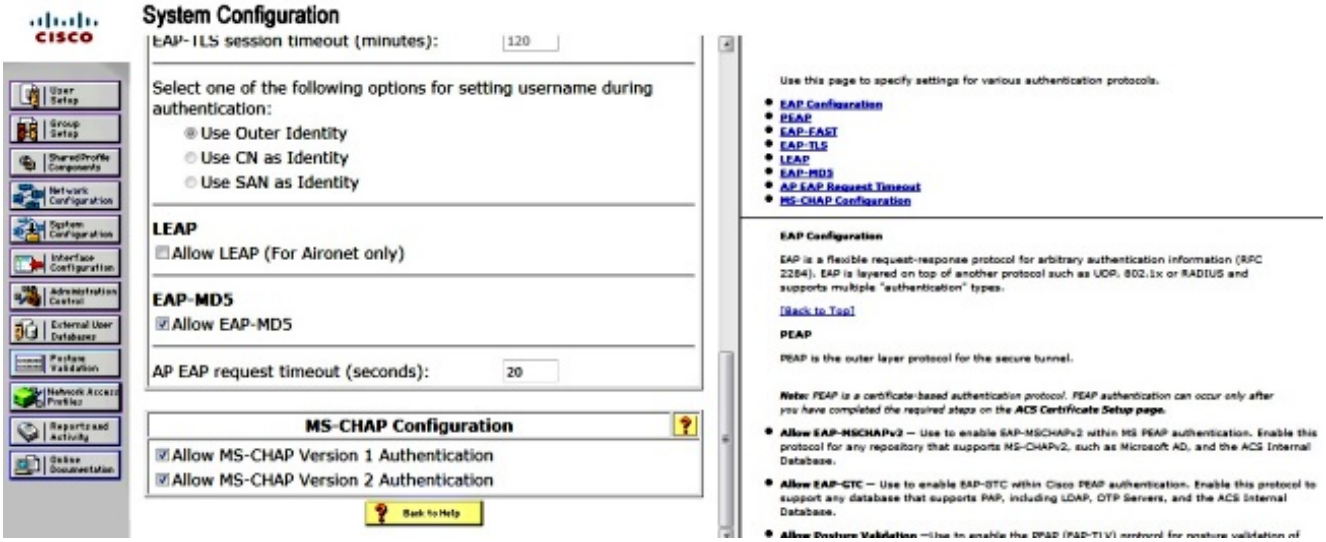
```
Switch(config-if)# switchport mode acces
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)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

ACS配置

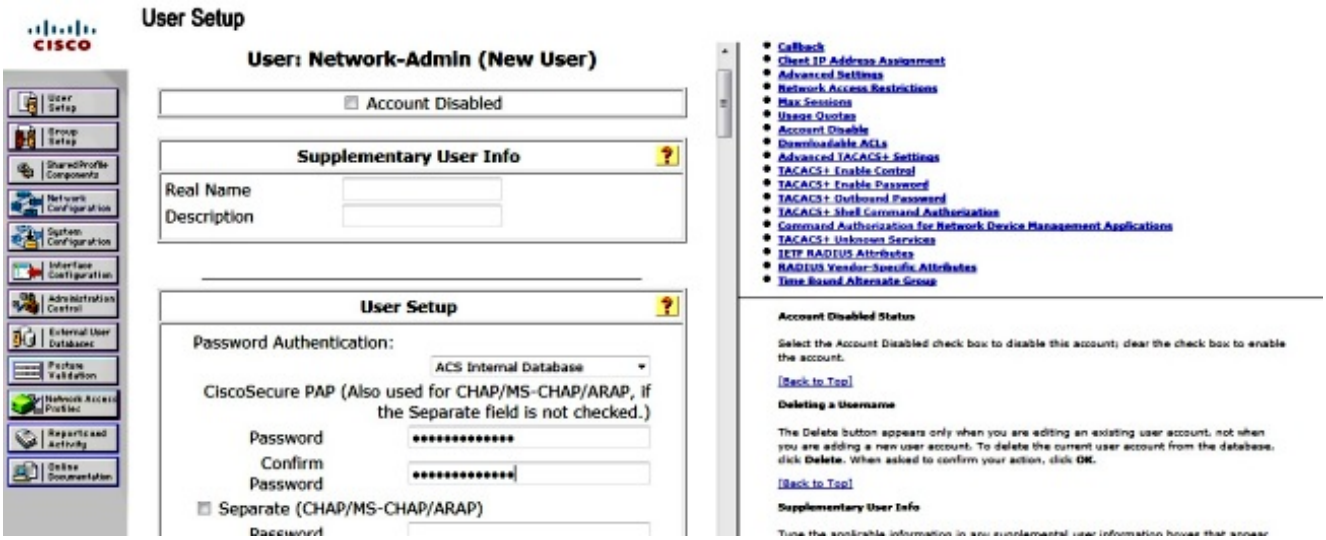
1. 要在ACS中将交换机添加为AAA客户端，请导航到**网络配置>添加条目AAA客户端**，然后输入以下信息：
   IP地址*:<IP>*共享密钥*:<key>*身份验证使用：Radius(Cisco IOS®/PIX 6.0)



2. 要配置身份验证设置，请导航到**System Configuration > Global Authentication Setup**，并验证**Allow MS-CHAP Version 2 Authentication**复选框是否已选中：



3. 要配置用户，请点击菜单上的**User Setup**，然后完成以下步骤：
输入**User**信息：Network-Admin *<username>*。单击**Add/Edit**。输入**Real Name**: Network-Admin *<descriptive name>*。添加**说明**: *<your choice>*。选择**Password Authentication**: ACS Internal Database。输入**Password**: ..... *<password>*。确认**密码**: *<password>*。单击“Submit”。



验证

命令输出解释程序工具（仅限注册用户）支持某些 show 命令。使用输出解释器工具来查看 show 命令输出的分析。

输入以下命令以确认您的配置是否正常工作：

- **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
```

故障排除

本节提供可用于对配置进行故障排除的debug命令。

> **注意**：使用debug命令之前，请参阅有关Debug命令**的重要**信息。

- debug dot1x all
- debug authentication all
- debug radius（**提供调试级别的**radius信息）
- debug aaa authentication(debug for authentication)
- debug aaa authorization(debug for authorization)

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。