

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
Switch(Config)# aaa authorization network default group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
```

```
Switch(config-if)# switchport mode access
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:</P>共享密钥:<key>身份验证使用：Radius(Cisco IOS®/PIX 6.0)

Network Configuration

AAA Client Hostname: switch
AAA Client IP Address: 192.168.1.2
Shared Secret: cisco123

RADIUS Key Wrap

Key Encryption Key: [redacted]
Message Authenticator Code Key: [redacted]
Key Input Format: ASCII Hexadecimal

Authenticate Using: RADIUS (Cisco IOS/PIX 6.0)

- Single Connect TACACS+ AAA Client (Record stop in accounting on failure)
- Log Update/Watchdog Packets from this AAA Client
- Log RADIUS Tunneling Packets from this AAA Client
- Replace RADIUS Port Info with Username from this AAA Client
- Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

You can use the wildcard asterisk (*) for an offset in the IP address. For example, if you want every AAA client in your 192.168.1.1 Class C network to be represented by a single AAA client entry, enter 192.168.1.* in the AAA Client IP Address box.

You can define ranges within an offset of an IP address. For example, if you want every AAA client with an IP address between 192.168.1.12 and 192.168.1.221 to be represented by a single AAA client entry, enter 192.168.1.12-221 in the AAA Client IP Address box.

[\[Back to Top\]](#)

Shared Secret

The Shared Secret is used to encrypt TACACS+ or the RADIUS AAA client and ACS. The shared secret must be configured in the AAA client and ACS identically, including case sensitivity.

[\[Back to Top\]](#)

Network Device Group

From the list, click the name of the Network Device Group (NDG) to which this AAA client belongs.

Note: To enable NDGs, click [Interface Configuration - Advanced Options: Network Device Groups](#).

[\[Back to Top\]](#)

RADIUS Key Wrap

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：

System Configuration

EAP-TLS session timeout (minutes): 120

Select one of the following options for setting username during authentication:

- Use Outer Identity
- Use CN as Identity
- Use SAN as Identity

LEAP

- Allow LEAP (For Aironet only)

EAP-MD5

- Allow EAP-MD5

AP EAP request timeout (seconds): 20

MS-CHAP Configuration

- Allow MS-CHAP Version 1 Authentication
- Allow MS-CHAP Version 2 Authentication

[\[Back to Help\]](#)

EAP Configuration

EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.

[\[Back to Top\]](#)

PEAP

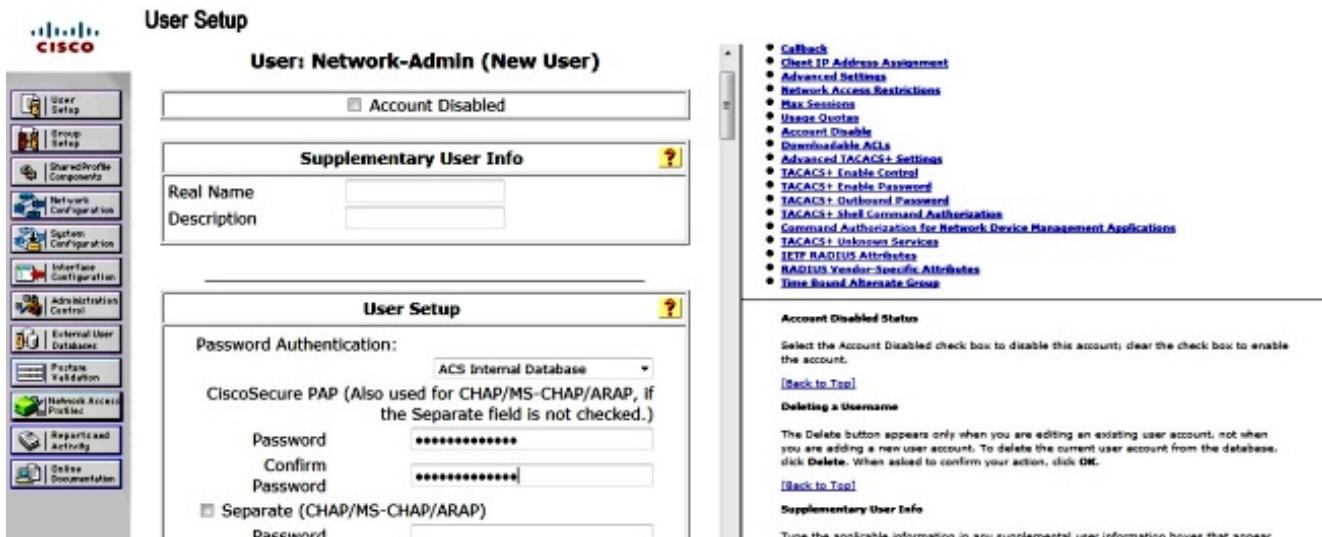
PEAP is the outer layer protocol for the secure tunnel.

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the ACS Certificate Setup page.

- Allow EAP-MSCHAPv2 — Use to enable MS-CHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPv2, such as Microsoft AD, and the ACS Internal Database.
- Allow EAP-GTC — Use to enable EAP-SC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
- Allow Diameter Validation — Use to enable the DPAZ (PAD-TLV) mechanism for remote validation of user credentials.

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）。