

o 802.1x prendeu a autenticação em um Catalyst 3550 Series Switch e em um exemplo de configuração da versão de ACS 4.2

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Configuração de switch do exemplo](#)

[Configuração ACS](#)

[Verificar](#)

[Troubleshooting](#)

Introdução

Este documento fornece um exemplo de configuração básico do IEEE 802.1X a versão 4.2 do Access Control Server de Cisco (ACS) e o seletor do Acesso remoto no protocolo do serviço de usuário (RAIO) para a autenticação prendida.

Pré-requisitos

Requisitos

Cisco recomenda que você:

- Confirme o IP reachability entre o ACS e o interruptor.
- Assegure-se de que as portas 1645 e 1646 do User Datagram Protocol (UDP) estejam abertas entre o ACS e o interruptor.

[Componentes Utilizados](#)

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

- Cisco Catalyst 3550 Series Switches
- Versão 4.2 do Cisco Secure ACS

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Configurar

Configuração de switch do exemplo

1. A fim de definir o servidor Radius e a chave pré-compartilhada, incorpore este comando:

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

2. A fim de permitir a funcionalidade do 802.1x, incorpore este comando:

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

3. A fim de globalmente permitir o Authentication, Authorization, and Accounting (AAA) e a autenticação RADIUS e a autorização, incorpore estes comandos:

Nota: Isto é necessário se você precisa de passar atributos do servidor Radius; se não, você pode saltá-lo.

```
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 <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>
```

Configuração ACS

1. A fim de adicionar o interruptor como um cliente de AAA no ACS, navegue ao **cliente de AAA da entrada do > Add da configuração de rede**, e incorpore esta informação:

Endereço IP: <IP>Segredo compartilhado: <key>Autentique usando-se: Raio (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: []
 Message Authenticator Code Key: []
 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

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.

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**.

RADIUS Key Wrap

2. A fim configurar a instalação da autenticação, navegue à **instalação da configuração de sistema > da autenticação global**, e verifique que a caixa de verificação da **autenticação da versão MS-CHAP 2** reservar está verificada:

System Configuration

EAP-ILS 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](#)

Use this page to specify settings for various authentication protocols.

- [EAP Configuration](#)
- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP-EAP Request Timeout](#)
- [MS-CHAP Configuration](#)

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.

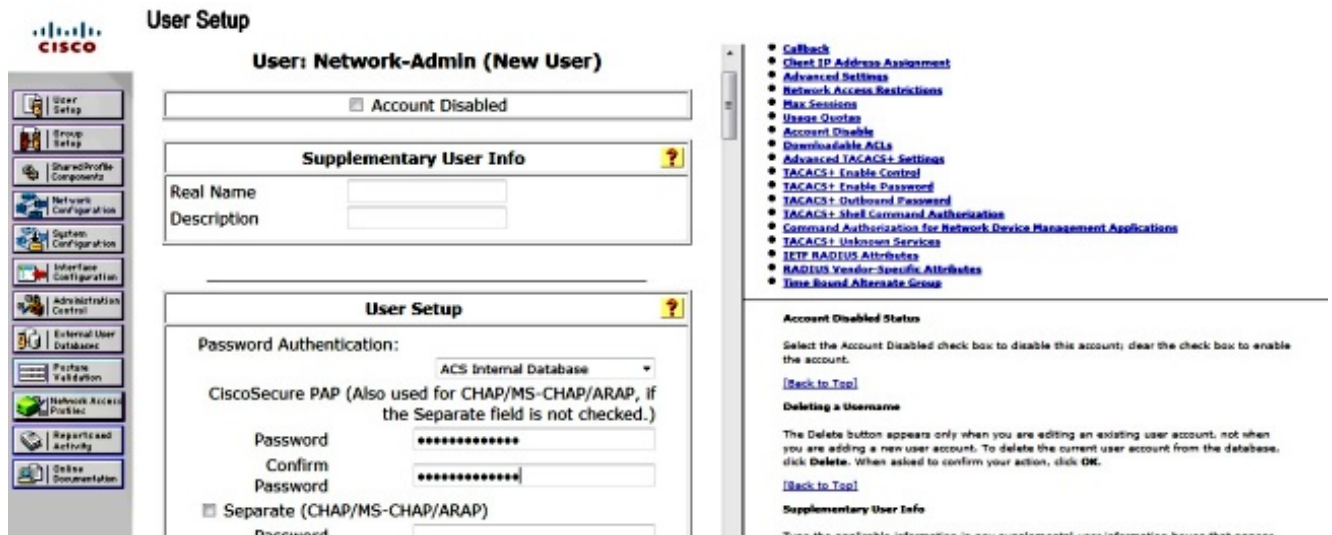
[Back to Top](#)

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 EAP-MSCHAPv2 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-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
- **Allow Dynamic Validation** — Use to enable the DPAD (PAP-TLV) protocol for dynamic validation of

3. A fim configurar um usuário, clique a **instalação de usuário** no menu, e termine estas etapas: Incorpore a **informação sobre o usuário**: <username> Rede-Admin. O clique **adiciona/edita**. Dê entrada com o nome real: Name> Rede-Admin <descriptive>. Adicionar uma **descrição**: choice> do <your>. Selecione a **autenticação de senha**: Base de dados interno ACS. Incorpore a **senha**: <password>. Confirme a **senha**: <password>. Clique em Submit.



Verificar

[A ferramenta Output Interpreter](#) ([clientes registrados somente](#)) apoia determinados comandos de exibição. Use a ferramenta Output Interpreter a fim ver uma análise do emissor de comando de execução.

Incorpore estes comandos a fim confirmar que sua configuração trabalha corretamente:

- mostre o dot1x
- mostre o sumário do dot1x
- mostre a relação do dot1x
- mostre o *<interface>* da relação das sessões da autenticação
- mostre o *<interface>* da relação da autenticação

```
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
```

Troubleshooting

Esta seção fornece os comandos debug que você pode usar a fim pesquisar defeitos sua configuração.

Nota: Consulte [Informações Importantes sobre Comandos de Depuração](#) antes de usar comandos **debug**.

- debug o dot1x todo
- debug authentication todo
- debug o raio (fornece a informação do raio a nível de debug)
- debug a autenticação aaa (debugar para a autenticação)
- debug aaa authorization (debugar para a autorização)