

# Exemplo de configuração PURO com Cisco Identity Services Engine

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Configuração de switch do autenticador](#)

[Configuração de switch do suplicante](#)

[Configuração ISE](#)

[Verificar](#)

[Autenticação do interruptor do suplicante ao interruptor do autenticador](#)

[Autenticação do PC Windows ao interruptor do suplicante](#)

[Remoção do cliente autenticado da rede](#)

[Remoção do interruptor do suplicante](#)

[Portas sem o dot1x no interruptor do suplicante](#)

[Troubleshooting](#)

## Introdução

Este documento descreve a configuração e o comportamento da topologia da autenticação da margem de rede (PURA) em um cenário simples. PURO utiliza a informação cliente que sinaliza o protocolo (CISP) a fim propagar endereços MAC de cliente e informação de VLAN entre o suplicante e o Switches do autenticador.

Neste exemplo de configuração, o interruptor do autenticador (igualmente chamado o autenticador) e o interruptor do suplicante (igualmente chamado o suplicante) executam a autenticação do 802.1x; o autenticador autentica o suplicante, que, por sua vez, autentica o PC de teste.

## Pré-requisitos

### Requisitos

Cisco recomenda que você tem o conhecimento do padrão da autenticação do IEEE 802.1X.

## Componentes Utilizados

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

- Dois Cisco Catalyst 3560 Series Switch com Cisco IOS® Software, liberação 12.2(55)SE8; um interruptor atua como um autenticador, e o outro atua como um suplicante.
- Cisco Identity Services Engine (ISE), liberação 1.2.
- PC com Microsoft Windows XP, pacote de serviços 3.

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

Este exemplo cobre configurações de amostra para:

- Interruptor do autenticador
- Interruptor do suplicante
- Cisco ISE

As configurações são o perform necessário mínimo este exercício do laboratório; não puderam ser ótimos para ou cumprir outras necessidades.

Nota: Use a [Command Lookup Tool](#) ( [somente clientes registrados](#)) para obter mais informações sobre os comandos usados nesta seção.

## Diagrama de Rede

Este diagrama da rede ilustra a Conectividade usada neste exemplo. As linhas pretas indicam lógico ou a conectividade física, e as linhas verde indicam os links autenticados com o uso do 802.1x.

## Configuração de switch do autenticador

O autenticador contém os elementos básicos necessários para o dot1x. Neste exemplo, os comandos que são específicos a PURO ou CISP são negritos.

Esta é a autenticação básica, a autorização, e a configuração da contabilidade (AAA):

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius

radius-server host 10.48.66.107 auth-port 1812 acct-port 1813 key cisco
```

```
! Enable authenticator switch to authenticate the supplicant switch.
dot1x system-auth-control
! Enable CISP framework.
cisp enable
```

```
! configure uplink port as access and dot1x authentication.
interface FastEthernet0/6
switchport mode access
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast
```

CISP é permitido globalmente, e a porta de interconexão é configurada no autenticador e no modo de acesso.

## Configuração de switch do suplicante

A configuração exata do suplicante é crucial para que a instalação inteira trabalhe como esperado. Este exemplo de configuração contém uma configuração típica AAA e de dot1x.

Esta é a configuração de AAA básica:

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
```

```
radius-server host 10.48.66.107 auth-port 1812 acct-port 1813 key cisco
```

```
! Enable supplicant switch to authenticate devices connected
dot1x system-auth-control
```

```
! Forces the switch to send only multicast EAPOL packets when it receives either
unicast or multicast packets, which allows NEAT to work on the supplicant
switch in all host modes.
```

```
dot1x supplicant force-multicast
```

```
! Enable CISP framework operation.
cisp enable
```

O suplicante deve ter configurado credenciais e deve fornecer um método do Extensible Authentication Protocol (EAP) a ser usado.

O suplicante pode usar o resumo de mensagem EAP 5 (MD5) e a Autenticação Flexível de EAP através do protocolo seguro (RÁPIDO) (entre outros tipos EAP) para a autenticação em caso de CISP. A fim manter a configuração ISE a um mínimo, este exemplo usa o EAP-MD5 para a autenticação do suplicante ao autenticador. (O padrão forçaria o uso de EAP-FAST, que exige o abastecimento credencial protegido do [PAC] do acesso; este documento não cobre essa encenação.)

```
! configure EAP mode used by supplicant switch to authenticate itself to
authenticator switch eap profile EAP_PRO
method md5
```

```
! Configure credentials use by supplicant switch during that authentication.
dot1x credentials CRED_PRO
username bsnsswitch
password 0 C1sco123
```

A conexão do suplicante ao autenticador é configurada já para ser uma porta de tronco (em

contraste com a configuração da porta de acesso no autenticador). Nesta fase, isto é esperado; a configuração mudará dinamicamente quando o ISE retorna o atributo correto.

```
interface FastEthernet0/6
switchport trunk encapsulation dot1q
switchport mode trunk
dot1x pae supplicant
dot1x credentials CRED_PRO
dot1x supplicant eap profile EAP_PRO
```

A porta que conecta ao PC Windows tem uma configuração mínima e é mostrada aqui para a referência somente.

```
interface FastEthernet0/5
switchport access vlan 200
switchport mode access
authentication port-control auto
dot1x pae authenticator
```

## Configuração ISE

Este procedimento descreve como estabelecer uma configuração básica ISE.

1. Permita os protocolos de autenticação requerida.

Neste exemplo, o dot1x prendido permite o EAP-MD5 autentique o suplicante ao autenticador e permite que o protocolo extensible authentication protegido (PEAP) - a versão 2 do protocolo microsoft challenge handshake authentication (MSCHAPv2) autentique o PC Windows ao suplicante.

Navegue à **política > aos resultados > à autenticação > protocolos permitidos**, selecione a **lista do serviço do protocolo** usada pelo dot1x prendido, e assegure-se de que os protocolos nesta etapa estejam permitidos.

2. Crie uma política da autorização. Navegue à **política > aos resultados > à autorização > à política da autorização**, e crie ou atualize uma política assim que contém PURO como um atributo retornado. Este é um exemplo de tal política:

Quando a opção PURA é girada sobre, o ISE retorna o device-traffic-class=switch como parte da autorização. Esta opção é necessária a fim mudar o modo de porta do autenticador do acesso ao tronco.

3. Crie uma regra da autorização para usar este perfil. Navegue à **política > à autorização**, e crie ou atualize uma regra.

Neste exemplo, um grupo especial do dispositivo chamado Authenticator\_switches é criado, e todos os suplicantes enviam um username que comece com o bsnsswitch.

4. Adicionar o Switches ao grupo apropriado. Navegue à **administração > aos recursos de rede > aos dispositivos de rede**, e o clique **adiciona**.

Neste exemplo, BSTP-3500-1 (o autenticador) é parte de grupo de Authenticator\_switches; BSTP-3500-2 (o suplicante) não precisa de ser parte de este grupo.

## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente. Esta seção descreve dois comportamentos:

- Autenticação entre o Switches
- Autenticação entre o PC Windows e o suplicante

Igualmente explica três situações adicionais:

- Remoção de um cliente autenticado da rede
- Remoção de um suplicante
- Portas sem dot1x em um suplicante

Notas:

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

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

## Autenticação do interruptor do suplicante ao interruptor do autenticador

Neste exemplo, o suplicante autentica ao autenticador. As etapas no processo são:

1. O suplicante é configurado e obstruído na porta fastethernet0/6. A troca do dot1x faz com que o suplicante use o EAP a fim enviar um nome de usuário e senha PRE-configurado ao autenticador.
2. O autenticador executa uma troca do RAIO e fornece credenciais para a validação ISE.
3. Se as credenciais estão corretas, o ISE retorna os atributos exigidos por PURO (device-traffic-class=switch), e o autenticador muda seu modo do switchport do acesso ao tronco.

Este exemplo mostra a troca da informação CISP entre o Switches:

```
bstp-3500-1#debug cisp all
Oct 15 13:51:03.672: %AUTHMGR-5-START: Starting 'dot1x' for client
(001b.0d55.2187) on Interface Fa0/6 AuditSessionID 0A3039E10000000600757ABB
Oct 15 13:51:03.723: %DOT1X-5-SUCCESS: Authentication successful for client
(001b.0d55.2187) on Interface Fa0/6 AuditSessionID
```

Oct 15 13:51:03.723: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client (001b.0d55.2187) on Interface Fa0/6 AuditSessionID 0A3039E10000000600757ABB

Oct 15 13:51:03.723: Applying command... 'no switchport access vlan 1' at Fa0/6

Oct 15 13:51:03.739: Applying command... 'no switchport nonegotiate' at Fa0/6

Oct 15 13:51:03.748: Applying command... 'switchport trunk encapsulation dot1q' at Fa0/6

Oct 15 13:51:03.756: Applying command... 'switchport mode trunk' at Fa0/6

Oct 15 13:51:03.756: Applying command... 'switchport trunk native vlan 1' at Fa0/6

Oct 15 13:51:03.764: Applying command... 'spanning-tree portfast trunk' at Fa0/6

Oct 15 13:51:04.805: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (001b.0d55.2187) on Interface Fa0/6 AuditSessionID 0A3039E10000000600757ABB

Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Received action Run Authenticator

Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Authenticator received event Start in state Not Running

Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Authenticator state changed to Waiting link UP

Oct 15 13:51:04.805: CISP-EVENT (Fa0/6): Sync supp\_id: 0

Oct 15 13:51:05.669: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state to up

Oct 15 13:51:06.793: CISP-EVENT (Fa0/6): Received action Run Authenticator

Oct 15 13:51:06.793: CISP-EVENT (Fa0/6): Authenticator received event Start in state Waiting link UP (no-op)

**Oct 15 13:51:07.799: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/6, changed state to up**

Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Authenticator received event Link UP in state Waiting link UP

Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Transmitting a CISP Packet

Oct 15 13:51:07.799: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018  
Type:HELLO

Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Proposing CISP version: 1

Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)

Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Authenticator state changed to Idle

Oct 15 13:51:07.799: CISP-EVENT (Fa0/6): Sync supp\_id: 0

Oct 15 13:51:07.799: CISP-EVENT: Received action Start Tick Timer

Oct 15 13:51:07.799: CISP-EVENT: Started CISP tick timer

Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): 'hello' timer expired

Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Authenticator received event Timeout in state Idle

Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Transmitting a CISP Packet

Oct 15 13:51:12.942: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018  
Type:HELLO

Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Proposing CISP version: 1

Oct 15 13:51:12.942: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)

Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): 'hello' timer expired

Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Authenticator received event Timeout in state Idle

Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Transmitting a CISP Packet

Oct 15 13:51:18.084: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018  
Type:HELLO

Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Proposing CISP version: 1

Oct 15 13:51:18.084: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)

Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): 'hello' timer expired

Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Authenticator received event Timeout in state Idle

Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Transmitting a CISP Packet

Oct 15 13:51:23.226: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x20 Length:0x0018  
Type:HELLO

Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Proposing CISP version: 1

Oct 15 13:51:23.226: CISP-EVENT (Fa0/6): Started 'hello' timer (5s)

Oct 15 13:51:28.377: CISP-EVENT (Fa0/6): 'hello' timer expired

Oct 15 13:51:28.377: CISP-EVENT (Fa0/6): Authenticator received event Timeout in

```

state Idle
Oct 15 13:51:29.400: CISP-EVENT: Stopped CISP tick timer
Oct 15 13:51:36.707: CISP-RXPAK (Fa0/6): Code:REQUEST ID:0x22 Length:0x001C
Type:REGISTRATION
Oct 15 13:51:36.707: Payload: 0200E84B
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Authenticator received event Receive
Packet in state Idle
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Proposed CISP version: 1
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Negotiated CISP version: 1
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Sync supp_id: 59467
Oct 15 13:51:36.707: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:36.707: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x22 Length:0x001C
Type:REGISTRATION
Oct 15 13:51:36.707: Payload: 01000000
Oct 15 13:51:36.724: CISP-RXPAK (Fa0/6): Code:REQUEST ID:0x23 Length:0x003A
Type:ADD_CLIENT
Oct 15 13:51:36.724: Payload: 010011020009001B0D5521C10300050 ...
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Authenticator received event Receive
Packet in state Idle
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client 001b.0d55.21c1 (vlan: 200)
to authenticator list
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Notifying interest parties about new
downstream client 001b.0d55.21c1 (vlan: 200)
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client info at Authenticator
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client 001b.0d55.21c0 (vlan: 1)
to authenticator list
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Notifying interest parties about new
downstream client 001b.0d55.21c0 (vlan: 1)
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Adding client info at Authenticator
Oct 15 13:51:36.724: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 13:51:36.724: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x23 Length:0x0018
Type:ADD_CLIENT

```

Uma vez que a authentication e autorização sucede, a troca CISP ocorre. Cada troca tem um PEDIDO, que seja enviado pelo suplicante, e uma RESPOSTA, que serve como uma resposta e um reconhecimento do autenticador.

Duas trocas distintas são executadas: REGISTRO e ADD\_CLIENT. Durante a troca do REGISTRO, o suplicante informa o autenticador que é CISP-capaz, e o autenticador a seguir reconhece esta mensagem. A troca ADD\_CLIENT é usada para informar o autenticador sobre os dispositivos conectados à porta local do suplicante. Como com REGISTRO, ADD-CLIENT é iniciado no suplicante e reconhecido pelo autenticador.

Inscreva estes comandos show a fim verificar a comunicação, os papéis, e os endereços:

```
bstp-3500-1#show cisp clients
```

```
Authenticator Client Table:
```

```

-----
MAC Address VLAN Interface
-----
001b.0d55.21c1 200 Fa0/6
001b.0d55.21c0 1 Fa0/6

```

```
bstp-3500-1#show cisp registrations
```

```
Interface(s) with CISP registered user(s):
```

```

-----
Fa0/6
Auth Mgr (Authenticator)

```

Neste exemplo, o papel do autenticador é atribuído corretamente à relação correta (fa0/6), e dois endereços MAC são registrados. Os endereços MAC são o suplicante na porta fa0/6 no VLAN1 e

em VLAN200.

A verificação de sessões da autenticação do dot1x pode agora ser executada. A porta fa0/6 no interruptor ascendente é autenticada já. Esta é a troca do dot1x que está provocada quando BSTP-3500-2 (o suplicante) é obstruído em:

```
bstp-3500-1#show authentication sessions
```

```
Interface MAC Address Method Domain Status Session ID
Fa0/6 001b.0d55.2187 dot1x DATA Authz Success 0A3039E10000000700FB3259
```

Como esperado nesta fase, não há nenhuma sessão no suplicante:

```
bstp-3500-2#show authentication sessions
```

```
No Auth Manager contexts currently exist
```

## Autenticação do PC Windows ao interruptor do suplicante

Neste exemplo, o PC Windows autentica ao suplicante. As etapas no processo são:

1. O PC Windows é obstruído em FastEthernet 0/5 de porta em BSTP-3500-2 (o suplicante).
2. O suplicante executa a authentication e autorização com o ISE.
3. O suplicante informa o autenticador que um cliente novo está conectado na porta.

Esta é a comunicação do suplicante:

```
Oct 15 14:19:37.207: %AUTHMGR-5-START: Starting 'dot1x' for client
(c464.13b4.29c3) on Interface Fa0/5 AuditSessionID 0A3039E200000013008F77FA
Oct 15 14:19:37.325: %DOT1X-5-SUCCESS: Authentication successful for client
(c464.13b4.29c3) on Interface Fa0/5 AuditSessionID
Oct 15 14:19:37.325: %AUTHMGR-7-RESULT: Authentication result 'success' from
'dot1x' for client (c464.13b4.29c3) on Interface Fa0/5 AuditSessionID
0A3039E200000013008F77FA
Oct 15 14:19:37.341: CISP-EVENT (Fa0/5): Received action Add Client
Oct 15 14:19:37.341: CISP-EVENT (Fa0/5): Adding client c464.13b4.29c3 (vlan: 200)
to supplicant list
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Supplicant received event Add Client in
state Idle
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Adding client c464.13b4.29c3 (vlan: 200)
to the ADD list
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Adding client c464.13b4.29c3 (vlan: 200)
to ADD CLIENT req
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 14:19:37.341: CISP-TXPAK (Fa0/6): Code:REQUEST ID:0x24 Length:0x0029
Type:ADD_CLIENT
Oct 15 14:19:37.341: Payload: 010011020009C46413B429C30300050 ...
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Started 'retransmit' timer (30s)
Oct 15 14:19:37.341: CISP-EVENT: Started CISP tick timer
Oct 15 14:19:37.341: CISP-EVENT (Fa0/6): Supplicant state changed to Request
Oct 15 14:19:37.341: CISP-RXPAK (Fa0/6): Code:RESPONSE ID:0x24 Length:0x0018
Type:ADD_CLIENT
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): Supplicant received event Receive Packet
in state Request
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): Stopped 'retransmit' timer
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): All Clients implicitly ACKed
Oct 15 14:19:37.350: CISP-EVENT (Fa0/6): Supplicant state changed to Idle
Oct 15 14:19:38.356: %AUTHMGR-5-SUCCESS: Authorization succeeded for client
(c464.13b4.29c3) on Interface Fa0/5 AuditSessionID 0A3039E200000013008F77FA
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Received action Run Authenticator
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Authenticator received event Start in
state Not Running
```



```
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Authenticator state changed to Waiting link UP
Oct 15 14:19:38.356: CISP-EVENT (Fa0/5): Sync supp_id: 0
Oct 15 14:19:38.373: CISP-EVENT: Stopped CISP tick timer
Oct 15 14:19:39.162: %LINK-3-UPDOWN: Interface FastEthernet0/5, changed state to up
```

Uma troca ADD\_CLIENT ocorre, mas nenhuma troca do REGISTRO é precisada.

A fim verificar o comportamento no suplicante, incorpore o comando dos registros do cisp da mostra:

```
bstp-3500-2#show cisp registrations
```

```
Interface(s) with CISP registered user(s):
```

```
-----
Fa0/5
Auth Mgr (Authenticator)
Fa0/6
802.1x Sup (Supplicant)
```

O suplicante tem o papel de um suplicante para o autenticador (relação fa0/6) e o papel de um autenticador para o PC Windows (relação fa0/5).

A fim verificar o comportamento no autenticador, incorpore o comando dos clientes do cisp da mostra:

```
bstp-3500-1#show cisp clients
```

```
Authenticator Client Table:
```

```
-----
MAC Address VLAN Interface
```

```
-----
001b.0d55.21c1 200 Fa0/6
001b.0d55.21c0 1 Fa0/6
c464.13b4.29c3 200 Fa0/6
```

Um MAC address novo aparece no autenticador sob VLAN 200. É o MAC address que foi observado em pedidos AAA no suplicante.

As sessões da autenticação devem indicar que o mesmo dispositivo está conectado na porta fa0/5 do suplicante:

```
bstp-3500-2#show authentication sessions
```

```
Interface MAC Address Method Domain Status Session ID
Fa0/5 c464.13b4.29c3 dot1x DATA Authz Success 0A3039E20000001501018B58
```

## Remoção do cliente autenticado da rede

Quando um cliente estiver removido (por exemplo, se uma porta está fechada), o autenticador está notificado com a troca DELETE\_CLIENT.

```
Oct 15 15:54:05.415: CISP-RXPAK (Fa0/6): Code:REQUEST ID:0x25 Length:0x0029
Type:DELETE_CLIENT
Oct 15 15:54:05.415: Payload: 010011020009C46413B429C30300050 ...
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Authenticator received event Receive Packet in state Idle
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Removing client c464.13b4.29c3 (vlan: 200) from authenticator list
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Notifying interest parties about
```

```
deletion of downstream client c464.13b4.29c3 (vlan: 200)
Oct 15 15:54:05.415: CISP-EVENT (Fa0/6): Transmitting a CISP Packet
Oct 15 15:54:05.415: CISP-TXPAK (Fa0/6): Code:RESPONSE ID:0x25 Length:0x0018
Type:DELETE_CLIENT
```

## Remoção do interruptor do suplicante

Quando um suplicante é desconectado ou removido, o autenticador introduz a configuração original de volta à porta a fim evitar interesses de segurança.

```
Oct 15 15:57:31.257: Applying command... 'no switchport nonegotiate' at Fa0/6
Oct 15 15:57:31.273: Applying command... 'switchport mode access' at Fa0/6
Oct 15 15:57:31.273: Applying command... 'no switchport trunk encapsulation
dot1q' at Fa0/6
Oct 15 15:57:31.290: Applying command... 'no switchport trunk native vlan 1' at
Fa0/6
Oct 15 15:57:31.299: Applying command... 'no spanning-tree portfast trunk' at
Fa0/6
Oct 15 15:57:31.307: Applying command... 'switchport access vlan 1' at Fa0/6
Oct 15 15:57:31.315: Applying command... 'spanning-tree portfast' at Fa0/6
Oct 15 15:57:32.247: %LINEPROTO-5-UPDOWN: Line protocol on Interface
FastEthernet0/6, changed state to down
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Authenticator received event Link DOWN
in state Idle
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Removing client 001b.0d55.21c1
(vlan: 200) from authenticator list
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Notifying interest parties about
deletion of downstream client 001b.0d55.21c1 (vlan: 200)
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Removing client 001b.0d55.21c0 (vlan: 1)
from authenticator list
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Notifying interest parties about
deletion of downstream client 001b.0d55.21c0 (vlan: 1)
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Authenticator state changed to Not
Running
Oct 15 15:57:32.247: CISP-EVENT (Fa0/6): Sync supp_id: 0
Oct 15 15:57:33.262: %LINK-3-UPDOWN: Interface FastEthernet0/6, changed state
to down
```

Ao mesmo tempo, o suplicante remove os clientes que representam o suplicante da tabela CISP e desativa CISP nessa relação.

## Portas sem o dot1x no interruptor do suplicante

A informação CISP que é propagada do suplicante ao autenticador serve somente como uma outra camada de aplicação. O suplicante informa o autenticador sobre todos os endereços permitidos MAC que lhe são conectados.

Uma encenação que seja entendida mal tipicamente é esta: se um dispositivo é obstruído em uma porta que não tenha o dot1x permitido, o MAC address é instruído e propagado ao interruptor ascendente com CISP.

O autenticador permite uma comunicação que venha de todos os clientes aprendidos com CISP.

Essencialmente, é o papel do suplicante para restringir o acesso dos dispositivos, com o dot1x ou os outros métodos, e para propagar o MAC address e a informação de VLAN ao autenticador. O autenticador atua como um impulsor da informação fornecido naquelas atualizações.

Como um exemplo, um VLAN novo (VLAN300) foi criado em ambos os Switches, e em um dispositivo foi obstruído na porta fa0/4 no suplicante. A porta fa0/4 é uma porta de acesso simples que não seja configurada para o dot1x.

Esta saída do suplicante mostra uma porta registrada nova:

```
bstp-3500-2#show cisp registrations
```

```
Interface(s) with CISP registered user(s):
```

```
-----  
Fa0/4  
Fa0/5  
Auth Mgr (Authenticator)  
Fa0/6  
802.1x Sup (SupPLICant)
```

No autenticador, um MAC address novo é visível em VLAN 300.

```
bstp-3500-1#show cisp clients
```

```
Authenticator Client Table:
```

```
-----  
MAC Address VLAN Interface  
-----  
001b.0d55.21c1 200 Fa0/6  
001b.0d55.21c0 1 Fa0/6  
001b.0d55.21c2 300 Fa0/6  
c464.13b4.29c3 200 Fa0/6  
 68ef.bdc7.13ff 300 Fa0/6
```

## Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Nota:

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

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

Estes comandos help você pesquisa defeitos PURO e CISP; este documento inclui exemplos para a maioria deles:

- **debugar o cisp todo** - mostra a troca da informação CISP entre os Switches.
- **mostre o sumário do cisp** - indica um sumário do status da interface CISP no interruptor.
- **mostre registros do cisp** - indica as relações que participam em trocas CISP, os papéis daquelas relações, e se as relações são parte de PURAS.
- **mostre clientes do cisp** - indica uma tabela de endereços do cliente conhecido MAC e de seu lugar (VLAN e relação). Isto é útil principalmente do autenticador.