Exemplo de configuração de NEAT com Cisco Identity Services Engine

Contents

[Introduction](#)
[Prerequisites](#)
[Requirements](#)
[Componentes Utilizados](#)
[Configurar](#)
[Diagrama de Rede](#)
[Configuração do Comutador do Autenticador](#)
[Configuração do switch solicitante](#)
[Configuração do ISE](#)
[Verificar](#)
[Autenticação do Comutador Requerente para o Comutador Autenticador](#)
[Autenticação do PC Windows para Comutador Requerente](#)
[Remoção de cliente autenticado da rede](#)
[Remoção do Comutador Requerente](#)
[Portas Sem dot1x no Switch Solicitante](#)
[Troubleshoot](#)

Introduction

Este documento descreve a configuração e o comportamento da Network Edge Authentication Topology (NEAT) em um cenário simples. A NEAT utiliza o Protocolo de Sinalização de Informações de Cliente (CISP - Client Information Signaling Protocol) para propagar endereços MAC de clientes e informações de VLAN entre switches suplicantes e autenticadores.

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

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento do padrão de autenticação IEEE 802.1x.

Componentes Utilizados

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

- Dois switches Cisco Catalyst 3560 Series com Cisco IOS® Software, versão 12.2(55)SE8; um switch atua como autenticador e o outro atua como solicitante.
- Cisco Identity Services Engine (ISE), versão 1.2.
- PC com Microsoft Windows XP, Service Pack 3.

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

Este exemplo abrange configurações de exemplo para:

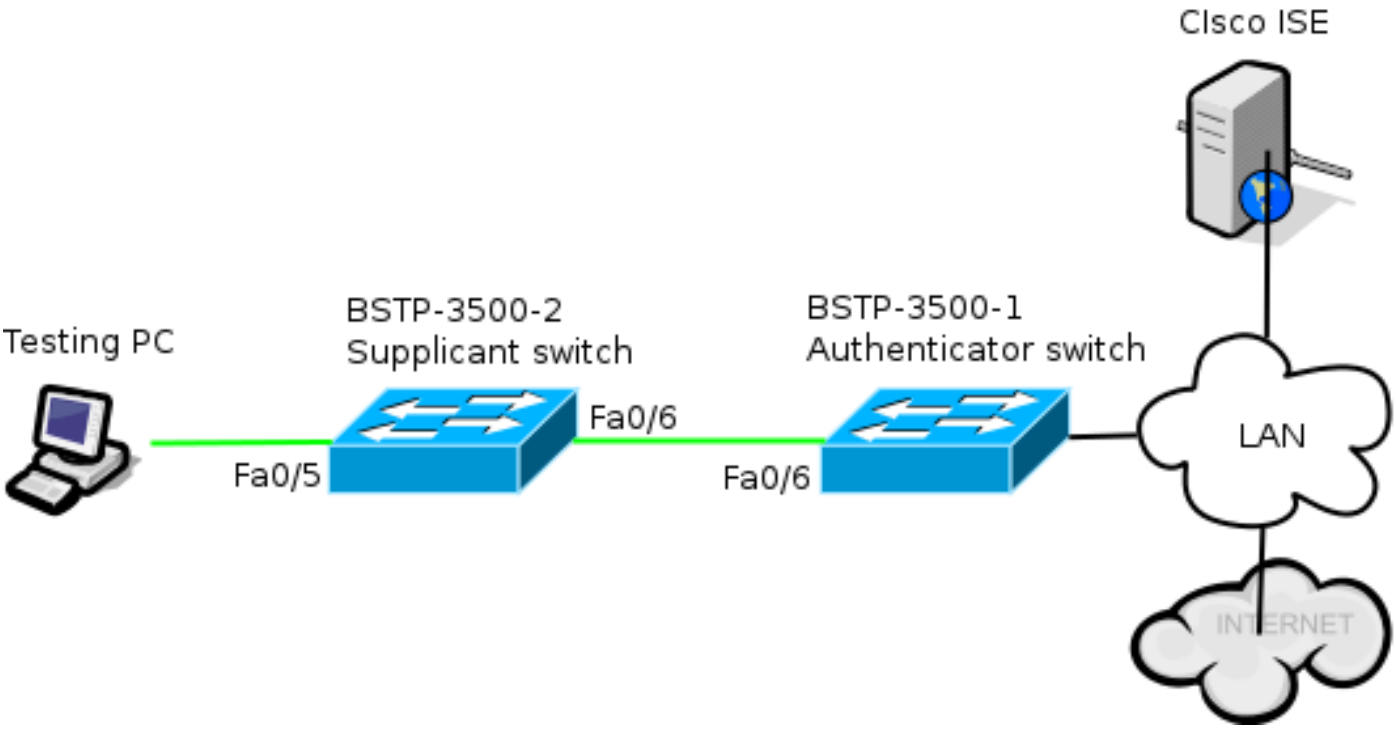
- Switch do autenticador
- Chave suplicante
- Cisco ISE

As configurações são o mínimo necessário para executar este exercício de laboratório; elas podem não ser ideais para atender a 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 de rede ilustra a conectividade usada neste exemplo. As linhas pretas indicam conectividade lógica ou física e as linhas verdes indicam links autenticados através do uso do 802.1x.



Configuração do Comutador do Autenticador

O autenticador contém os elementos básicos necessários para dot1x. Neste exemplo, os comandos específicos de NEAT ou CISP estão em negrito.

Esta é a configuração básica de autenticação, autorização e contabilização (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
```

O CISP é ativado globalmente e a porta de interconexão é configurada no modo autenticador e de acesso.

Configuração do switch solicitante

A configuração precisa do solicitante é crucial para que toda a configuração funcione como esperado. Esta configuração de exemplo contém uma configuração AAA e dot1x típica.

Esta é a configuração básica de 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 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 requerente deve ter credenciais configuradas e deve fornecer um método EAP (Extensible Authentication Protocol) a ser usado.

O requerente pode usar EAP-Message Digest 5 (MD5) e EAP-Flexible Authentication via Secure Protocol (FAST) (entre outros tipos de EAP) para autenticação no caso de CISP. Para manter a configuração do ISE em um nível mínimo, este exemplo usa EAP-MD5 para autenticação do solicitante no autenticador. (O padrão forçaria o uso de EAP-FAST, que requer o provisionamento de PAC (Protected Access Credential); este documento não cobre esse cenário.)

```
! 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 já está configurada para ser uma porta de tronco (ao contrário da configuração da porta de acesso no autenticador). Nesse estágio, isso é esperado; a configuração será alterada dinamicamente quando o ISE retornar 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 se conecta ao PC Windows tem uma configuração mínima e é mostrada aqui apenas para referência.

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

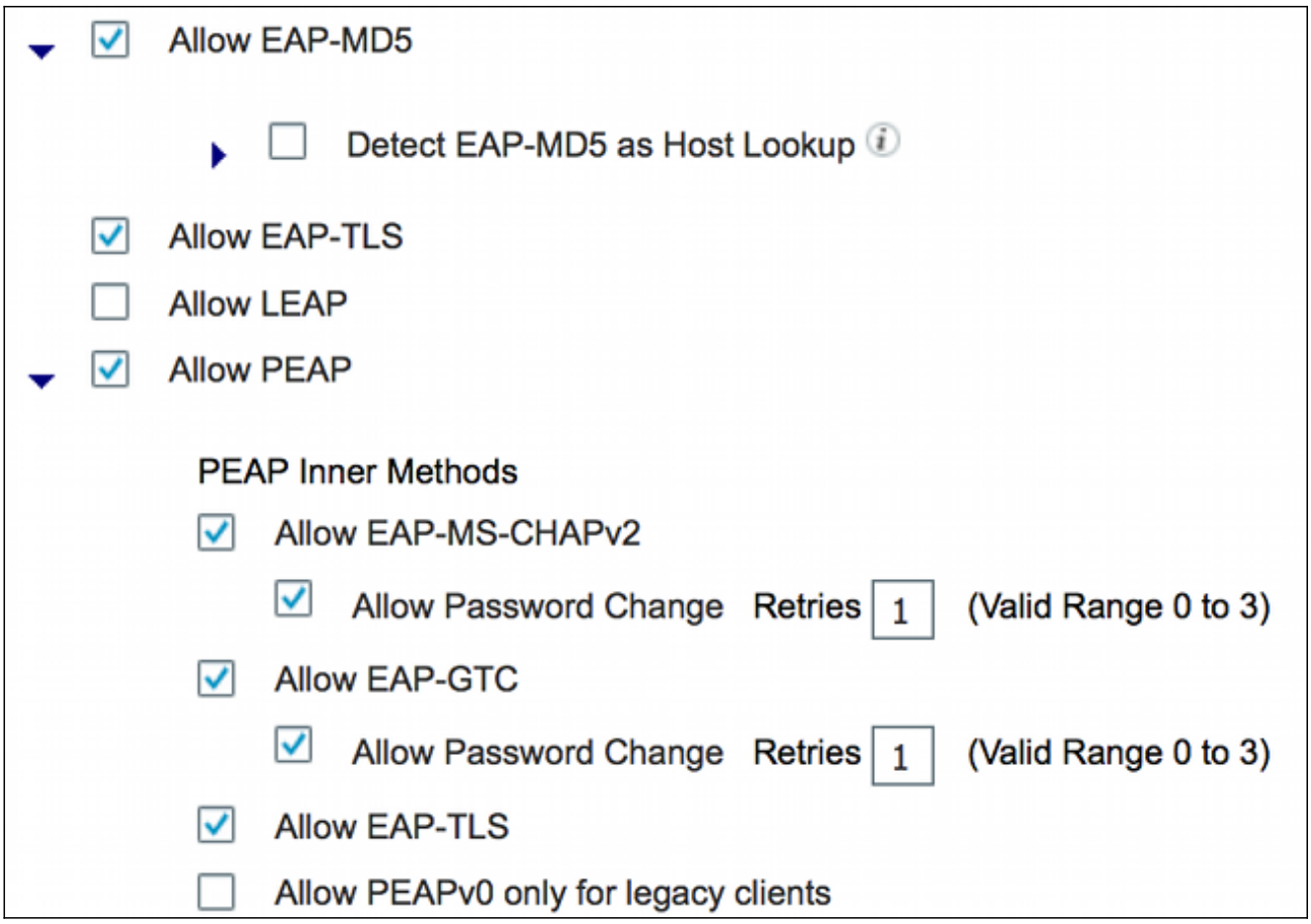
Configuração do ISE

Este procedimento descreve como definir uma configuração básica do ISE.

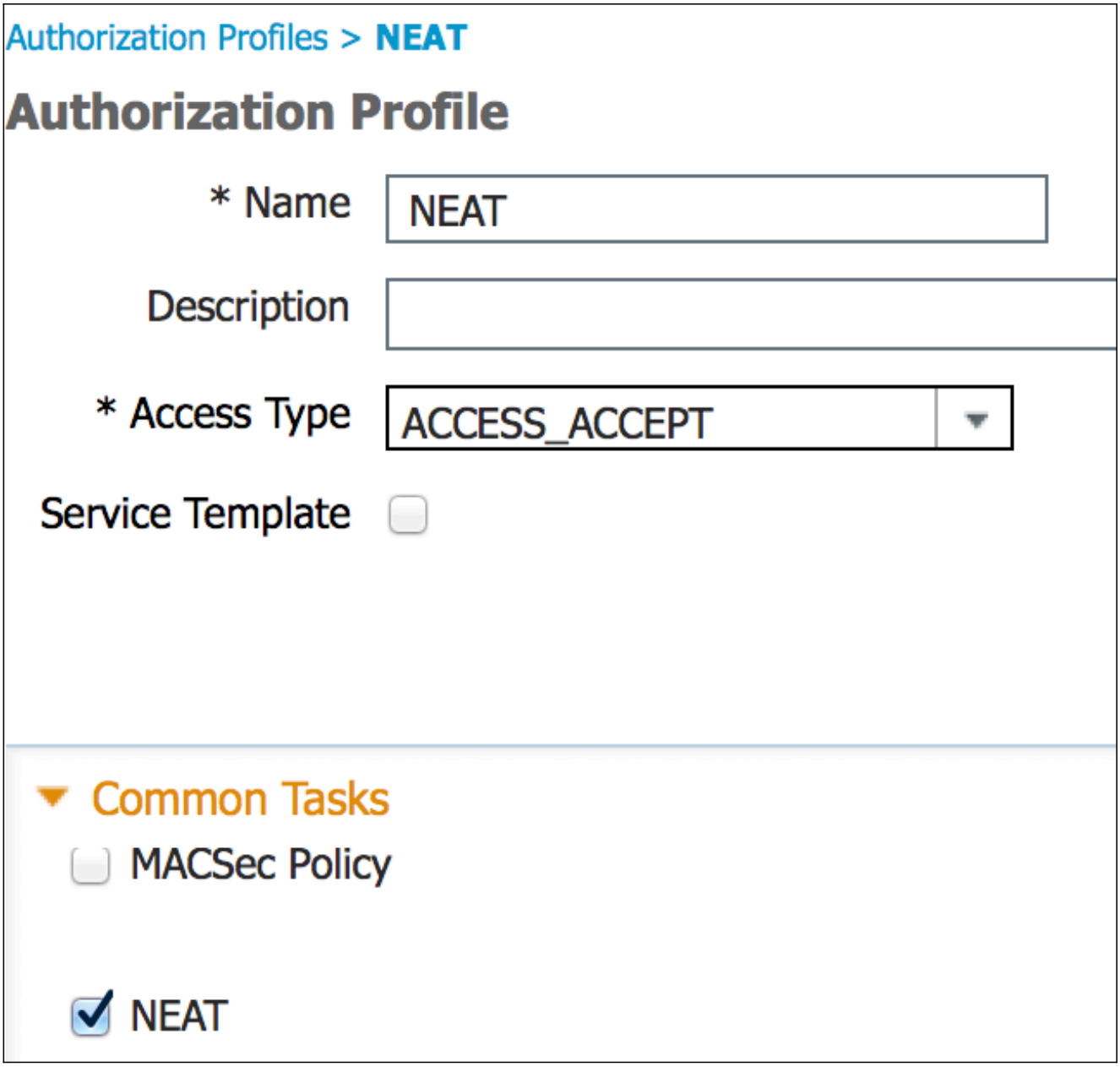
1. Habilite os protocolos de autenticação necessários.

   Neste exemplo, o dot1x com fio permite que o EAP-MD5 autentique o solicitante para o autenticador e permite que o Protected Extensible Authentication Protocol (PEAP)-Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2) autentique o Windows PC para o solicitante.

   Navegue para **Policy > Results > Authentication > Allowed protocols**, selecione a **protocol service list** usada por wired dot1x e verifique se os protocolos nesta etapa estão ativados.



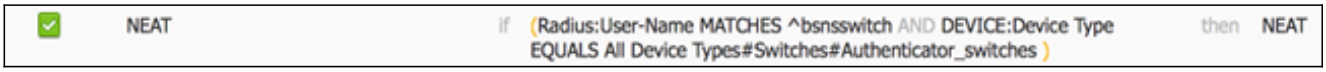
2. Crie uma política de autorização. Navegue para **Política > Resultados > Autorização > Política de autorização** e crie ou atualize uma política para que ela contenha NEAT como um atributo retornado. Este é um exemplo dessa política:



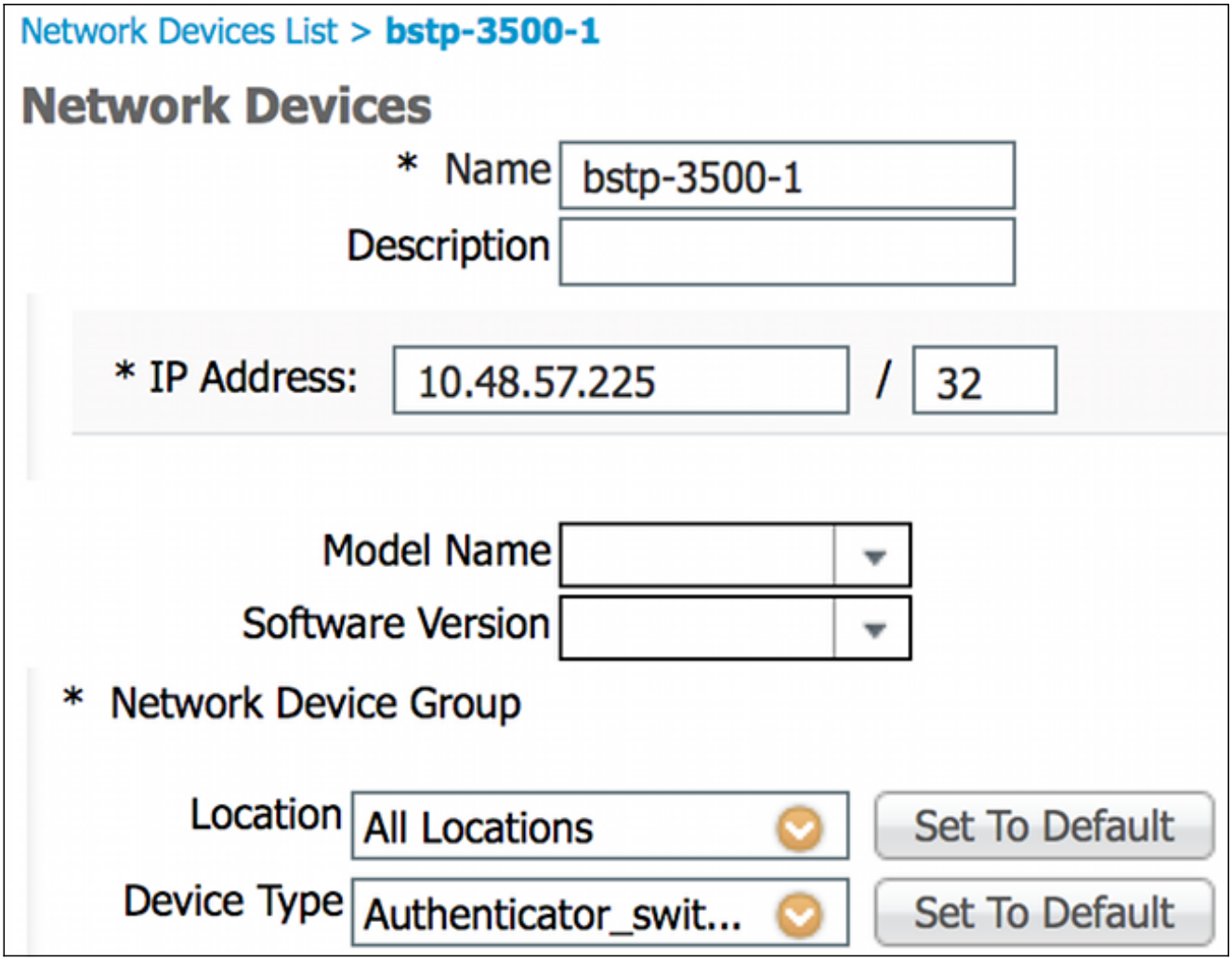
Quando a opção NEAT é ativada, o ISE retorna device-traffic-class=switch como parte da autorização. Esta opção é necessária para alterar o modo de porta do autenticador de acesso para tronco.

3. Crie uma regra de autorização para usar este perfil. Navegue até **Política > Autorização** e crie ou atualize uma regra.

   Neste exemplo, um grupo de dispositivos especial chamado Authenticator_switches é criado, e todos os suplicantes enviam um nome de usuário que começa com bsnsswitch.



4. Adicione os switches ao grupo apropriado. Navegue até **Administration > Network Resources > Network Devices** e clique em **Add**.



Neste exemplo, BSTP-3500-1 (o autenticador) faz parte do grupo Authenticator_switches; BSTP-3500-2 (o suplicante) não precisa fazer parte deste grupo.

Verificar

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

- Autenticação entre switches
- Autenticação entre o PC Windows e o requerente

Ele também explica três situações adicionais:

- Remoção de um cliente autenticado da rede
- Retirada do requerente
- Portas sem dot1x em um solicitante

Notas:

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..

Consulte Informações Importantes sobre Comandos de Depuração antes de usar comandos

debug.

Autenticação do Comutador Requerente para o Comutador Autenticador

Neste exemplo, o suplicante autentica para o autenticador. As etapas do processo são:

1. O suplicante está configurado e conectado à porta fastethernet0/6. A troca dot1x faz com que o solicitante use EAP para enviar um nome de usuário e uma senha pré-configurados para o autenticador.
2. O autenticador executa uma troca RADIUS e fornece credenciais para validação do ISE.
3. Se as credenciais estiverem corretas, o ISE retornará os atributos exigidos pelo NEAT (device-traffic-class=switch) e o autenticador alterará o modo da porta do switch de acesso para tronco.

Este exemplo mostra a troca de informações CISP entre 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
```

Quando a autenticação e a autorização forem bem-sucedidas, ocorrerá a troca de CISP. Cada troca tem um REQUEST, que é enviado pelo requerente, e um RESPONSE, que serve como uma resposta e confirmação do autenticador.

Duas trocas distintas são realizadas: REGISTRATION e ADD_CLIENT. Durante a troca de REGISTRO, o solicitante informa ao autenticador que é capaz de CISP, e o autenticador então confirma esta mensagem. A troca ADD_CLIENT é usada para informar o autenticador sobre dispositivos conectados à porta local do solicitante. Como no REGISTRO, o ADD-CLIENT é iniciado no solicitante e confirmado pelo autenticador.

Insira estes comandos show para verificar a comunicação, as funções 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, a função de Autenticador é atribuída corretamente à interface correta (fa0/6) e dois endereços MAC são registrados. Os endereços MAC são o solicitante na porta fa0/6 na VLAN1 e na VLAN200.

A verificação das sessões de autenticação dot1x pode agora ser executada. A porta fa0/6 no switch upstream já está autenticada. Esta é a troca dot1x que é disparada quando o BSTP-3500-2 (o suplicante) está conectado:

```
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 sessões sobre o requerente:

```
bstp-3500-2#show authentication sessions
No Auth Manager contexts currently exist
```

Autenticação do PC Windows para Comutador Requerente

Neste exemplo, o PC Windows autentica o solicitante. As etapas do processo são:

1. O PC Windows está conectado à porta FastEthernet 0/5 em BSTP-3500-2 (o solicitante).
2. O solicitante executa a autenticação e a autorização com o ISE.
3. O solicitante informa ao autenticador que um novo cliente está conectado à 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 REGISTRATION é necessária.

Para verificar o comportamento do solicitante, insira o comando **show cisp registations**:

```
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 a função de um suplicante em relação ao autenticador (interface fa0/6) e a função de um autenticador em relação ao Windows PC (interface fa0/5).

Para verificar o comportamento no autenticador, insira o comando **show cisp clients**:

```
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 novo endereço MAC aparece no autenticador na VLAN 200. É o endereço MAC que foi observado nas solicitações AAA no suplicante.

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

```
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 de cliente autenticado da rede

Quando um cliente é removido (por exemplo, se uma porta é desativada), o autenticador é notificado através da 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 Comutador Requerente

Quando um suplicante é desconectado ou removido, o autenticador introduz a configuração original de volta à porta para evitar preocupações 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 solicitante remove os clientes que representam o solicitante da tabela CISP e desativa o CISP nessa interface.

Portas Sem dot1x no Switch Solicitante

As informações do CISP que são propagadas do solicitante para o autenticador servem apenas como outra camada de aplicação. O suplicante informa o autenticador sobre todos os endereços MAC permitidos que estão conectados a ele.

Um cenário que normalmente é mal entendido é este: se um dispositivo estiver conectado a uma porta que não tem dot1x habilitado, o endereço MAC é aprendido e propagado para o switch upstream através do CISP.

O autenticador permite a comunicação que vem de todos os clientes aprendidos através do CISP.

Em essência, é função do requerente restringir o acesso de dispositivos, através de dot1x ou outros métodos, e propagar o endereço MAC e as informações de VLAN para o autenticador. O autenticador atua como um fiscalizador das informações fornecidas nessas atualizações.

Como exemplo, uma nova VLAN (VLAN300) foi criada em ambos os switches, e um dispositivo foi conectado à porta fa0/4 no solicitante. A porta fa0/4 é uma porta de acesso simples que não está configurada para dot1x.

Esta saída do solicitante mostra uma nova porta registrada:

```
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 novo endereço MAC é visível na 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
```

Troubleshoot

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

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

Estes comandos ajudam você a solucionar problemas de NEAT e CISP; este documento inclui exemplos para a maioria deles:

- **debug cisp all** - mostra a troca de informações CISP entre switches.
- **show cisp summary** - exibe um resumo do status da interface do CISP no switch.
- **show cisp registations** - indica as interfaces que participam de trocas CISP, as funções dessas interfaces e se as interfaces fazem parte do NEAT.
- **show cisp clients** - exibe uma tabela de endereços MAC de clientes conhecidos e sua localização (VLAN e interface). Isso é útil principalmente no autenticador.

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.