思科身份服务引擎的NEAT配置示例

目录

简介
先决条件
要求
使用的组件
配置
网络图
身份验证器交换机配置
Supplicant客户端交换机配置
ISE 配置
验证
Supplicant客户端交换机身份验证到身份验证器交换机
Windows PC对请求方交换机的身份验证
从网络中移除经过身份验证的客户端
移除请求方交换机
请求方交换机上没有dot1x的端口
故障排除

简介

本文档在一个简单的场景中描述网络边缘身份验证拓扑(NEAT)的配置和行为。NEAT利用客户端信息信令协议(CISP)在请求方和身份验证方交换机之间传播客户端MAC地址和VLAN信息。

在此配置示例中，身份验证器交换机（也称为身份验证器）和请求者交换机（也称为请求者）都执行802.1x身份验证；身份验证器对请求者进行身份验证，后者进而对测试PC进行身份验证。

先决条件

要求

Cisco建议您了解IEEE 802.1x身份验证标准。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 两台运行Cisco IOS®软件版本12.$^{2(55)}$SE8的Cisco Catalyst 3560系列交换机；一台交换机充当身份验证器，另一台充当请求方。
- 思科身份服务引擎(ISE)，版本1.2。
- 装有Microsoft Windows XP Service Pack 3的PC。

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

本示例介绍的示例配置：

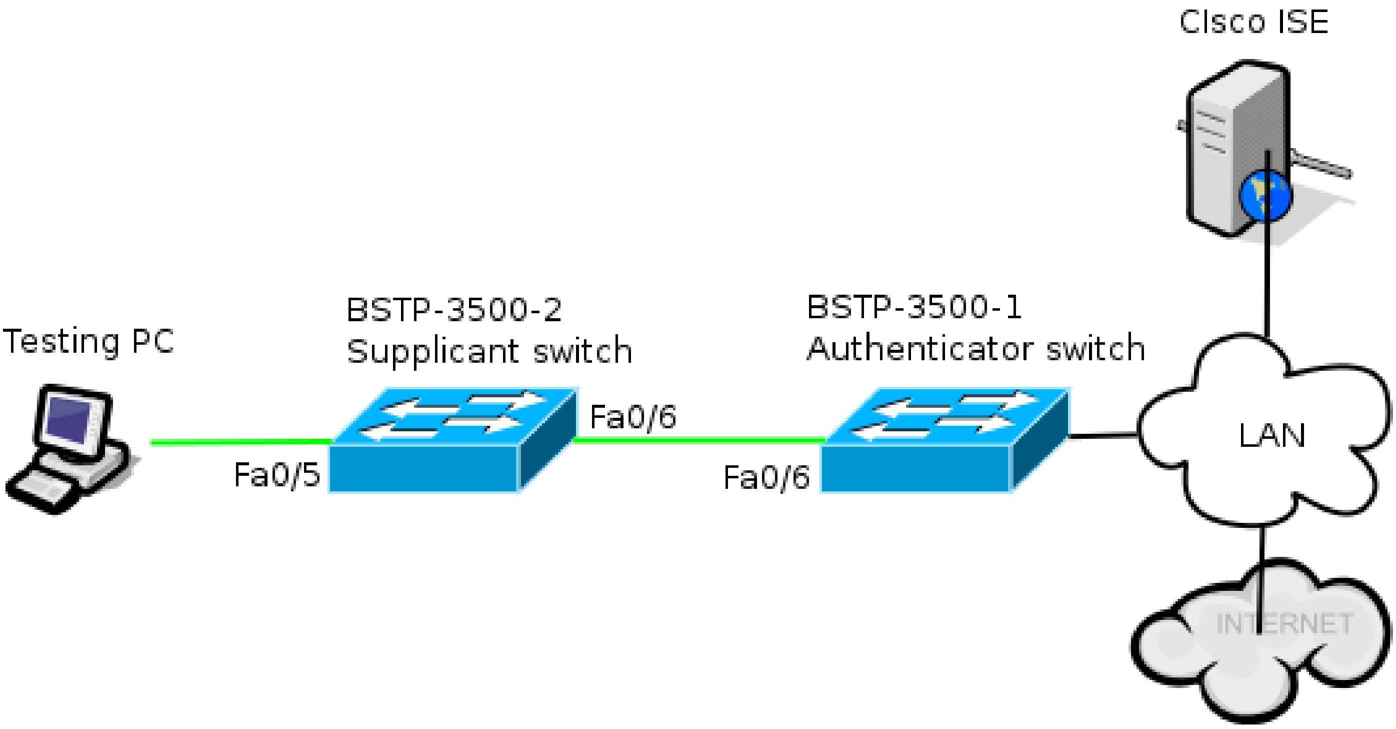
- 身份验证器交换机
- 请求方交换机
- 思科ISE

这些配置是执行本实验练习所需的最低配置；可能并不适用于其他需求或满足其他需求。

> **注意：要获取有关本部分中所使用命令的更多信息，可使用命令查找工具（仅限已注册客户）。**

网络图

此网络图说明本示例中使用的连接。黑色线表示逻辑或物理连接，绿色线表示通过使用802.1x进行身份验证的链路。



身份验证器交换机配置

身份验证器包含dot1x所需的基本元素。在本例中，特定于NEAT或CISP的命令是粗体的。

这是基本的身份验证、授权和记帐(AAA)配置：

```
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全局启用，互连端口在身份验证器和访问模式下配置。

Supplicant客户端交换机配置

准确的Supplicant客户端配置对整个设置能否如预期一样正常运行至关重要。此示例配置包含典型的AAA和dot1x配置。

以下是基本AAA配置：

```
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
```

请求方应已配置凭证，并且应提供要使用的可扩展身份验证协议(EAP)方法。

在CISP的情况下，请求方可以使用EAP-Message Digest 5(MD5)和EAP-Flexible Authentication via Secure Protocol(FAST)（其他EAP类型）进行身份验证。为了将ISE配置保持在最低水平，此示例使用EAP-MD5对身份验证器的请求方进行身份验证。（默认情况下将强制使用EAP-FAST，需要提供保护访问凭证[PAC]；本文档不涵盖此场景。）

```
! 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
```

请求方与身份验证器的连接已配置为中继端口（与身份验证器上的接入端口配置不同）。在此阶段，这是预期结果；当ISE返回正确的属性时，配置将动态更改。

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

连接到Windows PC的端口配置最少，此处仅作参考。

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

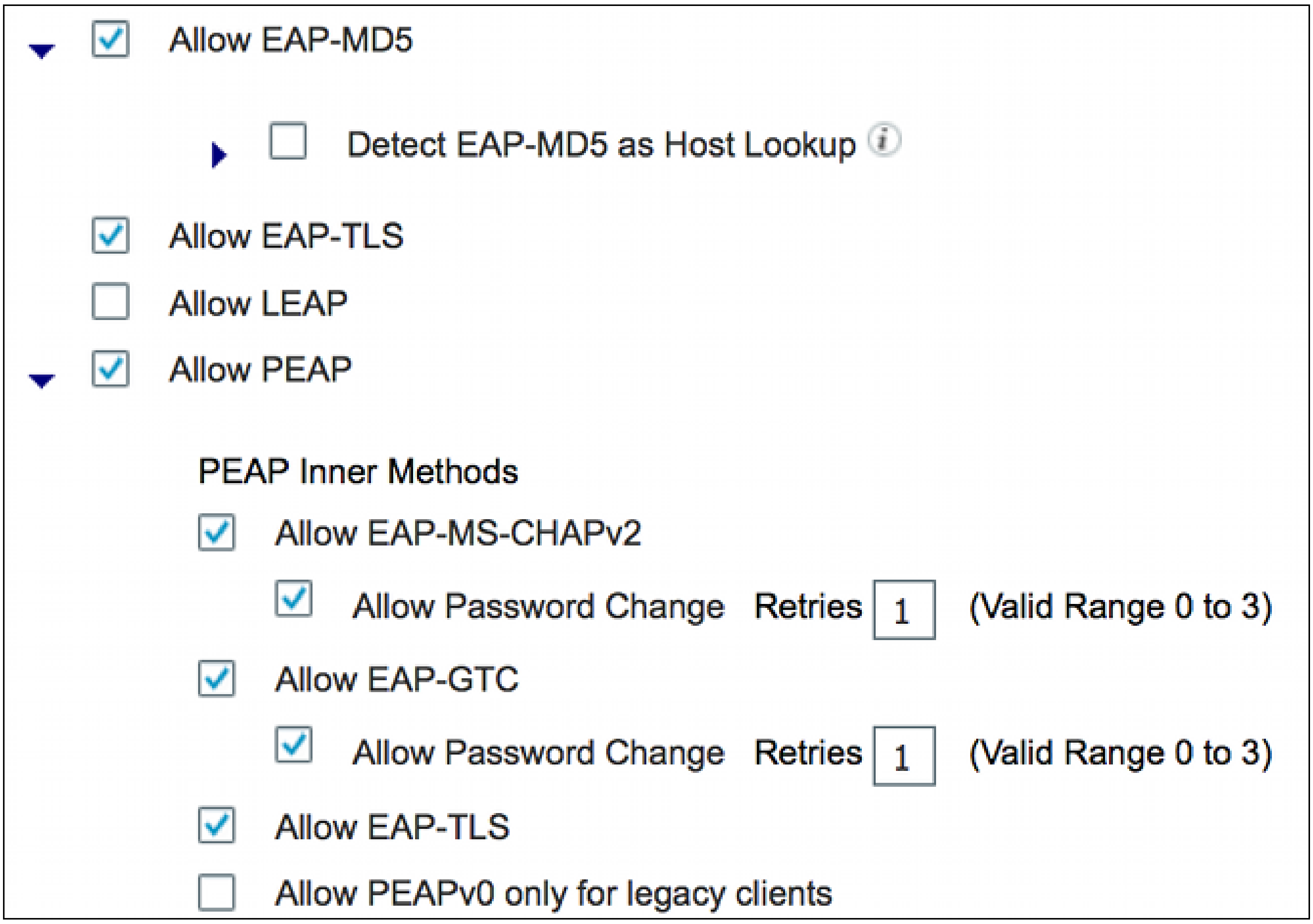
ISE 配置

此过程介绍如何设置基本ISE配置。

1. 启用所需的身份验证协议。

   在本示例中，有线dot1x允许EAP-MD5向身份验证器验证请求方，并允许受保护的可扩展身份验证协议(PEAP)- Microsoft质询握手身份验证协议版本2(MSCHAPv2)向请求方验证Windows PC。

   导航到**Policy > Results > Authentication > Allowed protocols**，选择**有线dot1x使用的协议服务列表**，并确保启用此步骤中的协议。



▼ ☑ Allow EAP-MD5

▶ ☐ Detect EAP-MD5 as Host Lookup

☑ Allow EAP-TLS

☐ Allow LEAP

▼ ☑ Allow PEAP

PEAP Inner Methods

☑ Allow EAP-MS-CHAPv2

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

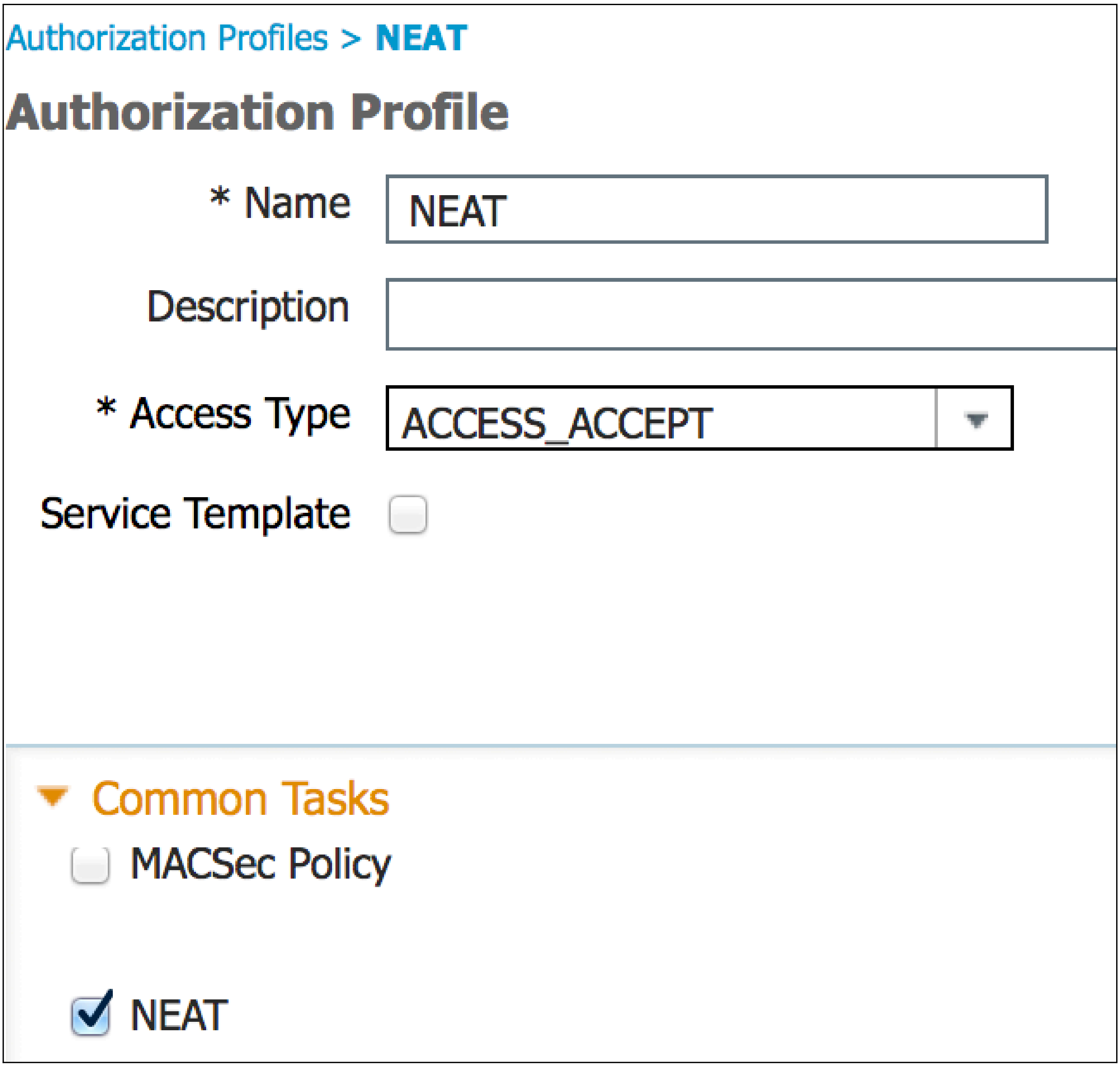
☑ Allow EAP-GTC

☑ Allow Password Change Retries 1 (Valid Range 0 to 3)

☑ Allow EAP-TLS

☐ Allow PEAPv0 only for legacy clients

2. 创建授权策略。导航到**Policy > Results > Authorization > Authorization Policy**，然后创建或更新策略，使其包含NEAT作为返回属性。以下即是此类策略的一个示例：



Authorization Profiles > NEAT

Authorization Profile

* Name: NEAT

Description:

* Access Type: ACCESS_ACCEPT

Service Template □

Common Tasks

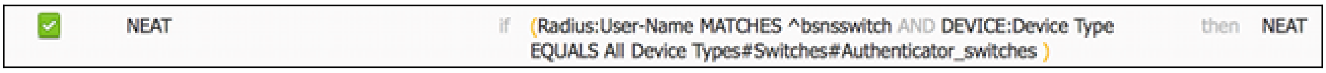
□ MACSec Policy

☑ NEAT

当NEAT选项打开时，ISE将返回device-traffic-class=switch作为授权的一部分。要将身份验证器的端口模式从access更改为trunk，需要使用此选项。

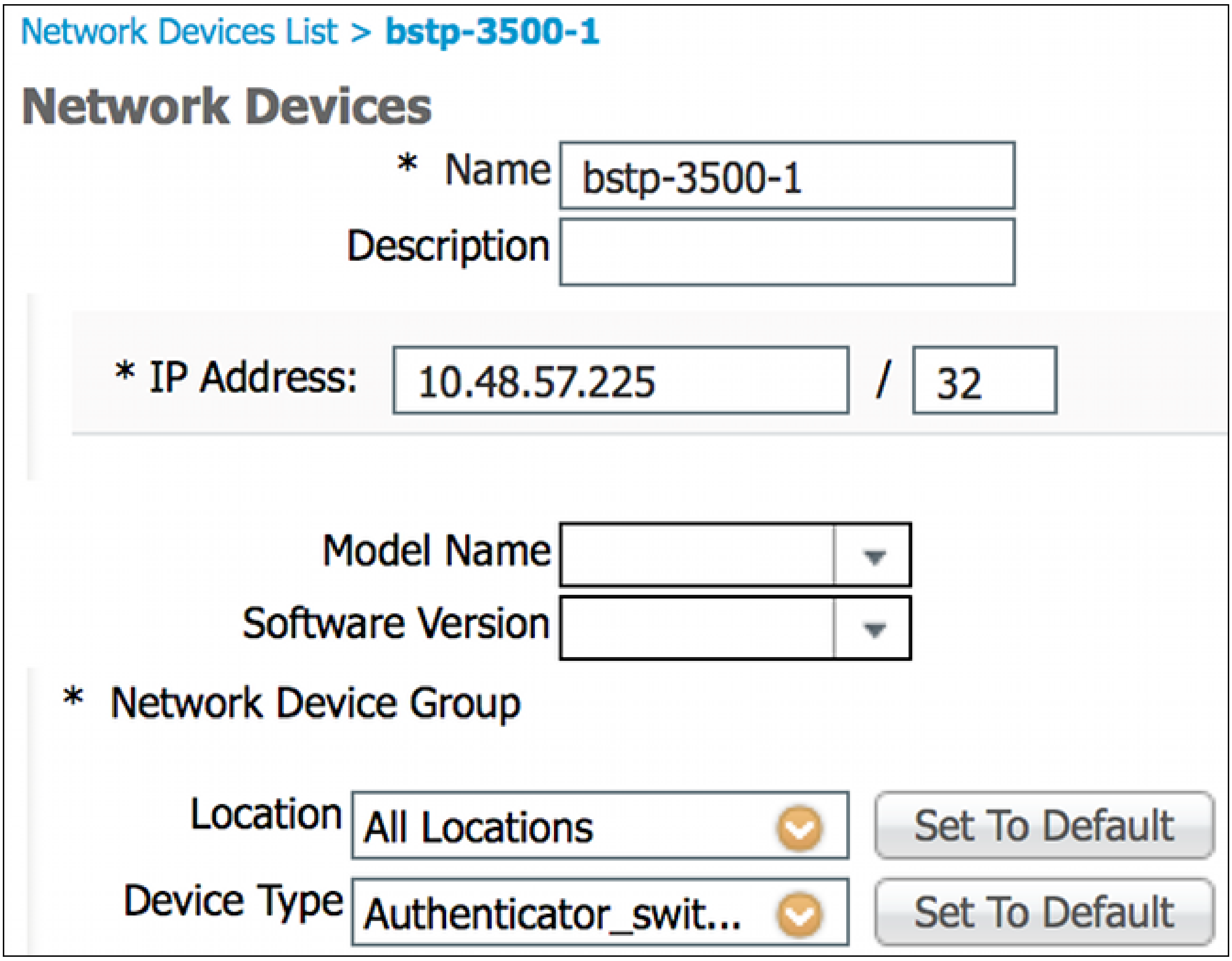
3. 创建授权规则以使用此配置文件。导航到**Policy > Authorization**，然后创建或更新规则。

   在本示例中，创建了一个名为Authenticator_switches的特殊设备组，所有请求方都发送一个以bsnsswitch开头的用户名。



✓ NEAT if (Radius:User-Name MATCHES ^bsnsswitch AND DEVICE:Device Type EQUALS All Device Types#Switches#Authenticator_switches) then NEAT

4. 将交换机添加到适当的组。导航到**Administration > Network Resources > Network Devices**，然后单击**Add**。


Network Devices List > bstp-3500-1

Network Devices

* Name	bstp-3500-1
Description	
* IP Address:	10.48.57.225 / 32
Model Name	
Software Version	

* Network Device Group

Location	All Locations	Set To Default
Device Type	Authenticator_swit...	Set To Default

在本示例中，BSTP-3500-1（身份验证器）是Authenticator_switches组的一部分；BSTP-3500-2（请求方）不需要是此组的一部分。

验证

使用本部分可确认配置能否正常运行。本节介绍两种行为：

- 交换机之间的身份验证
- Windows PC和请求方之间的身份验证

它还解释了三种其他情况：

- 从网络中移除经过身份验证的客户端
- 移除请求方
- 请求方上没有dot1x的端口

注意：

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。

使用 **debug 命令之前，请参阅**有关 Debug 命令的重要信息。

Supplicant客户端交换机身份验证到身份验证器交换机

在本示例中，请求方向身份验证器进行身份验证。此过程中的步骤如下：

1. 请求方已配置并插入端口fastethernet0/6。dot1x交换会导致请求方使用EAP以将预配置的用户名和密码发送到身份验证器。
2. 身份验证器执行RADIUS交换并提供ISE验证的凭证。
3. 如果凭证正确，ISE返回NEAT(device-traffic-class=switch)所需的属性，身份验证器将其交换机端口模式从访问更改为中继。

此示例显示交换机之间的CISP信息交换：

```
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
```

一旦身份验证和授权成功，CISP交换就会发生。每个交换都有一个REQUEST（由请求方发送）和一个RESPONSE（作为来自身份验证器的应答和确认）。

执行两个不同的交换：REGISTRATION和ADD_CLIENT。在注册交换期间，请求方通知身份验证器它支持CISP，然后身份验证器确认此消息。ADD_CLIENT交换用于向身份验证器通知连接到请求方本地端口的设备。与REGISTRATION一样，ADD-CLIENT在请求方启动，并由身份验证器确认。

输入以下show命令以验证通信、角色和地址：

```
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)
```

在本示例中，身份验证器的角色已正确分配到正确的接口(fa0/6)，并且注册了两个MAC地址。MAC地址是VLAN1端口fa0/6和VLAN200上的请求方。

现在可以执行dot1x身份验证会话的验证。上游交换机上的fa0/6端口已经过身份验证。这是插入BSTP-3500-2（请求方）时触发的dot1x交换：

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

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

在此阶段，请求方上没有会话：

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

Windows PC对请求方交换机的身份验证

在本示例中，Windows PC向请求方进行身份验证。此过程中的步骤如下：

1. Windows PC已插入BSTP-3500-2（请求方）的FastEthernet 0/5端口。
2. 请求方通过ISE执行身份验证和授权。
3. 请求方通知身份验证器端口上连接了新客户端。

这是来自请求方的通信：

```
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
```

发生ADD_CLIENT交换，但不需要REGISTRATION交换。

要验证请求方上的行为，请输入**show cisp registrations**命令：

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

Interface(s) with CISP registered user(s):
------------------------------------------
Fa0/5
Auth Mgr (Authenticator)
Fa0/6
802.1x Sup (Supplicant)
```

请求方对身份验证器（fa0/6接口）具有请求方角色，对Windows PC具有身份验证方角色（fa0/5接口）。

要验证身份验证器上的行为，请输入**show cisp clients**命令：

```
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
```

新的MAC地址出现在身份验证器的VLAN 200下。它是在Supplicant客户端上的AAA请求中观察到的MAC地址。

身份验证会话应指示同一设备连接到请求方的fa0/5端口：

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

Interface MAC Address Method Domain Status Session ID
Fa0/5 c464.13b4.29c3 dot1x DATA Authz Success 0A3039E2000000150101 8B58
```

从网络中移除经过身份验证的客户端

删除客户端时（例如，如果端口关闭），将通过DELETE_CLIENT交换通知身份验证器。

```
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
```

移除请求方交换机

当请求方被拔掉或移除时，身份验证器将原始配置引入端口，以避免安全隐患。

```
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
```

同时，请求方从CISP表中删除代表请求方的客户端，并停用该接口上的CISP。

请求方交换机上没有dot1x的端口

从请求方传播到身份验证器的CISP信息仅作为另一层实施。请求方将所允许的所有与其连接的MAC地址通知身份验证器。

通常误解的情况是：如果设备插入未启用dot1x的端口上，则会获取MAC地址并通过CISP传播到上游交换机。

身份验证器允许来自通过CISP学习的所有客户端的通信。

实际上，请求方的作用是通过dot1x或其他方法限制设备的访问，并将MAC地址和VLAN信息传播给身份验证器。身份验证器充当这些更新中提供的信息的执行器。

例如，两台交换机上都创建了新的VLAN(VLAN300)，并将设备插入了请求方的端口fa0/4。端口fa0/4是未为dot1x配置的简单接入端口。

请求方的以下输出显示一个新的注册端口：

```
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)
```

在身份验证器上，新的MAC地址在VLAN 300上可见。

```
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
```

故障排除

本部分提供的信息可用于对配置进行故障排除。

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

这些命令可帮助您对NEAT和CISP进行故障排除；本文档包含大多数命令的示例：

- **debug cisp all** — 显示交换机之间的CISP信息交换。
- **show cisp summary** — 显示交换机上CISP接口状态的摘要。
- **show cisp registrations** — 指示参与CISP交换的接口、这些接口的作用以及接口是否是NEAT的一部分。
- **show cisp clients** — 显示已知客户端MAC地址及其位置（VLAN和接口）的表。这主要对身份验证器有用。

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）。