

整洁的配置示例用思科身份服务引擎

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[证明人交换机配置](#)

[请求方交换机配置](#)

[ISE配置](#)

[Verify](#)

[请求方对证明人交换机的交换机认证](#)

[对请求方交换机的WINDOWS PC认证](#)

[验证的客户端删除从网络](#)

[请求方交换机删除](#)

[没有dot1x的端口在请求方交换机](#)

[Troubleshoot](#)

Introduction

本文在简单情况描述网络边缘认证拓扑配置和工作情况(整洁)。整洁使用客户端信息信令协议(CISP)为了传播客户端MAC地址和VLAN信息在请求方和证明人交换机之间。

在此配置示例中，证明人交换机(也称为证明人)和请求方交换机(也称为请求方)进行802.1x认证;证明人验证请求方，反过来，验证测试的PC。

Prerequisites

Requirements

Cisco建议您有IEEE 802.1X验证标准知识。

Components Used

本文档中的信息基于以下软件和硬件版本：

- 与Cisco IOS软件的两Cisco Catalyst 3560 Series switches，版本12.2(55)SE8;一台交换机作为证明人，并且其他作为请求方。
- 思科身份服务引擎(ISE)，版本1.2。
- PC用Microsoft Windows XP，服务包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.

Configure

此示例包括的配置示例：

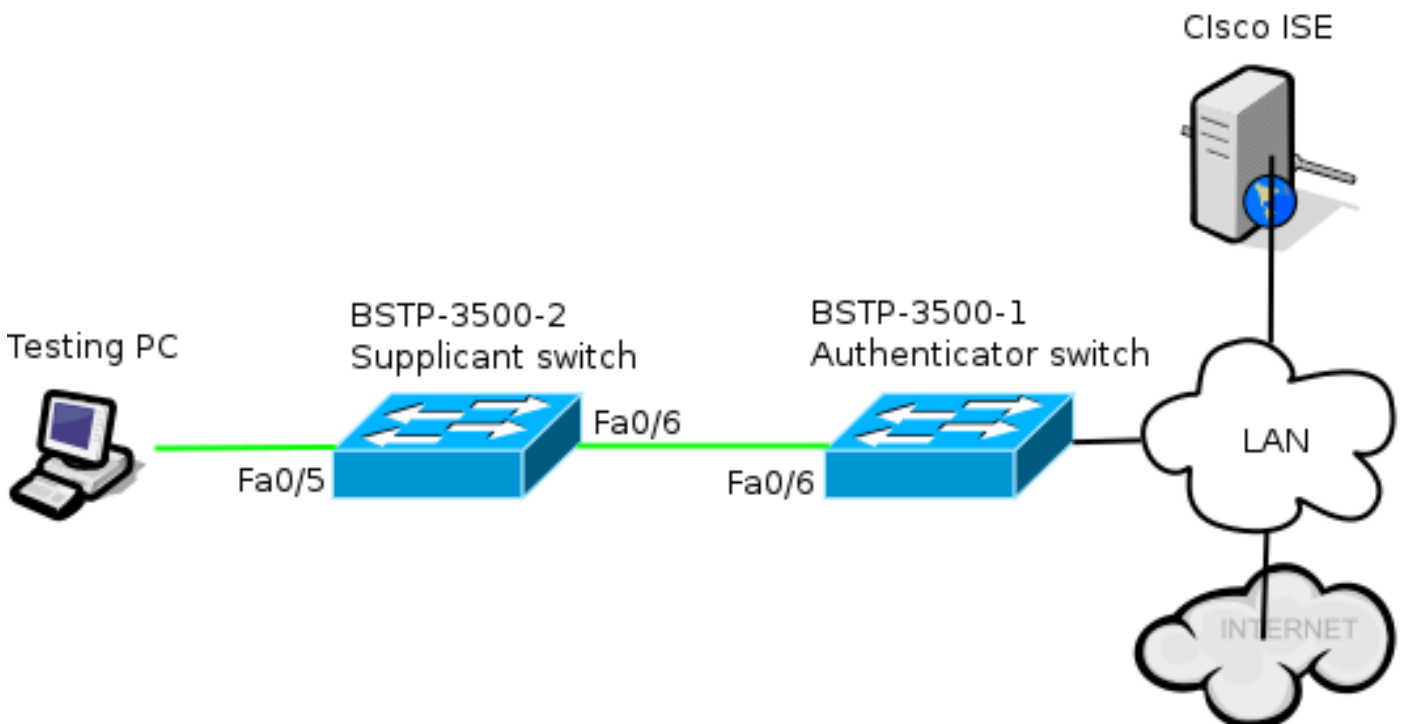
- 证明人交换机
- 请求方交换机
- Cisco ISE

配置是最小数量必要的为了perform此实验练习;他们也许是最佳的为或不满足其他需要。

Note:使用[命令查找工具](#) ([仅限注册用户](#)) 可获取有关本部分所使用命令的详细信息。

Network Diagram

此网络图说明用于此示例的连接。黑色线路指示逻辑或物理连接性和绿色线路指示通过使用验证的链路802.1x。



证明人交换机配置

证明人包含为dot1x需要的基本元素。在本例中，是特定的对整洁的命令或CISP粗体的。

这是基本认证、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被启用全局，并且互联的端口在证明人和接入模式被配置。

请求方交换机配置

准确请求方配置是关键为了整个设置能工作正如所料。此示例配置包含一种典型的AAA和dot1x配置

。

这是基本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
```

请求方应该配置了证件，并且应该供应将使用的可扩展的认证协议(EAP)方法。

请求方能通过安全协议使用消息摘要5 (MD5)和EAP灵活认证(快速) (在其他EAP类型中)认证在CISP的情况下。为了保持ISE配置到最低，此示例使用EAP-MD5请求方的认证对证明人。(默认值将强制使用EAP-FAST，要求受保护的访问证件[PAC]设置;本文不包括该方案。)

```
! 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
```

与证明人已经配置请求方的连接是中继端口(与在证明人的接入端口配置对比)。在此阶段，这预计;当ISE返回正确的属性，配置将动态地更改。

```
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的端口有一个最小配置和显示这里供仅参考。

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

ISE配置

此程序描述如何设置一种基本的ISE配置。

1. Enable (event)必要的验证协议。

在本例中，有线dot1x允许EAP-MD5验证请求方到证明人并且允许Protected Extensible Authentication Protocol (PEAP) -微软询问握手认证协议版本2 (MSCHAPv2)验证WINDOWS PC到请求方。

连接对策略>结果>认证>允许的协议，选择有线dot1x使用的协议服务列表，并且保证在此步骤的协议是启用的。

▼ 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 (Valid Range 0 to 3)

Allow EAP-GTC

- Allow Password Change Retries (Valid Range 0 to 3)

Allow EAP-TLS

Allow PEAPv0 only for legacy clients

2. 创建一个授权策略。连接对策略>结果>授权>授权策略，并且创建或者更新策略，因此包含整洁，一个返回的属性。这是这样策略示例：

Authorization Profile

* Name

Description

* Access Type ▼

Service Template

▼ Common Tasks

MACSec Policy

NEAT

当整洁的选项打开时，作为授权一部分，ISE返回device-traffic-class=switch。此选项是必要为了从访问更改Port模式证明人建立中继。

3. 创建一个授权规则使用此配置文件。连接对**策略>授权**，并且创建或者更新规则。

在本例中，称为Authenticator_switches的一个特殊设备组创建，并且所有恳求者发送从bsnswitch开始的用户名。

<input checked="" type="checkbox"/>	NEAT	if (Radius:User-Name MATCHES ^bsnswitch AND DEVICE:Device Type EQUALS All Device Types#Switches#Authenticator_switches)	then NEAT
-------------------------------------	------	--	-----------

4. 添加交换机到适当的组。连接到**Administration >网络资源>网络设备**，并且点击**添加**。

Network Devices List > **bstp-3500-1**

Network Devices

* Name

Description

* IP Address: /

Model Name

Software Version

* Network Device Group

Location

Device Type

在本例中，BSTP-3500-1 (证明人)是Authenticator_switches组的一部分;BSTP-3500-2 (请求方)不需要是此组的一部分。

Verify

Use this section to confirm that your configuration works properly.此部分描述两个工作情况：

- 在交换机之间的认证
 - 在WINDOWS PC和请求方之间的认证
- 它也解释三个另外的情况：

- 一个验证的客户端的删除从网络
- 请求方的删除
- 没有dot1x的端口在请求方

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](#)。

请求方对证明人交换机的交换机认证

在本例中，请求方验证对证明人。步骤在进程中是：

1. 请求方被配置并且插入端口fastethernet0/6。dot1x交换造成请求方使用EAP为了发送一个预先配置的用户名和密码到证明人。
2. 证明人进行RADIUS交换并且为ISE验证提供证件。
3. 如果证件是正确的，ISE返回整洁需要的属性(device-traffic-class=switch)，并且证明人从访问更改其交换端口模式建立中继。

此示例显示CISP信息交换在交换机之间的：

```
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: 010011020009001B0D5521C103000050 ...
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

```

一旦认证和授权成功，CISP交换发生。每交换有REQUEST，请求方发送和一种回应，担当一回复和确认从证明人。

两明显的交换进行：注册和ADD_CLIENT。在注册交换期间，请求方通知证明人是CISP能够的，并且证明人然后承认此消息。ADD_CLIENT交换用于通知关于设备的证明人被连接到恳求者的本地端口。如同注册，ADD-CLIENT在请求方被起动的并且由证明人承认。

输入这些显示命令为了验证通信、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)
```

在本例中，证明人的角色正确地分配到正确的接口(fa0/6)，并且两MAC地址注册。MAC地址是在端口fa0/6的请求方在VLAN1和在VLAN200。

dot1x认证会话的验证可能当前进行。在上行交换机的fa0/6端口已经验证。这是被触发的dot1x交换，当BSTP-3500-2 (请求方)时插入在：

```
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)
```

正如所料在此阶段，没有在请求方的会话：

```
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)
```

对请求方交换机的WINDOWS PC认证

在本例中，WINDOWS PC验证对请求方。步骤在进程中是：

1. WINDOWS PC插入在BSTP-3500-2 (请求方)的FastEthernet0/5端口。
2. 请求方进行认证和授权与ISE。
3. 请求方通知证明人一个新的客户端在端口被联络。

这是从请求方的通信：

```
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
```

ADD_CLIENT交换发生，但是注册交换不是需要的。

为了验证在请求方的工作情况，请输入显示cisp注册命令：

```
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**

请求方有一请求方的角色往证明人(fa0/6接口)的和一个人证明人的角色往WINDOWS PC (fa0/5接口)的。

为了验证在证明人的工作情况，请输入显示cisp客户端命令：

```
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地址出现在证明人在VLAN 200下。它是在请求方的AAA请求被观察的MAC地址。

认证会话应该表明同一个设备在请求方fa0/5端口被连接：

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

```
Interface MAC Address Method Domain Status Session ID
```

```
Fa0/5 c464.13b4.29c3 dot1x DATA Authz Success 0A3039E20000001501018B58
```

验证的客户端删除从网络

当去除客户端(例如，如果端口被关闭)，证明人通过DELETE_CLIENT交换被通知。

```
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
```

请求方交换机删除

当拔掉请求方或被去除时，证明人引入原始配置回到端口为了避免安全性问题。

```
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，请求方去除表示从CISP表的请求方的客户端并且撤销在该接口的CISP。

没有dot1x的端口在请求方交换机

从请求方被传播到证明人的CISP信息仅担当实施另一个层。请求方通知关于被连接到它的所有的证明人允许的MAC地址。

典型地被误会的方案是这：如果没有被启用的dot1x的设备在端口插入，MAC地址是获知和传播对上行交换机通过CISP。

证明人允许来自通过CISP了解的所有客户端的通信。

实质上，它是限制设备访问，通过dot1x或其他方法和传播MAC地址和VLAN信息的请求方的角色对证明人。证明人作为在那些更新提供的信息的实施者。

为例，新的VLAN (VLAN300)在两交换机和设备被创建了插入在请求方的端口fa0/4。端口fa0/4是没有为dot1x被配置的一个简单的接入端口。

请求方的此输出显示一个新的注册的端口：

```
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
```

在证明人，新的MAC地址是可视的在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

本部分提供的信息可用于对配置进行故障排除。

Note:

[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help命令您排除整洁和CISP故障;本文包括大多数的示例：

- **全调试的cisp**显示CISP信息交换在交换机之间的。
- **显示cisp汇总**-显示CISP接口状态的汇总在交换机的。
- **显示cisp注册**-指示参加CISP交换，那些接口的角色的接口，并且接口是否是一部分的整洁。
- **显示cisp客户端**-显示已知客户端MAC地址和他们的位置表(VLAN和接口)。这主要从证明人是有用的。