思科身份服務引擎的NEAT配置示例

目錄

簡介

本檔案介紹網路邊緣驗證拓撲(NEAT)在簡單情況下的設定和行為。NEAT利用使用者端資訊訊號通訊協定(CISP)來在請求方和驗證方交換器之間傳播使用者端MAC位址和VLAN資訊。

在此配置示例中，身份驗證器交換機（也稱為身份驗證器）和請求者交換機（也稱為請求者）都執行802.1x身份驗證；身份驗證器對請求者進行身份驗證，後者進而對測試PC進行身份驗證。

必要條件

需求

思科建議您瞭解IEEE 802.1x身份驗證標準。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 兩台採用Cisco IOS®軟體版本12.2(55)SE8的Cisco Catalyst 3560系列交換器；一台交換器擔任驗證器，另一台擔任請求者。
- 思科身分識別服務引擎(ISE)版本1.2。
- 裝有Microsoft Windows XP Service Pack 3的PC。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

設定

本示例介紹的示例配置：

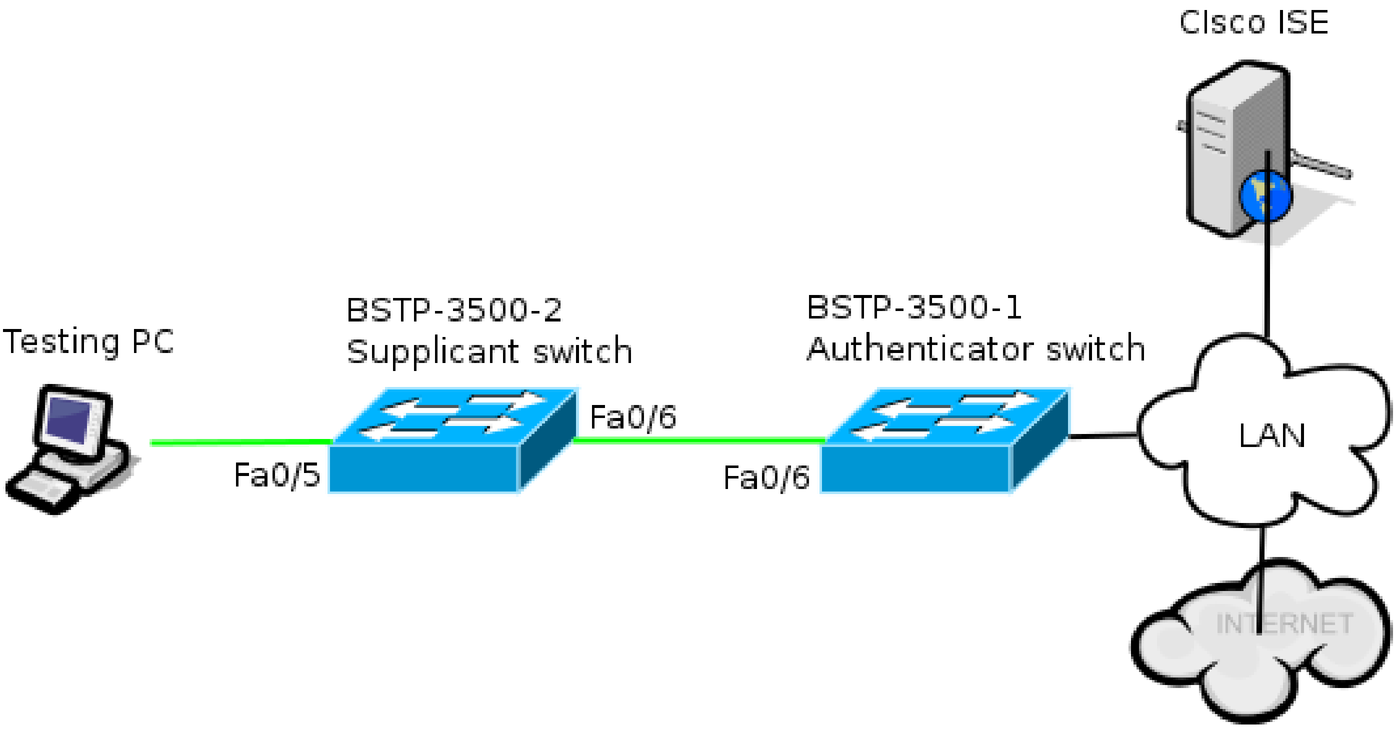
- 身份驗證器交換機
- Supplicant客戶端交換機
- 思科ISE

這些配置是執行本實驗練習所需的最低配置；可能並不適用於其他需求或滿足其他需求。

> **註**：使用命令查詢工具(僅限註冊客戶)可獲取本節中使用的命令的詳細資訊。

網路圖表

此網路圖說明此範例中使用的連線。黑色線表示邏輯或物理連線，綠色線表示使用802.1x進行身份驗證的鏈路。



驗證器交換機配置

驗證器包含dot1x所需的基本元素。在本示例中，特定於NEAT或CISP的命令是粗體的。

以下是基本驗證、授權及記帳(AAA)設定：

```
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是全域性啟用的，互連連線埠是在驗證器和存取模式下設定的。

Supplicant客戶端交換機配置

準確的Supplicant客戶端配置對於整個設定正常運行至關重要。此示例配置包含典型的AAA和dot1x配置。

以下是基本AAA組態：

```
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
```

請求方應配置憑證，並且應提供要使用的可擴展身份驗證協定(EAP)方法。

在CISP的情況下，請求方可以使用EAP-Message Digest 5(MD5)和EAP-Flexible Authentication via Secure Protocol(FAST)（以及其他EAP型別）進行身份驗證。為了將ISE配置保持在最低水準，此示例使用EAP-MD5對身份驗證器的請求方進行身份驗證。（預設設定將強制使用EAP-FAST，它需要提供保護訪問憑證[PAC]；本文檔不涵蓋此場景。）

```
! 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
```

請求方與身份驗證器的連線已配置為中繼埠（與身份驗證器上的訪問埠配置相反）。在這個階段，這是預期的；當ISE返回正確的屬性時，配置將動態更改。

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

連線到Windows PC的埠具有最小配置，此處僅作參考。

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

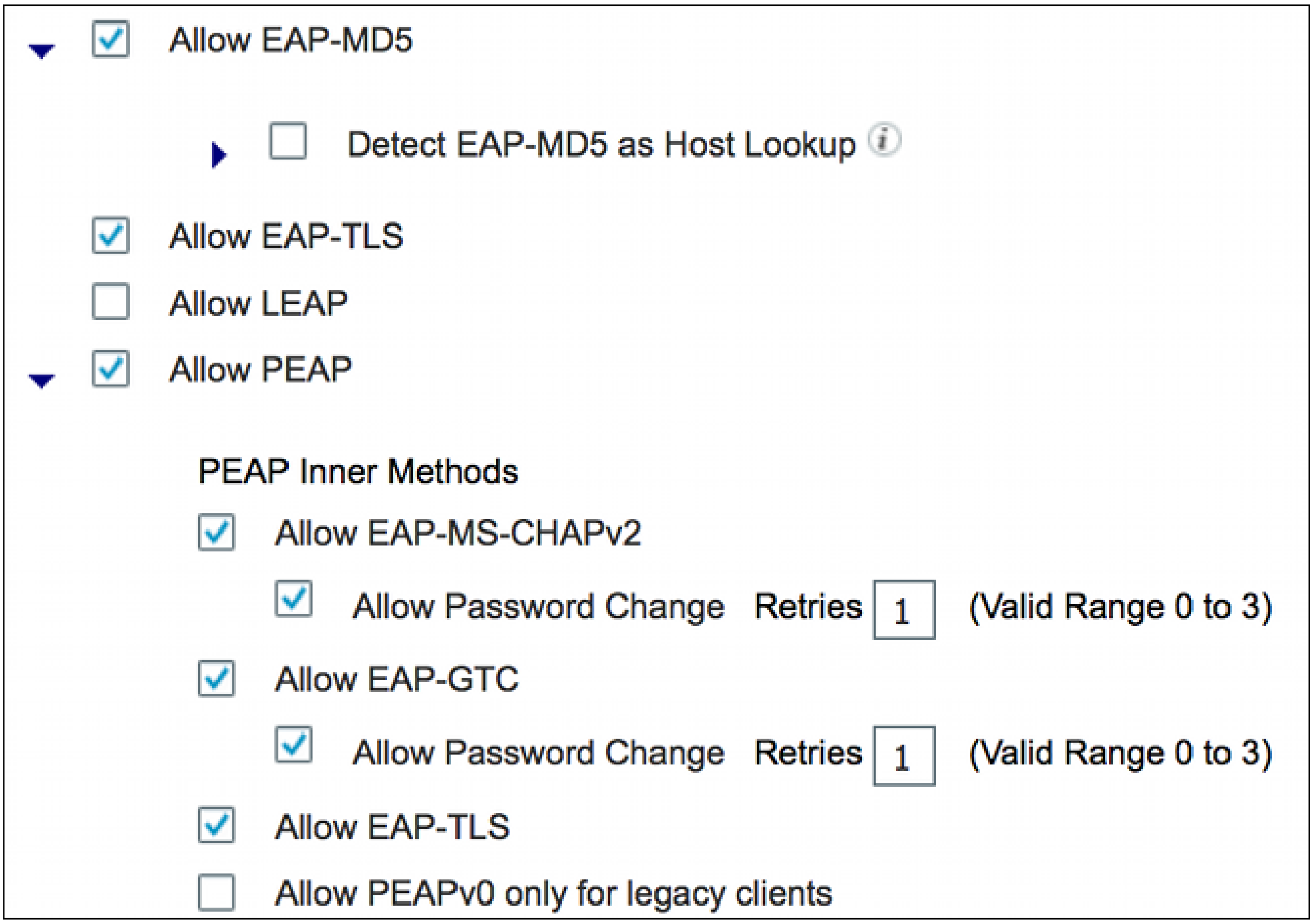
ISE 組態

此過程介紹如何設定基本ISE配置。

1. 啟用所需的身份驗證協定。

   在本示例中，有線dot1x允許EAP-MD5對驗證方的請求方進行身份驗證，並允許受保護的可擴展身份驗證協定(PEAP)- Microsoft質詢握手身份驗證協定版本2(MSCHAPv2)對請求方的Windows PC進行身份驗證。

   導覽至**Policy > Results > Authentication > Allowed protocols**，選擇**protocol service list**供有線dot1x使用，並確保啟用此步驟中的協定。



☑ 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)

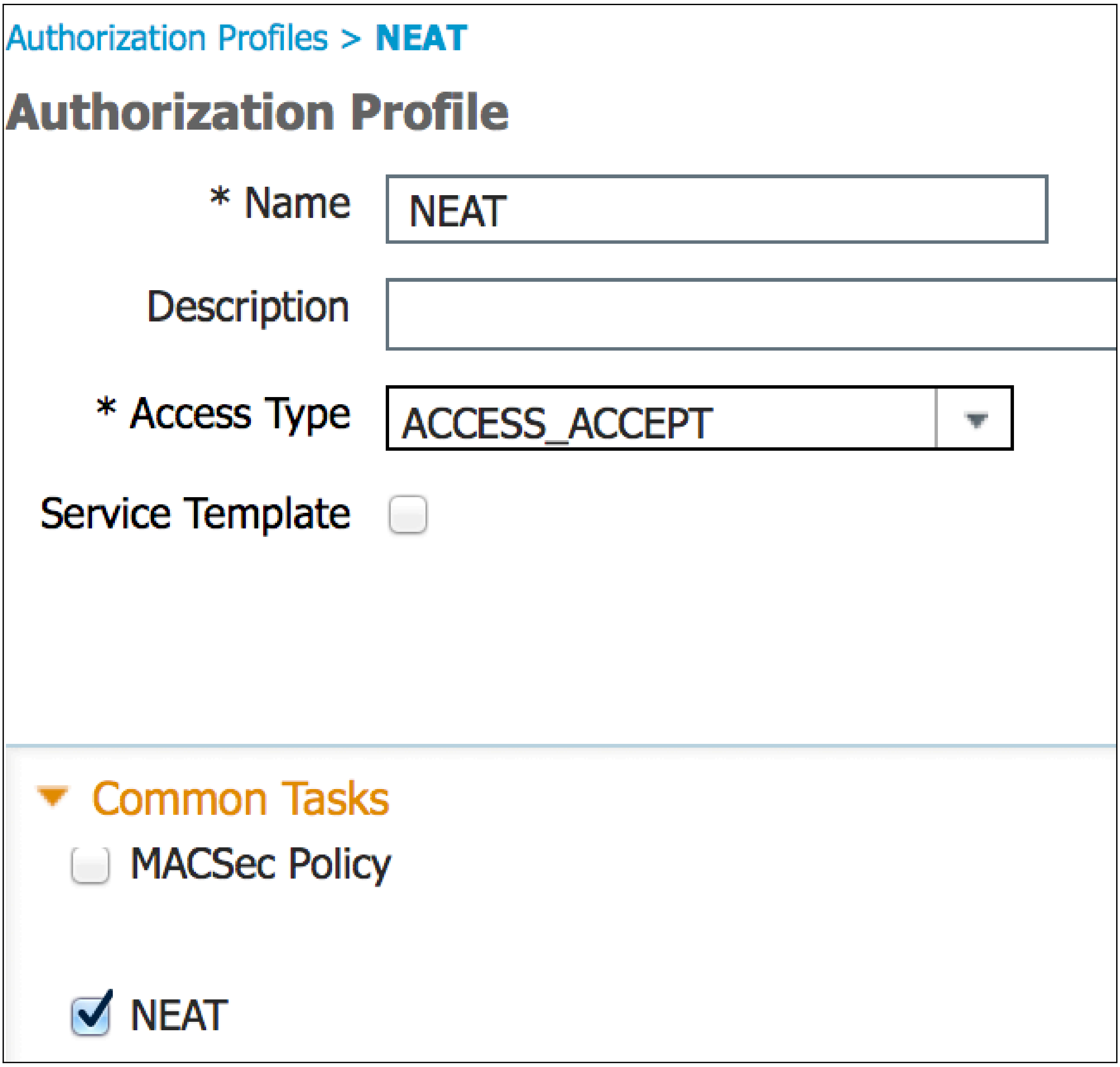
☑ Allow EAP-GTC

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

☑ Allow EAP-TLS

□ Allow PEAPv0 only for legacy clients

2. 建立授權策略。導航到**Policy > Results > Authorization > Authorization Policy**，然後建立或更新策略，使其包含NEAT作為返回屬性。以下是此類策略的一個示例：



Authorization Profiles > NEAT

Authorization Profile

* Name: NEAT

Description:

* Access Type: ACCESS_ACCEPT

Service Template □

Common Tasks

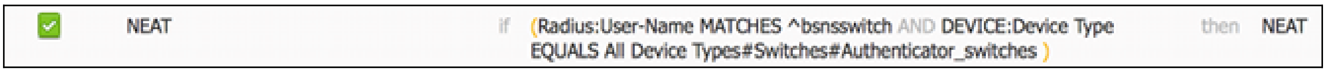
□ MACSec Policy

☑ NEAT

當NEAT選項開啟時，ISE將返回device-traffic-class=switch作為授權的一部分。若要將驗證器的連線埠模式從存取變更為TRUNK，必須選擇此選項。

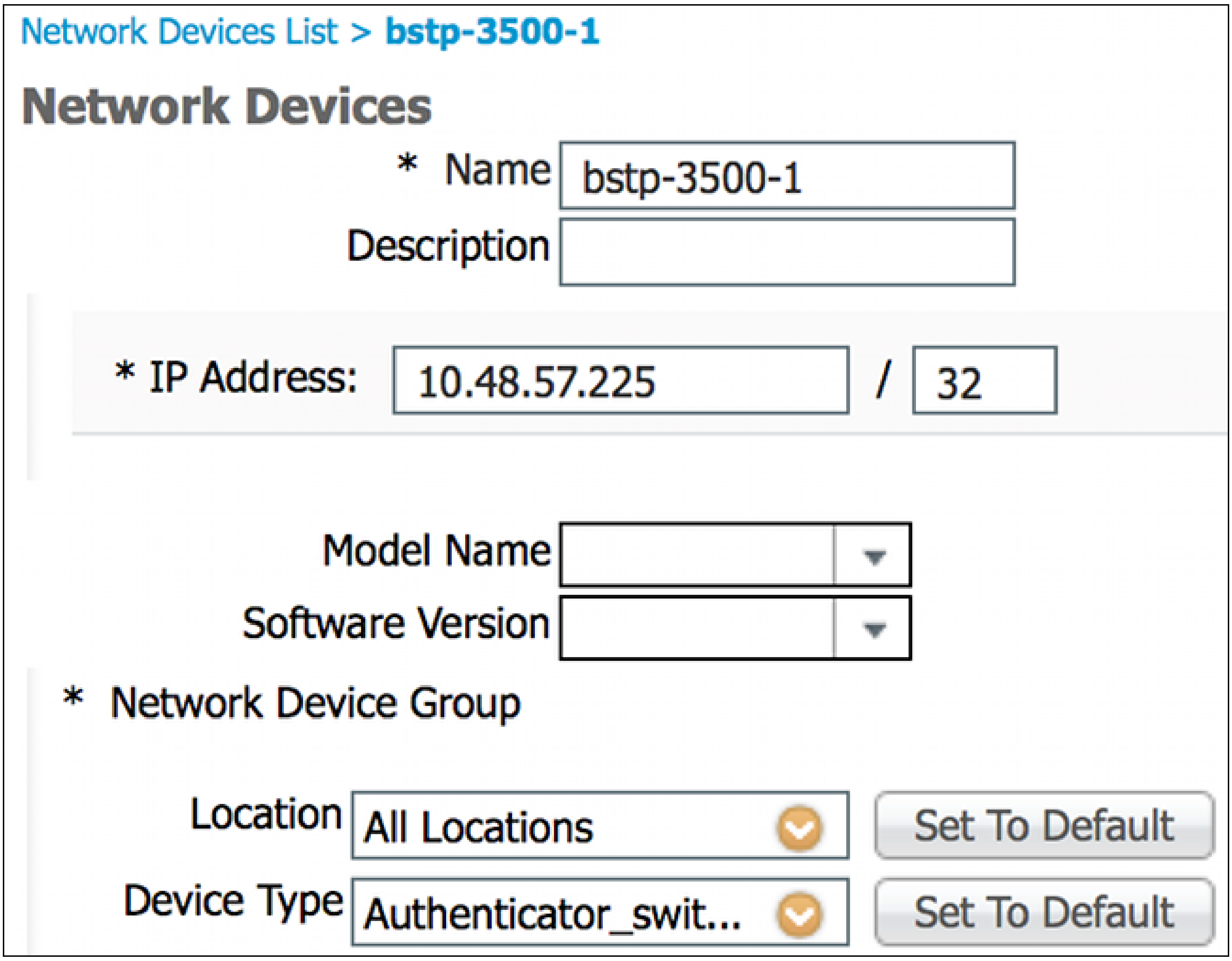
3. 建立授權規則以使用此配置檔案。導航到**Policy > Authorization**，然後建立或更新規則。

   在此示例中，建立了一個名為Authenticator_switches的特殊裝置組，所有請求方都傳送一個以bsnsswitch開頭的使用者名稱。



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

4. 將交換機新增到相應的組中。導覽至**Administration > Network Resources > Network Devices**，然後按一下**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

在本例中，BSTP-3500-1（身份驗證器）是Authenticator_switches組的一部分；BSTP-3500-2（請求者）無需是此組的一部分。

驗證

使用本節內容，確認您的組態是否正常運作。本節介紹兩種行為：

- 交換機之間的身份驗證
- Windows PC與請求方之間的身份驗證

它還說明了三種其他情況：

- 從網路中移除經過身份驗證的客戶端
- 請求方的移除
- 請求方上沒有dot1x的埠

附註：

輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用Output Interpreter工具檢視**show**指令輸出的分析。

使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

Supplicant客戶端交換機身份驗證到身份驗證器交換機

在此示例中，請求方向驗證方進行身份驗證。此過程中的步驟如下：

1. 請求方已配置並插入埠fastethernet0/6。dot1x交換使請求方使用EAP以將預配置的使用者名稱和密碼傳送到驗證器。
2. 身份驗證器執行RADIUS交換並提供用於ISE驗證的憑證。
3. 如果憑證正確，則ISE返回NEAT(device-traffic-class=switch)所需的屬性，並且身份驗證器將其switchport模式從訪問更改為中繼。

此範例顯示交換器之間的CISP資訊交換：

```
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
```

身份驗證和授權成功後，就會進行CISP交換。每個交換都有一個REQUEST（由請求方傳送）和一個RESPONSE（作為來自身份驗證器的回覆和確認）。

執行兩個不同的交換：REGISTRATION和ADD_CLIENT。在註冊交換期間，請求方通知身份驗證器它支援CISP，然後身份驗證器確認此消息。ADD_CLIENT交換用於向身份驗證器通知與請求者的本地埠連線的裝置。與REGISTRATION一樣，ADD-CLIENT在請求方上啟動，並由身份驗證器確認。

輸入以下show命令以驗證通訊、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，身份驗證器的角色已正確分配到正確的介面(fa0/6)，並且註冊了兩個MAC地址。MAC地址是VLAN1上埠fa0/6和VLAN200上的請求方。

現在可以執行dot1x身份驗證會話的驗證。上游交換機上的fa0/6埠已經過身份驗證。這是BSTP-3500-2（請求方）插入時觸發的dot1x交換：

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

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

如本階段所預期的那樣，請求方上沒有會話：

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

對請求方交換機進行Windows PC身份驗證

在此示例中，Windows PC會向請求方進行身份驗證。此過程中的步驟如下：

1. Windows PC插入BSTP-3500-2（請求方）上的FastEthernet 0/5埠。
2. 請求方通過ISE執行身份驗證和授權。
3. 請求方通知身份驗證器埠上連線了新客戶端。

這是來自請求方的通訊：

```
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
```

發生ADD_CLIENT交換，但不需要REGISTRATION交換。

若要驗證請求方上的行為，請輸入**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)
```

請求方對身份驗證器（fa0/6介面）具有請求方角色，對Windows PC具有身份驗證方角色（fa0/5介面）。

若要驗證驗證驗證器上的行為，請輸入**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地址出現在身份驗證器的VLAN 200下。是在請求方的AAA請求中觀察到的MAC地址。

驗證作業階段應表示同一裝置已連線到請求方的fa0/5連線埠：

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

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

從網路中刪除經過身份驗證的客戶端

刪除客戶端時（例如，如果埠關閉），將通過DELETE_CLIENT交換通知身份驗證器。

```
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
```

刪除Supplicant客戶端交換機

拔下或移除請求方時，驗證器會將原始組態重新引入連線埠，以避免產生安全顧慮。

```
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
```

同時，請求方從CISP表中刪除代表請求方的客戶端，並停用該介面上的CISP。

Supplicant客戶端交換機上沒有dot1x的埠

從請求方傳播到驗證方的CISP資訊僅用作另一個實施層。請求方將連線到身份驗證方的所有允許的MAC地址告知身份驗證方。

通常誤解的情況如下：如果裝置插入了未啟用dot1x的連線埠，則會獲知MAC位址，並通過CISP傳播到上游交換器。

身份驗證器允許來自通過CISP學習的所有客戶端的通訊。

實質上，請求方的作用是通過dot1x或其他方法限制裝置的訪問，並將MAC地址和VLAN資訊傳播給身份驗證器。驗證器充當這些更新中所提供資訊的執行器。

例如，兩台交換器上建立新的VLAN(VLAN300)，並將一個裝置插入要求者的連線埠fa0/4。埠fa0/4是未為dot1x配置的簡單接入埠。

請求方的以下輸出顯示一個新的註冊埠：

```
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)
```

在驗證器上，新的MAC地址在VLAN 300上可見。

```
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
```

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

> **附註**：
>
> 輸出直譯器工具(僅供已註冊客戶使用)支援某些**show**命令。使用Output Interpreter工具檢視**show**指令輸出的分析。
>
> 使用 **debug 指令之前，請先參閱**有關 Debug 指令的重要資訊。

這些命令可幫助您對NEAT和CISP進行故障排除；本文檔包含大多數命令的示例：

- **debug cisp all** — 顯示交換器之間的CISP資訊交換。
- **show cisp summary** — 顯示交換器上CISP介面狀態的摘要。
- **show cisp registrations** — 指示參與CISP交換的介面、這些介面的角色以及介面是否屬於NEAT。
- **show cisp clients** — 顯示已知客戶端MAC地址及其位置（VLAN和介面）的表。這主要對身份驗證器有用。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。