مثال تكوين أنيق باستخدام محرك خدمات الهوية من Cisco

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
التكوين
الرسم التخطيطي للشبكة
تكوين محول مصادق
تكوين المحول للمطالب
تكوين ISE
التحقق من الصحة
مصادقة المحول إلى محول مصادق
مصادقة كمبيوتر Windows لمحول العميل
إزالة العميل المصادق عليه من الشبكة
إزالة المحول المكمل
المنافذ بدون dot1x على المحول المحول
استكشاف الأخطاء وإصلاحها

المقدمة

يصف هذا المستند تكوين مخطط مصادقة حافة الشبكة (NEAT) وسلوكه في سيناريو بسيط. يستخدم NEAT بروتوكول إرسال إشارات معلومات العميل (CISP) من أجل نشر عناوين MAC الخاصة بالعميل ومعلومات شبكة VLAN بين محولات العميل والمصادقة.

في مثال التكوين هذا، يقوم كل من المحول المصدق (المعروف أيضا باسم المصدق) والمحول الملحق (المعروف أيضا باسم المتلقي) بإجراء مصادقة 802.1x، ويقوم المصدق بمصادقة المتلقي، والذي يقوم بدوره بمصادقة جهاز الكمبيوتر للاختبار.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من ال IEEE 802.1x صحة هوية معيار.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- محولا Cisco Catalyst 3560 Series مع برنامج Cisco IOS®، الإصدار 12.2(55)SE8؛ يعمل أحد المحولات كمصدق، ويعمل الآخر كمسبب.
- Cisco Identity Services Engine (ISE)، الإصدار 1.2.
- كمبيوتر مزود بنظام التشغيل Microsoft Windows XP و Service Pack 3.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

التكوين

يغطي هذا المثال نموذجا لتكوينات:

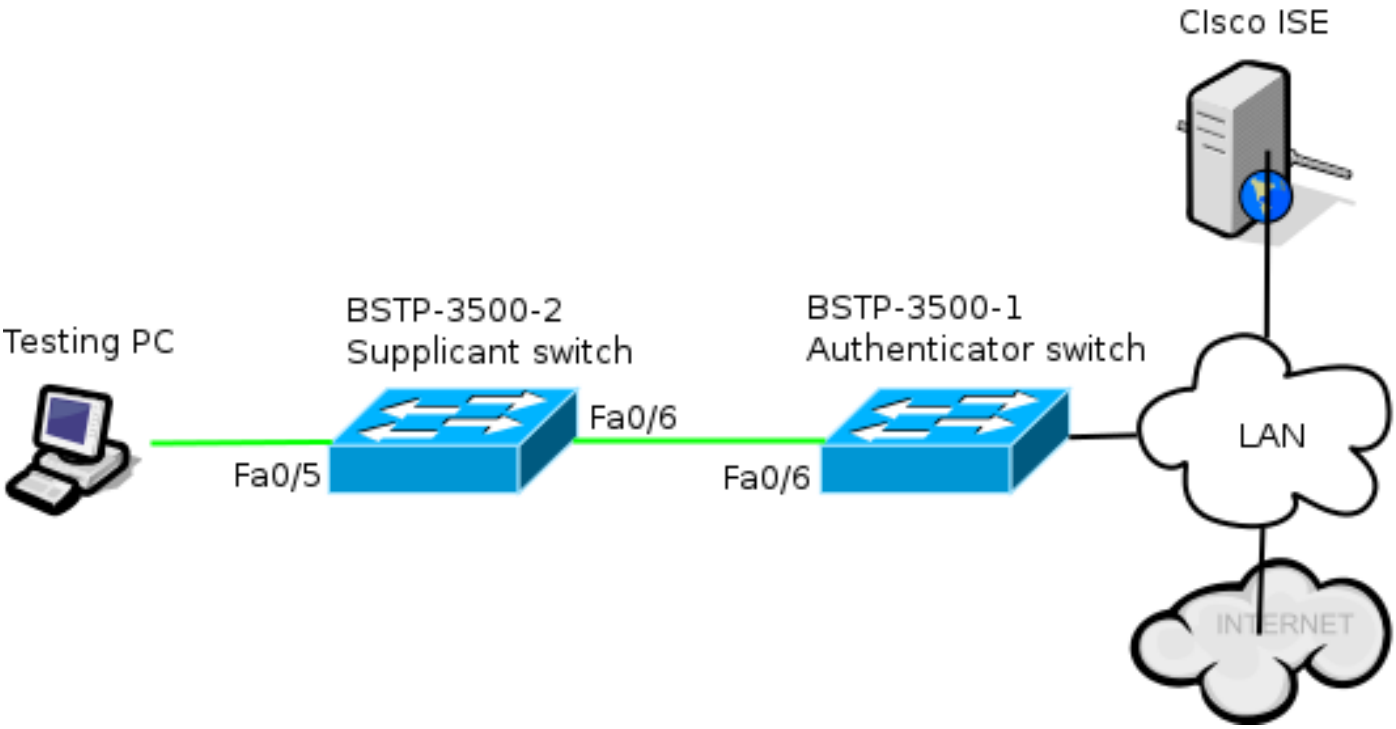
- مبدل مصادق
- مبدل التواضع
- Cisco ISE

التكوينات هي الحد الأدنى المطلوب لإجراء هذا التمرين المعملي، وقد لا تكون مثالية لتلبية الاحتياجات الأخرى أو قد تلبيها.

ملاحظة: أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

الرسم التخطيطي للشبكة

يوضح هذا الرسم التخطيطي للشبكة الاتصال المستخدم في هذا المثال. تشير الخطوط السوداء إلى الاتصال المنطقي أو المادي، بينما تشير الخطوط الخضراء إلى الروابط المصادق عليها من خلال إستخدام 802.1x.



تكوين محول مصادق

يحتوي المصدق على العناصر الأساسية اللازمة ل dot1x. في هذا المثال، يتم زيادة كثافة الأوامر الخاصة ب NEAT أو CISP.

هذا هو تكوين المصادقة والتفويض والمحاسبة (AAA) الأساسي:

```
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
```

يتم تمكين CISP بشكل عام، ويتم تكوين منفذ الاتصال البيني في وضع المصادقة والوصول.

تكوين المحول للمطالب

يعد التكوين الدقيق للمطالب أمرا بالغ الأهمية لكي يعمل الإعداد بالكامل كما هو متوقع. يحتوي مثال التكوين هذا على تكوين AAA و dot1x نموذجي.

هذا هو تكوين AAA الأساسي:

```
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
```

يجب أن يكون الطالب قد قام بتكوين بيانات الاعتماد ويجب أن يوفر أسلوب بروتوكول المصادقة المتوسع (EAP) لاستخدامه.

يمكن للمطالب إستخدام مصادقة EAP-Message Digest 5 (MD5) والمصادقة المرنة ل EAP عبر البروتوكول الآمن (FAST) (من بين أنواع EAP الأخرى) للمصادقة في حالة CISP. للحفاظ على تكوين ISE إلى الحد الأدنى، يستخدم هذا المثال EAP-MD5 لمصادقة المسبب على المصدق. (يفرض الإعداد الافتراضي إستخدام EAP-FAST، الذي يتطلب توفير بيانات اعتماد الوصول المحمي [PAC]، ولا يغطي هذا المستند هذا السيناريو.)

```
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
```

تم تكوين اتصال الطالب بالمصادقة بالفعل ليكون منفذ خط اتصال (على النقيض من تكوين منفذ الوصول على المصدق). في هذه المرحلة، من المتوقع حدوث ذلك، وسوف يتغير التكوين بشكل ديناميكي عند إرجاع ISE للسمة الصحيحة.

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

يحتوي المنفذ الذي يتصل بالكمبيوتر الشخصي ل Windows على تكوين أقل، ويتم عرضه هنا للمرجع فقط.

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

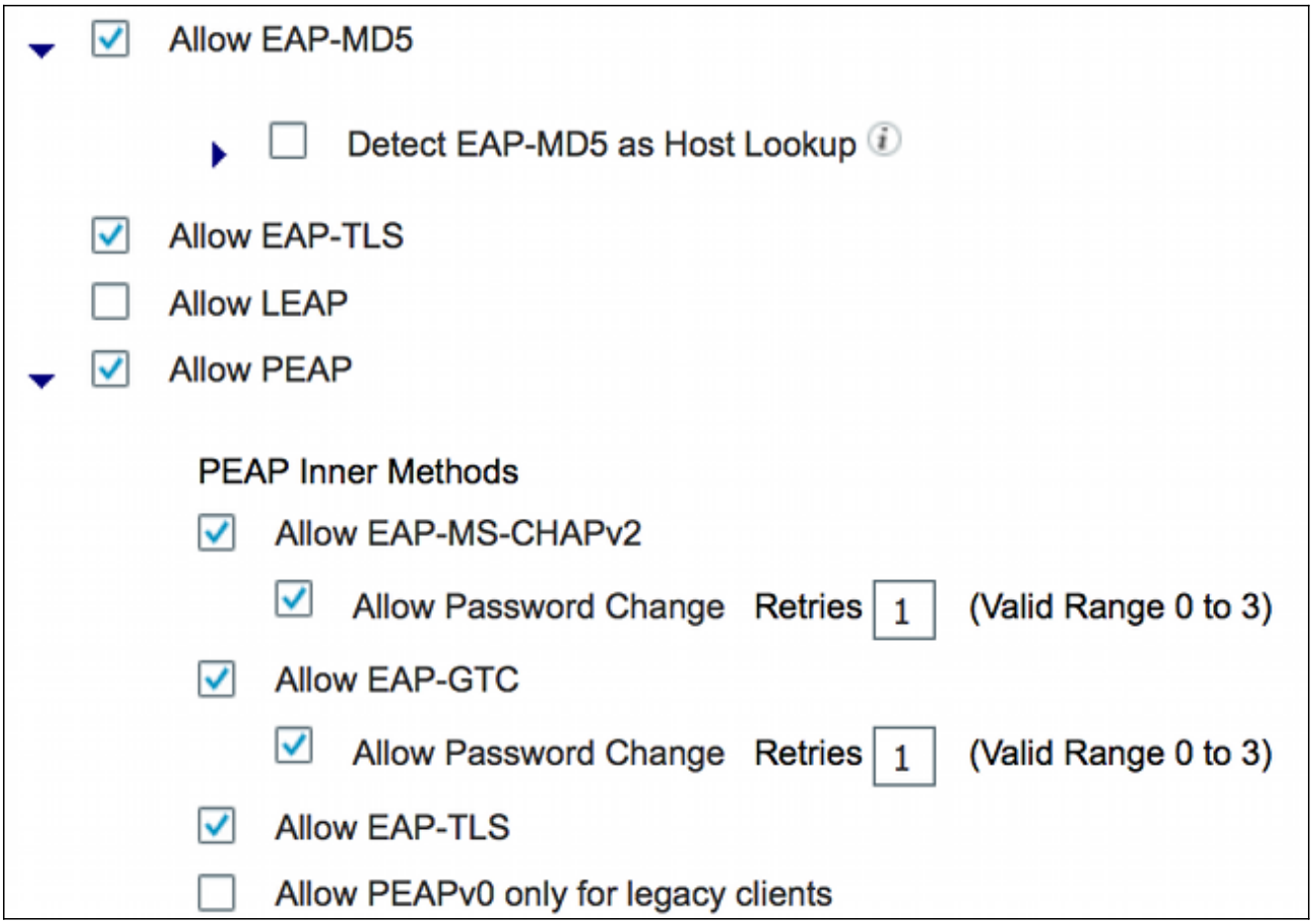
تكوين ISE

يوضح هذا الإجراء كيفية إعداد تكوين ISE أساسي.

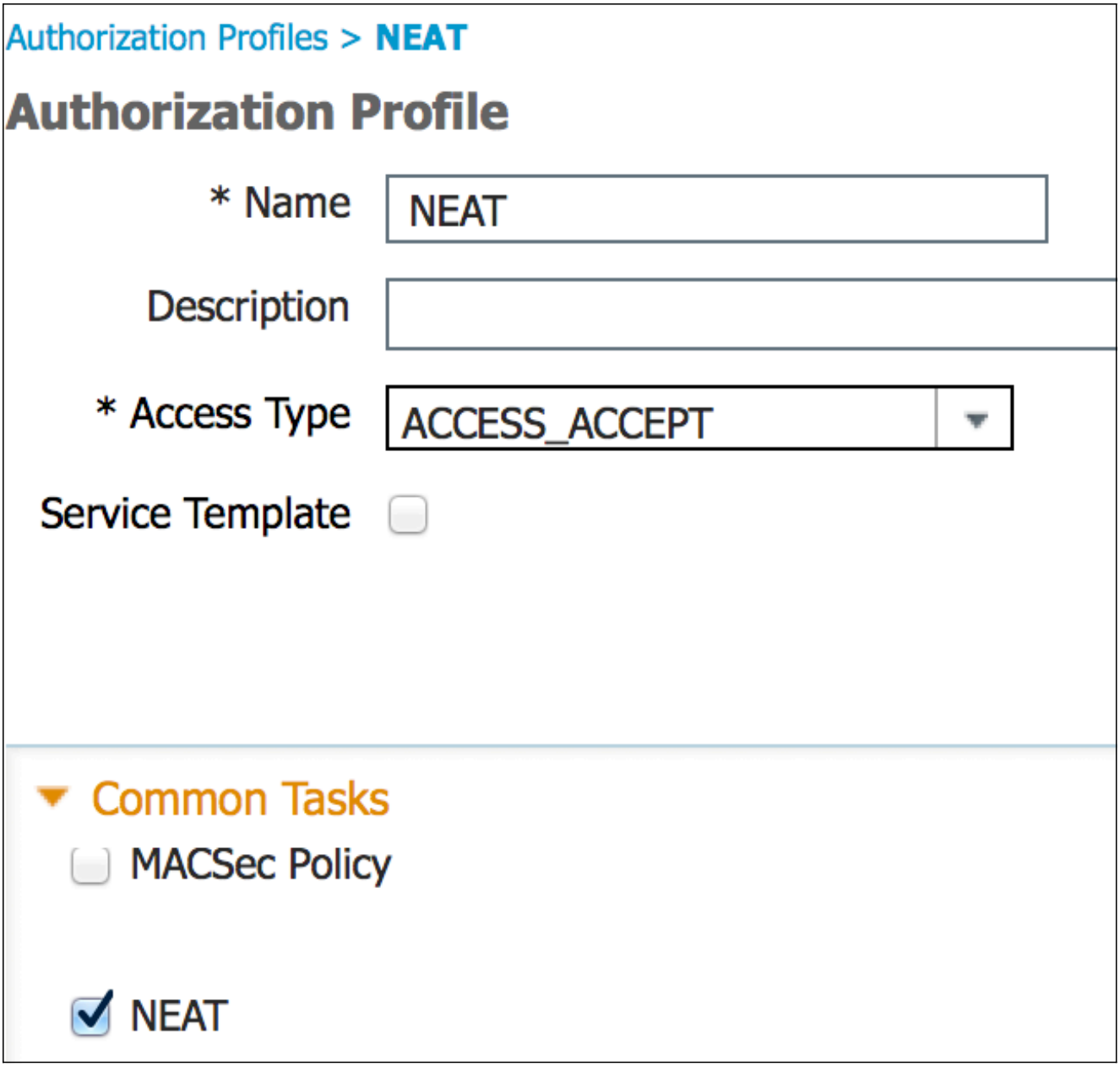
1. تمكين بروتوكولات المصادقة المطلوبة.

في هذا المثال، تسمح النقطة السلكية1x ل EAP-MD5 بمصادقة المتلقي إلى المصدق وتسمح لبروتوكول المصادقة المتوسع المحمي (PEAP)-بروتوكول المصادقة لتأكيد الاتصال بقيمة التحدي ل Microsoft الإصدار 2 (MSCHAPv2) لمصادقة جهاز كمبيوتر Windows إلى المتلقي.

انتقل إلى **السياسة > النتائج > المصادقة > البروتوكولات المسموح بها**، وحدد **قائمة خدمات البروتوكول** المستخدمة من قبل Wired dot1x، وتأكد من تمكين البروتوكولات الموجودة في هذه الخطوة.



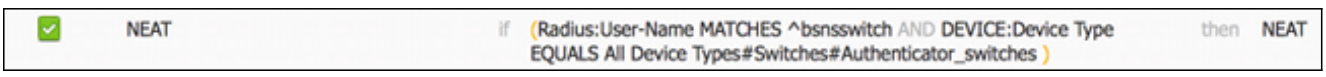
2. إنشاء سياسة تخويل. انتقل إلى **السياسة > النتائج > التخويل > نهج التخويل**، وقم بإنشاء سياسة أو تحديثها بحيث تحتوي على NEAT كسمة مرتجعة. وهذا مثال على مثل هذه السياسة:



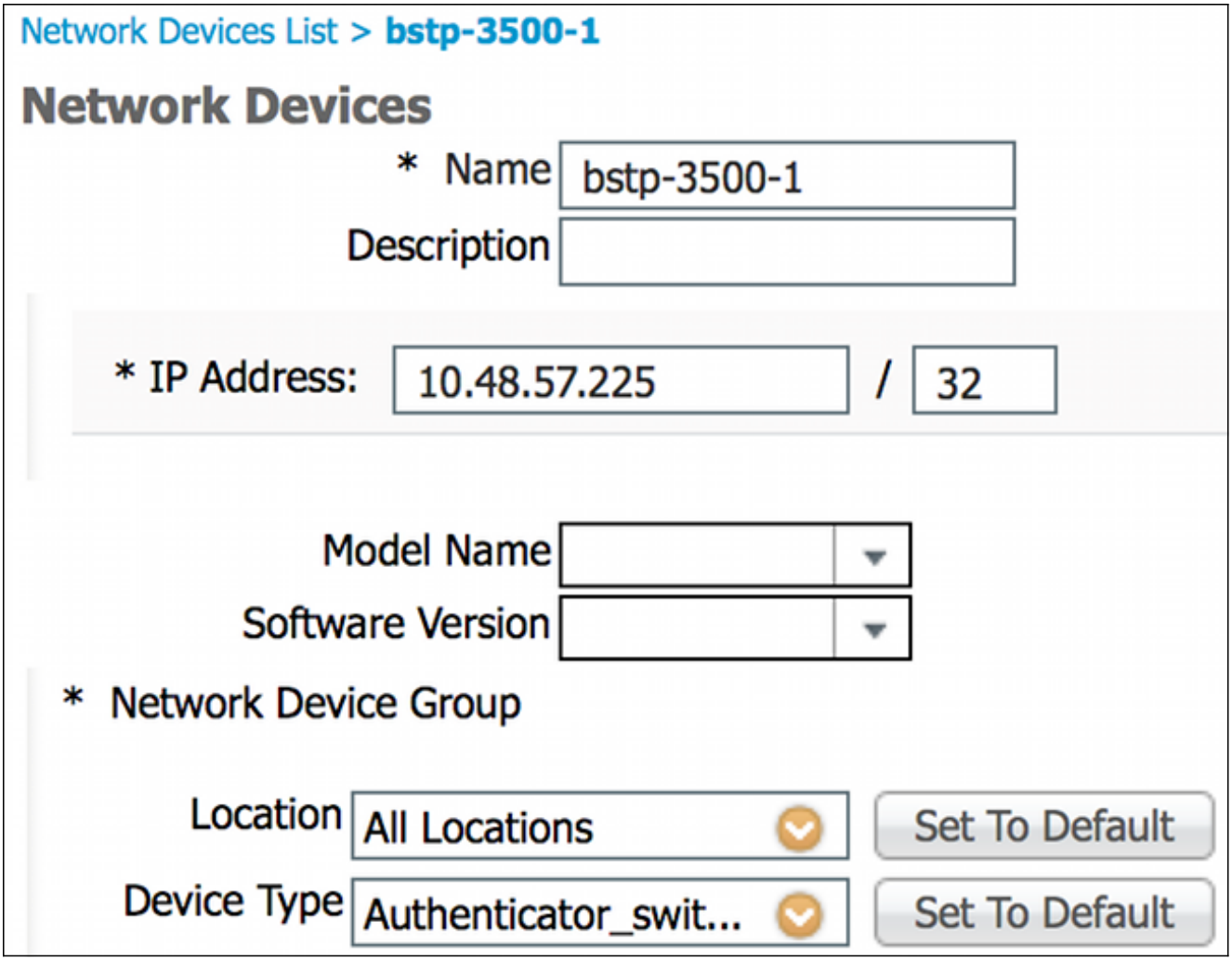
عند تشغيل خيار NEAT، ترجع ISE المحول device-traffic-class=switch كجزء من التفويض. هذا خيار ضروري in order to غيرت الميناء أسلوب من المصدق من منفذ إلى شنطة.

3. إنشاء قاعدة تخويل لاستخدام ملف التعريف هذا. انتقل إلى **نهج > تفويض**، وقم بإنشاء قاعدة أو تحديثها.

في هذا المثال، يتم إنشاء مجموعة أجهزة خاصة تسمى Authenticator_switches، ويرسل جميع المكلفين اسم مستخدم يبدأ ب bsnsswitch.



4. قم بإضافة المحولات إلى المجموعة المناسبة. انتقل إلى **إدارة > موارد الشبكة > أجهزة الشبكة**، وانقر **إضافة**.



في هذا المثال، يعد BSTP-3500-1 (المصدق) جزءا من مجموعة Authenticator_switches، ولا يلزم أن يكون BSTP-3500-2 (المتلقي) جزءا من هذه المجموعة.

التحقق من الصحة

استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح. يصف هذا القسم سلوكين:

- المصادقة بين المحولات
- المصادقة بين كمبيوتر Windows والمطالب

ويشرح أيضا ثلاث حالات اضافية:

- إزالة عميل مصدق عليه من الشبكة
- إزالة ملتمس
- المنافذ بدون dot1x على ملتمس

ملاحظات:

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر **debug**.

مصادقة المحول إلى محول مصادق

في هذا مثال، يصادق الطالب إلى المصدق. الخطوات في العملية هي:

1. يتم تكوين الطالب وتوصيله بمنفذ FastEthernet0/6. يسبب ال dot1x exchange الطالب أن يستعمل EAP in order to أرسلت تشكيل مسبق username وكلمة إلى المصدق.
2. يقوم المصدق بإجراء تبادل RADIUS ويوفر بيانات اعتماد للتحقق من ISE.
3. إذا كانت بيانات الاعتماد صحيحة، فإن ISE ترجع السمات المطلوبة بواسطة NEAT (device-traffic-class=switch)، ويقوم المصدق بتغيير وضع switchport الخاص به من الوصول إلى خط الاتصال.

يوضح هذا المثال تبادل معلومات CISP بين المحولات:

```
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
```

بمجرد نجاح المصادقة والتفويض، يحدث تبادل CISP. تحتوي كل عملية تبادل على طلب، يتم إرساله من قبل المتلقي، مع إستجابة تستخدم كرد وإقرار من المصدق.

يتم إجراء عمليتي تبادل متميزتين: التسجيل و add_client. أثناء تبادل التسجيل، يقوم مقدم الطلب بإعلام المصدق بأنه متوافق مع CISP، ويقوم المصدق بعد ذلك بإقرار هذه الرسالة. يتم إستخدام تبادل ADD_CLIENT لإعلام المصدق عن الأجهزة المتصلة بالمنفذ المحلي للمزود. وكما هو الحال بالنسبة للتسجيل، يتم بدء تشغيل العميل الإضافي على مقدم الطلب ويتم إقراره من قبل المصدق.

دخلت هذا عرض أمر in order to دققت الاتصال، أدوار، وعناوين:

```
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
```

في هذا المثال، يتم تعيين دور المصدق بشكل صحيح إلى الواجهة الصحيحة (Fa0/6)، ويتم تسجيل عنواني MAC. ماك عنوان المفتاح على ميناء fa0/6 على VLAN1 وعلى VLAN200.

يمكن الآن إجراء التحقق من جلسات مصادقة dot1x. تمت مصادقة منفذ Fa0/6 على محول الخادم بالفعل. هذا هو تبادل dot1x الذي يتم تشغيله عندما يتم توصيل BSTP-3500-2 (المتطلب) في:

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

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

كما هو متوقع في هذه المرحلة، لا توجد جلسات عمل حول المتلقي:

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

مصادقة كمبيوتر Windows لمحول العميل

في هذا المثال، يقوم كمبيوتر Windows بالمصادقة على الطالب. الخطوات في العملية هي:

1. يتم توصيل كمبيوتر Windows بمنفذ FastEthernet 0/5 على BSTP-3500-2 (الملحق).
2. يقوم الطالب بإجراء المصادقة والتفويض باستخدام ISE.
3. يقوم الطالب بإعلام المصدق بأن عميل جديد متصل على المنفذ.

هذا هو التواصل من الملتمس:

```
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
```

يحدث تبادل ADD_CLIENT، ولكن لا توجد حاجة إلى تبادل التسجيل.

دخلت to order in دقةت تصرف على الطالب، **العرض cisp تسجيل** أمر:

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

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

يحتوي الطالب على دور ملاحق تجاه المصدق (واجهة Fa0/6) ودور المصدق تجاه واجهة Windows PC (واجهة Fa0/5).

دخلت to order in دقةت تصرف على المصدق، **العرض cisp زبون** أمر:

```
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
```

يظهر عنوان MAC جديد على المصدق تحت 200 VLAN. إنه عنوان MAC الذي تمت ملاحظته في طلبات AAA على المطالب.

يجب أن تشير جلسات المصادقة إلى أن نفس الجهاز متصل على Fa0/5 منفذ الطالب:

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

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

إزالة العميل المصادق عليه من الشبكة

عند إزالة عميل (على سبيل المثال، إذا تم إيقاف تشغيل منفذ ما)، يتم إعلام المصدق من خلال تبادل 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
```

إزالة المحول المكمل

عندما يتم إلغاء توصيل مدعي أو إزالته، يقوم المصدق بتقديم التكوين الأصلي مرة أخرى إلى المنفذ لتجنب هموم الأمان.

```
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
```

في الوقت نفسه، يزيل المطالب العملاء الذين يمثلون المطالب من جدول CISP ويبطل CISP على تلك الواجهة.

المنافذ بدون dot1x على المحول المحول

لا تخدم معلومات CISP التي يتم نشرها من مقدم الطلب إلى المصدق إلا كطبقة أخرى من الإنفاذ. يقوم الطالب بإعلام المصدق عن جميع عناوين MAC المسموح بها المتصلة به.

السيناريو الذي عادة ما يساء فهمه هو هذا: إذا كان الجهاز موصلا على منفذ لا يحتوي على dot1x ممكن، يتم التعرف على عنوان MAC ونشره إلى محول الخادم من خلال CISP.

يسمح المصدق بالاتصال الذي يأتي من جميع العملاء الذين تم التعرف عليهم من خلال CISP.

وفي جوهر الأمر، يتمثل دور المطالب في تقييد وصول الأجهزة، من خلال dot1x أو أساليب أخرى، ونشر عنوان MAC ومعلومات شبكة VLAN إلى المصدق. ويعمل المصدق كعامل إنفاذ للمعلومات المقدمة في هذه التحديثات.

كمثال، VLAN جديد (VLAN300) خلقت على كلا مفتاح، وجهاز كان ربطت في ميناء Fa0/4 على المفتاح. ميناء Fa0/4 هو منفذ وصول بسيط أن لا يشكل ل dot1x.

يبدي هذا إنتاج من الطالب ميناء جديد مسجل:

```
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
```

على المصدق، رأيت عنوان MAC جديد على 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
```

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

ملاحظة:

تدعم أداة مترجم الإخراج (للعملاءالمسجلين فقط) بعض أوامر show. استخدم "أداة مترجم الإخراج" لعرض تحليل لمُخرَج الأمر **show**.

ارجع إلى معلومات مهمة عن أوامر تصحيح الأخطاء قبل أن تستخدم أوامر **debug**.

تساعدك هذه الأوامر على أستكشاف أخطاء NEAT و CISP وإصلاحها، ويتضمن هذا المستند أمثلة لمعظمهم:

- **debug cisp all** - يعرض تبادل معلومات CISP بين المحولات.
- **show cisp summary** - يعرض ملخصا من ال CISP قارن وضع على المفتاح.
- **إظهار تسجيلات CISP** - يشير إلى الواجهات التي تشارك في عمليات تبادل CISP، وأدوار هذه الواجهات، وما إذا كانت الواجهات جزءا من NEAT.
- **عرض عملاء Cisco** - يعرض جدول لعناوين MAC الخاصة بالعميل المعروفة ومواقعها (شبكة VLAN والواجهة). وهذا مفيد أساسا من المصدق.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).