NEAT-Konfigurationsbeispiel mit Cisco Identity Services Engine

Inhalt

[Einleitung](#)
[Voraussetzungen](#)
[Anforderungen](#)
[Verwendete Komponenten](#)
[Konfigurieren](#)
[Netzwerkdiagramm](#)
[Konfiguration des Authentifizierungs-Switches](#)
[Supplicant Switch-Konfiguration](#)
[ISE-Konfiguration](#)
[Überprüfung](#)
[Supplicant Switch Authentication to Authenticator Switch](#)
[Windows-PC-Authentifizierung für zusätzlichen Switch](#)
[Entfernen des authentifizierten Clients aus dem Netzwerk](#)
[Entfernen eines zusätzlichen Switches](#)
[Ports ohne dot1x auf Supplicant Switch](#)
[Fehlerbehebung](#)

Einleitung

In diesem Dokument werden die Konfiguration und das Verhalten der Network Edge Authentication Topology (NEAT) in einem einfachen Szenario beschrieben. NEAT verwendet das Client Information Signaling Protocol (CISP), um MAC-Adressen und VLAN-Informationen von Clients zwischen den Switches des Supplicant und des Authentifikators weiterzugeben.

In diesem Konfigurationsbeispiel führen sowohl der Authentifikator-Switch (auch Authentifikator genannt) als auch der Supplicant-Switch (auch Supplicant genannt) eine 802.1x-Authentifizierung durch; der Authentifikator authentifiziert die Supplicant, die wiederum den Test-PC authentifiziert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse des IEEE 802.1x-Authentifizierungsstandards verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Zwei Cisco Catalyst Switches der Serie 3560 mit Cisco IOS® Software, Version 12.2(55)SE8; ein Switch fungiert als Authentifizierer und der andere als Supplicant.
- Cisco Identity Services Engine (ISE) Version 1.2
- PC mit Microsoft Windows XP, Service Pack 3.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konfigurieren

In diesem Beispiel werden Beispielkonfigurationen für die folgenden Elemente beschrieben:

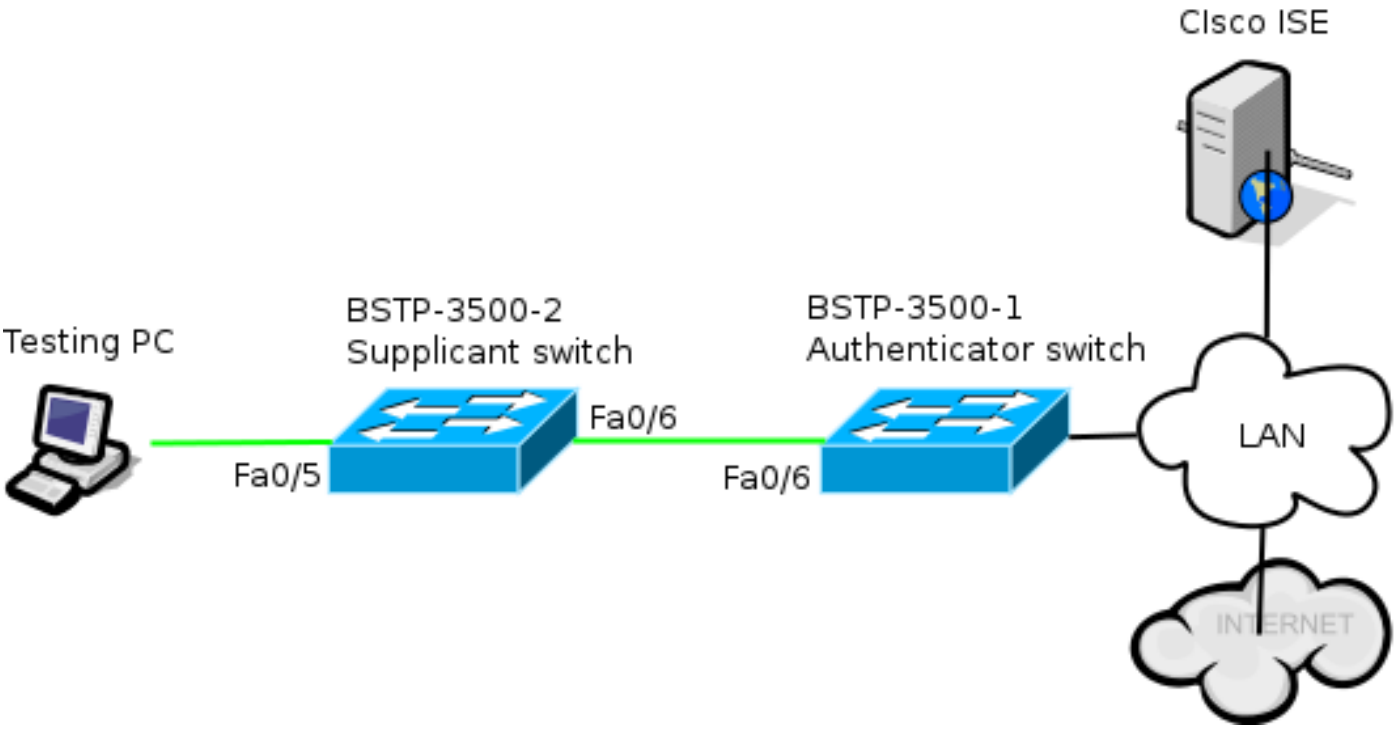
- Authentifizierer-Switch
- Supplicant Switch
- Cisco ISE

Die zur Durchführung dieser Übung erforderlichen Konfigurationen sind möglicherweise nicht optimal oder erfüllen andere Anforderungen nicht.

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur für registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Netzwerkdiagramm

Dieses Netzwerkdiagramm zeigt die in diesem Beispiel verwendete Verbindung. Schwarze Linien weisen auf logische oder physische Verbindungen hin, während grüne Linien auf Verbindungen hinweisen, die mithilfe von 802.1x authentifiziert wurden.



Konfiguration des Authentifizierungs-Switches

Der Authentifikator enthält die grundlegenden Elemente, die für dot1x benötigt werden. In diesem Beispiel werden Befehle, die spezifisch für NEAT oder CISP sind, fett formatiert.

Dies ist die AAA-Konfiguration (Basic Authentication, Authorization, and Accounting):

```
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 ist global aktiviert, und der Verbindungsport wird im Authentifizierungs- und Zugriffsmodus konfiguriert.

Supplicant Switch-Konfiguration

Eine präzise Supplicant-Konfiguration ist von entscheidender Bedeutung, damit das gesamte Setup wie erwartet funktioniert. Diese Beispielkonfiguration enthält eine typische AAA- und dot1x-Konfiguration.

Dies ist die grundlegende AAA-Konfiguration:

```
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
```

Der Supplicant muss über konfigurierte Anmeldedaten verfügen und eine Extensible Authentication Protocol (EAP)-Methode bereitstellen, die verwendet werden soll.

Der Supplicant kann EAP-Message Digest 5 (MD5) und EAP-Flexible Authentication via Secure Protocol (FAST) (neben anderen EAP-Typen) für die Authentifizierung bei CISP verwenden. Um die ISE-Konfiguration auf ein Minimum zu reduzieren, wird in diesem Beispiel EAP-MD5 für die Authentifizierung des Supplicant gegenüber dem Authentifizierer verwendet. (Standardmäßig wird EAP-FAST verwendet, wozu PAC-konforme (Protected Access Credential) bereitgestellt werden muss. Dieses Szenario wird in diesem Dokument nicht behandelt.)

```
! 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
```

Die Verbindung des Supplicant mit dem Authentifikator ist bereits als Trunk-Port konfiguriert (im Gegensatz zur Access-Port-Konfiguration auf dem Authentifikator). Zu diesem Zeitpunkt wird dies erwartet. Die Konfiguration wird dynamisch geändert, wenn die ISE das richtige Attribut zurückgibt.

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

Der Anschluss, der an den Windows-PC angeschlossen wird, ist minimal konfiguriert und wird hier nur als Referenz angezeigt.

```
interface FastEthernet0/5
switchport access vlan 200
switchport mode access
```

```
authentication port-control auto
dot1x pae authenticator
```

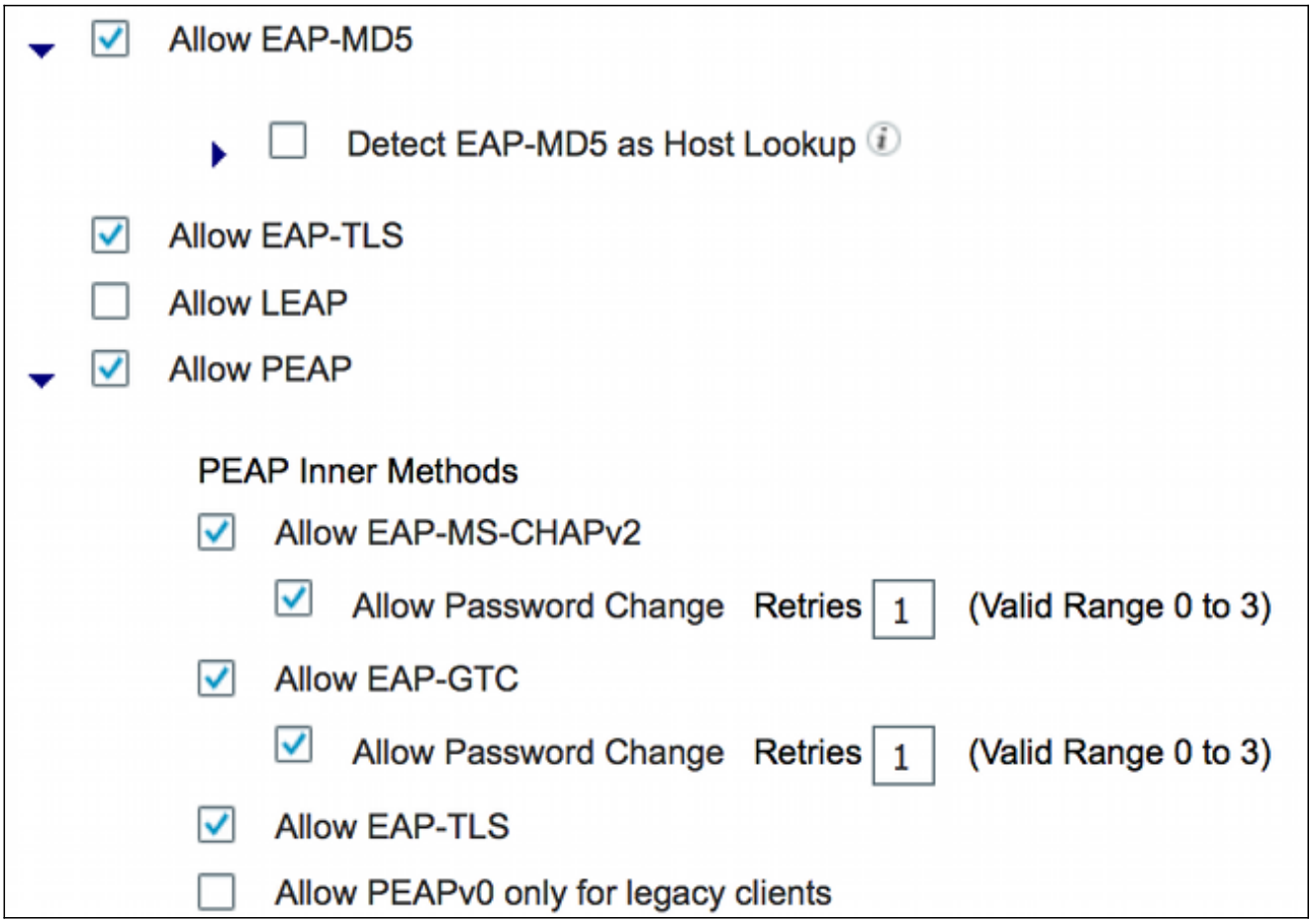
ISE-Konfiguration

Dieses Verfahren beschreibt die Einrichtung einer grundlegenden ISE-Konfiguration.

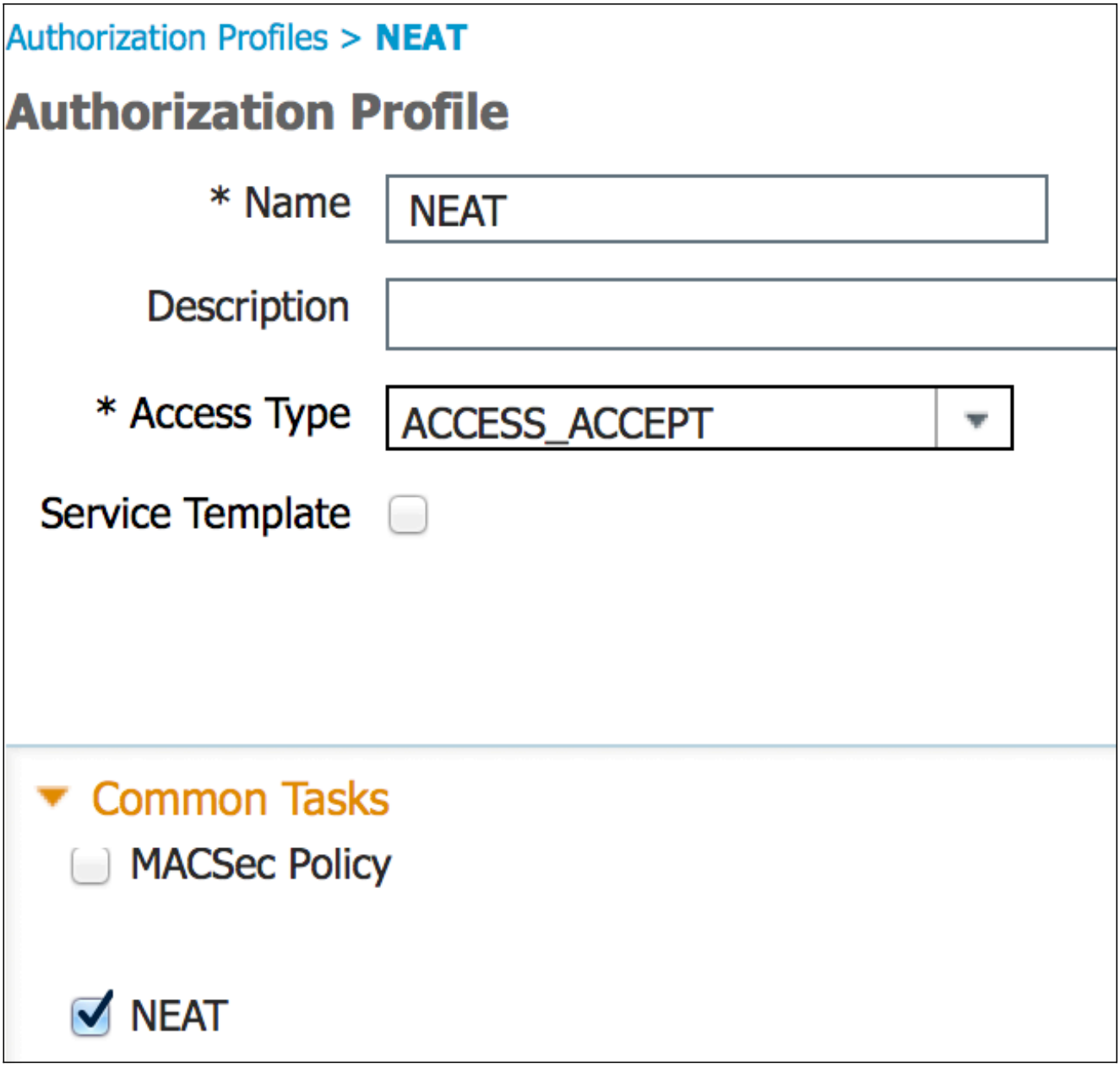
1. Aktivieren der erforderlichen Authentifizierungsprotokolle

   In diesem Beispiel ermöglicht der Wired dot1x-Modus EAP-MD5, die Komponente gegenüber dem Authentifizierer zu authentifizieren, und erlaubt dem Protected Extensible Authentication Protocol (PEAP)-Microsoft Challenge Handshake Authentication Protocol Version 2 (MSCHAPv2), den Windows-PC gegenüber der Komponente zu authentifizieren.

   Navigieren Sie zu **Richtlinie > Ergebnisse > Authentifizierung > Zulässige Protokolle,** wählen Sie die **Protokolldienstliste aus, die** von wired dot1x verwendet wird, und stellen Sie sicher, dass die Protokolle in diesem Schritt aktiviert sind.



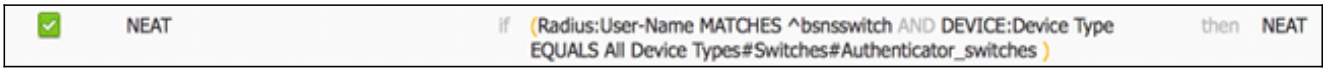
2. Erstellen einer Autorisierungsrichtlinie Navigieren Sie zu **Policy > Results > Authorization > Authorization Policy,** und erstellen oder aktualisieren Sie eine Richtlinie, sodass sie NEAT als zurückgegebenes Attribut enthält. Dies ist ein Beispiel für eine solche Politik:



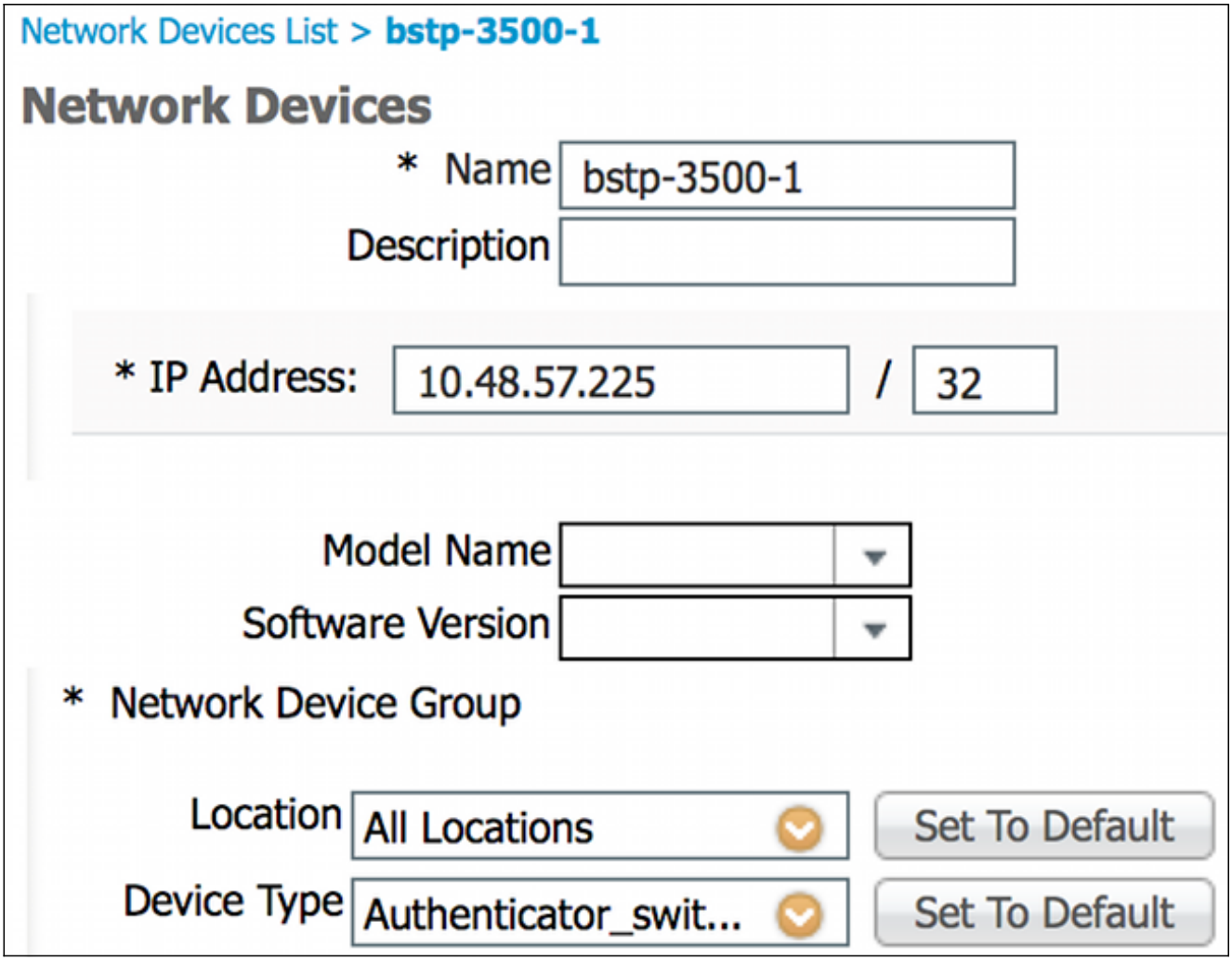
Wenn die NEAT-Option aktiviert ist, gibt die ISE im Rahmen der Autorisierung "device-traffic-class=switch" zurück. Diese Option ist erforderlich, um den Port-Modus des Authentifizierers vom Zugriff auf den Trunk zu ändern.

3. Erstellen Sie eine Autorisierungsregel, um dieses Profil zu verwenden. Navigieren Sie zu **Richtlinie > Autorisierung**, und erstellen oder aktualisieren Sie eine Regel.

   In diesem Beispiel wird eine spezielle Gerätegruppe namens Authenticator_switches erstellt, und alle Supplicants senden einen Benutzernamen, der mit bsnsswitch beginnt.



4. Fügen Sie die Switches der entsprechenden Gruppe hinzu. Navigieren Sie zu **Administration > Network Resources > Network Devices,** und klicken Sie auf **Add**.



In diesem Beispiel ist BSTP-3500-1 (der Authentifikator) Teil der Gruppe Authenticator_switches; BSTP-3500-2 (die Komponente) muss nicht Teil dieser Gruppe sein.

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert. In diesem Abschnitt werden zwei Verhaltensweisen beschrieben:

- Authentifizierung zwischen Switches
- Authentifizierung zwischen dem Windows-PC und dem Supplicant

Außerdem werden drei weitere Situationen erläutert:

- Entfernen eines authentifizierten Clients aus dem Netzwerk
- Entfernen eines Supplicant
- Ports ohne dot1x auf einem Supplicant

Hinweise:

Das Output Interpreter-Tool (nur registrierte Kunden) unterstützt bestimmte show-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Lesen Sie den Artikel Wichtige Informationen zu Debug-Befehlen, bevor Sie **debug**-Befehle

verwenden.

Supplicant Switch Authentication to Authenticator Switch

In diesem Beispiel führt die Komponente eine Authentifizierung beim Authentifizierer durch. Der Prozess umfasst folgende Schritte:

1. Die Komponente wird konfiguriert und an den Port fastethernet0/6 angeschlossen. Der dot1x-Austausch veranlasst den Supplicant, EAP zu verwenden, um einen vorkonfigurierten Benutzernamen und ein Passwort an den Authentifikator zu senden.
2. Der Authentifizierer führt einen RADIUS-Austausch durch und stellt Anmeldeinformationen für die ISE-Validierung bereit.
3. Wenn die Anmeldeinformationen korrekt sind, gibt die ISE die von NEAT (device-traffic-class=switch) benötigten Attribute zurück, und der Authentifikator ändert seinen Switch-Port-Modus von Zugriff auf Trunk.

Dieses Beispiel zeigt den Austausch von CISP-Informationen zwischen 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
```

Nach erfolgreicher Authentifizierung und Autorisierung findet der CISP-Austausch statt. Jede

Vermittlungsstelle verfügt über einen REQUEST, der vom Supplicant verschickt wird, und eine RESPONSE, die als Antwort und Bestätigung vom Authentifikator dient.

Es werden zwei unterschiedliche Austauschvorgänge durchgeführt: REGISTRATION und ADD_CLIENT. Während des REGISTRATION-Austauschs informiert der Supplicant den Authentifikator, dass er CISP-fähig ist, und der Authentifikator bestätigt diese Nachricht. Der ADD_CLIENT-Austausch wird verwendet, um den Authentifikator über Geräte zu informieren, die mit dem lokalen Port des Supplicants verbunden sind. Wie bei REGISTRATION wird ADD-CLIENT auf dem Supplicant initiiert und vom Authentifikator bestätigt.

Geben Sie die folgenden show-Befehle ein, um die Kommunikation, die Rollen und die Adressen zu überprüfen:

```
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)
```

In diesem Beispiel wird die Authentifizierer-Rolle der richtigen Schnittstelle (fa0/6) richtig zugewiesen, und es werden zwei MAC-Adressen registriert. Die MAC-Adressen sind die Komponente auf Port fa0/6 in VLAN1 und auf VLAN200.

Die 802.1x-Authentifizierungssitzungen können jetzt überprüft werden. Der fa0/6-Port am Upstream-Switch ist bereits authentifiziert. Dies ist der dot1x-Austausch, der ausgelöst wird, wenn BSTP-3500-2 (die Komponente) angeschlossen wird:

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

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

Wie zu diesem Zeitpunkt erwartet, gibt es keine Sitzungen zum Bewerber:

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

Windows-PC-Authentifizierung für zusätzlichen Switch

In diesem Beispiel wird der Windows-PC bei der Komponente authentifiziert. Der Prozess umfasst folgende Schritte:

1. Der Windows-PC ist an den FastEthernet 0/5-Port am BSTP-3500-2 (der Komponente) angeschlossen.

2. Der Supplicant führt eine Authentifizierung und Autorisierung mit der ISE durch.
3. Der Supplicant informiert den Authentifikator, dass ein neuer Client am Port angeschlossen ist.

Dies ist die Mitteilung des Antragstellers:

```
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
```

Ein ADD_CLIENT-Austausch findet statt, es ist jedoch kein REGISTRIERUNGSAUSTAUSCH erforderlich.

Um das Verhalten des Supplicant zu überprüfen, geben Sie den Befehl **show cisp registrations** ein:

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

Interface(s) with CISP registered user(s):
----------------------------------------
Fa0/5
Auth Mgr (Authenticator)
```

```
Fa0/6
802.1x Sup (Supplicant)
```

Der Supplicant hat die Rolle eines Supplicant gegenüber dem Authentifikator (fa0/6-Schnittstelle) und die Rolle eines Authentifikators gegenüber dem Windows-PC (fa0/5-Schnittstelle).

Um das Verhalten auf dem Authentifizierer zu überprüfen, geben Sie den Befehl **show cisp clients** ein:

```
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
```

Unter VLAN 200 wird auf dem Authentifizierer eine neue MAC-Adresse angezeigt. Es handelt sich um die MAC-Adresse, die bei AAA-Anfragen für die Komponente beobachtet wurde.

Authentifizierungssitzungen sollten angeben, dass dasselbe Gerät an den fa0/5-Port des Supplicant angeschlossen ist:

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

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

Entfernen des authentifizierten Clients aus dem Netzwerk

Wenn ein Client entfernt wird (z. B. wenn ein Port heruntergefahren wird), wird der Authentifikator über den DELETE_CLIENT-Austausch benachrichtigt.

```
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
```

Entfernen eines zusätzlichen Switches

Wenn eine Komponente vom Netz getrennt oder entfernt wird, führt der Authentifikator die ursprüngliche Konfiguration wieder am Port ein, um Sicherheitsbedenken zu vermeiden.

```
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
```

Gleichzeitig entfernt der Supplicant Clients, die den Supplicant darstellen, aus der CISP-Tabelle und deaktiviert CISP auf dieser Schnittstelle.

Ports ohne dot1x auf Supplicant Switch

CISP-Informationen, die vom Supplicant an den Authentifikator weitergeleitet werden, dienen lediglich als weitere Durchsetzungsebene. Die Komponente informiert den Authentifizierer über alle zulässigen MAC-Adressen, die mit ihr verbunden sind.

In der Regel wird folgendes Szenario missverstanden: Wenn ein Gerät an einen Port angeschlossen wird, auf dem dot1x nicht aktiviert ist, wird die MAC-Adresse erfasst und über CISP an den Upstream-Switch weitergeleitet.

Der Authentifikator ermöglicht die Kommunikation, die von allen über CISP gelernten Clients ausgeht.

Im Wesentlichen handelt es sich um eine Supplicant-Funktion, die den Zugriff auf Geräte mithilfe von dot1x oder anderen Methoden einschränkt und dem Authentifizierer MAC-Adressen- und VLAN-Informationen zuweist. Der Authentifikator fungiert als Durchsetzer für die Informationen, die in diesen Updates bereitgestellt werden.

Als Beispiel wurde ein neues VLAN (VLAN300) auf beiden Switches erstellt und ein Gerät an den Port fa0/4 der Komponente angeschlossen. Port fa0/4 ist ein einfacher Zugriffsport, der nicht für dot1x konfiguriert ist.

Diese Ausgabe des Supplicants zeigt einen neuen registrierten Port an:

```
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)
```

Auf dem Authentifikator ist eine neue MAC-Adresse im VLAN 300 sichtbar.

```
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
```

Fehlerbehebung

In diesem Abschnitt finden Sie Informationen zur Behebung von Fehlern in Ihrer Konfiguration.

> **Anmerkung:**
>
> Das Output Interpreter-Tool (nur registrierte Kunden) unterstützt bestimmte show-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.
>
> Lesen Sie den Artikel Wichtige Informationen zu Debug-Befehlen, bevor Sie **debug**-Befehle verwenden.

Diese Befehle unterstützen Sie bei der Fehlerbehebung von NEAT und CISP. Dieses Dokument enthält für die meisten Befehle Beispiele:

- **debug cisp all** - Zeigt den Austausch von CISP-Informationen zwischen Switches.
- **show cisp summary**: Zeigt eine Zusammenfassung des CISP-Schnittstellenstatus auf dem Switch an.
- **show cisp registration**: Zeigt die Schnittstellen an, die an CISP-Austauschen teilnehmen, die Rollen dieser Schnittstellen und ob die Schnittstellen Teil von NEAT sind.
- **show cisp clients**: Zeigt eine Tabelle mit bekannten Client-MAC-Adressen und deren Standort (VLAN und Schnittstelle) an. Dies ist vor allem vom Authentifikator aus nützlich.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.