NEAT-configuratievoorbeeld met Cisco Identity Services Engine

Inhoud

Inleiding

In dit document worden de configuratie en het gedrag van Network Edge Verification Topology (NEAT) in een eenvoudig scenario beschreven. NEAT maakt gebruik van het Client Information Signaling Protocol (CISP) om client-MAC-adressen en VLAN-informatie te verspreiden tussen aanvragers en switches van verificateurs.

In dit configuratievoorbeeld, zowel de authenticator switch (ook wel de authenticator genoemd) en de supplicant switch (ook wel de supplicant genoemd) voeren 802.1x authenticatie uit; de authenticator authenticeert de supplicant, die op zijn beurt de test PC authenticeert.

Voorwaarden

Vereisten

Cisco raadt u aan bekend te zijn met de IEEE 802.1x-verificatiestandaard.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Twee Cisco Catalyst 3560 Series-switches met Cisco IOS®-software, release 12.2(55)SE8; één switch fungeert als een verificator en de andere als een aanvrager.
- Cisco Identity Services Engine (ISE), release 1.2.
- PC met Microsoft Windows XP, Service Pack 3.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Configureren

Dit voorbeeld heeft betrekking op voorbeeldconfiguraties voor:

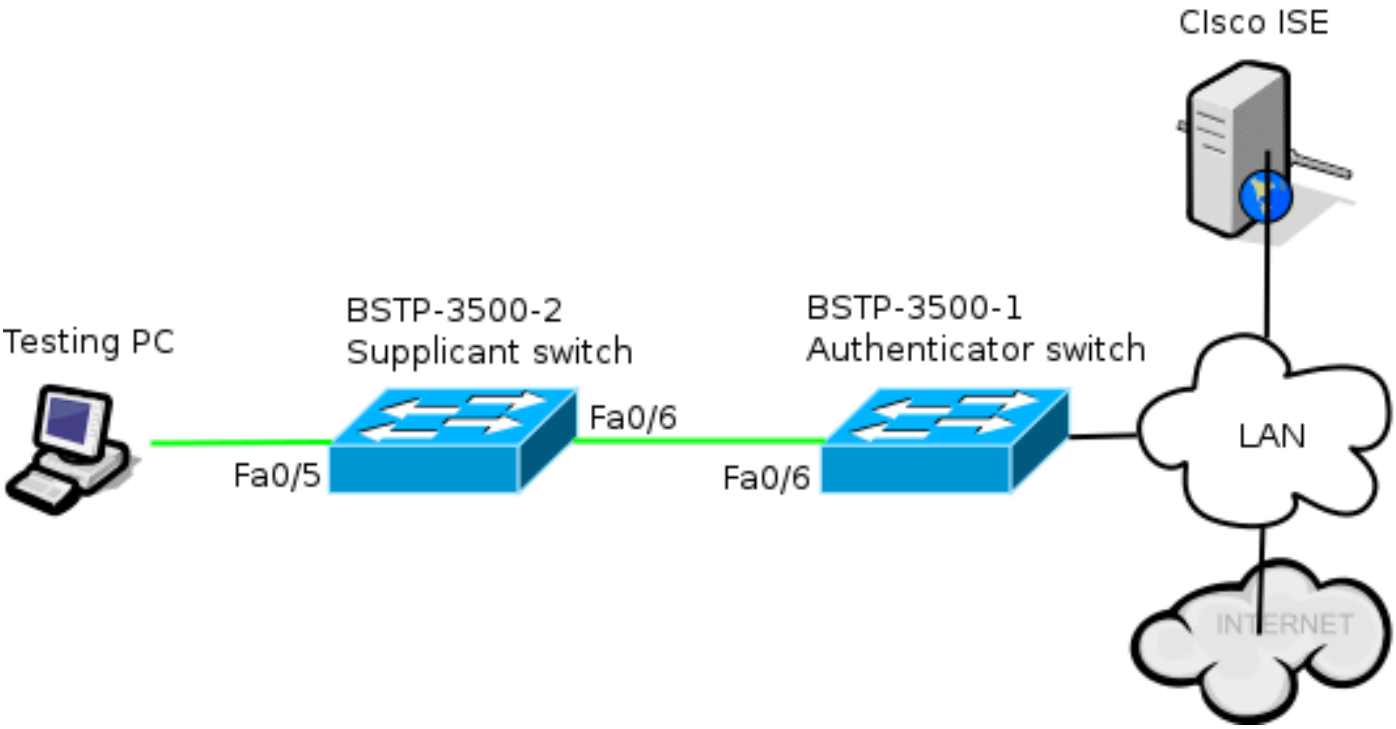
- Verificator-switch
- Supplicant switch
- Cisco ISE-software

De configuraties zijn het minimum dat nodig is om deze lab oefening uit te voeren; ze zijn mogelijk niet optimaal voor of voldoen aan andere behoeften.

> **Opmerking**: Gebruik de Command Lookup Tool (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Netwerkdiagram

Dit netwerkdiagram illustreert de connectiviteit die in dit voorbeeld wordt gebruikt. Zwarte lijnen geven logische of fysieke connectiviteit aan, en groene lijnen geven links aan die zijn geverifieerd door het gebruik van 802.1x.



Configuratie van Authenticator Switch

De verificator bevat de basiselementen die nodig zijn voor dot1x. In dit voorbeeld worden opdrachten die specifiek zijn voor NEAT of CISP, vet weergegeven.

Dit is de basisconfiguratie voor verificatie, autorisatie en accounting (AAA):

```
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 is wereldwijd ingeschakeld en de interconnectiepoort is ingesteld in verificator- en toegangsmodus.

Configuratie supplicant Switch

Nauwkeurige supplicantconfiguratie is essentieel voor de gehele installatie om te werken zoals verwacht. Deze voorbeeldconfiguratie bevat een typische AAA- en dot1x-configuratie.

Dit is de basis-AAA-configuratie:

```
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
```

De aanvrager moet referenties hebben geconfigureerd en een EAP-methode (Extensible Authentication Protocol) leveren die moet worden gebruikt.

De aanvrager kan EAP-Message Digest 5 (MD5) en EAP-Flexibele verificatie via Secure Protocol (FAST) (onder andere EAP-typen) gebruiken voor verificatie in het geval van CISP. Om de ISE-configuratie tot een minimum te beperken, wordt in dit voorbeeld EAP-MD5 gebruikt voor de verificatie van de aanvrager naar de verificator. (Het gebrek zou gebruik van EAP-FAST dwingen, die Beschermde Toegang Credentiële [PAC] levering vereist; dit document behandelt dat scenario niet.)

```
! 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
```

De verbinding van de aanvrager met de verificator is al geconfigureerd om een trunkpoort te zijn (in tegenstelling tot de toegangspoortconfiguratie op de verificator). In dit stadium wordt dit verwacht; de configuratie zal dynamisch veranderen wanneer de ISE de juiste attributen teruggeeft.

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

De poort die is aangesloten op de Windows PC heeft een minimale configuratie en wordt hier alleen ter referentie weergegeven.

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

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

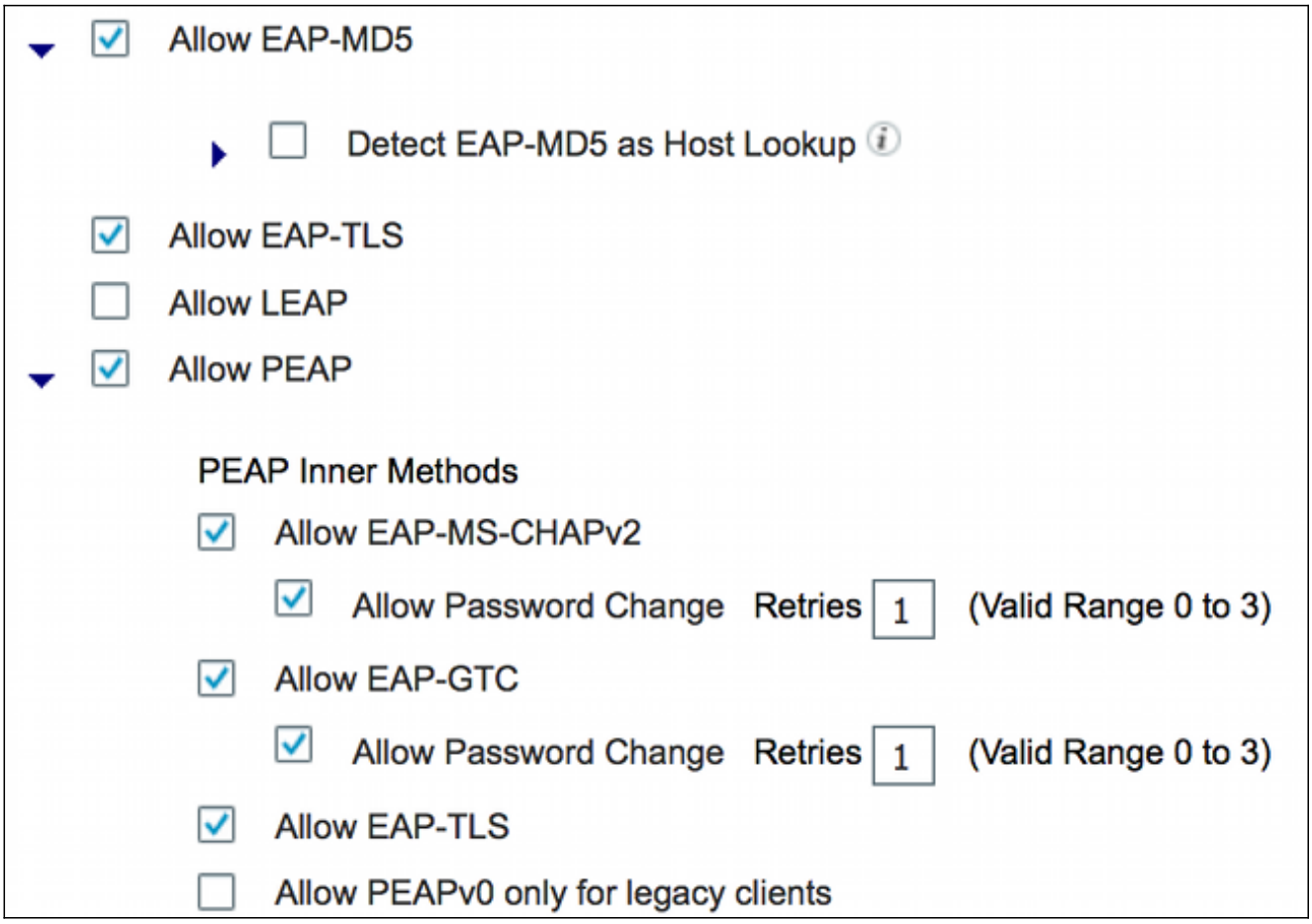
ISE-configuratie

In deze procedure wordt beschreven hoe u een basis-ISE-configuratie kunt instellen.

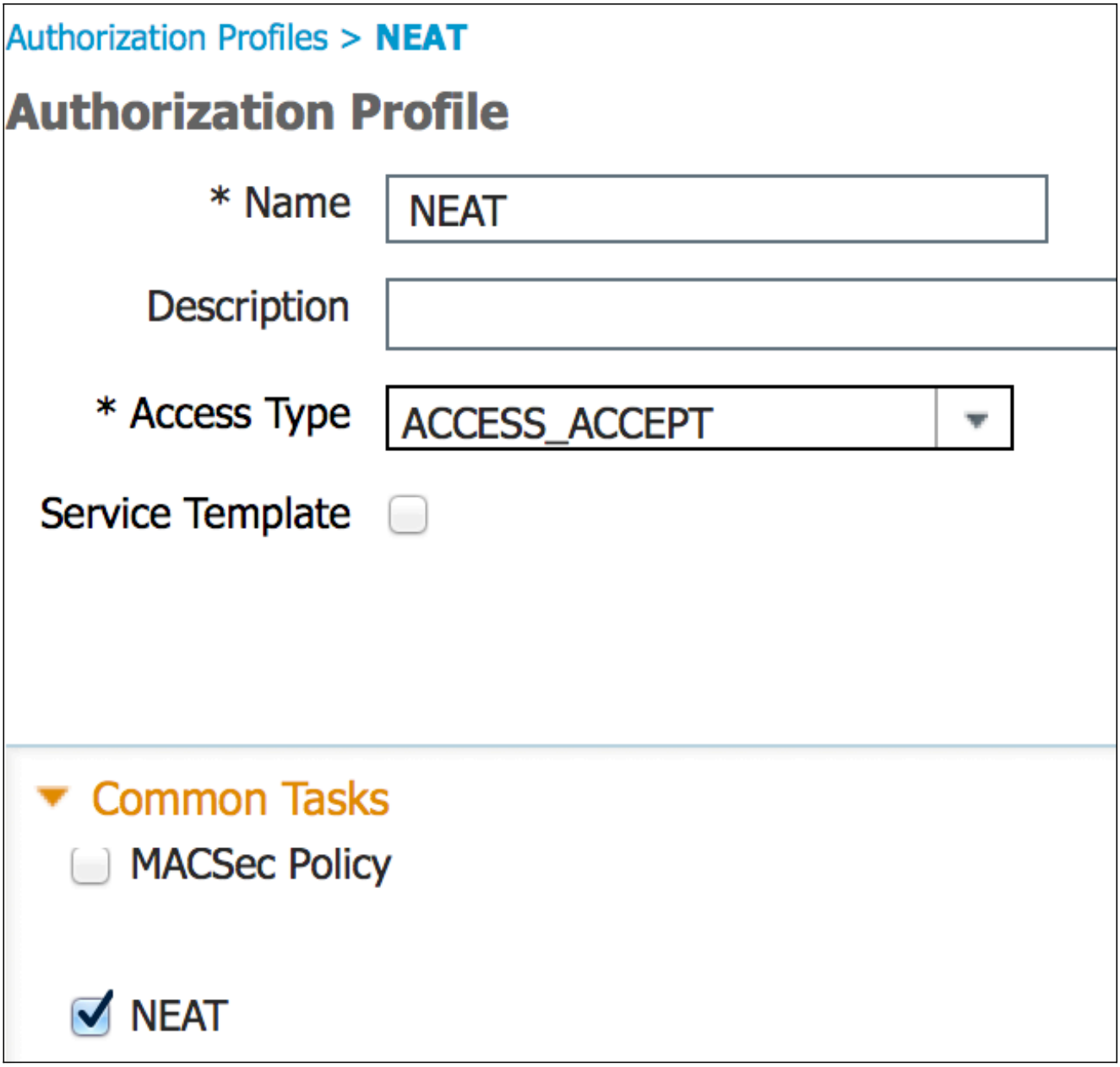
1. Schakel de vereiste verificatieprotocollen in.

   In dit voorbeeld is met bekabeld dot1x EAP-MD5 in staat om de aanvrager te authenticeren voor de verificator en maakt het mogelijk dat met het PEAP-protocol (Protected Extensible Authentication Protocol)-Microsoft Challenge Handshake Verification Protocol versie 2 (MSCHAPv2) de Windows-pc voor de aanvrager wordt geverifieerd.

   Navigeer naar **Beleid > Resultaten > Verificatie > Toegestane protocollen**, selecteer de **protocolservicelijst** die wordt gebruikt door bekabeld dot1x en controleer of de protocollen in deze stap zijn ingeschakeld.



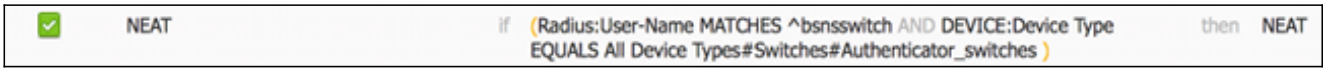
2. Creëer een autorisatiebeleid. Navigeer naar **Beleid > Resultaten > Autorisatie > Autorisatiebeleid** en maak of update een beleid zodat het NEAT bevat als een teruggegeven kenmerk. Dit is een voorbeeld van een dergelijk beleid:



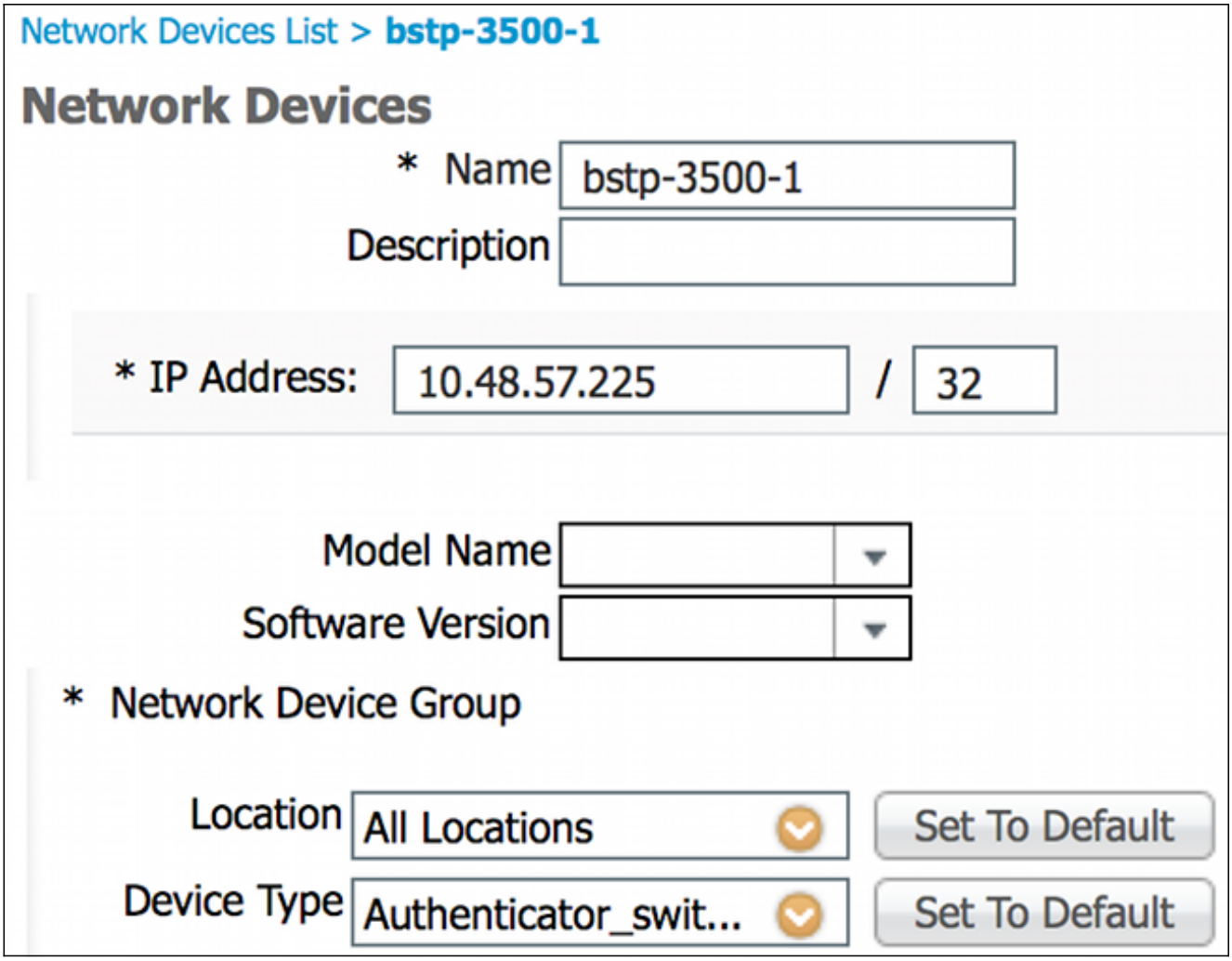
Wanneer de NEAT optie is ingeschakeld, retourneert de ISE device-traffic-class=switch als onderdeel van de autorisatie. Deze optie is nodig om de poortmodus van de verificator van toegang tot de trunk te wijzigen.

3. Maak een autorisatieregel om dit profiel te gebruiken. Navigeer naar **Beleid > Autorisatie** en maak of update een regel.

   In dit voorbeeld wordt een speciale apparaatgroep met de naam Authenticator_switches aangemaakt en alle aanvragers sturen een gebruikersnaam die begint met bsnsswitch.



4. Voeg de switches toe aan de juiste groep. Navigeer naar **Beheer > Netwerkbronnen > Netwerkapparaten** en klik op **Toevoegen**.



In dit voorbeeld maakt BSTP-3500-1 (de authenticator) deel uit van de groep Authenticator_switches; BSTP-3500-2 (de aanvrager) hoeft geen deel uit te maken van deze groep.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt. In deze sectie worden twee gedragingen beschreven:

- Verificatie tussen switches
- Verificatie tussen de Windows-pc en de aanvrager

Het verklaart ook drie bijkomende situaties:

- Verwijdering van een geverifieerde client uit het netwerk
- Verwijdering van een verzoeker
- Poorten zonder dot1x op een applicator

Opmerkingen:

De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**

Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Switch-verificatie voor verificator Switch

In dit voorbeeld wordt de aanvrager geauthenticeerd voor de authenticator. De stappen in het proces zijn:

1. De supplicant is geconfigureerd en aangesloten op poort fasteEthernet0/6. De dot1x-uitwisseling zorgt ervoor dat de aanvrager EAP gebruikt om een vooraf ingestelde gebruikersnaam en wachtwoord naar de verificator te sturen.
2. De verificator voert een RADIUS-uitwisseling uit en biedt referenties voor ISE-validatie.
3. Als de referenties juist zijn, retourneert de ISE kenmerken die vereist zijn door NEAT (device-traffic-class=switch) en verandert de verificator de switchport-modus van toegang tot de trunk.

Dit voorbeeld toont de uitwisseling van CISP-informatie tussen 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
```

Zodra de authentificatie en de vergunning slagen, vindt de uitwisseling van CISP plaats. Elke

uitwisseling heeft een VERZOEK, dat wordt verzonden door de aanvrager, en een ANTWOORD, dat dient als antwoord en bevestiging van de authenticator.

Er worden twee verschillende uitwisselingen uitgevoerd: REGISTRATIE en ADD_CLIENT. Tijdens de uitwisseling van de REGISTRATIE, informeert de aanvrager de authenticator dat het CISP-Geschikt is, en de authenticator erkent dan dit bericht. De ADD_CLIENT exchange wordt gebruikt om de authenticator te informeren over apparaten die zijn aangesloten op de lokale poort van de aanvrager. Zoals met REGISTRATIE, wordt ADD-CLIENT geïnitieerd op de aanvrager en erkend door de authenticator.

Voer deze showopdrachten in om de communicatie, rollen en adressen te verifiëren:

```
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 dit voorbeeld, wordt de rol van Authenticator correct toegewezen aan de juiste interface (fa0/6), en twee MAC-adressen worden geregistreerd. De MAC-adressen zijn de aanvrager op poort fa0/6 op VLAN1 en op VLAN200.

Verificatie van dot1x-verificatiesessies kan nu worden uitgevoerd. De fa0/6 poort op de upstream switch is al geverifieerd. Dit is de dot1x-uitwisseling die wordt geactiveerd wanneer BSTP-3500-2 (de aanvrager) is aangesloten:

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

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

Zoals in dit stadium verwacht, zijn er geen sessies over de aanvrager:

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

Windows PC-verificatie naar Supplicant Switch

In dit voorbeeld wordt de Windows-pc geverifieerd op verzoek. De stappen in het proces zijn:

1. De Windows PC is aangesloten op Fast Ethernet 50/500-2 poort (de aanvrager).
2. De aanvrager voert verificatie en autorisatie uit met de ISE.
3. De aanvrager informeert de verificator dat er een nieuwe client is aangesloten op de poort.

Dit is de mededeling van de aanvrager:

```
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
```

Er vindt een ADD_CLIENT-uitwisseling plaats, maar er is geen REGISTRATIE-uitwisseling nodig.

Om gedrag op de aanvrager te verifiëren, voer de opdracht **show cisp registrations in**:

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

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

De aanvrager heeft de rol van een aanvrager naar de authenticator (fa0/6 interface) en de rol van een authenticator naar de Windows PC (fa0/5 interface).

Om gedrag op de authenticator te verifiëren, voer je de opdracht **show cisp clients in**:

```
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
```

Er verschijnt een nieuw MAC-adres op de verificator onder VLAN 200. Het is het MAC-adres dat werd waargenomen in AAA-verzoeken op de aanvrager.

Verificatiesessies moeten aangeven dat hetzelfde apparaat is aangesloten op een fa0/5-poort van de aanvrager:

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

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

Verwijdering van geverifieerde client uit netwerk

Wanneer een client is verwijderd (bijvoorbeeld als een poort is uitgeschakeld), wordt de authenticator op de hoogte gebracht via 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
```

Verwijdering van de Switch van de applicator

Wanneer een supplicant wordt losgekoppeld of verwijderd, introduceert de verificator de oorspronkelijke configuratie terug naar de poort om beveiligingsproblemen te voorkomen.

```
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
```

Tezelfdertijd verwijdert de aanvrager clients die de aanvrager vertegenwoordigen uit de CISP-tabel en desactiveert CISP op die interface.

Poorten zonder dot1x op Switch van de applicator

De informatie van CISP die van de aanvrager aan de authenticator wordt verspreid dient slechts als een andere laag van handhaving. De aanvrager informeert de authenticator over alle toegestane MAC-adressen die ermee verbonden zijn.

Een scenario dat meestal verkeerd wordt begrepen is dit: als een apparaat is aangesloten op een poort die geen dot1x ingeschakeld heeft, wordt het MAC-adres geleerd en verspreid naar de upstream switch via CISP.

De authenticator maakt communicatie mogelijk die afkomstig is van alle clients die door CISP zijn geleerd.

In essentie is het de rol van de aanvrager om de toegang van apparaten te beperken, door dot1x of andere methoden, en om MAC-adres en VLAN-informatie te verspreiden naar de verificator. De authenticator fungeert als een afdwinger van de informatie die in deze updates wordt verstrekt.

Als voorbeeld, werd nieuw VLAN (VLAN300) gemaakt op beide switches, en een apparaat werd aangesloten op poort fa0/4 op de aanvrager. Port FA0/4 is een eenvoudige toegangspoort die niet voor dot1x is geconfigureerd.

Deze uitvoer van de aanvrager toont een nieuwe geregistreerde poort:

```
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)
```

Op de verificator is een nieuw MAC-adres zichtbaar op 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
```

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

> **Opmerking:**
>
> De Output Interpreter Tool (alleen voor geregistreerde klanten) ondersteunt bepaalde opdrachten met show. Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show.**
>
> Raadpleeg Important Information on Debug Commands (Belangrijke informatie over opdrachten met debug) voordat u opdrachten met **debug opgeeft.**

Deze opdrachten helpen u bij het oplossen van problemen met NEAT en CISP; dit document bevat voorbeelden voor de meeste ervan:

- **debug cisp all** - toont de uitwisseling van CISP-informatie tussen switches.
- **cisp-overzicht tonen** - geeft een samenvatting van de status van de CISP-interface op de switch weer.
- **cisp-registraties tonen** - geeft aan welke interfaces deelnemen aan CISP-uitwisselingen, de rollen van die interfaces en of de interfaces deel uitmaken van NEAT.
- **cisp-clients tonen** - geeft een tabel weer met bekende client-MAC-adressen en hun locatie (VLAN en interface). Dit is vooral handig vanuit de authenticator.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.