Exemple de configuration NEAT avec Cisco Identity Services Engine

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Configurer
Diagramme du réseau
Configuration du commutateur Authenticator
Configuration du commutateur demandeur
Configuration ISE
Vérifier
Authentification du commutateur demandeur vers le commutateur authentificateur
Authentification de PC Windows au commutateur demandeur
Suppression du client authentifié du réseau
Retrait du commutateur demandeur
Ports sans dot1x sur le commutateur demandeur
Dépannage

Introduction

Ce document décrit la configuration et le comportement de la topologie NEAT (Network Edge Authentication Topology) dans un scénario simple. NEAT utilise le protocole CISP (Client Information Signaling Protocol) afin de propager les adresses MAC et les informations VLAN des clients entre les commutateurs demandeur et authentificateur.

Dans cet exemple de configuration, le commutateur d'authentification (également appelé l'authentificateur) et le commutateur demandeur (également appelé le demandeur) effectuent l'authentification 802.1x ; l'authentificateur authentifie le demandeur, qui, à son tour, authentifie le PC de test.

Conditions préalables

Exigences

Cisco vous recommande de connaître la norme d'authentification IEEE 802.1x.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Deux commutateurs de la gamme Cisco Catalyst 3560 avec le logiciel Cisco IOS®, version 12.2(55)SE8 ; un commutateur agit en tant qu'authentificateur et l'autre en tant que demandeur.
- Cisco Identity Services Engine (ISE), version 1.2.
- PC avec Microsoft Windows XP, Service Pack 3.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Configurer

Cet exemple couvre des exemples de configuration pour :

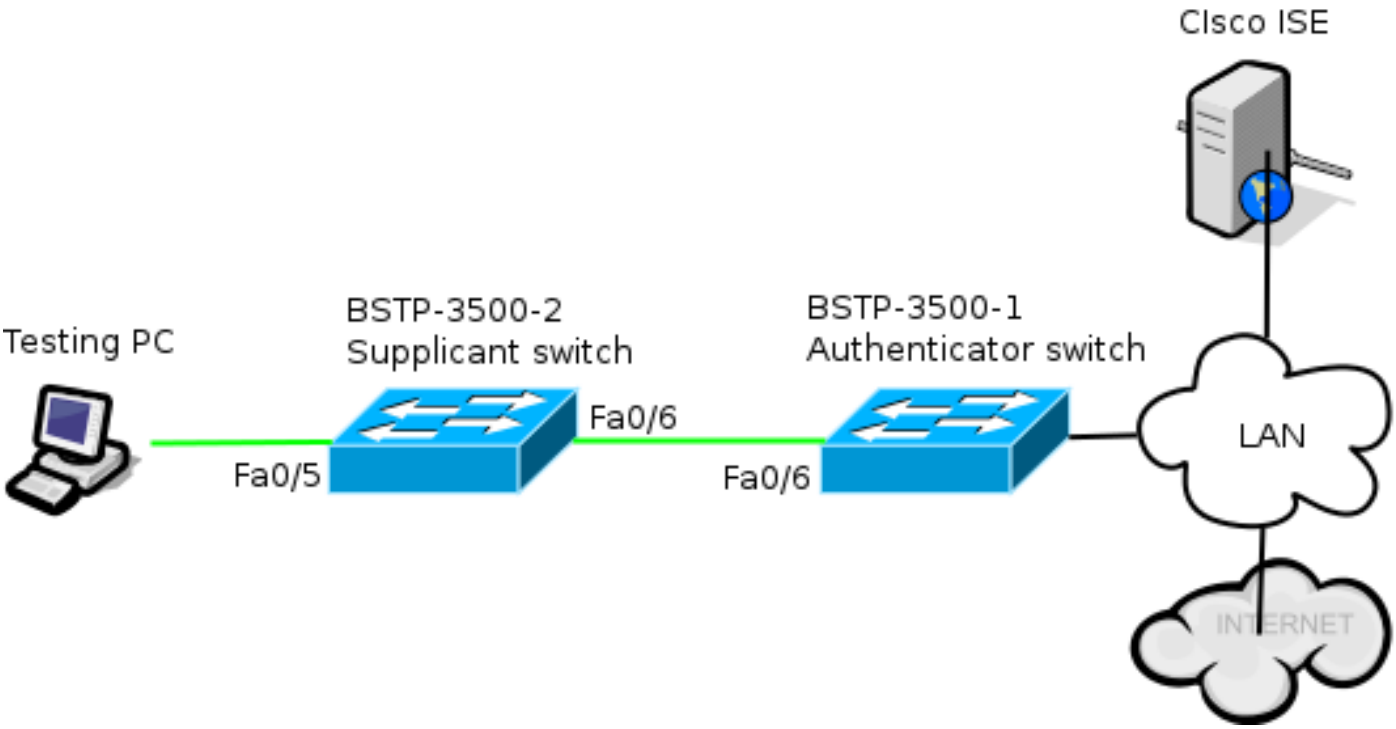
- Commutateur Authenticator
- Commutateur demandeur
- Cisco ISE

Les configurations sont le minimum requis pour effectuer cet exercice de travaux pratiques ; elles peuvent ne pas être optimales pour répondre à d'autres besoins.

> **Remarque** : utilisez l'outil de recherche de commandes (clients enregistrés uniquement) afin d'obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce schéma de réseau illustre la connectivité utilisée dans cet exemple. Les lignes noires indiquent une connectivité logique ou physique et les lignes vertes, des liaisons authentifiées via l'utilisation de la norme 802.1x.



Configuration du commutateur Authenticator

L'authentificateur contient les éléments de base nécessaires pour dot1x. Dans cet exemple, les commandes spécifiques à NEAT ou CISP sont en gras.

Il s'agit de la configuration AAA (Authentication, Authorization, and Accounting) de base :

```
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 est activé globalement et le port d'interconnexion est configuré en mode d'authentification et d'accès.

Configuration du commutateur demandeur

Une configuration précise du demandeur est essentielle pour que la configuration fonctionne comme prévu. Cet exemple de configuration contient une configuration type AAA et dot1x.

Voici la configuration AAA de base :

```
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
```

Le demandeur doit disposer d'informations d'identification configurées et doit fournir une méthode EAP (Extensible Authentication Protocol) à utiliser.

Le demandeur peut utiliser EAP-Message Digest 5 (MD5) et EAP-Flexible Authentication via Secure Protocol (FAST) (entre autres types EAP) pour l'authentification en cas de protocole CISP. Afin de maintenir la configuration ISE à un minimum, cet exemple utilise EAP-MD5 pour l'authentification du demandeur auprès de l'authentificateur. (La valeur par défaut forcerait l'utilisation d'EAP-FAST, ce qui nécessite la mise en service des informations d'identification d'accès protégé [PAC] ; ce document ne couvre pas ce scénario.)

```
! 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
```

La connexion du demandeur à l'authentificateur est déjà configurée comme port agrégé (contrairement à la configuration du port d'accès sur l'authentificateur). À ce stade, ceci est prévu ; la configuration changera dynamiquement lorsque l'ISE retournera l'attribut correct.

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

Le port qui se connecte au PC Windows a une configuration minimale et est affiché ici à titre de référence uniquement.

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

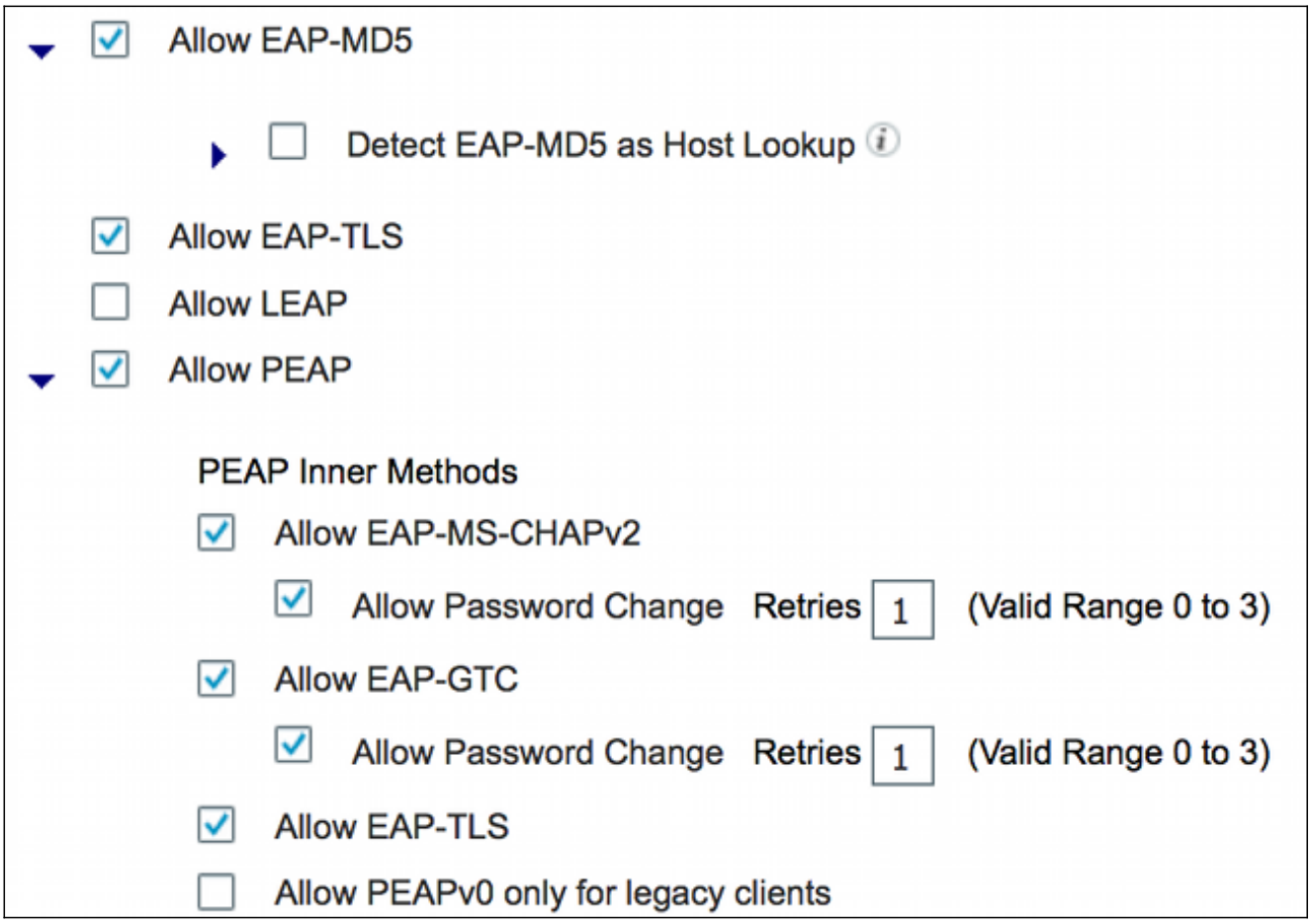
Configuration ISE

Cette procédure décrit comment configurer une configuration ISE de base.

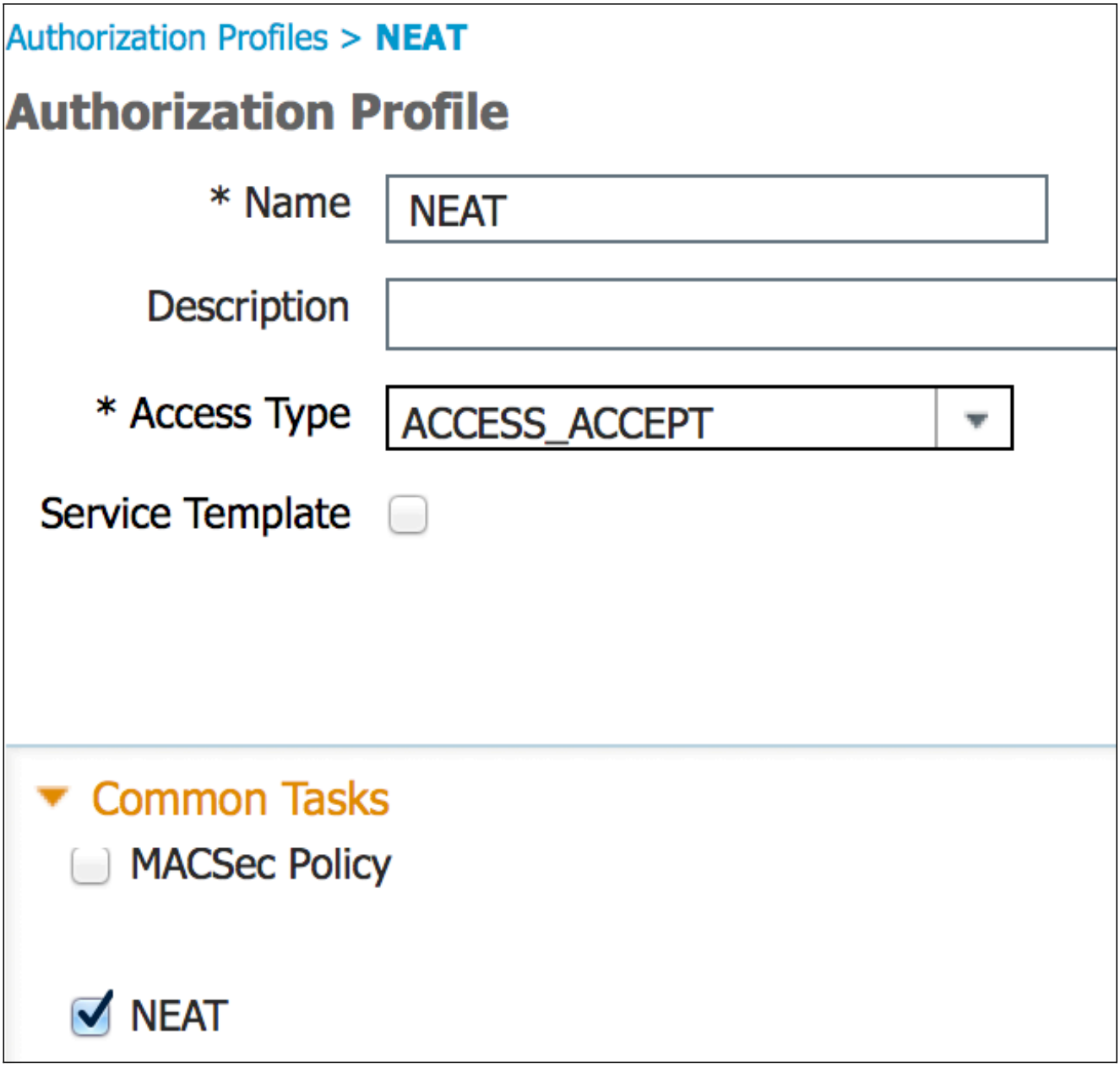
1. Activez les protocoles d'authentification requis.

   Dans cet exemple, le point1x filaire permet à EAP-MD5 d'authentifier le demandeur auprès de l'authentificateur et permet au protocole PEAP (Protected Extensible Authentication Protocol)-MSCHAPv2 (Microsoft Challenge Handshake Authentication Protocol Version 2) d'authentifier le PC Windows auprès du demandeur.

   Accédez à **Policy > Results > Authentication > Allowed protocols**, sélectionnez la **protocol service list** utilisée par wired dot1x, et assurez-vous que les protocoles de cette étape sont activés.



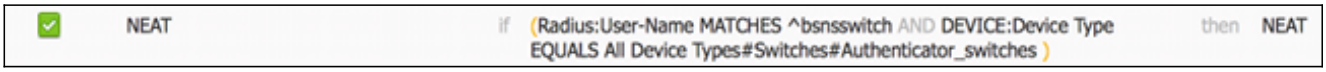
2. Créez une stratégie d'autorisation. Naviguez jusqu'à **Policy > Results > Authorization > Authorization Policy**, et créez ou mettez à jour une stratégie de sorte qu'elle contienne NEAT comme attribut renvoyé. Voici un exemple d'une telle politique :



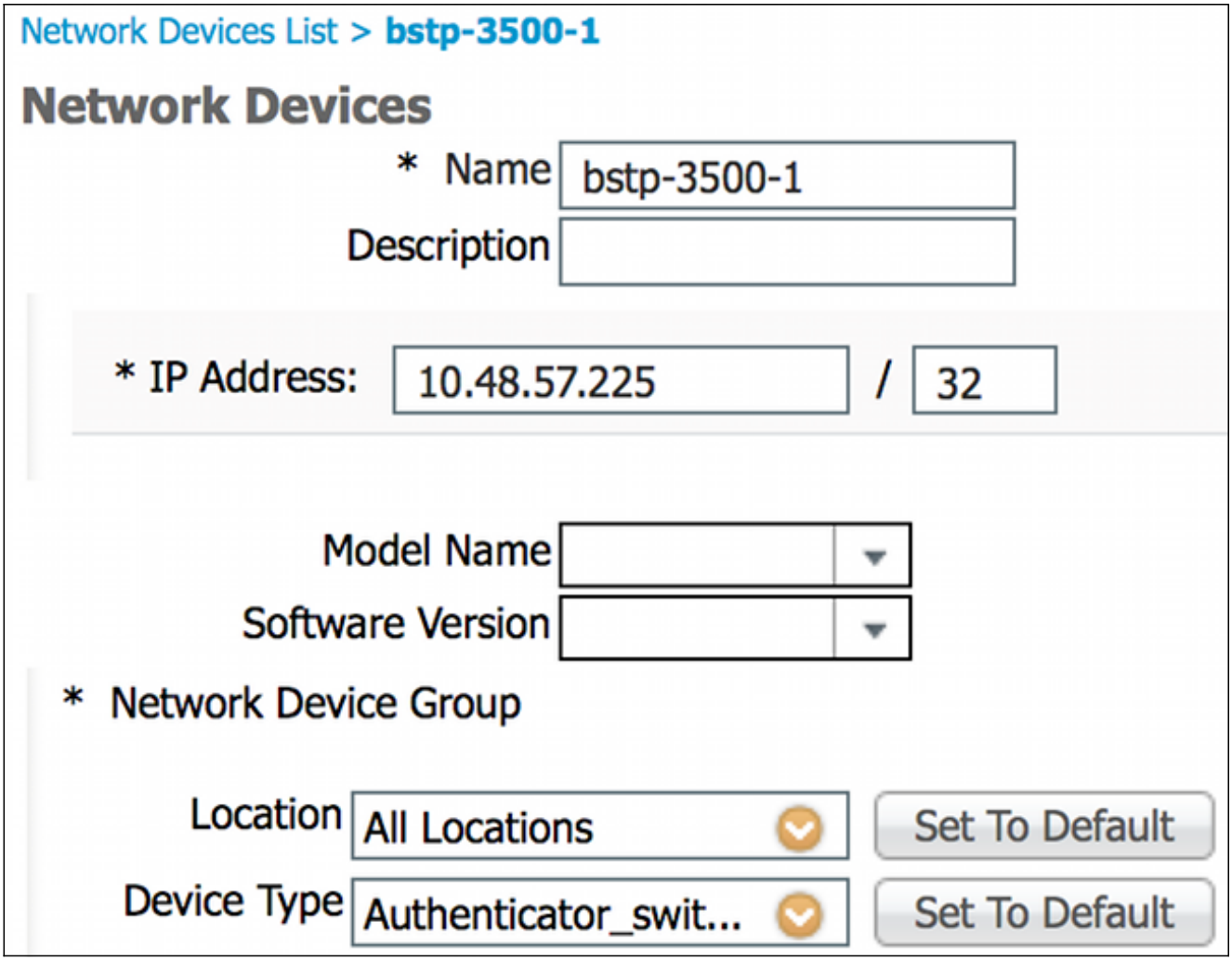
Lorsque l'option NEAT est activée, l'ISE renvoie device-traffic-class=switch dans le cadre de l'autorisation. Cette option est nécessaire afin de changer le mode de port de l'authentificateur de l'accès à l'agrégation.

3. Créez une règle d'autorisation pour utiliser ce profil. Accédez à **Policy > Authorization**, et créez ou mettez à jour une règle.

   Dans cet exemple, un groupe de périphériques spécial appelé Authenticator_switches est créé et tous les demandeurs envoient un nom d'utilisateur commençant par bsnswitch.



4. Ajoutez les commutateurs au groupe approprié. Accédez à **Administration > Network Resources > Network Devices**, et cliquez sur **Add**.



Dans cet exemple, BSTP-3500-1 (l'authentificateur) fait partie du groupe Authenticator_switches ; BSTP-3500-2 (le demandeur) ne doit pas nécessairement faire partie de ce groupe.

Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration. Cette section décrit deux comportements :

- Authentification entre commutateurs
- Authentification entre le PC Windows et le demandeur

Il explique également trois situations supplémentaires :

- Suppression d'un client authentifié du réseau
- Retrait d'un demandeur
- Ports sans dot1x sur un demandeur

Remarques :

L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .

Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Authentification du commutateur demandeur vers le commutateur authentificateur

Dans cet exemple, le demandeur s'authentifie auprès de l'authentificateur. Les étapes du processus sont les suivantes :

1. Le demandeur est configuré et connecté au port fastethernet0/6. L'échange dot1x amène le demandeur à utiliser EAP afin d'envoyer un nom d'utilisateur et un mot de passe préconfigurés à l'authentificateur.
2. L'authentificateur effectue un échange RADIUS et fournit des informations d'identification pour la validation ISE.
3. Si les informations d'identification sont correctes, l'ISE renvoie les attributs requis par la fonction NEAT (device-traffic-class=switch) et l'authentificateur change son mode de port de commutateur, qui passe de l'accès à l'agrégation.

Cet exemple montre l'échange d'informations CISP entre des commutateurs :

```
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
```

Une fois l'authentification et l'autorisation réussies, l'échange CISP a lieu. Chaque échange comporte une REQUÊTE, qui est envoyée par le demandeur, et une RÉPONSE, qui sert de réponse et d'accusé de réception de l'authentificateur.

Deux échanges distincts sont effectués : REGISTRATION et ADD_CLIENT. Lors de l'échange REGISTRATION, le demandeur informe l'authentificateur qu'il est compatible CISP, puis l'authentificateur accuse réception de ce message. L'échange ADD_CLIENT est utilisé pour informer l'authentificateur des périphériques connectés au port local du demandeur. Comme pour l'ENREGISTREMENT, ADD-CLIENT est initié sur le demandeur et reconnu par l'authentificateur.

Entrez ces commandes show afin de vérifier la communication, les rôles et les adresses :

```
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)
```

Dans cet exemple, le rôle d'authentificateur est correctement attribué à l'interface correcte (fa0/6) et deux adresses MAC sont enregistrées. Les adresses MAC sont le demandeur sur le port fa0/6 sur VLAN1 et sur VLAN200.

La vérification des sessions d'authentification dot1x peut maintenant être effectuée. Le port fa0/6 du commutateur en amont est déjà authentifié. Il s'agit de l'échange dot1x qui est déclenché lorsque BSTP-3500-2 (le demandeur) est branché :

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

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

Comme prévu à ce stade, il n'y a pas de séances sur le demandeur :

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

Authentification de PC Windows au commutateur demandeur

Dans cet exemple, le PC Windows s'authentifie auprès du demandeur. Les étapes du processus sont les suivantes :

1. Le PC Windows est connecté au port FastEthernet 0/5 sur BSTP-3500-2 (le demandeur).
2. Le demandeur effectue l'authentification et l'autorisation avec l'ISE.
3. Le demandeur informe l'authentificateur qu'un nouveau client est connecté au port.

Voici la communication du demandeur :

```
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
```

Un échange ADD_CLIENT a lieu, mais aucun échange REGISTRATION n'est nécessaire.

Afin de vérifier le comportement sur le demandeur, entrez la commande **show cisp registrations** :

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

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

Le demandeur a le rôle de demandeur vers l'authentificateur (interface fa0/6) et le rôle d'authentificateur vers le PC Windows (interface fa0/5).

Afin de vérifier le comportement sur l'authentificateur, entrez la commande **show cisp clients** :

```
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
```

Une nouvelle adresse MAC apparaît sur l'authentificateur sous VLAN 200. Il s'agit de l'adresse MAC qui a été observée dans les requêtes AAA sur le demandeur.

Les sessions d'authentification doivent indiquer que le même périphérique est connecté sur le port fa0/5 du demandeur :

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

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

Suppression du client authentifié du réseau

Lorsqu'un client est supprimé (par exemple, si un port est arrêté), l'authentificateur en est informé via l'échange 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
```

Retrait du commutateur demandeur

Lorsqu'un demandeur est débranché ou retiré, l'authentificateur réintroduit la configuration d'origine sur le port afin d'éviter des problèmes de sécurité.

```
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
```

Dans le même temps, le demandeur supprime les clients qui le représentent de la table CISP et désactive le protocole CISP sur cette interface.

Ports sans dot1x sur le commutateur demandeur

Les informations CISP qui sont propagées du demandeur à l'authentificateur servent uniquement d'autre couche d'application. Le demandeur informe l'authentificateur de toutes les adresses MAC autorisées qui lui sont connectées.

Un scénario généralement mal compris est le suivant : si un périphérique est branché sur un port dont dot1x n'est pas activé, l'adresse MAC est apprise et propagée au commutateur en amont via CISP.

L'authentificateur autorise la communication provenant de tous les clients appris via CISP.

Essentiellement, le demandeur a pour rôle de restreindre l'accès aux périphériques, via dot1x ou d'autres méthodes, et de propager l'adresse MAC et les informations VLAN à l'authentificateur. L'authentificateur agit comme un exécuteur des informations fournies dans ces mises à jour.

Par exemple, un nouveau VLAN (VLAN300) a été créé sur les deux commutateurs et un périphérique a été connecté au port fa0/4 du demandeur. Le port fa0/4 est un port d'accès simple qui n'est pas configuré pour dot1x.

Ce résultat du demandeur montre un nouveau port enregistré :

```
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)
```

Sur l'authentificateur, une nouvelle adresse MAC est visible sur le 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
```

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

> **Note**:
>
> L'Outil d'interprétation de sortie (clients enregistrés seulement) prend en charge certaines commandes d'affichage. Utilisez l'Outil d'interprétation de sortie afin de visualiser une analyse de commande d'affichage de sortie .
>
> Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de débogage.

Ces commandes vous aident à dépanner les protocoles NEAT et CISP ; ce document inclut des exemples pour la plupart d'entre elles :

- **debug cisp all** - affiche l'échange d'informations CISP entre les commutateurs.
- **show cisp summary** - affiche un résumé de l'état de l'interface CISP sur le commutateur.
- **show cisp registrations** : indique les interfaces qui participent aux échanges CISP, les rôles de ces interfaces et si les interfaces font partie de NEAT.
- **show cisp clients** - affiche une table des adresses MAC de client connues et leur emplacement (VLAN et interface). Cela est utile principalement à partir de l'authentificateur.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.