Exemple ORDONNÉ de configuration avec le Logiciel Cisco Identity Services Engine

Contenu

Introduction

Ce document décrit la configuration et le comportement de la topologie d'authentification de frontière du réseau (ORDONNÉE) dans un scénario simple. ORDONNÉ utilise les informations de client signalant Protocol (CISP) afin de propager des adresses MAC de client et des informations VLAN entre le suppliant et les Commutateurs d'authentificateur.

Dans cet exemple de configuration, le commutateur d'authentificateur (également appelé l'authentificateur) et le commutateur de suppliant (également appelé le suppliant) exécutent l'authentification de 802.1x ; l'authentificateur authentifie le suppliant, qui, consécutivement, authentifie le PC de test.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de la norme d'authentification de 802.1x

d'IEEE.

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 de Cisco IOS®, version 12.2(55)SE8 ; un commutateur agit en tant qu'authentificateur, et l'autre agit en tant que suppliant.
- Logiciel Cisco Identity Services Engine (ISE), version 1.2.
- PC avec Microsoft Windows XP, Service Pack 3.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Configurez

Cet exemple couvre des configurations d'échantillon pour :

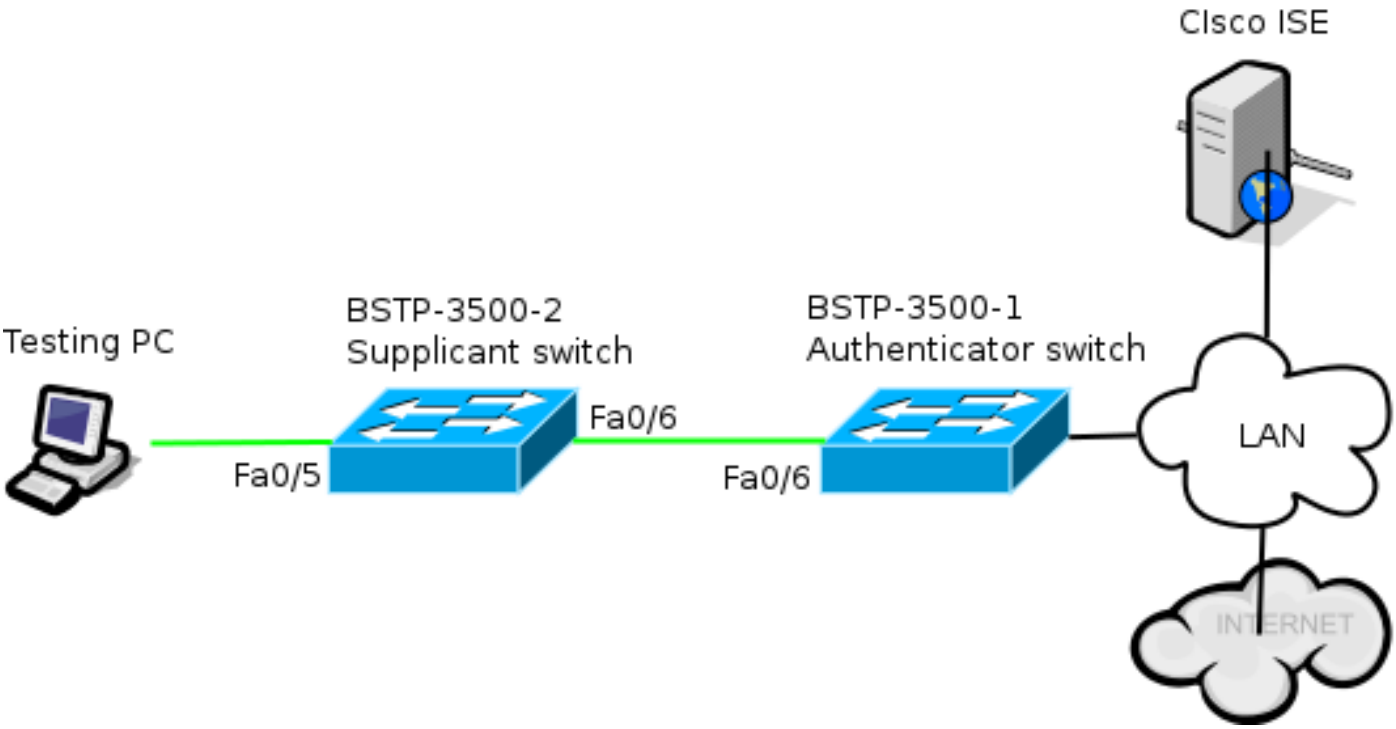
- Commutateur d'authentificateur
- Commutateur de suppliant
- Cisco ISE

Les configurations sont le perfom nécessaire par minimum cet exercice pratique ; ils ne pourraient pas être optimaux pour ou accomplir d'autres besoins.

> Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce schéma de réseau montre la Connectivité utilisée dans cet exemple. Les lignes noires indiquent la Connectivité logique ou physique, et les lignes vertes indiquent des liens authentifiés par l'utilisation du 802.1x.



Configuration de commutateur d'authentificateur

L'authentificateur contient les éléments de base requis pour le dot1x. Dans cet exemple, les commandes qui sont spécifiques à ORDONNÉ ou les CISP sont bolded.

C'est la configuration de base d'Authentification, autorisation et comptabilité (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 est activé globalement, et le port de interconnexion est configuré dans l'authentificateur et le mode d'accès.

Configuration de commutateur de suppliant

Il est cruciale pour que l'installation entière fonctionne configuration précise de suppliant comme prévue. Cet exemple de configuration contient un AAA et une configuration typiques de dot1x.

C'est la configuration de base d'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 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 suppliant devrait avoir configuré des qualifications et devrait fournir une méthode de Protocole EAP (Extensible Authentication Protocol) à utiliser.

Le suppliant peut utiliser le Digest 5 d'Eap-message (MD5) et l'authentification Eap-flexible par l'intermédiaire du protocole sécurisé (JEÛNEZ) (entre d'autres types d'EAP) pour l'authentification en cas de CISP. Afin de garder la configuration ISE à un minimum, cet exemple utilise EAP-MD5 pour l'authentification du suppliant à l'authentificateur. (Le par défaut forcerait l'utilisation de l'EAP-FAST, qui exige le ravitaillement du laisser-passer de Protected Access [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 suppliant à l'authentificateur est déjà configurée pour être un port de joncteur réseau (contrairement à la configuration de port d'accès sur l'authentificateur). À ce stade, ceci est prévu ; la configuration changera dynamiquement quand l'ISE renvoie 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 pour la référence seulement.

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

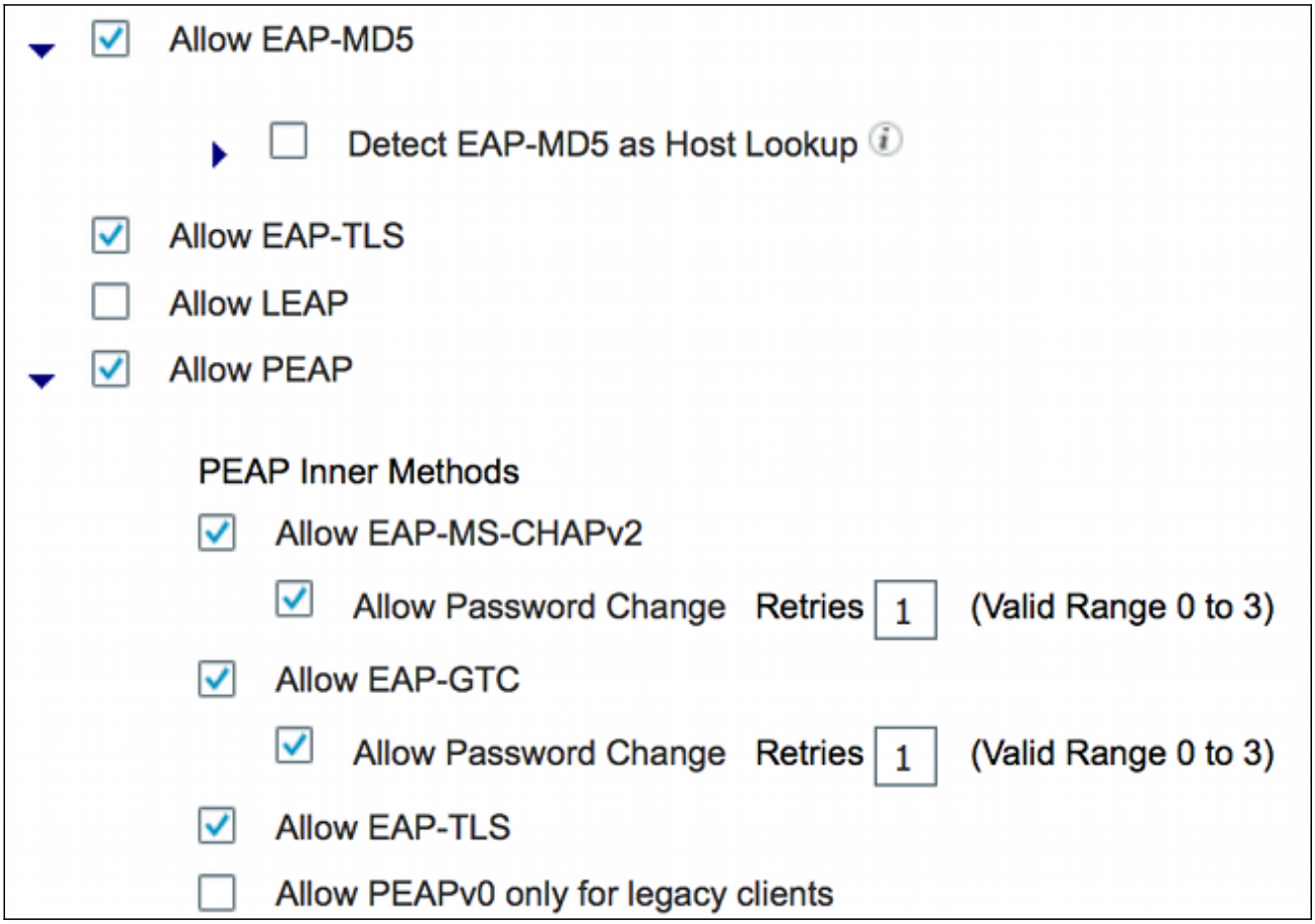
Configuration ISE

Cette procédure décrit comment installer une configuration de base ISE.

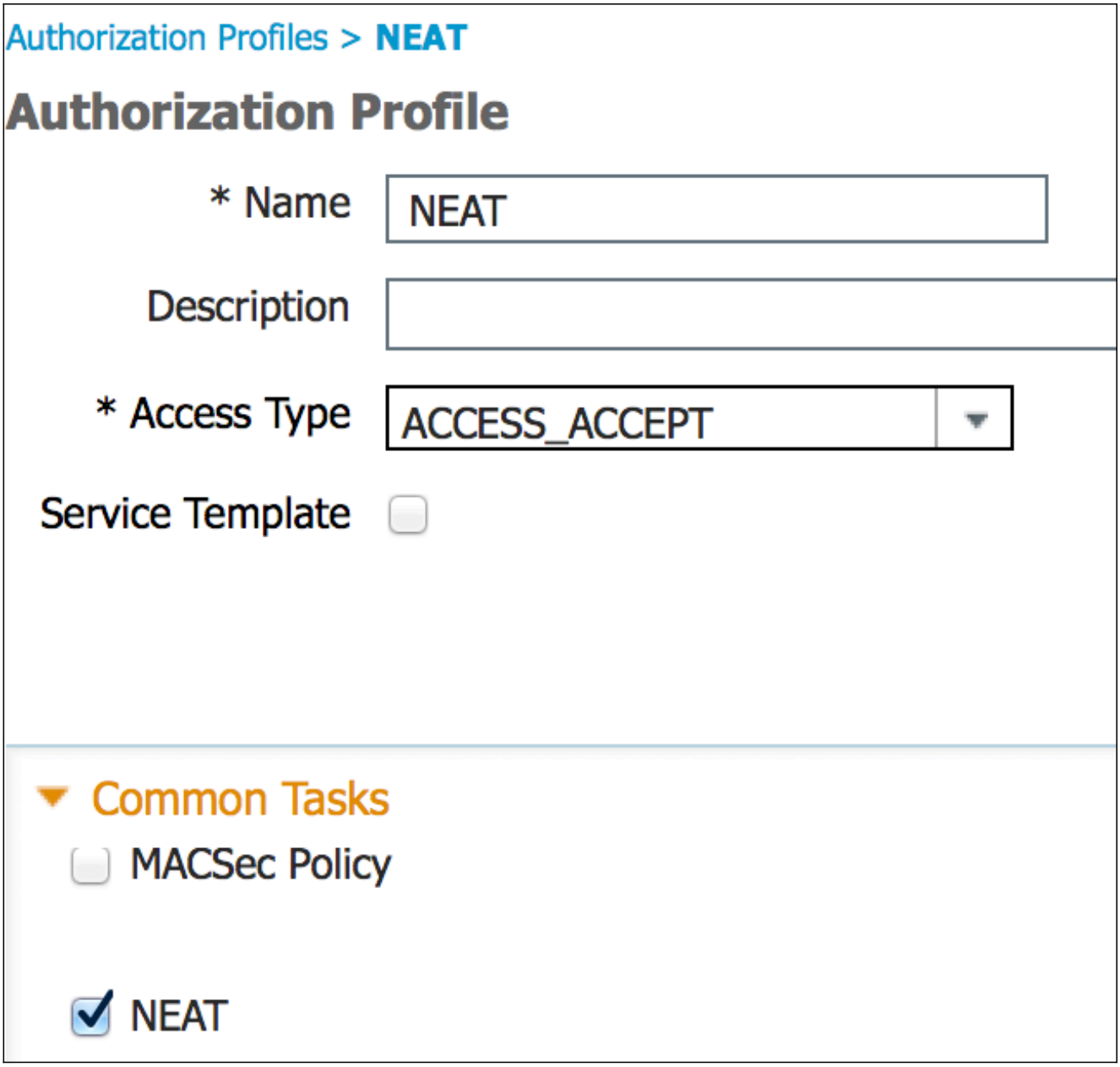
1. Activez les Protocoles d'authentification requis.

   Dans cet exemple, le dot1x de câble permet à EAP-MD5 pour authentifier le suppliant à l'authentificateur et permet au Protected Extensible Authentication Protocol (PEAP) - la version 2 (MSCHAPv2) de Microsoft Challenge Handshake Authentication Protocol pour authentifier le PC Windows au suppliant.

   Naviguez vers la **stratégie > les résultats > l'authentification > des protocoles permis**, sélectionnez la **liste de service de protocole** utilisée par dot1x de câble, et l'assurez que les protocoles dans cette étape sont activés.



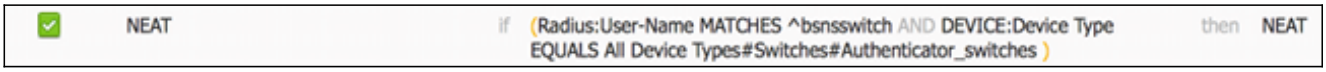
2. Créez une stratégie d'autorisation. Naviguez vers la **stratégie > les résultats > l'autorisation > la stratégie d'autorisation**, et créez ou mettez à jour une stratégie ainsi elle contient ORDONNÉ comme un attribut retourné. C'est un exemple d'une telle stratégie :



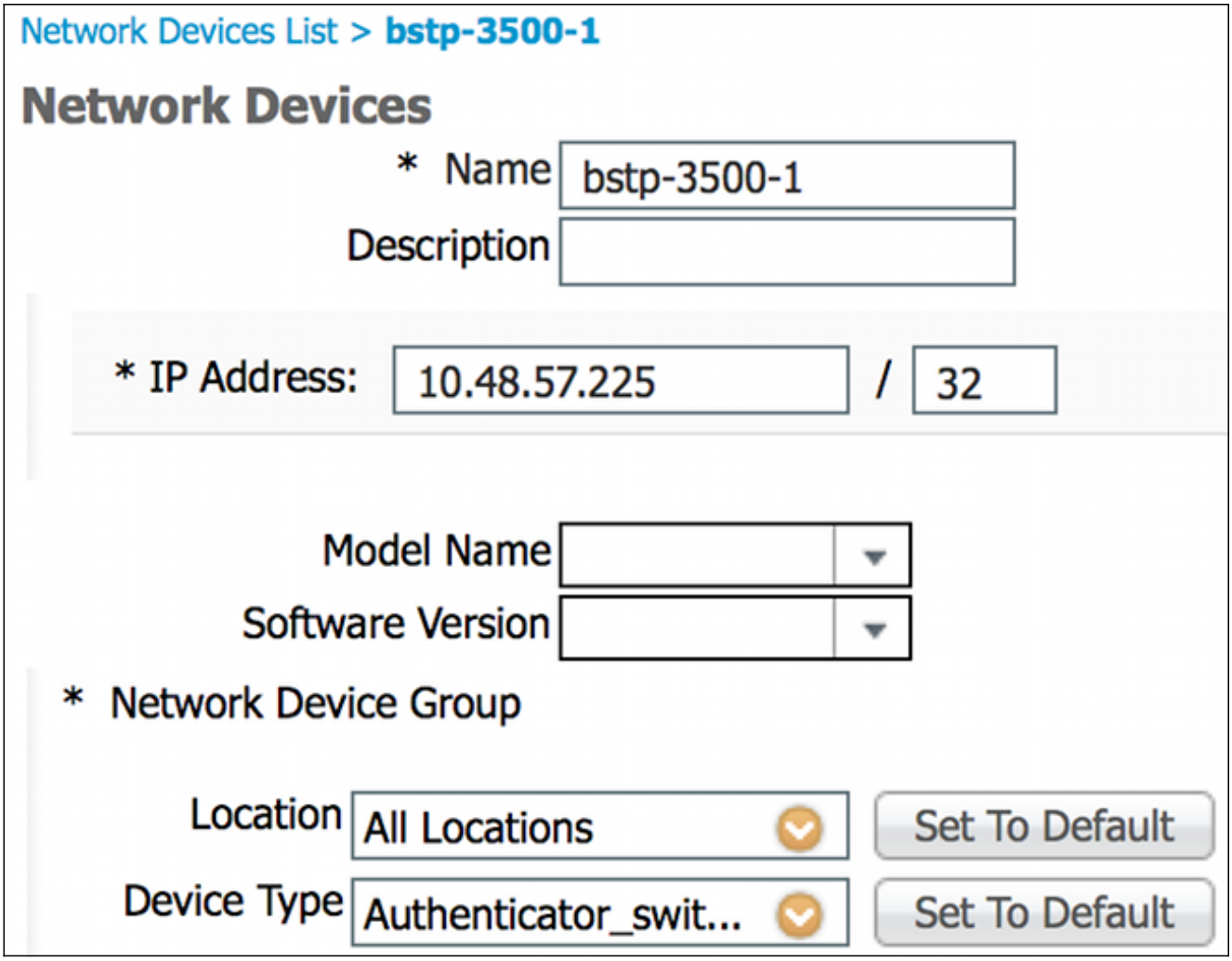
Quand l'option ORDONNÉE est activée, l'ISE renvoie le device-traffic-class=switch en tant qu'élément de l'autorisation. Cette option est nécessaire afin de changer le mode de port de l'authentificateur de l'accès au joncteur réseau.

3. Créez une règle d'autorisation d'utiliser ce profil. Naviguez vers la **stratégie > l'autorisation**, et créez ou mettez à jour une règle.

   Dans cet exemple, un groupe d'engin spécial appelé Authenticator_switches est créé, et tous les suppliants envoient un nom d'utilisateur qui commence par le bsnsswitch.



4. Ajoutez les Commutateurs au groupe approprié. Naviguez vers la **gestion > les ressources de réseau > les périphériques de réseau**, et cliquez sur Add.



Dans cet exemple, BSTP-3500-1 (l'authentificateur) fait partie de groupe d'Authenticator_switches ; BSTP-3500-2 (le suppliant) n'a pas besoin de faire partie de ce groupe.

Vérifiez

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

- Authentification entre les Commutateurs
- Authentification entre le PC Windows et le suppliant

Il explique également trois situations supplémentaires :

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

Remarques :

L'Output Interpreter Tool (clients enregistrés seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

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

Authentification de commutateur de suppliant au commutateur d'authentificateur

Dans cet exemple, le suppliant authentifie à l'authentificateur. Les étapes dans le processus sont :

1. Le suppliant est configuré et branché au port fastethernet0/6. L'échange de dot1x fait employer le suppliant l'EAP afin d'envoyer un nom d'utilisateur et mot de passe préconfiguré à l'authentificateur.
2. L'authentificateur exécute un échange de RAYON et fournit des qualifications pour la validation ISE.
3. Si les qualifications sont correctes, l'ISE renvoie des attributs exigés par ORDONNÉ (device-traffic-class=switch), et l'authentificateur change son mode de switchport de l'accès au joncteur réseau.

Cet exemple affiche l'échange des informations CISP entre les 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 que l'authentification et l'autorisation réussissent, l'échange CISP se produit. Chaque échange a une DEMANDE, qui est envoyée par le suppliant, et une RÉPONSE, qui sert de

réponse et d'accusé de réception de l'authentificateur.

Deux échanges distincts sont exécutés : ENREGISTREMENT et ADD_CLIENT. Pendant l'échange d'ENREGISTREMENT, le suppliant informe l'authentificateur qu'il est CISP-capable, et l'authentificateur puis reconnaît ce message. L'échange ADD_CLIENT est utilisé pour informer l'authentificateur au sujet des périphériques connectés au port local du suppliant. Comme avec l'ENREGISTREMENT, ADD-CLIENT est initié sur le suppliant et reconnu par l'authentificateur.

Sélectionnez ces commandes show afin de vérifier la transmission, 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 de l'authentificateur est correctement assigné à l'interface appropriée (fa0/6), et deux adresses MAC sont enregistrées. Les adresses MAC sont le suppliant sur le port fa0/6 sur VLAN1 et sur VLAN200.

La vérification des sessions d'authentification de dot1x peut maintenant être exécutée. Le port fa0/6 sur le commutateur en amont est déjà authentifié. C'est l'échange de dot1x qui est déclenché quand BSTP-3500-2 (le suppliant) est branché dans :

```
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)
```

Comme prévu à ce stade, il n'y a aucune session sur le suppliant :

```
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)
```

Authentification de PC Windows au commutateur de suppliant

Dans cet exemple, le PC Windows authentifie au suppliant. Les étapes dans le processus sont :

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

C'est la transmission du suppliant :

```
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 se produit, mais aucun échange d'ENREGISTREMENT n'est nécessaire.

Afin de vérifier le comportement sur le suppliant, sélectionnez la commande d'**enregistrements de cisp d'exposition** :

```
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
```

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

Afin de vérifier le comportement sur l'authentificateur, sélectionnez la commande de **clients de cisp d'exposition** :

```
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. C'est l'adresse MAC qui a été observée dans des demandes d'AAA sur le suppliant.

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

```
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 de client authentifié de réseau

Quand un client est retiré (par exemple, si un port est arrêté), on annonce l'authentificateur par 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
```

Suppression de commutateur de suppliant

Quand un suppliant est débranché ou retiré, l'authentificateur introduit la configuration d'origine de nouveau au 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
```

En même temps, le suppliant retire les clients qui représentent le suppliant de la table CISP et

désactive CISP sur cette interface.

Ports sans dot1x sur le commutateur de suppliant

Les informations CISP qui sont propagées du suppliant à l'authentificateur servent seulement d'une autre couche d'application. Le suppliant informe l'authentificateur au sujet de toutes les adresses MAC permises qui sont connectées à lui.

Un scénario qui est typiquement mal compris est ceci : si un périphérique est branché sur un port qui n'a pas le dot1x activé, l'adresse MAC est apprise et propagée au commutateur en amont par CISP.

L'authentificateur permet la transmission qui provient tous les clients appris par CISP.

Essentiellement, c'est le rôle du suppliant pour limiter l'accès des périphériques, par le dot1x ou d'autres méthodes, et pour propager l'adresse MAC et les informations VLAN à l'authentificateur. L'authentificateur agit en tant qu'autorité des informations fournie dans ces mises à jour.

Comme exemple, un nouveau VLAN (VLAN300) a été créé sur les deux Commutateurs, et un périphérique a été branché au port fa0/4 sur le suppliant. Le port fa0/4 est un port d'accès simple qui n'est pas configuré pour le dot1x.

Cette sortie du suppliant affiche un nouveau port enregistré :

```
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
```

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

Dépannez

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

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

Ces commandes vous aident à dépanner ORDONNÉ et CISP ; ce document comporte des exemples pour la plupart d'entre elles :

- **mettez au point le cisp** affiche **entièrement l'**échange des informations CISP entre les Commutateurs.
- **affichez le résumé de cisp** - affiche un résumé de l'état d'interface CISP sur le commutateur.
- **affichez les enregistrements de cisp** - indique les interfaces qui participent aux échanges CISP, les rôles de ces interfaces, et si les interfaces font partie d'ORDONNÉ.
- **affichez les clients de cisp** - affiche une table des adresses MAC connues de client et de leur emplacement (VLAN et interface). C'est utile principalement de l'authentificateur.