Ejemplo de configuración ASEADO con el Cisco Identity Services Engine

Contenido

Introducción

Este documento describe la configuración y el comportamiento de la topología de la autenticación del borde de la red (ASEADA) en un simple escenario. ASEADO utiliza la información del cliente que señala el protocolo (CISP) para propagar los MAC Address del cliente y la información de VLAN entre el supplicant y el Switches del authenticator.

En este ejemplo de configuración, ambos el Switch del authenticator (también llamado el authenticator) y Switch del supplicant (también llamado el supplicant) realizan la autenticación del 802.1x; el authenticator autentica el supplicant, que, a su vez, autentica el PC de prueba.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento del estándar de la autenticación del IEEE 802.1X.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dos Cisco Catalyst 3560 Series Switch con el Cisco IOS ® Software, versión 12.2(55)SE8; un Switch actúa como authenticator, y el otro actúa como supplicant.
- Cisco Identity Services Engine (ISE), versión 1.2.
- PC con el Microsoft Windows XP, Service Pack 3.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configurar

Este ejemplo cubre las configuraciones de muestra para:

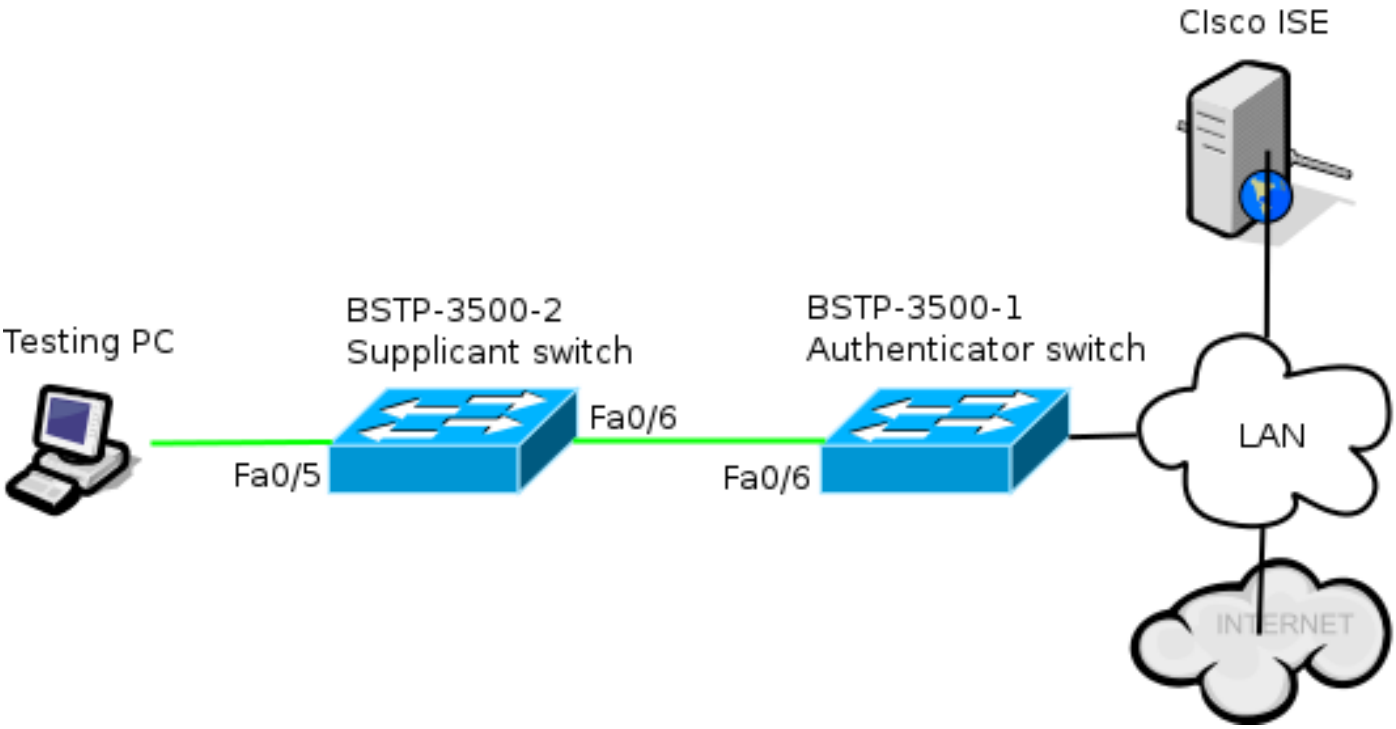
- Switch del authenticator
- Switch del supplicant
- Cisco ISE

Las configuraciones son para el perfom necesario mínimo este ejercicio del laboratorio; puede ser que no sean óptimas para ni satisfagan otras necesidades.

> Nota: Use la Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos usados en esta sección.

Diagrama de la red

Este diagrama de la red ilustra la Conectividad usada en este ejemplo. Las líneas negras indican lógico o conectividad física, y las líneas verdes indican los links autenticados con el uso del 802.1x.



Configuración del switch del authenticator

El authenticator contiene los elementos básicos necesarios para el dot1x. En este ejemplo, los comandos que son específicos a ASEADO o CISP son enes negrita.

Ésta es la autenticación básica, la autorización, y la configuración de las estadísticas (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 se habilita global, y el puerto de interconexión se configura en el authenticator y el modo de acceso.

Configuración del switch del supplicant

La configuración exacta del supplicant es crucial para que la configuración entera trabaje como se esperaba. Este ejemplo de configuración contiene una configuración típica AAA y del dot1x.

Ésta es la configuración AAA básica:

```
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
```

El supplicant debe haber configurado las credenciales y debe suministrar un método del Protocolo de Autenticación Extensible (EAP) que se utilizará.

El supplicant puede utilizar la publicación de mensaje EAP 5 (MD5) y la autenticación adaptable de EAP vía el protocolo seguro (RÁPIDO) (entre otros tipos EAP) para la autenticación en caso de CISP. Para guardar la configuración ISE a un mínimo, este ejemplo utiliza el EAP-MD5 para la autenticación del supplicant al authenticator. (El valor por defecto forzaría el uso del EAP-FAST, que requiere la disposición credencial protegida del [PAC] del acceso; este documento no cubre ese escenario.)

```
! 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 conexión del supplicant al authenticator se configura ya para ser un puerto troncal (en contraste con la configuración del puerto de acceso en el authenticator). En esta etapa, se espera esto; la configuración cambiará dinámicamente cuando el ISE vuelve el atributo correcto.

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

El puerto que conecta con el PC de Windows tiene una configuración mínima y se muestra aquí para la referencia solamente.

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

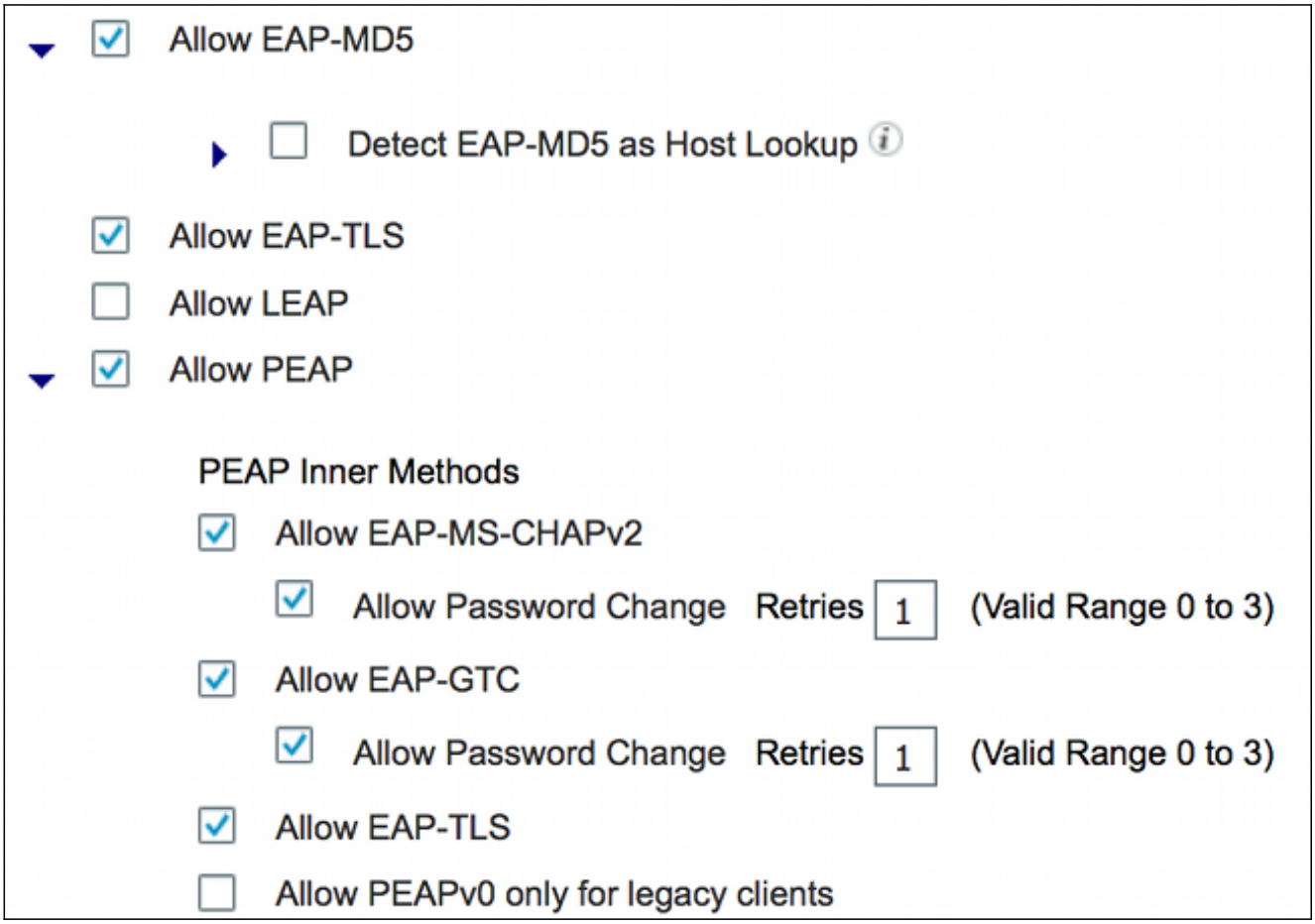
Configuración ISE

Este procedimiento describe cómo configurar una configuración básica ISE.

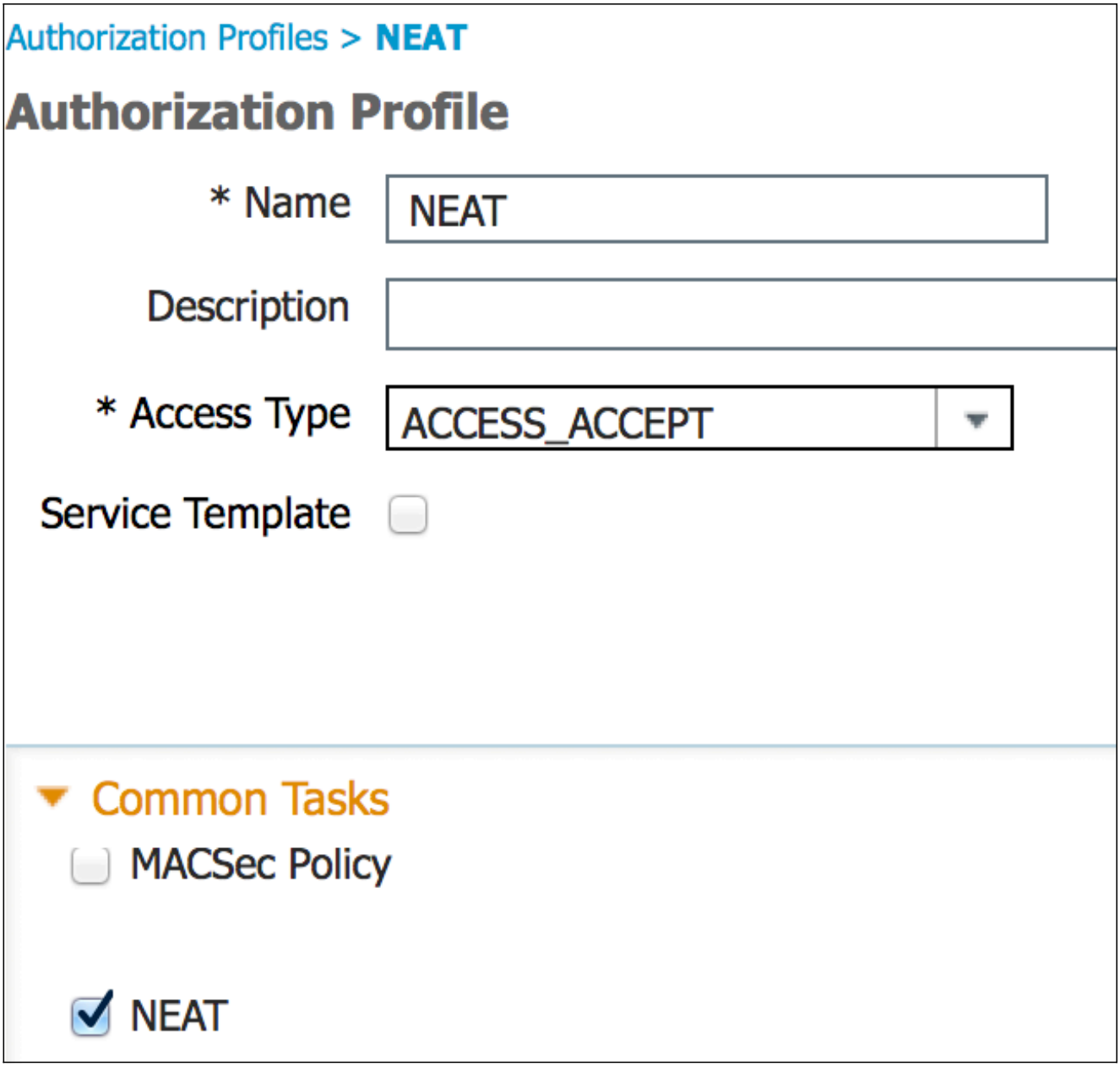
1. Habilite los protocolos de autenticación necesaria.

   En este ejemplo, el dot1x atado con alambre permite el EAP-MD5 autentique el supplicant al authenticator y permite que el protocolo extensible authentication protegido (PEAP) - protocolo microsoft challenge handshake authentication versión 2 (MSCHAPv2) autentique el PC de Windows al supplicant.

   Navegue a la **directiva > a los resultados > a la autenticación > los protocolos permitidos**, seleccione la **lista del servicio del protocolo** usada por el dot1x atado con alambre, y asegúrese que los protocolos en este paso están habilitados.



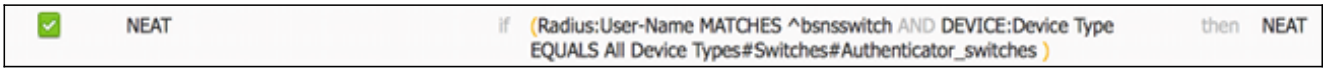
2. Cree una directiva de la autorización. Navegue a la **directiva > a los resultados > a la autorización > a la directiva de la autorización**, y cree o ponga al día una directiva así que contiene ASEADO como un atributo vuelto. Éste es un ejemplo de tal directiva:



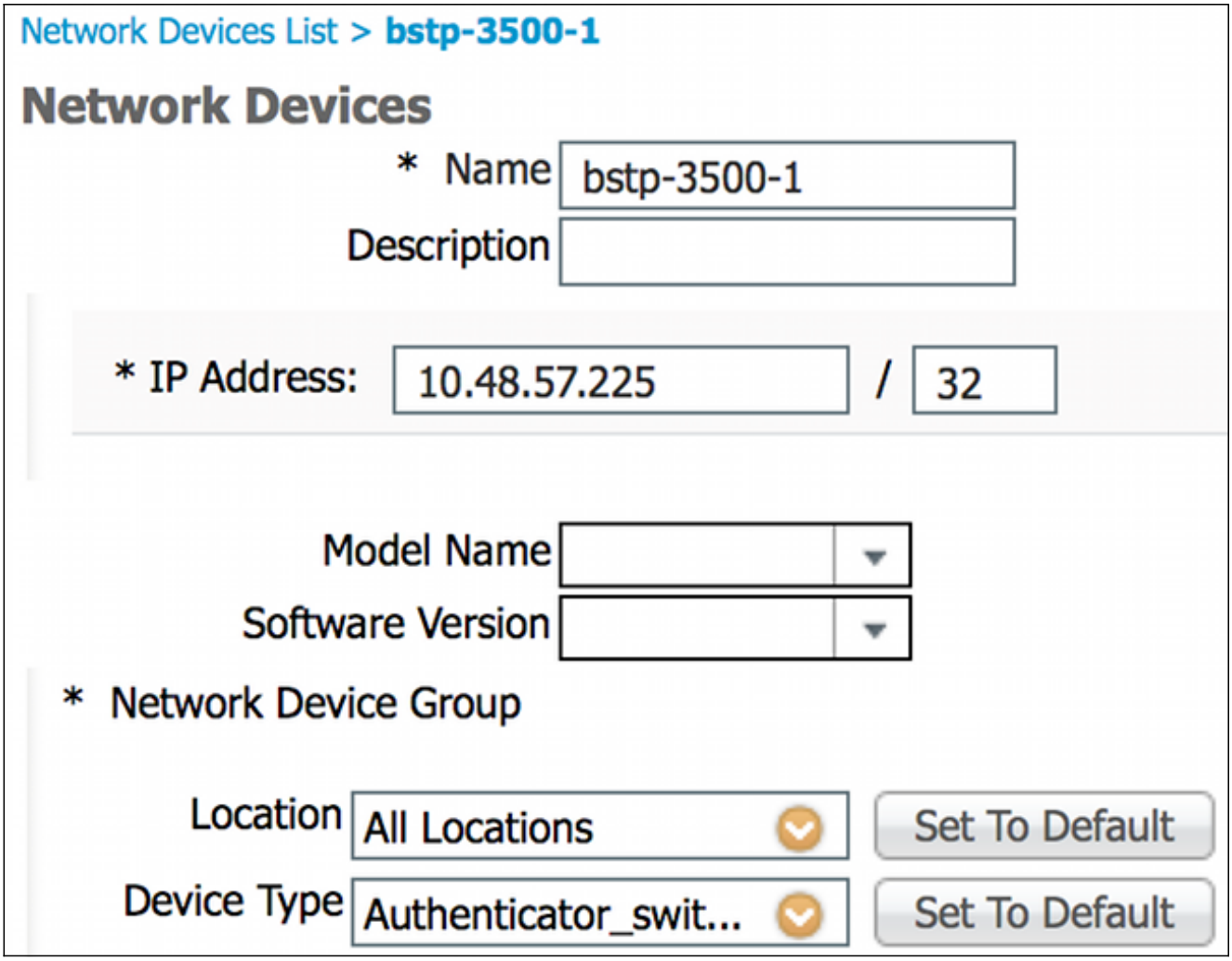
Cuando se gira la opción ASEADA, el ISE vuelve el device-traffic-class=switch como parte de la autorización. Esta opción es necesaria para cambiar al modo de puerto del authenticator del acceso al trunk.

3. Cree una regla de la autorización para utilizar este perfil. Navegue a la **directiva > a la autorización**, y cree o ponga al día una regla.

   En este ejemplo, crean a un grupo de dispositivos especial llamado Authenticator_switches, y todos los suplicantes envían un nombre de usuario que comience con el bsnsswitch.



4. Agregue el Switches al grupo apropiado. Navegue a la **administración > a los recursos de red > a los dispositivos de red**, y el haga click en Add



En este ejemplo, BSTP-3500-1 (el authenticator) es grupo de Authenticator_switches de la parte de; BSTP-3500-2 (el supplicant) no necesita ser parte de este grupo.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente. Esta sección describe dos comportamientos:

- Autenticación entre el Switches
- Autenticación entre el PC de Windows y el supplicant

También explica tres situaciones adicionales:

- Retiro de un cliente autenticado de la red
- Retiro de un supplicant
- Puertos sin el dot1x en un supplicant

Notas:

Los ciertos comandos show de los soportes de la herramienta del Output Interpreter (clientes registrados solamente). Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.

Consulte Información Importante sobre Comandos de Debug antes de usar un **comando**

debug.

Autenticación del Switch del supplicant al Switch del authenticator

En este ejemplo, el supplicant autentica al authenticator. Los pasos en el proceso son:

1. El supplicant se configura y está conectado en el puerto fastethernet0/6. El intercambio del dot1x hace el supplicant utilizar el EAP para enviar un nombre de usuario y contraseña preconfigurado al authenticator.
2. El authenticator realiza un intercambio RADIUS y proporciona las credenciales para la validación ISE.
3. Si las credenciales están correctas, el ISE vuelve los atributos requeridos por ASEADO (device-traffic-class=switch), y el authenticator cambia su modo del switchport del acceso al trunk.

Este ejemplo muestra el intercambio de la información CISP entre el 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
```

Una vez que la autenticación y autorización tiene éxito, el intercambio CISP ocurre. Cada intercambio tiene una PETICIÓN, que es enviada por el supplicant, y una RESPUESTA, que sirve como una contestación y acuse de recibo del authenticator.

Se realizan dos intercambios distintos: REGISTRO y ADD_CLIENT. Durante el intercambio del REGISTRO, el supplicant informa al authenticator que es CISP-capaz, y el authenticator después reconoce este mensaje. El intercambio ADD_CLIENT se utiliza para informar al authenticator sobre los dispositivos conectados con el puerto local del suplicante. Como con el REGISTRO, ADD-CLIENT se inicia en el supplicant y es reconocido por el authenticator.

Ingrese estos comandos show para verificar la comunicación, los papeles, y los direccionamientos:

```
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)
```

En este ejemplo, el papel del authenticator se asigna correctamente a la interfaz correcta (fa0/6), y se registran dos direcciones MAC. Las direcciones MAC son el supplicant en el puerto fa0/6 en el VLAN1 y en VLAN200.

La verificación de las sesiones de la autenticación del dot1x puede ahora ser realizada. El puerto fa0/6 en el Switch por aguas arriba se autentica ya. Éste es el intercambio del dot1x se acciona que cuando BSTP-3500-2 (el supplicant) está conectado en:

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

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

Como se esperaba en esta etapa, no hay sesiones sobre el supplicant:

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

Autenticación del PC de Windows al Switch del supplicant

En este ejemplo, el PC de Windows autentica al supplicant. Los pasos en el proceso son:

1. El PC de Windows está conectado en el FastEthernet 0/5 puerto en BSTP-3500-2 (el supplicant).
2. El supplicant realiza la autenticación y autorización con el ISE.
3. El supplicant informa al authenticator que un nuevo cliente está conectado en el puerto.

Ésta es la comunicación del supplicant:

```
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 intercambio ADD_CLIENT ocurre, pero no hay intercambio del REGISTRO necesario.

Para verificar el comportamiento en el supplicant, ingrese el comando de los **registros del cisp de la demostración**:

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

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

El supplicant tiene el papel de un supplicant hacia el authenticator (interfaz fa0/6) y el papel de un authenticator hacia el PC de Windows (interfaz fa0/5).

Para verificar el comportamiento en el authenticator, ingrese el comando de los **clientes del cisp de la demostración**:

```
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
```

Una nueva dirección MAC aparece en el authenticator bajo el VLA N 200. Es la dirección MAC que fue observada en las peticiones AAA en el supplicant.

Las sesiones de la autenticación deben indicar que el mismo dispositivo está conectado en el puerto fa0/5 de supplicant:

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

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

Retiro del cliente autenticado de la red

Cuando quitan a un cliente (por ejemplo, si se apaga un puerto), el authenticator se notifica con el intercambio 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
```

Retiro del Switch del supplicant

Cuando se desenchufa o se quita un supplicant, el authenticator introduce la configuración de origen de nuevo al puerto para evitar los problemas de seguridad.

```
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
```

Al mismo tiempo, el supplicant quita a los clientes que representan el supplicant de la tabla CISP y desactiva CISP en esa interfaz.

Puertos sin el dot1x en el Switch del supplicant

La información CISP que se propaga del supplicant al authenticator sirve solamente como otra capa de aplicación. El supplicant informa al authenticator sobre todas las direcciones MAC permitidas que estén conectadas con él.

Un escenario que se entiende mal típicamente es éste: si un dispositivo está conectado en un puerto que no tenga dot1x habilitado, la dirección MAC es docta y propagada al Switch por aguas arriba con CISP.

El authenticator permite la comunicación que viene de todos los clientes aprendidos con CISP.

Esencialmente, es el papel del supplicant para restringir el acceso de los dispositivos, con el dot1x u otros métodos, y para propagar la dirección MAC y la información de VLAN al authenticator. El authenticator actúa como guardián de la información proporcionado en esas actualizaciones.

Como un ejemplo, un nuevo VLA N (VLAN300) fue creado en ambo Switches, y un dispositivo fue conectado en el puerto fa0/4 en el supplicant. El puerto fa0/4 es un puerto de acceso simple que no se configura para el dot1x.

Esta salida del supplicant muestra un nuevo puerto registrado:

```
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)
```

En el authenticator, una nueva dirección MAC es visible en el VLA N 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
```

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

> Nota:
>
> La herramienta del Output Interpreter (clientes registrados solamente) apoya los ciertos comandos show. Utilice la herramienta del Output Interpreter para ver una análisis de la salida del comando show.
>
> Consulte Información Importante sobre Comandos de Debug antes de usar un **comando debug**.

Estos comandos help usted resuelve problemas ASEADO y CISP; este documento incluye los ejemplos para la mayor parte de ellos:

- **cisp todo del debug** - muestra el intercambio de la información CISP entre el Switches.
- **muestre el resumen del cisp** - visualiza un resumen del estatus de la interfaz CISP en el Switch.
- **muestre los registros del cisp** - indica las interfaces que participan en los intercambios CISP, el papeles de esas interfaces, y si las interfaces son parte de ASEADA.
- **muestre a los clientes del cisp** - visualiza una tabla de direcciones MAC del cliente conocido y de su ubicación (VLA N y interfaz). Esto es útil principalmente del authenticator.