Cisco Identity Services Engine의 깔끔한 구성 예

목차

소개

이 문서에서는 간단한 시나리오에서 NEAT(Network Edge Authentication Topology)의 컨피그레이션 및 동작에 대해 설명합니다. NEAT는 CISP(Client Information Signaling Protocol)를 사용하여 신청자와 인증자 스위치 간에 클라이언트 MAC 주소와 VLAN 정보를 전파합니다.

이 컨피그레이션 예에서는 인증자 스위치(인증자라고도 함)와 신청자 스위치(신청자라고도 함)가 모두 802.1x 인증을 수행합니다. 인증자는 신청자를 인증하고, 이는 테스트 PC를 인증합니다.

사전 요구 사항

요구 사항

IEEE 802.1x 인증 표준에 대해 알고 있는 것이 좋습니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco IOS® Software, Release 12.2(55)SE8을 사용하는 Cisco Catalyst 3560 Series 스위치 2개, 스위치 1개는 인증자 역할을 하고 나머지 1개는 신청자 역할을 합니다.
- Cisco ISE(Identity Services Engine), 릴리스 1.2.
- Microsoft Windows XP, 서비스 팩 3이 설치된 PC.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

이 예에서는 다음에 대한 샘플 컨피그레이션을 다룹니다.

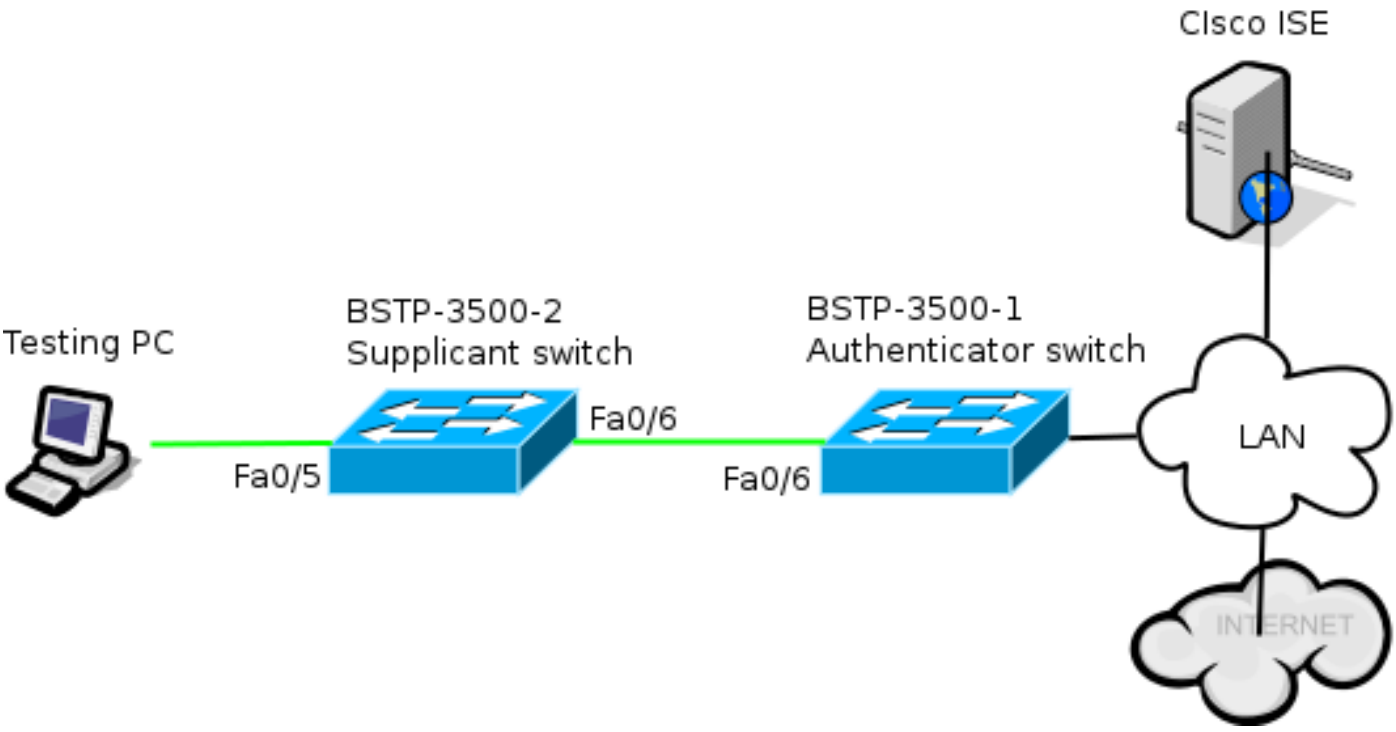
- 인증자 스위치
- 서플리컨트 스위치
- Cisco ISE

이 구성은 이 실습을 수행하기 위해 필요한 최소 구성이며, 다른 요구 사항을 충족하거나 충족하지 못할 수 있습니다.

> **참고**: 이 섹션에서 사용된 명령에 대한 자세한 내용을 보려면 Command Lookup Tool(등록된 고객만 해당)을 사용하십시오.

네트워크 다이어그램

이 네트워크 다이어그램은 이 예에서 사용된 연결을 보여줍니다. 검은색 선은 논리적 또는 물리적 연결을 나타내고, 녹색 선은 802.1x를 사용하여 인증된 링크를 나타냅니다.



인증자 스위치 컨피그레이션

인증자에는 dot1x에 필요한 기본 요소가 포함되어 있습니다. 이 예제에서는 NEAT 또는 CISP에 특정한 명령을 굵게 표시합니다.

기본 AAA(Authentication, Authorization, and Accounting) 컨피그레이션입니다.

```
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
```

CISP는 전역적으로 활성화되며, 상호 연결 포트는 인증자 및 액세스 모드로 구성됩니다.

신청자 스위치 컨피그레이션

전체 설정이 예상대로 작동하려면 정확한 신청자 컨피그레이션이 중요합니다. 이 예제 컨피그레이션에는 일반적인 AAA 및 dot1x 컨피그레이션이 포함되어 있습니다.

다음은 기본 AAA 컨피그레이션입니다.

```
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
```

신청자는 자격 증명을 구성해야 하며 사용할 EAP(Extensible Authentication Protocol) 방법을 제공해야 합니다.

신청자는 CISP의 경우 인증에 EAP-MD5(Message Digest 5) 및 EAP-FAST(Flexible Authentication via Secure Protocol)(다른 EAP 유형 중)를 사용할 수 있습니다. ISE 컨피그레이션을 최소한으로 유지하기 위해 이 예에서는 인증자에 대한 신청자 인증에 EAP-MD5를 사용합니다. (기본값은

PAC(Protected Access Credential) 프로비저닝을 필요로 하는 EAP-FAST를 강제로 사용하는 것입니다. 이 문서에서는 이 시나리오를 다루지 않습니다.)

```
! 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
```

인증자에 대한 신청자의 연결이 이미 트렁크 포트로 구성되어 있습니다(인증자의 액세스 포트 컨피그레이션과 반대). 이 단계에서는 이 작업이 필요합니다. ISE에서 올바른 특성을 반환하면 컨피그레이션이 동적으로 변경됩니다.

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

Windows PC에 연결되는 포트는 최소 구성이며 참조용으로만 여기에 표시됩니다.

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

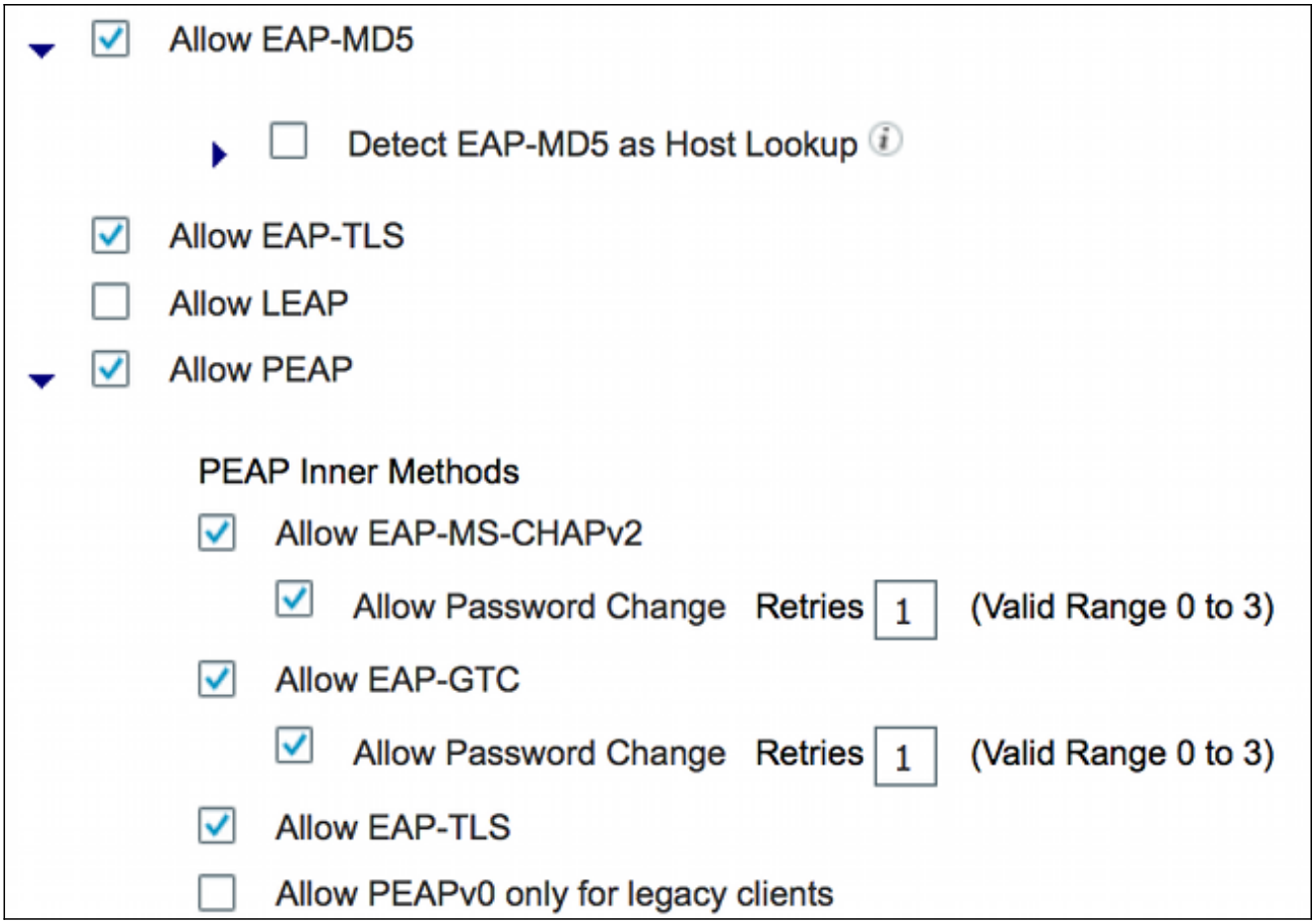
ISE 구성

이 절차에서는 기본 ISE 컨피그레이션을 설정하는 방법에 대해 설명합니다.

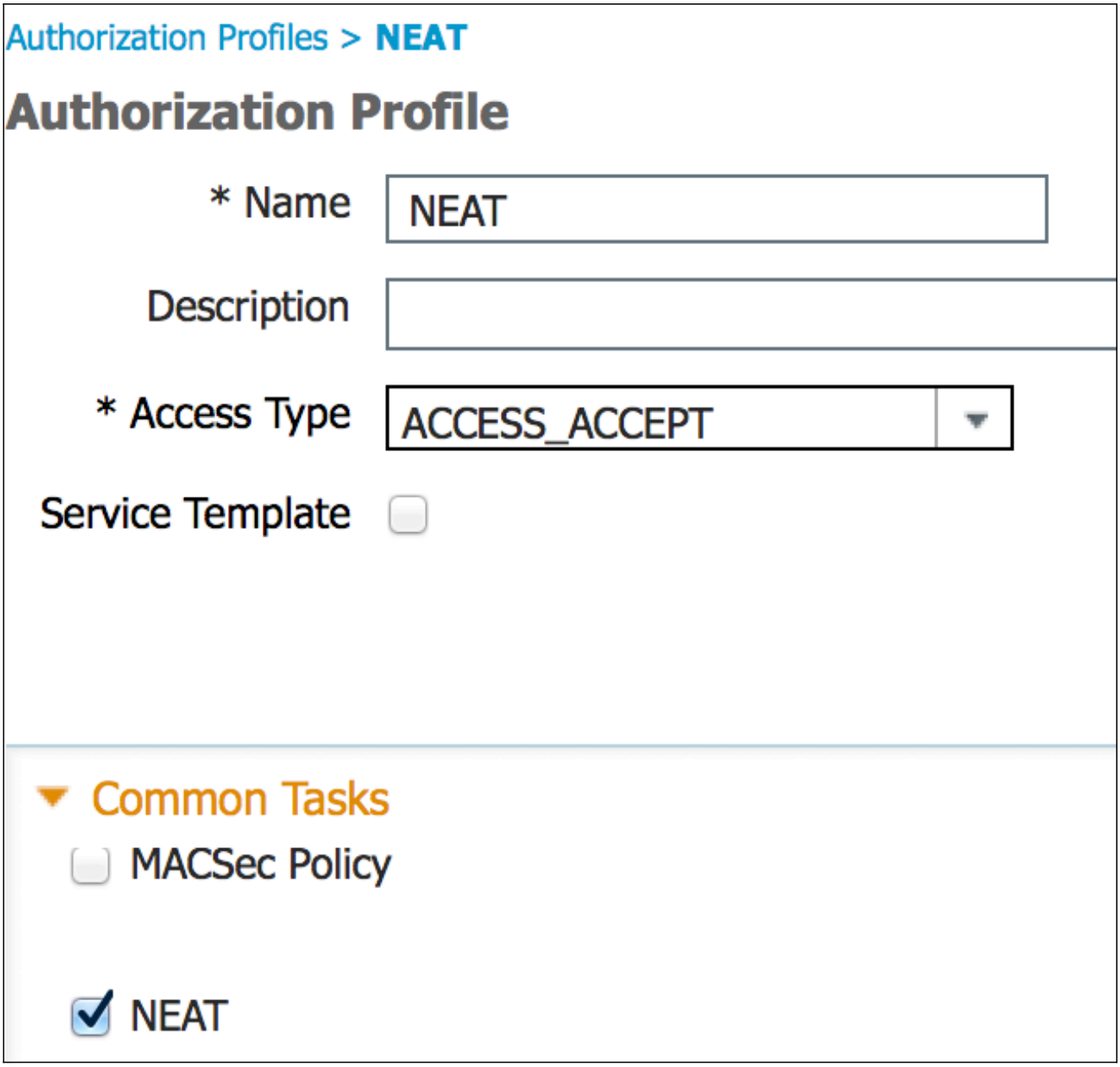
1. 필요한 인증 프로토콜을 활성화합니다.

   이 예에서 유선 dot1x는 EAP-MD5가 인증자에게 신청자를 인증하고 PEAP(Protected Extensible Authentication Protocol)-MSCHAPv2(Microsoft Challenge Handshake Authentication Protocol Version 2)가 신청자에게 Windows PC를 인증하도록 허용합니다.

   Policy(정책) > Results(결과) > Authentication(인증) > Allowed protocols(허용되는 프로토콜)로 이동하고 유선 dot1x에서 사용하는 **프로토콜 서비스 목록**을 선택하고 이 단계의 프로토콜이 활성화되어 있는지 확인합니다.



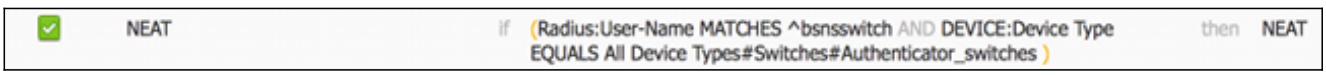
2. 권한 부여 정책을 생성합니다. Policy(**정책) > Results(결과) > Authorization(권한 부여) > Authorization Policy(권한 부여 정책)**로 이동하고 반환된 특성으로 NEAT를 포함하도록 정책을 생성하거나 업데이트합니다. 다음은 그러한 정책의 예입니다.



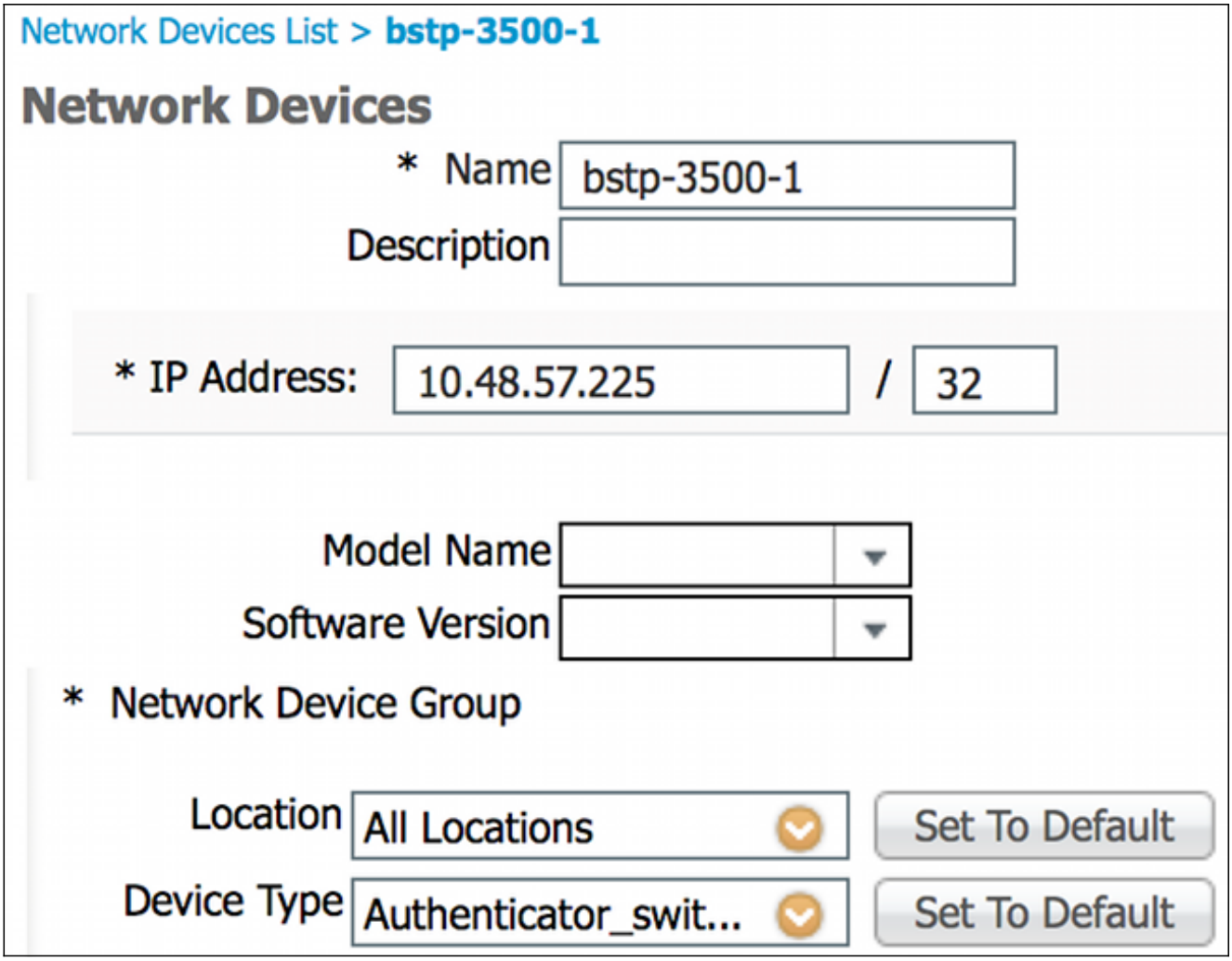
NEAT 옵션이 켜지면 ISE는 권한 부여의 일부로 device-traffic-class=switch를 반환합니다. 인증자의 포트 모드를 액세스에서 트렁크로 변경하려면 이 옵션이 필요합니다.

3. 이 프로파일을 사용하려면 권한 부여 규칙을 만듭니다. **Policy(정책) > Authorization(권한 부여)**으로 이동하고 규칙을 생성하거나 업데이트합니다.

   이 예에서는 Authenticator_switches라는 특수 디바이스 그룹이 생성되고 모든 신청자가 bsnswitch로 시작하는 사용자 이름을 보냅니다.



4. 스위치를 적절한 그룹에 추가합니다. Administration(**관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)**로 이동하고 Add(추가)**를 클릭합니다**.



이 예에서 BSTP-3500-1(인증자)은 Authenticator_switches 그룹의 일부입니다. BSTP-3500-2(신청자)는 이 그룹의 일부가 될 필요가 없습니다.

다음을 확인합니다.

설정이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오. 이 섹션에서는 두 가지 동작에 대해 설명합니다.

- 스위치 간 인증
- Windows PC와 신청자 간의 인증

또한 다음과 같은 세 가지 추가 상황도 설명합니다.

- 네트워크에서 인증된 클라이언트 제거
- 서플리컨트 제거
- 서 플리 컨 트의 dot1x 없는 포트

참고:

아웃풋 인터프리터 툴(등록 고객 전용)은 특정 show 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

debug 명령을 사용하기 전에 debug 명령에 대한 중요한 정보를 참조하십시오.

인증자 스위치에 서 플리 컨 트 스위치 인증

이 예에서 신청자는 인증자에게 인증합니다. 프로세스의 단계는 다음과 같습니다.

1. 신청자가 구성되어 포트 fastethernet0/6에 연결됩니다. dot1x 교환은 신청자가 인증자에게 미리 구성된 사용자 이름 및 비밀번호를 보내기 위해 EAP를 사용하도록 합니다.
2. 인증자는 RADIUS 교환을 수행하고 ISE 검증을 위한 자격 증명을 제공합니다.
3. 자격 증명이 올바르면 ISE는 NEAT(device-traffic-class=switch)에 필요한 특성을 반환하고 인증자는 스위치 포트 모드를 액세스에서 트렁크로 변경합니다.

다음 예에서는 스위치 간 CISP 정보 교환을 보여줍니다.

```
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
```

인증 및 권한 부여가 성공하면 CISP 교환이 발생합니다. 각 교환에는 신청자가 보낸 REQUEST와 인증자의 응답 및 확인 응답 역할을 하는 RESPONSE가 있습니다.

REGISTRATION과 ADD_CLIENT라는 두 가지 서로 다른 교환이 수행됩니다. REGISTRATION 교환 과정에서 신청자는 인증자에게 CISP를 사용할 수 있음을 알리고 인증자는 이 메시지를 승인합니다. ADD_CLIENT 교환은 신청자의 로컬 포트에 연결된 장치에 대해 인증자에게 알리는 데 사용됩니다. REGISTRATION과 마찬가지로, ADD-CLIENT는 신청자에서 시작되고 인증자가 승인합니다.

통신, 역할 및 주소를 확인하려면 다음 show 명령을 입력합니다.

```
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)
```

이 예에서는 인증자의 역할이 올바른 인터페이스(fa0/6)에 올바르게 할당되고 두 개의 MAC 주소가 등록됩니다. MAC 주소는 VLAN1 및 VLAN200의 fa0/6 포트에 있는 신청자입니다.

이제 dot1x 인증 세션의 확인을 수행할 수 있습니다. 업스트림 스위치의 fa0/6 포트는 이미 인증되었습니다. BSTP-3500-2(신청자)가 연결될 때 트리거되는 dot1x 교환입니다.

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

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

이 단계에서 예상한 대로 신청자에 세션이 없습니다.

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

서 플리 컨 트 스위치에 Windows PC 인증

이 예에서 Windows PC는 신청자에 대해 인증합니다. 프로세스의 단계는 다음과 같습니다.

1. Windows PC가 BSTP-3500-2(신청자)의 FastEthernet 0/5 포트에 연결됩니다.
2. 신청자는 ISE와 인증 및 권한 부여를 수행합니다.
3. 신청자는 인증자에게 새 클라이언트가 포트에 연결되었음을 알립니다.

이것은 서 플리 컨 트의 통신 입니다.

```
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
```

ADD_CLIENT 교환이 발생하지만 REGISTRATION 교환이 필요하지 않습니다.

신청자에 대한 동작을 확인하려면 **show** cisp **registrations 명령을** 입력합니다.

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

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

신청자에는 인증자에 대한 신청자 역할(fa0/6 인터페이스)과 Windows PC에 대한 인증자 역할(fa0/5 인터페이스)이 있습니다.

인증자에 대한 동작을 확인하려면 show cisp clients **명령을** 입력합니다.

```
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
```

VLAN 200 아래의 인증자에 새 MAC 주소가 나타납니다. 신청자의 AAA 요청에서 관찰된 MAC 주소입니다.

인증 세션은 동일한 디바이스가 신청자의 fa0/5 포트에 연결되어 있음을 나타내야 합니다.

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

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

네트워크에서 인증된 클라이언트 제거

클라이언트가 제거되면(예: 포트가 종료된 경우) 인증자는 DELETE_CLIENT 교환을 통해 알림을 받습니다.

```
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
```

서 플리 컨 트 스위치 제거

신청자가 플러그를 뽑거나 제거되면 인증자는 보안 문제를 방지하기 위해 원래 컨피그레이션을 다시 포트에 도입합니다.

```
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
```
동시에 신청자는 신청자를 나타내는 클라이언트를 CISP 테이블에서 제거하고 해당 인터페이스에서 CISP를 비활성화합니다.

서 플리 컨 트 스위치에 dot1x 없는 포트

신청자에서 인증자로 전파되는 CISP 정보는 또 다른 시행 레이어로만 사용됩니다. 신청자는 인증자에게 연결된 모든 허용된 MAC 주소에 대해 알립니다.

일반적으로 잘못 이해되는 시나리오는 다음과 같습니다. 장치가 dot1x가 활성화되지 않은 포트에 연결되어 있으면 MAC 주소가 학습되어 CISP를 통해 업스트림 스위치에 전파됩니다.

인증자는 CISP를 통해 학습된 모든 클라이언트에서 오는 통신을 허용합니다.

본질적으로, dot1x 또는 다른 방법을 통해 디바이스의 액세스를 제한하고 MAC 주소 및 VLAN 정보를 인증자에게 전파하는 것은 신청자의 역할입니다. 인증자는 이러한 업데이트에서 제공되는 정보의 적용자 역할을 합니다.

예를 들어, 두 스위치 모두에서 새 VLAN(VLAN300)이 생성되었으며, 디바이스가 신청자의 포트 fa0/4에 연결되었습니다. 포트 fa0/4는 dot1x에 대해 구성되지 않은 단순 액세스 포트입니다.

서 플리 컨 트의 이 출력은 새 등록 된 포트를 보여줍니다.

```
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)
```
인증자의 경우 VLAN 300에 새 MAC 주소가 표시됩니다.

```
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
```

문제 해결

이 섹션에서는 설정 문제 해결에 사용할 수 있는 정보를 제공합니다.

참고:

아웃풋 인터프리터 툴(등록 고객 전용)은 특정 show 명령을 지원합니다. **show** 명령 출력의 분석을 보려면 아웃풋 인터프리터 툴을 사용합니다.

debug 명령을 사용하기 전에 debug 명령에 대한 중요한 정보를 참조하십시오.

이러한 명령은 NEAT 및 CISP 문제를 해결하는 데 도움이 됩니다. 이 문서에는 대부분의 예가 포함되어 있습니다.

- **debug cisp all** - 스위치 간의 CISP 정보 교환을 표시합니다.
- **show cisp summary** - 스위치의 CISP 인터페이스 상태에 대한 요약을 표시합니다.
- **show cisp registrations** - CISP 교환에 참여하는 인터페이스, 해당 인터페이스의 역할 및 인터페이스가 NEAT의 일부인지 여부를 나타냅니다.
- **show cisp clients** - 알려진 클라이언트 MAC 주소와 그 위치(VLAN 및 인터페이스) 테이블을 표시합니다. 이 기능은 주로 인증자에게 유용합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.