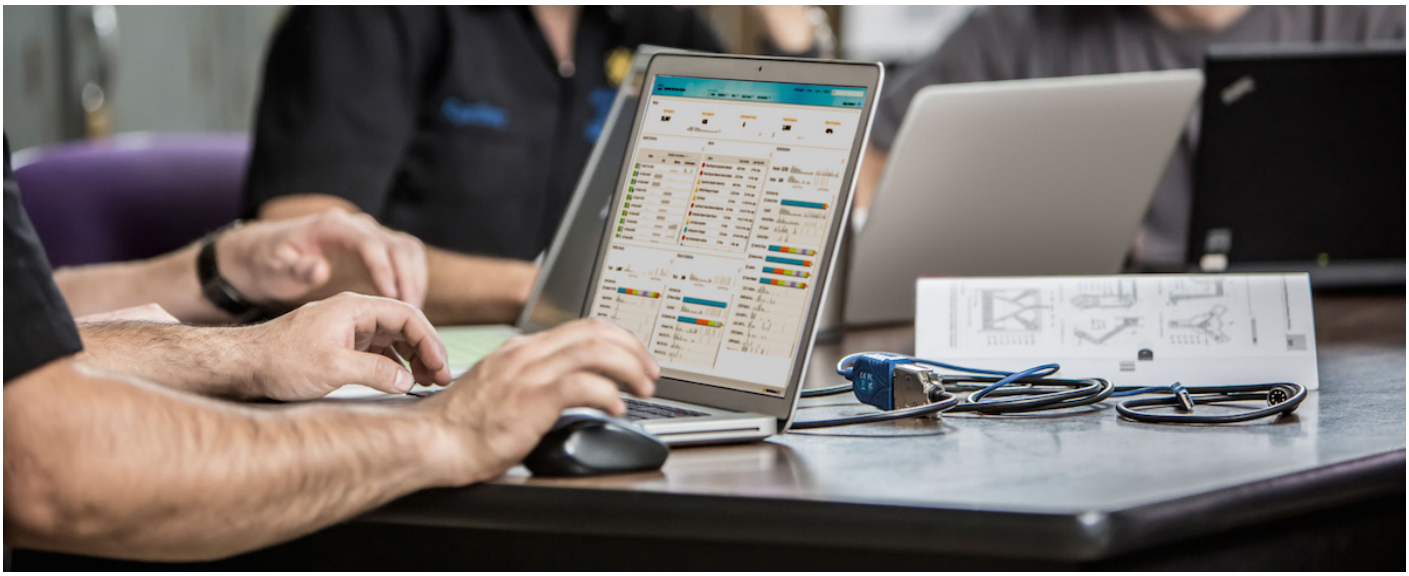


Cisco Identity Services Engine의 범용 스위치 컨피그레이션

보안 액세스 방법 가이드 시리즈

작성자: Hosuk Won

날짜: 2016년 1월

목차

소개

Cisco Identity Services Engine이란?

Cisco ISE(Identity Services Engine)는 포괄적이고 안전한 유선, 무선 및 VPN(Virtual Private Networking) 액세스를 가능하게 하는 올인원 엔터프라이즈 정책 제어 제품입니다.

Cisco ISE는 하나의 RADIUS 기반 제품에서 종합적으로 정책을 관리하고 시행할 수 있는 중앙 집중식 제어 포인트를 제공합니다. Cisco ISE의 고유한 아키텍처를 통해 기업은 네트워크, 사용자 및 디바이스로부터 실시간 상황 정보를 수집할 수 있습니다. 그러면 관리자는 능동적인 거버넌스 결정을 내리는 데 해당 정보를 사용할 수 있습니다. Cisco ISE는 Cisco Secure Access의 내부 구성 요소입니다.

Cisco Secure Access는 네트워크 인프라에 통합된 고급 NAC(Network Access Control) 및 ID 솔루션입니다. 이는 완전히 테스트되고 검증된 솔루션으로, 솔루션 내의 모든 구성 요소는 통합 시스템으로 엄격하게 테스트되며 철저하게 조사됩니다.

Cisco Catalyst 스위치

오버레이 NAC(Network Access Control) 솔루션과 달리 Cisco Secure Access는 시행을 위해 액세스 레이어 디바이스(스위치, 무선 컨트롤러 등)를 활용합니다. 흔히 어플라이언스 및 기타 오버레이 디바이스로 처리되었던 웹 인증을 위한 URL 리디렉션 등의 기능을 이제는 액세스 디바이스가 자체적으로 처리합니다.

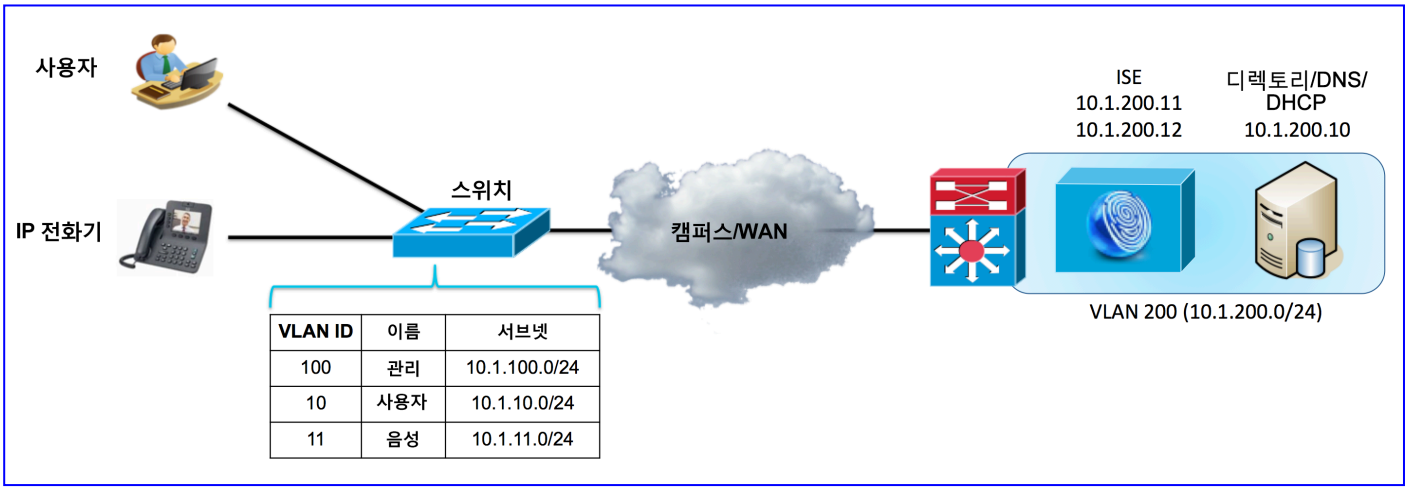
Cisco Secure Access에는 IEEE 802.1X 및 VLAN 제어와 같은 표준 기반 ID 및 시행 모델이 결합되어 있을 뿐 아니라 다양한 고급 ID 및 시행 기능도 포함되어 있습니다. 이러한 기능으로는 유연한 인증, dACL(Downloadable Access Control Lists), SGT(Security Group Tagging), 디바이스 프로파일링, 게스트 및 웹 인증 서비스, 보안 상태 평가 및 네트워크 액세스 전과 도중에 모바일 디바이스의 컴플라이언스 검증을 위한 업계 최고의 MDM(Mobile Device Management) 벤더와의 통합 등이 있습니다.

문서 정보

이 문서에서는 Cisco Identity Services Engine과의 통합을 위한 Cisco Catalyst 스위치에서의 모범 사례 컨피그레이션을 제공합니다. 이 문서의 주요 섹션은 세 부분으로 나뉘어 있습니다. 전역 컨피그레이션은 모니터/로우-임팩트 및 폐쇄 모드 단계 구축에 모두 적용됩니다. 두 가지 인터페이스 컨피그레이션이 제공되는데, 그 중 첫 번째는 모니터/로우-임팩트 모드 컨피그레이션이고 두 번째는 폐쇄 모드 인터페이스 컨피그레이션입니다. '선택 사항'으로 표시된 컨피그레이션은 ISE 통합 측면에서는 필수적이지 않지만 특정 사용자 환경을 다룰 때는 중요한 컨피그레이션입니다. 여기에는 RADIUS 서버 장애 중 인터페이스 행동과 HTTPS 트래픽에 대한 URL 리디렉션 처리가 포함됩니다.

아래 다이어그램은 구성 요소의 전반적인 레이아웃을 보여줍니다. 여기에는 액세스 VLAN 2개가 있는데 그 중 하나는 직원 사용자용 액세스 VLAN이고 다른 하나는 IP 전화기용 음성 VLAN입니다. 관리 VLAN은 스위치가 관리 사용자 및 ISE 노드와 통신하는 데 사용됩니다. 이 문서에는 BYOD, Posture Assessment, 프로파일링 등 ISE에 대한 정책 컨피그레이션은 포함되어 있지 않지만, 여기서 제공하는 컨피그레이션은 그러한 작업에 대한 기준을 제공할 수 있습니다.

그림 1 구성 요소



또한 부록에는 최소한으로만 수정하여 복사한 다음 붙여 넣을 수 있는 샘플 컨피그레이션이 있습니다.

컨피그레이션

전역 컨피그레이션

이 컨피그레이션에서는 이중화를 위해 ISE PSN 노드 2개가 정의됩니다. 또한 스위치에서 연결할 수 있는 ISE 노드가 없을 때는 중요 권한 부여 기능을 사용하여 네트워크 액세스를 허용합니다.

참고: IOS 및 IOS XE 버전에 따라 여기에 나와 있는 일부 명령은 기본적으로 활성화될 수 있습니다.

1 단계 기본적으로 시스템에는 명령이 필요합니다. https 리디렉션을 활성화할 때는 도메인 이름이 필요합니다.

```
SWITCH(config)#ip domain-name EXAMPLE.COM
```

2 단계 (선택 사항) 이 'RADIUS-TEST' 어카운트는 ISE용 RADIUS 테스트 메시지를 생성하는 데 사용됩니다.

```
SWITCH(config)#username RADIUS-TEST password 0 PASSWORD
```

참고: 사용자 이름과 비밀번호는 ISE 내 ID 데이터베이스에서 유효한 어카운트일 필요는 없습니다. ISE 노드가 성공한 인증에 대해 ACCESS-ACCEPT를 다시 보내든, 장애가 발생한 인증에 대해 ACCESS_REJECT를 다시 보내든 관계없이 스위치는 두 응답을 모두 RADIUS 데드 설정에 대한 라이브 서버의 유효한 응답으로 간주합니다. 그러나 MS Active Directory 또는 LDAP와 같은 외부 ID 저장소에서 유효한 어카운트를 제공하는 것이 좋습니다. 그러면 스위치가 백엔드 ID 저장소까지 전체 경로를 테스트할 수 있으며, ISE 노드가 외부 ID 데이터베이스에 연결되어 있는지를 확인할 수 있습니다.

3 단계 (선택 사항) HTTPS 서비스에 사용할 키를 생성합니다.

```
SWITCH(config)#crypto key generate rsa general-keys mod 2048
```

참고: 키를 생성하기 전에 'ip http secure-server' 명령을 실행하지 마십시오. 명령을 잘못된 순서로 수행하면 스위치가 더 작은 키 크기를 가지는 인증서를 자동으로 생성합니다. 이 인증서를 사용하면 HTTPS 트래픽을 리디렉션할 때 원치 않은 동작이 발생할 수 있습니다.

4 단계 AAA를 활성화합니다.

```
SWITCH(config)#aaa new-model
```

5 단계 정의된 RADIUS 서버를 사용하도록 네트워크 인증을 활성화합니다.

```
SWITCH(config)#aaa authentication dot1x default group ISE
```

6 단계 802.1x로 인증된 세션에 대해 url-redirect, dVLAN(Dynamic VLAN) 및 dACL(Downloadable ACL)과 같은 네트워크 권한 부여를 활성화합니다.

```
SWITCH(config)#aaa authorization network default group ISE
```

7 단계 세션이 시작 및 정지될 때마다 NAD에서 ISE로 계정 관리 정보를 보냅니다.

```
SWITCH(config)#aaa accounting dot1x default start-stop group ISE
```

8 단계 NAD의 활성화된 세션도 ISE에서 유지 보수되도록 새 업데이트가 있는 경우 및 2일마다 계정 관리 업데이트를 보냅니다.

```
SWITCH(config)#aaa accounting update newinfo periodic 2880
```

참고: 세션이 아직 그대로 유지되고 있음을 알리기 위해 중간 RADIUS 계정 관리 메시지가 ISE로 전송됩니다. ISE는 지정된 엔드포인트에 대해 장시간 RADIUS 계정 관리 메시지를 수신하지 못하면 세션 테이블에서 해당 세션을 제거합니다. ISE는 스위치에서 엔드포인트를 제거하지는 않으므로, 활성화된 세션 측면에서 ISE와 스위치 간의 연결이 끊어집니다. 이러한 연결 끊김은 어떤 이유에서든 엔드포인트 액세스를 재평가해야 할 때도 영향을 줄 수 있습니다. 기본적으로 ISE는 인증된 모든 세션에 대해 5일 동안 중간 RADIUS 계정 관리 메시지가 없는 세션을 지웁니다. 스위치가 5일 이내에 ISE 노드로 주기적인 RADIUS 계정 관리 메시지를 전송하여 ISE에서 세션이 유지 보수되도록 합니다. 여기서 2일은 RADIUS 계정 관리 패킷 중 하나가 ISE 노드에 도달하지 못한 경우 5일 이내에 2개의 업데이트를 제공하기 위한 것입니다.

9 단계 이를 통해 NAD가 ISE로부터의 CoA 요청을 수락하도록 구성됩니다. 이 NAD가 CoA에 대한 요청을 보내는 PSN도 추가하는 것이 좋습니다. 이는 BYOD(NSP), 포스처, CWA, MDM 등의 ISE 고급 활용 사례에 필요합니다.

```
SWITCH(config)#aaa server radius dynamic-author
SWITCH(config-locsvr-da-radius)# client 10.1.200.11 server-key RADIUS_KEY
SWITCH(config-locsvr-da-radius)# client 10.1.200.12 server-key RADIUS_KEY
```

10 단계 NAD는 클라이언트에 대해 서로 다른 인증 방법 간에 공통 세션 ID를 사용합니다. 이 세션 ID는 보고, CoA 및 ISE 세션 관리용으로 사용됩니다.

```
SWITCH(config)#aaa session-id common
```

11 단계 (선택 사항) 이 선택적 명령은 같은 스위치에 있는 다른 포트에 동일 MAC 주소에 대한 기존 세션이 있을 때 포트에서 새 세션을 허용합니다. 이는 관리되지 않는 허브 또는 스위치를 사용 중이거나 엔드 유저가 서드파티 IP 전화기를 사용 중인 경우 유용합니다.

```
SWITCH(config)#authentication mac-move permit
```

참고: 이 기능은 관리되지 않는 스위치/허브 또는 서드파티 IP 전화기를 사용 중인 환경에서 특히 유용합니다. 이러한 유형의 디바이스를 사용 중인 경우에는 인증된 디바이스가 하나의 인터페이스에서 다른 인터페이스로 이동할 때 Catalyst 스위치가 충분한 알림을 받지 못하므로 스위치가 액세스를 거부할 수 있습니다. 이 명령을 사용하면 디바이스가 처음 확인된 시점부터 스위치가 원래 세션을 분할할 수 있으며, 디바이스는 같은 스위치의 다른 인터페이스에서 인증할 수 있습니다. 이는 Cisco IP 전화기의 경우 필요하지 않습니다. Cisco IP 전화기는 전화기 뒤의 디바이스 연결이 끊기면 CDP 메시지를 사용하여 스위치에 알릴 수 있으므로 스위치가 효율적으로 세션을 제거할 수 있습니다.

12 단계 (선택 사항) 이 명령은 dACL이 없는 세션이 전체 액세스가 가능하며 ACL이 활성화된 인터페이스에 연결하도록 허용합니다.

```
SWITCH(config)#epm access-control open
```

참고: 이 기능은 dACL을 사용하는 인증 프로파일과 사용하지 않는 인증 프로파일이 혼합되어 있는 환경에서 유용합니다. 예를 들어 사용자 디바이스는 네트워크 액세스를 제한하기 위해 dACL로 시행되지만 IP 전화기에서는 dACL이 사용되지 않습니다. IP 전화기는 연결되면 MAB/802.1X(dACL 없음)에 의해 음성 리소스에 대한 권한을 부여받습니다. 사용자 디바이스가 IP 전화기 뒤에 연결되어 있으면 스위치는 사용자 디바이스 dACL을 시행하며, 그러면 인터페이스 레벨에서 ACL이 적용됩니다. 이 경우 IP 전화기에 대한 IP 액세스가 거부됩니다. IP 전화기에 권한 부여를 위한 dACL이 없기 때문입니다. 그러나 이 명령을 전역적으로 입력하면 스위치가 IP 전화기를 포함하여 dACL이 없는 모든 세션에 대해 'permit ip any any' ACL을 동적으로 삽입합니다. 관리되지 않는 허브를 통해 연결된 여러 디바이스의 경우에도 마찬가지입니다. dACL이 없는 여러 디바이스가 이미 연결되어 있는 상태에서 관리되지 않는 허브가 연결되어 있는 동일 인터페이스에 dACL AuthZ가 있는 새 디바이스가 인증되면 이 기능은 이전에 연결된 디바이스 세션에 'ip permit any any' ACL을 적용합니다.

13 단계 시스템 전체에서 802.1x를 활성화합니다.

```
SWITCH(config)#dot1x system-auth-control
```

참고: 이 명령을 제거해도 모든 포트에서 802.1X가 비활성화되지는 않으며, 이 명령이 없으면 스위치가 엔드포인트에서 EAP 프레임을 무시합니다. 포트에서 802.1X를 비활성화하려는 경우에는 interface range 명령을 사용하여 인증 관련 명령을 제거하십시오.

14 단계 (선택 사항) 연결 가능한 RADIUS 서버가 없을 때 포트에 열기/닫기 장애가 발생하면 미리 작성된 EAPoL 성공 메시지를 클라이언트로 보냅니다.

```
SWITCH(config)#dot1x critical eapol
```

참고: 스위치에 인증 서비스를 제공하기 위해 구성된 ISE 노드에 연결할 수 없으면 중요 인증이 수행됩니다. 중요 인증을 기반으로 하여 엔드포인트에 권한을 부여할 때 엔드포인트 신청자는 사용자 환경에 영향을 주는 인증을 재시작할 수 있습니다. 인증 중에는 네트워크 연결이 끊기기 때문입니다. 이 기능은 인증이 재시작되지 않도록 엔드포인트 신청자에게 미리 작성된 EAPoL 성공 메시지를 보냅니다. 신청자가 미리 작성된 메시지의 내용을 따르는지 여부는 신청자 설정, 신청자 벤더, EAP 유형 등 신청자에 따라 다릅니다.

15 단계 IP 디바이스 추적을 활성화하여 엔드포인트 IP를 찾습니다. 이는 프로파일링을 수행하고 세션에 dACL, 필터 ID 및 URL 리디렉션을 적용하는 데 필수적입니다.

```
SWITCH(config)#ip device tracking
```

참고: ip device tracking을 활성화한 후 Windows 머신에서 사용자에게 중복 IP 메시지가 표시되면 신청자 설정, 신청자 벤더 및 EAP 유형 명령을 실행합니다.

16 단계 (선택 사항) 'ip device tracking'을 활성화한 후 Windows 머신에서 사용자에게 중복 IP 메시지가 표시되면 다음 명령을 사용하여 그러한 메시지가 표시되지 않도록 할 수 있습니다. IOS 15.2(2)E 및 IOS-XE 03.06.00E 이상을 실행 중인 스위치 코드의 경우 다음 명령을 사용합니다.

```
SWITCH(config)#ip device tracking probe auto-source
```

참고: 이전 버전 IOS 코드의 경우에는 다음 명령을 실행합니다.

```
SWITCH(config)#ip device tracking probe delay 10
```

참고: 위의 명령으로도 문제가 해결되지 않고 스위치가 엔드포인트 VLAN용 SVI로 구성되어 있는 경우 다음 명령을 사용하여 중복 IP 메시지 문제를 해결할 수 있습니다.

```
SWITCH(config)#ip device tracting probe use-svi
```

17 단계 VLAN을 생성합니다.

```
SWITCH(config)#vlan 10
SWITCH(config-vlan)# name USER

SWITCH(config)#vlan 11
SWITCH(config-vlan)# name VOICE

SWITCH(config)#vlan 100
SWITCH(config-vlan)# name MGMT
```

18 단계 사용자 VLAN에 대한 SVI 컨피그레이션을 수행합니다.

```
SWITCH(config)#interface 10
SWITCH(config-if)# ip address 10.1.10.1 255.255.255.0
```

19 단계 DHCP 서버에 DHCP 패킷을 전송합니다.

```
SWITCH(config-if)# ip helper-address 10.1.200.10
```

20 단계 (선택 사항) 프로파일링용으로 ISE에 DHCP 패킷을 전송합니다.

```
SWITCH(config-if)#ip helper-address 10.1.200.11
```

참고: ISE 노드 간의 복제 트래픽을 줄일 수 있도록 여러 노드가 아닌 ISE 노드 중 하나에만 패킷을 전송하는 것이 좋습니다. 또한 디바이스 센서를 사용하는 경우에는 'helper-address'를 동시에 사용하여 DHCP를 전달하지 않는 것이 좋습니다. 이렇게 하면 프로파일링 정보가 중복되어 ISE 노드 간의 복제 트래픽이 증가할 수 있기 때문입니다.

21 단계 음성 VLAN에 대한 SVI 컨피그레이션을 수행합니다.

```
SWITCH(config)#interface 11
SWITCH(config-if)#ip address 10.1.11.1 255.255.255.0
SWITCH(config-if)#ip helper-address 10.1.200.10
SWITCH(config-if)#! ip helper-address 10.1.200.11
```

22 단계 관리 VLAN에 대한 SVI 컨피그레이션을 수행합니다.

```
SWITCH(config)#interface 100
SWITCH(config-if)#ip address 10.1.100.1 255.255.255.0
```

23 단계 이는 스위치의 http 리디렉션 기능을 사용하기 위해 필요합니다.

```
SWITCH(config)#ip http server
```

24 단계 (선택 사항) 이는 스위치의 https 리디렉션 기능을 사용하기 위해 필요합니다.

```
SWITCH(config)#ip http secure-server
```

참고: HTTPS 리디렉션을 사용하는 경우 스위치의 CPU에 영향을 주므로, 고밀도 스위치에서 HTTPS 리디렉션을 활성화하기 전에 성능을 모니터링하는 것이 좋습니다.

25 단계 (선택 사항) 다음을 구성하여 URL 리디렉션은 계속 작동하도록 허용하면서 스위치에 대한 http 기반 관리 액세스는 비활성화합니다.

```
SWITCH(config)#ip http active-session-modules none
SWITCH(config)#ip http secure-active-session-modules none
```

26 단계 (선택 사항) 이는 동시에 존재할 수 있는 URL 리디렉션 세션의 수에 영향을 줍니다. 고밀도 액세스 스위치에서는 여러 사용자가 URL 리디렉션을 동시에 사용하려는 경우 이 값을 늘려야 할 수 있습니다. 기본값과 최대값은 코드 버전 및 플랫폼에 따라 달라질 수 있습니다. 15.2(2)E3을 실행 중인 3560CG 플랫폼에서 기본값은 16이고 최대값은 48입니다.

```
SWITCH(config)#ip http max-connections 48
```

참고: 이전 버전의 IOS에서는 사용할 수 없습니다.

27 단계 이 ACL은 CWA, BYOD 및 포스처 중에 ISE로 리디렉션되는 트래픽을 정의합니다. ACL당 허용되는 모든 트래픽이 리디렉션됩니다. 암시적 거부 시에는 기타 트래픽 유형의 리디렉션이 차단됩니다. 이 트래픽은 스위치 CPU로 푸시되므로 여기서는 HTTP(및 HTTPS)만 허용하도록 지정하는 것이 좋습니다. 리디렉션 ACL과 함께 추가적인 액세스 제어가 필요한 경우에는 리디렉션 ACL과 함께 dACL을 사용하는 것이 좋습니다.

```
SWITCH(config)#ip access-list extended ACL_WEBAUTH_REDIRECT
SWITCH(config-ext-nacl)#permit tcp any any eq www
SWITCH(config-ext-nacl)#permit tcp any any eq 443
```

참고: 위에서 참조하는 ACL 이름은 새 ISE 2.0 설치에서 사용되는 기본 리디렉션 ACL 이름과 동일합니다. 다른 이름을 원하는 경우 스위치 및 ISE 권한 부여 프로파일을 모두 새 리디렉션 ACL 이름으로 업데이트해야 합니다.

28 단계 이 ACL은 블랙리스트 디바이스에 대해 ISE로 리디렉션되는 트래픽을 정의합니다. ACL당 허용되는 모든 트래픽이 리디렉션됩니다. 암시적 거부 시에는 기타 트래픽 유형의 리디렉션이 차단됩니다. 이 트래픽은 스위치 CPU로 푸시되므로 여기서는 HTTP(및 HTTPS)만 허용하도록 지정하는 것이 좋습니다. 리디렉션 ACL과 함께 추가적인 액세스 제어가 필요한 경우에는 리디렉션 ACL과 함께 dACL을 사용하는 것이 좋습니다.

```
SWITCH(config)#ip access-list extended BLACKHOLE
SWITCH(config-ext-nacl)#permit tcp any any eq www
SWITCH(config-ext-nacl)#permit tcp any any eq 443
```

참고: 위에서 참조하는 ACL 이름은 새 ISE 2.0 설치에서 사용되는 기본 리디렉션 ACL 이름과 동일합니다. 다른 이름을 원하는 경우 스위치 및 ISE 권한 부여 프로파일을 모두 새 리디렉션 ACL 이름으로 업데이트해야 합니다.

29 단계 RADIUS 인증 전에 적용할 ACL을 수행합니다. 이는 유선 액세스를 위한 단계별 구축의 개방형 모드 또는 로우-임팩트 모드를 사용할 때 필요합니다.

```
SWITCH(config)#ip access-list extended ACL-DEFAULT
SWITCH(config-ext-nacl)#permit udp any any eq domain
SWITCH(config-ext-nacl)#permit udp any eq bootpc any eq bootps
SWITCH(config-ext-nacl)#deny ip any any
```

참고: 로우-임팩트 모드 구축에서는 인터페이스가 중요 인증 상태가 될 때 이 ACL이 적용됩니다. 즉, 연결 가능한 ISE 노드가 없을 때 엔드포인트가 연결을 시도하는 경우 각 인터페이스 컨피그레이션에 대해 구성된 중요 VLAN에 엔드포인트가 배치되어 있으면 중요 상태에서도 엔드포인트는 이 ACL만 사용하도록 계속 제한됩니다.

30 단계 인증 요청 및 계정 관리 업데이트 중에 정의된 VSA(Vendor Specific Attribute)를 ISE에 전송하도록 NAD를 구성합니다.

```
SWITCH(config)#radius-server vsa send authentication
SWITCH(config)#radius-server vsa send accounting
```

31 단계 RADIUS 서버에 추가 특성을 전송합니다(ISE의 경우 필수).

```
SWITCH(config)#radius-server attribute 6 on-for-login-auth
SWITCH(config)#radius-server attribute 8 include-in-access-req
SWITCH(config)#radius-server attribute 25 access-request include
```

32 단계 ISE PSN을 RADIUS 서버로 추가합니다.

```
SWITCH(config)#radius server ISE01
SWITCH(config-radius-server)#address ipv4 10.1.200.11
```

33 단계 IOS 15.2(2)E 및 IOS-XE 03.06.00E 이상을 실행 중인 스위치 코드에 대해 RADIUS 상태를 테스트하기 위한 방법과 사용자 이름을 정의합니다. 이 명령은 RADIUS 서버가 각 데드 기준에 대해 데드로 표시되어 있을 때만 서버에 RADIUS 테스트 메시지를 전송합니다. 데드 타임이 만료되면 프로브가 전송되며, RADIUS 서버가 계속 응답하지 않으면 더 높은 빈도로 전송됩니다. 이 명령은 프로브가 지속적으로 전송되지 않아 NAD 수가 많은 대규모 조직에서 유용합니다. 이 명령과 다음 명령은 함께 사용할 수 없습니다.

```
SWITCH(config-radius-server)# automate-tester username RADIUS-TEST probe-on
```

참고: 다음 명령은 이전 버전의 IOS에서 지원됩니다. 이 명령은 서버 상태에 관계없이 구성된 간격으로 서버에 RADIUS 테스트 메시지를 전송합니다. 구축에 NAD 수가 많은 경우에는 프로브 간격을 늘려 RADIUS 서버에 대한 영향을 제한하는 것이 좋습니다. 유휴 시간 값을 늘릴 때는 프로브 유휴 시간이 데드 타임보다 짧도록 글로벌 데드 타임 값도 늘려야 합니다. 이렇게 하면 중요 상태에 대해 권한이 부여된 엔드포인트가 데드 타임 만료 시 중요 상태에 대한 권한을 다시 부여받기 위한 목적만으로 다시 초기화되지 않습니다. 여기서 값은 10분으로 설정됩니다(기본값은 60분).

```
SWITCH(config-radius-server)# automate-tester username RADIUS-TEST ignore-acct-port idle-time 10
```

참고: 이러한 프로브 메시지는 일반 사용자 인증 이벤트와 함께 ISE RADIUS LiveLog에서 볼 수 있습니다. ISE에서는 프로브 메시지를 필터링하여 LiveLog에서 사용자 인증 이벤트만 볼 수 있도록 컬렉션 필터를 구성할 수 있습니다.

34 단계 RADIUS 키를 설정합니다.

```
SWITCH(config-radius-server)#key RADIUS_KEY
```

35 단계 추가 ISE PSN을 RADIUS 서버로 구성합니다.

```
SWITCH(config)#radius server ISE02
SWITCH(config-radius-server)#address ipv4 10.1.200.12
SWITCH(config-radius-server)#automate-tester username RADIUS-TEST probe-on
SWITCH(config-radius-server)#! automate-tester username RADIUS-TEST idle-time 10
SWITCH(config-radius-server)#key RADIUS_KEY
```

36 단계 AAA 지시문에서 참조하도록 RADIUS 서버 그룹을 추가합니다.

```
SWITCH(config)#aaa group server radius ISE
SWITCH(config-sg-radius)#server name ISE01
SWITCH(config-sg-radius)#server name ISE02
```

37 단계 서버가 응답하지 못하는 경우 NAD가 RADIUS 서버를 데드로 표시하는 데 걸리는 시간을 정의합니다. 단일 ISE 노드가 RADIUS 서버로 정의된 환경에서는 이렇게 하면 서버가 다시 온라인 상태가 된 후 인터페이스 컨피그레이션이 다시 초기화되도록 구성되어 있다고 가정하여 NAD가 포트를 열기/닫기 장애(중요)가 발생한 상태로 유지하는 기간도 정의됩니다. 모든 ISE 노드가 다시 서비스 상태가 되면 스위치는 리스트의 첫 번째 ISE 노드로 되돌아갑니다. 이 예에서 값은 15분으로 설정되었습니다.

```
SWITCH(config-sg-radius)#deadtime 15
```

참고: 이 값은 이전에 구성한 RADIUS 프로브의 유휴 시간 설정보다 커야 합니다. 데드 타임을 RADIUS 서버 그룹에서 정의하는 대신 'radius-server deadtime 15' 명령을 사용하여 전역적으로 구성할 수도 있습니다.

38 단계 서버를 데드로 표시할 RADIUS 데드 기준을 설정합니다.

```
SWITCH(config)#radius-server dead-criteria time 10 tries 3
```

39 단계 (선택 사항) RADIUS 요청을 생성할 인터페이스를 정의합니다.

```
SWITCH(config)#ip radius source-interface vlan 100
```

참고: 위의 예에서는 관리 SVI를 사용하지만, RADIUS 서버로의 경로가 여러 개인 경우 RADIUS 요청의 소스 IP가 같은 소스 IP에서 도착하도록 루프백 인터페이스를 활용하는 것이 좋습니다.

40 단계 (선택 사항) 프로파일링에 사용됩니다. 이를 실행하면 ISE가 NAD에서 CDP/LLDP/ARP 테이블을 폴링할 수 있습니다. 디바이스 센서 기능을 사용하는 경우에는 중복 프로파일링 데이터를 줄이기 위해 SNMP를 동시에 사용하지 않는 것이 좋습니다.

```
SWITCH(config)#snmp-server community SNMP_COMMUNITY_STRING RO
```

참고: 맞춤형 SNMP 커뮤니티 문자열 외에, ISE 노드와 관리 서버가 SNMP를 통해 스위치에 액세스할 수 있도록 하기 위한 용도만으로 ACL도 사용하는 것이 좋습니다.

41 단계 (선택 사항) 디바이스 센서를 사용하여 프로파일링용으로 클라이언트에서 DHCP 정보를 수집하도록 DHCP 스누핑을 활성화합니다. 'ip helper-address' 명령을 사용하는 대신 이 방법을 사용하여 DHCP 정보를 수집하는 것이 좋습니다.

```
SWITCH(config)#ip dhcp snooping
```

참고: 엔드포인트에 고정 IP 주소를 사용하는 경우에는 이 단계를 건너뜁니다.

42 단계 (선택 사항) 엔드포인트가 배치될 VLAN에서 DHCP 스누핑을 활성화합니다.

```
SWITCH(config)#ip dhcp snooping vlan 10, 11
```

참고: 엔드포인트에 고정 IP 주소를 사용하는 경우에는 이 단계를 건너뜁니다.

43 단계 (선택 사항) DHCP에 대해 디바이스 센서를 활성화합니다.

```
SWITCH(config)#device-sensor filter-list dhcp list TLV-DHCP
SWITCH(config-sensor-dhcplist)#option name host-name
SWITCH(config-sensor-dhcplist)#option name requested-address
SWITCH(config-sensor-dhcplist)#option name parameter-request-list
SWITCH(config-sensor-dhcplist)#option name class-identifier
SWITCH(config-sensor-dhcplist)#option name client-identifier
SWITCH(config)#device-sensor filter-spec dhcp include list TLV-DHCP
```

44 단계 (선택 사항) CDP를 전역적으로 활성화합니다.

```
SWITCH(config)#cdp run
```

45 단계 (선택 사항) CDP에 대해 디바이스 센서를 활성화합니다.

```
SWITCH(config)#device-sensor filter-list cdp list TLV-CDP
SWITCH(config-sensor-cdplist)#tlv name device-name
SWITCH(config-sensor-cdplist)#tlv name address-type
SWITCH(config-sensor-cdplist)#tlv name capabilities-type
SWITCH(config-sensor-cdplist)#tlv name platform-type
SWITCH(config)#device-sensor filter-spec cdp include list TLV-CDP
```

46 단계 (선택 사항) LLDP를 전역적으로 활성화합니다.

```
SWITCH(config)#lldp run
```

47 단계 (선택 사항) LLDP에 대해 디바이스 센서를 활성화합니다.

```
SWITCH(config)#device-sensor filter-list lldp list TLV-LLDP
SWITCH(config-sensor-lldplist)#tlv name system-name
SWITCH(config-sensor-lldplist)#tlv name system-description
SWITCH(config)#device-sensor filter-spec lldp include list TLV-LLDP
```

48 단계 (선택 사항) RADIUS 계정 관리에서 모든 변경 사항을 포함한 센서 데이터가 전송되도록 합니다.

```
SWITCH(config)#device-sensor accounting
SWITCH(config)#device-sensor notify all-changes
```

49 단계 (선택 사항) 로컬 애널라이저를 비활성화하여 중복된 업데이트가 ISE로 전송되지 않도록 합니다.

```
SWITCH(config)#no macro auto monitor
SWITCH(config)#access-session template monitor
```

50 단계 컨피그레이션 모드를 종료하고 컨피그레이션을 저장합니다.

```
SWITCH(config)#end
SWITCH#write memory
Building configuration…
[OK]
SWITCH#
```

인터페이스 레벨 컨피그레이션(모니터 모드/로우-임팩트 모드 컨피그레이션)

다음 인터페이스 컨피그레이션을 사용하면 모니터 모드 및 로우-임팩트 모드 컨피그레이션의 주요 명령인 'authentication open' 지시문을 사용할 수 있습니다. 두 모드의 주요 차이점은 포트 ACL의 유무입니다. 일반적으로 모니터 모드의 경우에는 포털 ACL이 적용되지 않는 반면 로우-임팩트 모드의 경우에는 DHCP, DNS 및 경우에 따라 TFTP에 대한 트래픽을 제한하기 위해 ACL이 적용됩니다. 이 컨피그레이션은 'authentication host-mode multi-auth'를 활용하므로 단일 인터페이스에 호스트를 수에 제한 없이 사용할 수 있습니다.

51 단계 인터페이스 컨피그레이션 모드를 시작합니다.

```
SWITCH(config)#interface GigabitEthernetX/Y
SWITCH(config-if)#description ACCESS (Multi-Auth w/ Low-Impact Mode)
```

52 단계 포트를 액세스 모드로 설정합니다. 이 명령을 실행하지 않으면 인터페이스가 'authentication' 관련 명령을 가져오지 않습니다.

```
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport access vlan 10
SWITCH(config-if)#switchport voice vlan 11
```

53 단계 (선택 사항) 디바이스 센서에 대해 CDP 및 LLDP를 활성화합니다(기본적으로 활성화되어야 함).

```
SWITCH(config-if)#cdp enable
SWITCH(config-if)#lldp receive
```

54 단계 로우-임팩트 모드의 경우 사전 인증 ACL을 적용합니다.

```
SWITCH(config-if)#ip access-group ACL-DEFAULT in
```

55 단계 RADIUS 응답에 관계없이 네트워크 액세스를 허용합니다. 이는 인증 시 장애가 발생하는 디바이스에 대해 제공할 액세스 권한의 정도를 제어하기 위해 위의 ACL과 결합되어야 합니다.

```
SWITCH(config-if)#authentication open
```

참고: 위의 명령은 인증 전 그리고 인증 시 장애가 발생하는 경우 액세스를 허용합니다(RADIUS에서 ACCESS-REJECT를 다시 전송함). 그러나 RADIUS 서버가 dVLAN 및 dACL과 같은 권한 부여 특성과 함께 ACCESS-ACCEPT를 다시 전송하는 경우에는 세션에 대해 권한 부여가 시행됩니다. 즉, 'authentication open' 지시문에 관계없이 dACL이 네트워크에 대한 제한적 액세스를 제공하는 경우 엔드포인트는 각 dACL에 대해 제한적 액세스 권한을 갖게 됩니다.

56 단계 (선택 사항) 네트워크에서 인증되지 않은 포트로 브로드캐스트 트래픽을 허용합니다. 이는 WoL(Wake on LAN) 프로세스를 보완하므로 네트워크 관리 서버가 온디맨드 방식으로 클라이언트의 절전 모드를 해제할 수 있습니다. 또한 다른 호스트의 네트워크 요청이 없으면 자체적으로는 많은 트래픽을 생성하지 않는 특정 디바이스 유형에 대한 MAB 프로세스도 보완합니다.

```
SWITCH(config-if)#authentication control-direction in
```

57 단계 802.1x 인증에서 장애가 발생한 후 포트를 MAB로 이동할 수 있도록 합니다.

```
SWITCH(config-if)#authentication event fail action next-method
```

58 단계 (선택 사항) 인증 중에 RADIUS 서버를 사용할 수 없으면 포트에 열기/닫기 장애가 발생할 수 있도록 합니다. 포트에 열기 장애가 발생하도록 하려면 액세스 VLAN과 같은 VLAN을 할당합니다. 포트에 닫기 장애가 발생하도록 하려면 SVI가 없는 더미(dummy) VLAN을 할당합니다. 이렇게 하면 연결 가능한 RADIUS 서버가 없는 상태에서 연결하는 디바이스에만 영향을 줍니다. 이 이벤트 전에 이미 연결된 디바이스는 영향을 받지 않습니다. DEFAULT-ACL은 이 포트에 계속 적용됩니다.

```
SWITCH(config-if)#authentication event server dead action reinitialize vlan 10
```

참고: VLAN ID는 로컬 스위치에 정의되어 있는 모든 VLAN일 수 있습니다. ISE 노드를 사용할 수 없는 상황에서 열기 장애를 발생시키려면 이를 일반 사용자 VLAN과 같은 VLAN ID로 설정하는 것이 좋습니다. 반면 닫기 장애를 발생시키려는 경우에는 이를 SVI가 없는 VLAN ID로 설정할 수 있습니다.

59 단계 (선택 사항) 사용 가능한 RADIUS 서버가 없을 때 음성 디바이스가 할당된 음성 VLAN에 대한 권한을 부여받을 수 있도록 합니다.

```
SWITCH(config-if)#authentication event server dead action authorize voice
```

60 단계 (선택 사항) RADIUS 서버에 연결할 수 있을 때 포트가 다시 초기화됩니다. 그러면 인터페이스에 있는 각 엔드포인트가 재인증됩니다. 원하는 동작이 서버에 다시 연결할 수 있게 된 후에도 포트를 열기/닫기 장애가 발생하는 상태로 유지하는 것이라면 이 명령을 생략할 수 있습니다.

```
SWITCH(config-if)#authentication event server alive action reinitialize
```

61 단계 포트를 다중 인증 모드로 설정합니다. 그러면 음성 디바이스는 하나를, 데이터 디바이스는 수에 제한 없이 사용할 수 있습니다. 스위칭 플랫폼에 따라 포트를 모든 데이터 엔드포인트에 대해 같은 VLAN 또는 여러 VLAN으로 강제 지정할 수 있습니다.

```
SWITCH(config-if)#authentication host-mode multi-auth
```

62 단계 (선택 사항) 디바이스가 802.1x가 활성화된 포트에 연결할 때 해당 포트에서 디바이스에 대해 허용되는 최대 수가 인증된 경우 802.1x 포트가 종료되거나 syslog 오류를 생성하거나 새 디바이스로부터의 패킷을 삭제하도록 구성할 수 있습니다. 기본 설정은 'shutdown'이며, 이 설정을 사용하는 경우 조건이 충족되면 포트는 오류가 발생하며 비활성화됩니다. 'restrict'를 사용하면 포트가 작동하는 상태로 유지되지만 사고가 기록됩니다. 일반적으로 다중 인증 포트는 같은 인터페이스에서 여러 디바이스를 허용하므로 이러한 현상이 문제가 되지 않습니다. 하지만 둘 이상의 음성 디바이스가 연결되어 있거나 인터페이스가 다중 도메인 또는 단일 호스트 모드인 경우에는 포트가 인증을 위반하게 될 수 있습니다.

```
SWITCH(config-if)#authentication violation restrict
```

63 단계 (선택 사항) 포트에 대한 재인증 및 비활성 타이머를 활성화합니다. 이 명령은 값이 포트에 정적으로 할당되든 RADIUS 서버에서 파생되든 관계없이 필요합니다.

```
SWITCH(config-if)#authentication periodic
```

64 단계 (선택 사항) 재인증 타이머 간격(세션 타이머)을 RADIUS 서버에서 스위치로 다운로드하도록 허용합니다.

```
SWITCH(config-if)#authentication timer reauthenticate server
```

참고: RADIUS 서버에서 특성 27(Session-Timeout) 및 29(Terminate-Action)를 설정할 수 있습니다. 특성 28 값인 'RADIUS-Request'를 사용하면 세션이 재인증됩니다. 이 특성을 'Default'로 설정하면 세션이 종료되고 서버가 강제로 재시작됩니다. RADIUS 서버에서 값이 전송되지 않으면 세션에 대해 재인증 타이머가 적용되지 않습니다.

65 단계 (선택 사항) 비활성 타이머 간격을 RADIUS 서버에서 스위치로 다운로드하도록 허용합니다. 'dynamic' 키워드는 디바이스 연결이 실제로 끊겼는지를 확인하기 위해 세션을 제거하기 전에 ARP-Probe를 전송하도록 NAD에 명령합니다.

```
SWITCH(config-if)#authentication timer inactivity server dynamic
```

참고: RADIUS 서버에서는 특성 28(Idle-Timeout)을 사용하면 이를 설정할 수 있습니다. RADIUS 서버에서 값이 전송되지 않으면 세션에 대해 유휴 타임아웃 타이머가 적용되지 않습니다.

66 단계 포트에서 MAC(Mac 인증 우회)를 활성화합니다.

```
SWITCH(config-if)#mab
```

67 단계 스위치에서 EAPoL ID 요청 프레임에 대한 간격을 줄입니다. 재시작 값이 이와 결합되면 네트워크에 대한 게스트 액세스를 대기하는 시간은 30초가 됩니다. tx-period의 기본값은 30초이므로 게스트 디바이스의 총 대기 시간은 90초가 됩니다. 대기 시간이 90초이면 많은 디바이스가 네트워크에서 IP 주소를 가져오는 시도를 중단합니다. 10초에서 시작하여 필요에 따라 게스트 사용자 환경을 개선하기 위해 더 작은 값으로 줄이는 것이 좋습니다.

```
SWITCH(config-if)#dot1x timeout tx-period 10
```

참고: 802.1x 인증 전에 네트워크 액세스용으로 포트가 이미 열린 상태이므로 인터페이스에서 'authentication open' 지시문을 사용할 때는 이 값이 주는 영향이 감소합니다.

68 단계 액세스 포트에 대해 spanning-tree portfast를 활성화합니다.

```
SWITCH(config-if)#spanning-tree portfast
```

69 단계 이 명령은 기본적으로 포트에서 802.1x를 활성화합니다. 이 명령은 802.1x 명령의 나머지 부분을 입력한 후 마지막에 실행하는 것이 좋습니다.

```
SWITCH(config-if)#authentication port-control auto
```

인터페이스 레벨 컨피그레이션(폐쇄 모드 컨피그레이션)

다음 인터페이스 컨피그레이션은 폐쇄 모드 컨피그레이션입니다. 이 모드에서 엔드포인트는 802.1X 또는 MAB를 통해 정상적으로 인증될 때까지 트래픽을 전달할 수 없습니다. 필수 조건은 아니지만, 이 컨피그레이션은 'authentication host-mode multi-domain'을 활용하므로 단일 인터페이스에서 음성 디바이스와 데이터 디바이스를 하나씩 사용할 수 있습니다.

70 단계 인터페이스 컨피그레이션 모드를 시작합니다.

```
SWITCH(config)#interface GigabitEthernetX/Y
SWITCH(config-if)#description ACCESS (Multi-Domain w/ Closed Mode)
```

71 단계 포트를 액세스 모드로 설정합니다. 이 명령을 실행하지 않으면 인터페이스가 'authentication' 관련 명령을 가져오지 않습니다.

```
SWITCH(config-if)#switchport mode access
SWITCH(config-if)#switchport access vlan 10
SWITCH(config-if)#switchport voice vlan 11
```

참고: 사용자 이름과 비밀번호는 ISE가 활용 중인 ID 데이터베이스에서 유효한 어카운트일 필요는 없습니다. ISE 노드가 성공한 인증에 대해 ACCESS-ACCEPT를 다시 보내든, 장애가 발생한 인증에 대해 ACCESS_REJECT를 다시 보내든 관계없이 스위치는 두 응답을 모두 RADIUS 데드 설정을 위한 라이브 서버의 유효한 응답으로 간주합니다. MS Active Directory 또는 LDAP와 같은 외부 ID 저장소를 사용하는 경우 여기서 유효한 어카운트를 제공할 수 있다는 이점이 있습니다. 유효한 어카운트를 사용하면 스위치가 백엔드 ID 저장소까지 전체를 테스트할 수 있으며, ISE 노드가 외부 ID 데이터베이스에 연결되어 있는지를 확인할 수 있습니다.

72 단계 (선택 사항) 디바이스 센서에 대해 CDP 및 LLDP를 활성화합니다(기본적으로 활성화되어야 함).

```
SWITCH(config-if)#cdp enable
SWITCH(config-if)#lldp receive
```

73 단계 (선택 사항) 네트워크에서 인증되지 않은 포트로 브로드캐스트 트래픽을 허용합니다. 이는 WoL 프로세스를 보완하므로 네트워크 관리 서버가 온디맨드 방식으로 클라이언트의 절전 모드를 해제할 수 있습니다. 또한 다른 호스트의 네트워크 요청이 없으면 자체적으로는 많은 트래픽을 생성하지 않는 특정 디바이스 유형에 대한 MAB 프로세스도 보완합니다.

```
SWITCH(config-if)#authentication control-direction in
```

74 단계 802.1x 인증에서 장애가 발생한 후 포트를 MAB로 이동할 수 있도록 합니다.

```
SWITCH(config-if)#authentication event fail action next-method
```

75 단계 (선택 사항) 인증 중에 RADIUS 서버를 사용할 수 없으면 포트에 열기/닫기 장애가 발생할 수 있도록 합니다. 포트에 열기 장애가 발생하도록 하려면 액세스 VLAN과 같은 VLAN을 할당합니다. 포트에 닫기 장애가 발생하도록 하려면 SVI가 없는 더미(dummy) VLAN을 할당합니다. 이렇게 하면 연결 가능한 RADIUS 서버가 없을 때 연결하는 디바이스에만 영향을 줍니다. 이 이벤트 전에 이미 연결된 디바이스는 영향을 받지 않습니다. DEFAULT-ACL은 이 포트에 계속 적용됩니다.

```
SWITCH(config-if)#authentication event server dead action authorize
```

참고: 중요 이벤트 발생 시 사용할 VLAN ID를 지정하기 위해 명령 끝에 VLAN ID를 지정할 수 있습니다. 이를 생략하면 'switchport access vlan' 명령에 지정된 VLAN을 사용합니다.

76 단계 (선택 사항) 사용 가능한 RADIUS 서버가 없을 때 음성 디바이스가 할당된 음성 VLAN에 대한 권한을 부여받을 수 있도록 합니다.

```
SWITCH(config-if)#authentication event server dead action authorize voice
```

77 단계 (선택 사항) RADIUS 서버에 연결할 수 있을 때 포트가 다시 초기화됩니다. 그러면 인터페이스에 있는 각 엔드포인트가 재인증됩니다. 원하는 동작이 서버에 연결할 수 있게 된 후에도 포트를 열기/닫기 장애가 발생하는 상태로 유지하는 것이라면 이 명령을 생략할 수 있습니다.

```
SWITCH(config-if)#authentication event server alive action reinitialize
```

78 단계 포트를 다중 인증 모드로 설정합니다. 그러면 음성 디바이스와 데이터 디바이스를 하나씩 사용할 수 있습니다.

```
SWITCH(config-if)#authentication host-mode multi-domain
```

79 단계 (선택 사항) 새 디바이스가 802.1x가 활성화된 포트에 연결할 때 해당 포트에서 디바이스에 대해 허용되는 최대 수가 인증된 경우 802.1x 포트가 종료되거나 syslog 오류를 생성하거나 패킷을 삭제하도록 구성할 수 있습니다. 기본 설정은 'shutdown'이며, 이 설정을 사용하는 경우 조건이 충족되면 포트는 오류가 발생하며 비활성화됩니다. 'restrict'를 사용하면 포트가 작동하는 상태로 유지되며 사고가 기록됩니다. 일반적으로 다중 인증 포트는 같은 인터페이스에서 여러 디바이스를 허용하므로 이러한 현상이 문제가 되지 않습니다. 하지만 둘 이상의 음성 디바이스가 연결되어 있는 경우에는 포트가 인증을 위반하게 될 수 있습니다.

```
SWITCH(config-if)#authentication violation restrict
```

80 단계 (선택 사항) 포트에 대한 재인증 및 비활성 타이머를 활성화합니다. 이 명령은 값이 포트에 정적으로 할당되든 RADIUS 서버에서 파생되든 관계없이 필요합니다.

```
SWITCH(config-if)#authentication periodic
```

81 단계 (선택 사항) 재인증 타이머 간격(세션 타이머)을 RADIUS 서버에서 스위치로 다운로드하도록 허용합니다.

```
SWITCH(config-if)#authentication timer reauthenticate server
```

82 단계 (선택 사항) 비활성 타이머 간격을 RADIUS 서버에서 스위치로 다운로드하도록 허용합니다. 'dynamic' 키워드는 디바이스 연결이 실제로 끊겼는지를 확인하기 위해 세션을 제거하기 전에 ARP-Probe를 전송하도록 NAD에 명령합니다.

```
SWITCH(config-if)#authentication timer inactivity server dynamic
```

83 단계 포트에서 MAC(Mac 인증 우회)를 활성화합니다.

```
SWITCH(config-if)#mab
```

84 단계 스위치에서 EAPoL ID 요청 프레임에 대한 간격을 줄입니다. 재시작 값이 이와 결합되면 게스트 액세스 네트워크를 대기하는 시간은 30초가 됩니다. tx-period의 기본값은 30초이므로 게스트 디바이스의 총 대기 시간은 90초가 됩니다. 많은 디바이스가 90초가 되기 전에 네트워크에서 IP 주소를 가져오려는 시도를 정지합니다. 10초에서 시작하여 필요에 따라 게스트 사용자 환경을 개선하기 위해 더 작은 값으로 줄이는 것이 좋습니다.

```
SWITCH(config-if)#dot1x timeout tx-period 10
```

85 단계 액세스 포트에 대해 spanning-tree portfast를 활성화합니다.

```
SWITCH(config-if)#spanning-tree portfast
```

86 단계 포트에서 802.1x를 활성화합니다. 이 명령은 802.1x 명령의 나머지 부분을 입력한 후 마지막에 실행하는 것이 좋습니다.

```
SWITCH(config-if)#authentication port-control auto
```

부록 A: 샘플 컨피그레이션

디바이스 센서가 있는 전역 컨피그레이션

```
ip domain-name EXAMPLE.COM
username RADIUS-TEST password 0 PASSWORD
crypto key generate rsa general-keys mod 2048
aaa new-model
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting update newinfo periodic 2880
aaa server radius dynamic-author
 client 10.1.200.11 server-key RADIUS_KEY
 client 10.1.200.11 server-key RADIUS_KEY
aaa session-id common
dot1x system-auth-control
dot1x critical eapol
ip device tracking
vlan 10
 name USER
vlan 11
 name VOICE
vlan 100
 name MGMT
interface 10
 ip address 10.1.10.1 255.255.255.0
ip helper-address 10.1.200.10
interface 11
 ip address 10.1.11.1 255.255.255.0
ip helper-address 10.1.200.10
interface 100
 ip address 10.1.100.1 255.255.255.0
ip http server
ip access-list extended ACL_WEBAUTH_REDIRECT
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended BLACKHOLE
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended ACL-DEFAULT
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 deny   ip any any
radius-server vsa send authentication
radius-server vsa send accounting
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius server ISE01
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST probe-on
 # For IOS & IOS-XE without 'probe-on' feature use following command instead
 ! automate-tester username RADIUS-TEST idle-time 10
 key RADIUS_KEY
radius server ISE02
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST probe-on
 # For IOS & IOS-XE without 'probe-on' feature use following command instead
 ! automate-tester username RADIUS-TEST idle-time 10
 key RADIUS_KEY
aaa group server radius ISE
 server name ISE01
```

```
 server name ISE02
 deadtime 15
radius-server dead-criteria time 10 tries 3
ip radius source-interface vlan 100
device-sensor filter-list dhcp list TLV-DHCP
 option name host-name
 option name requested-address
 option name parameter-request-list
 option name class-identifier
 option name client-identifier
device-sensor filter-spec dhcp include list TLV-DHCP
cdp run
device-sensor filter-list cdp list TLV-CDP
 tlv name device-name
 tlv name address-type Craig may not be needed
 tlv name capabilities-type
 tlv name platform-type
device-sensor filter-spec cdp include list TLV-CDP
lldp run
device-sensor filter-list lldp list TLV-LLDP
 tlv name system-name
 tlv name system-description
device-sensor filter-spec lldp include list TLV-LLDP
device-sensor accounting
device-sensor notify all-changes
no macro auto monitor
access-session template monitor
end
write memory
```

디바이스 센서가 없는 전역 컨피그레이션

```
ip domain-name EXAMPLE.COM
username RADIUS-TEST password 0 PASSWORD
crypto key generate rsa general-keys mod 2048
aaa new-model
aaa authentication dot1x default group ISE
aaa authorization network default group ISE
aaa accounting dot1x default start-stop group ISE
aaa accounting update newinfo periodic 2880
aaa server radius dynamic-author
 client 10.1.200.11 server-key RADIUS_KEY
 client 10.1.200.11 server-key RADIUS_KEY
aaa session-id common
dot1x system-auth-control
dot1x critical eapol
ip device tracking
vlan 10
 name USER
vlan 11
 name VOICE
vlan 100
 name MGMT
interface 10
 ip address 10.1.10.1 255.255.255.0
 ip helper-address 10.1.200.10
 ip helper-address 10.1.200.11
interface 11
 ip address 10.1.11.1 255.255.255.0
 ip helper-address 10.1.200.10
 ip helper-address 10.1.200.11
interface 100
 ip address 10.1.100.1 255.255.255.0
ip http server
ip access-list extended ACL_WEBAUTH_REDIRECT
```

```
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended BLACKHOLE
 permit tcp any any eq www
 permit tcp any any eq 443
ip access-list extended ACL-DEFAULT
 permit udp any any eq domain
 permit udp any eq bootpc any eq bootps
 deny   ip any any
radius-server vsa send authentication
radius-server vsa send accounting
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius server ISE01
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST idle-time 10
 key RADIUS_KEY
radius server ISE02
 address ipv4 10.1.200.11
 automate-tester username RADIUS-TEST idle-time 10
 key RADIUS_KEY
aaa group server radius ISE
 server name ISE01
 server name ISE02
 deadtime 15
radius-server dead-criteria time 10 tries 3
ip radius source-interface vlan 100
snmp-server community SNMP_COMMUNITY_STRING RO
ip dhcp snooping
ip dhcp snooping vlan 10, 11
end
write memory
```

로우-임팩트 모드용 인터페이스 레벨 컨피그레이션

```
description ACCESS (Multi-Auth w/ Low-Impact Mode)
switchport mode access
switchport access vlan 10
switchport voice vlan 11
ip access-group ACL-DEFAULT in
authentication open
authentication event fail action next-method
authentication event server dead action reinitialize vlan 10
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-auth
mab
authentication violation restrict
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
dot1x timeout tx-period 10
spanning-tree portfast
authentication port-control auto
```

폐쇄 모드용 인터페이스 레벨 컨피그레이션

```
description ACCESS (Closed Mode)
switchport mode access
switchport access vlan 10
switchport voice vlan 11
authentication event fail action next-method
authentication event server dead action authorize
authentication event server dead action authorize voice
authentication event server alive action reinitialize
authentication host-mode multi-domain
mab
authentication violation restrict
authentication periodic
authentication timer reauthenticate server
authentication timer inactivity server dynamic
dot1x timeout tx-period 10
spanning-tree portfast
authentication port-control auto
```