Cisco AnyConnect 및 ISE 컨피그레이션을 사용하는 MACsec 스위치 호스트 암호화 예

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[구성](#)
[네트워크 다이어그램 및 트래픽 흐름](#)
[구성](#)
[ISE](#)
[스위치](#)
[AnyConnect NAM](#)
[다음을 확인합니다.](#)
[문제 해결](#)
[작업 시나리오에 대한 디버깅](#)
[실패한 시나리오에 대한 디버깅](#)
[패킷 캡처](#)
[MACsec 및 802.1x 모드](#)
[관련 정보](#)

소개

이 문서에서는 802.1x 신청자(Cisco AnyConnect Mobile Security)와 인증자(스위치) 간의 MACsec(Media Access Control Security) 암호화에 대한 컨피그레이션 예를 제공합니다. Cisco ISE(Identity Services Engine)는 인증 및 정책 서버로 사용됩니다.

MACsec은 802.1AE에서 표준화되었으며 Cisco 3750X, 3560X 및 4500 SUP7E 스위치에서 지원됩니다.802.1AE는 대역외 키를 사용하는 유선 네트워크에서 링크 암호화를 정의합니다.이러한 암호화 키는 802.1x 인증 성공 후 사용되는 MACsec MKA(Key Agreement) 프로토콜과 협상됩니다 .MKA는 IEEE 802.1X-2010에서 표준화됩니다.

패킷은 PC와 스위치 간의 링크에서만 암호화됩니다(포인트-투-포인트 암호화). 스위치에서 수신한 패킷은 해독되고 암호화되지 않은 업링크를 통해 전송됩니다.스위치 간 전송을 암호화하려면 스위치 스위치 암호화를 사용하는 것이 좋습니다.이 암호화의 경우 SAP(Security Association Protocol)를 사용하여 키를 협상하고 재생성합니다.SAP는 Cisco에서 개발한 표준 키 계약 프로토콜입니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 802.1x 구성에 대한 기본 지식
- Catalyst 스위치의 CLI 구성에 대한 기본 지식
- ISE 구성 경험

사용되는 구성 요소

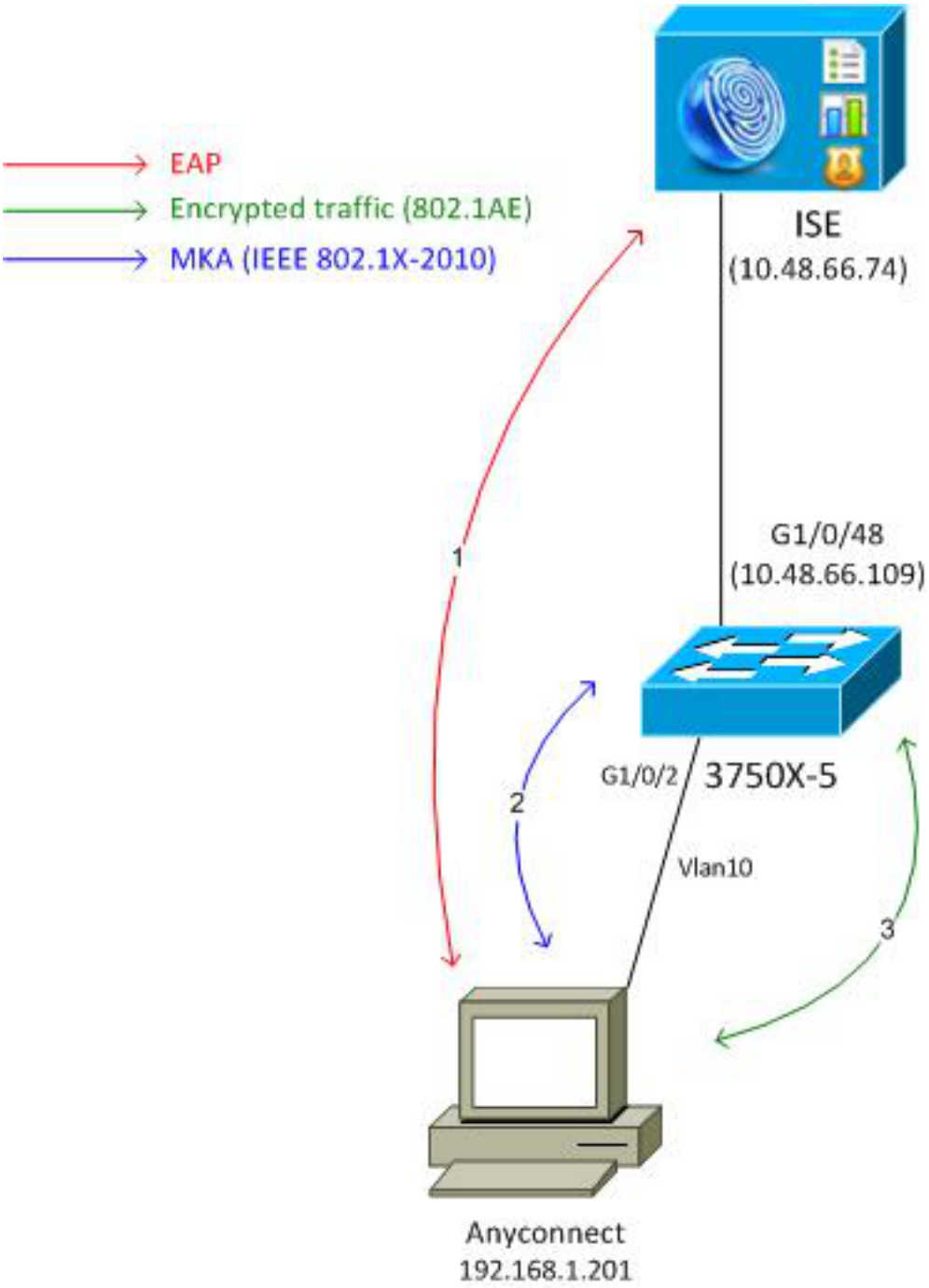
이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Microsoft Windows 7 및 Microsoft Windows XP 운영 체제
- Cisco 3750X 소프트웨어, 버전 15.0 이상
- Cisco ISE 소프트웨어, 버전 1.1.4 이상
- Cisco AnyConnect Mobile Security with Network Access Manager(NAM), 버전 3.1 이상

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

네트워크 다이어그램 및 트래픽 흐름



1단계. 신청자(AnyConnect NAM)가 802.1x 세션을 시작합니다.스위치는 인증자이고 ISE는 인증 서버입니다.EAPOL(Extensible Authentication Protocol over LAN) 프로토콜은 신청자와 스위치 간의 EAP에 대한 전송으로 사용됩니다.RADIUS는 스위치와 ISE 간의 EAP에 대한 전송 프로토콜로 사용됩니다.ISE에서 EAPOL 키를 반환하고 MKA(MACsec Key Agreement) 세션에 사용해야 하므로 MAB(MAC Authentication Bypass)를 사용할 수 없습니다.

2단계. 802.1x 세션이 완료되면 스위치는 EAPOL을 전송 프로토콜로 사용하여 MKA 세션을 시작합니다.신청자가 올바르게 구성된 경우 대칭 128비트 AES-GCM(Galois/Counter Mode) 암호화 키가 일치합니다.

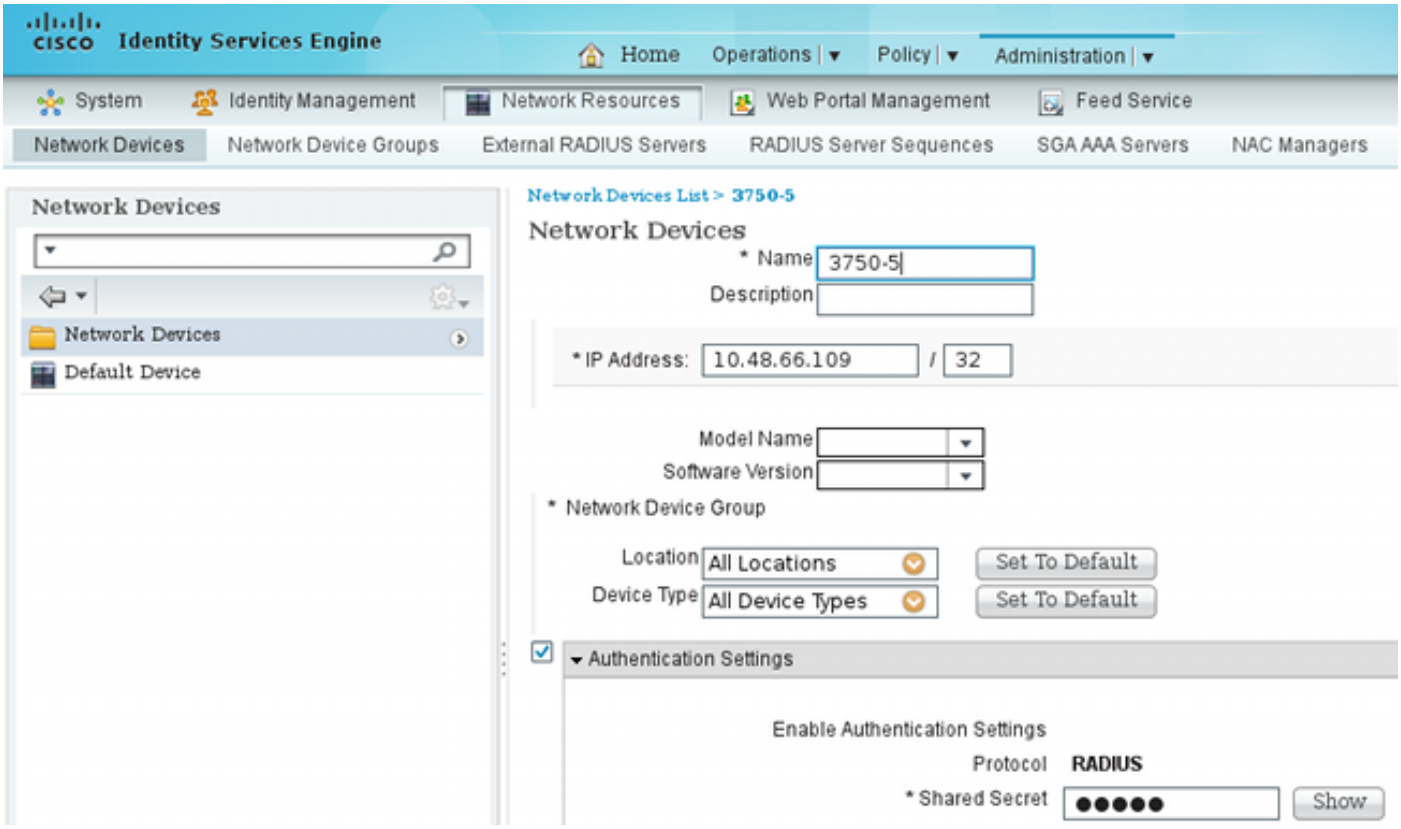
3단계. 신청자와 스위치 간의 모든 후속 패킷은 암호화됩니다(802.1AE 캡슐화).

구성

ISE

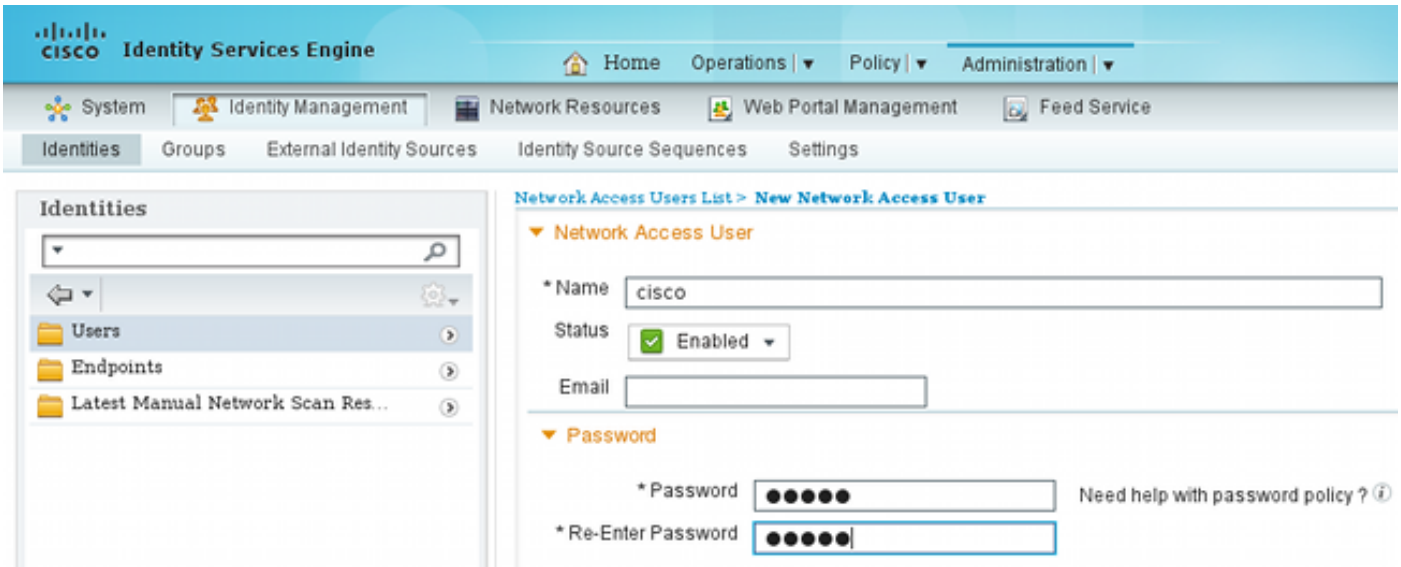
ISE 컨피그레이션에는 암호화 정책을 포함할 수 있는 권한 부여 프로파일을 제외하고 일반적인 802.1x 시나리오가 포함됩니다.

스위치를 네트워크 디바이스로 추가하려면 **Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)**를 선택합니다.RADIUS 사전 공유 키(공유 암호)를 입력합니다.

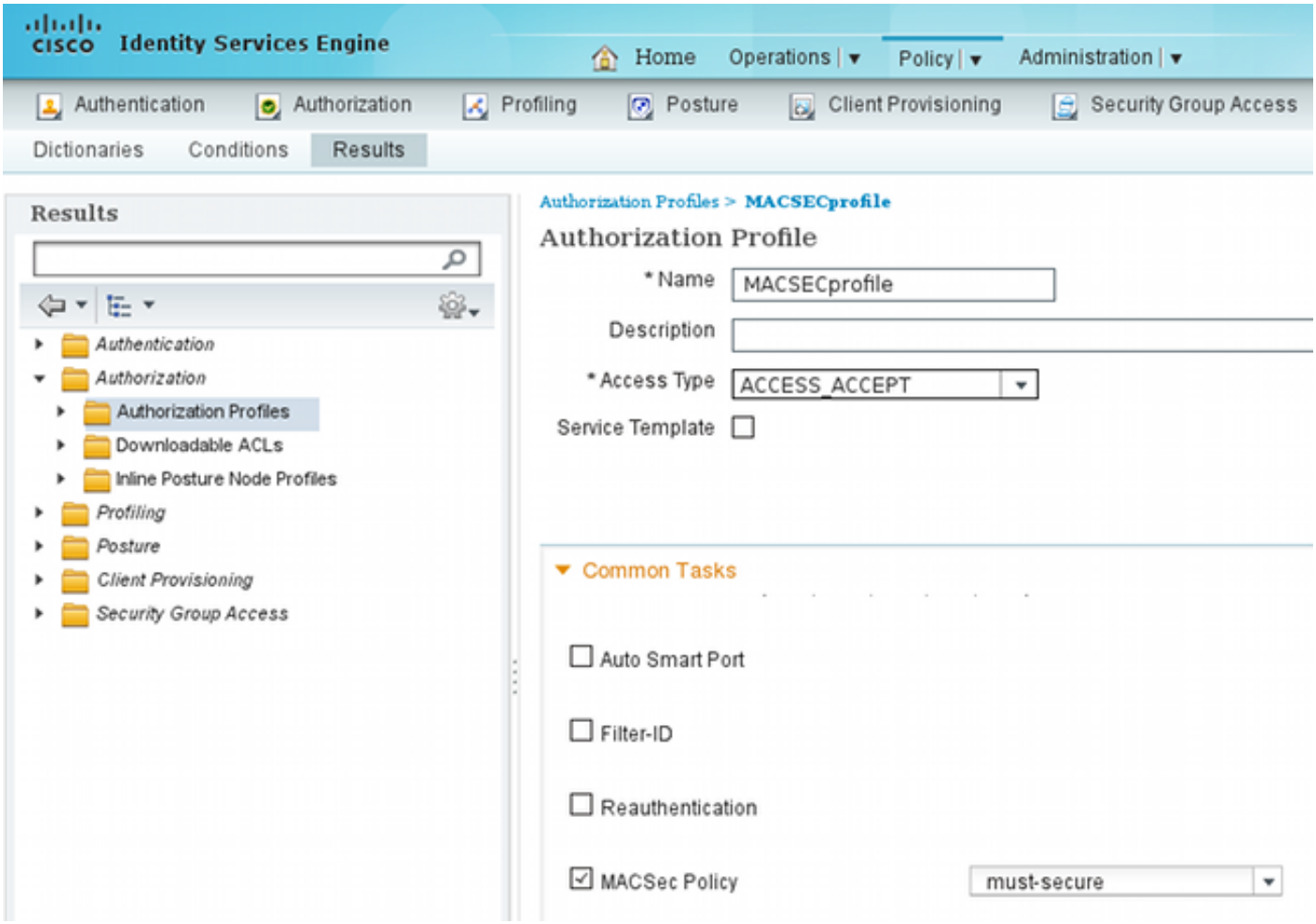


기본 인증 규칙을 사용할 수 있습니다(ISE에서 로컬로 정의된 사용자).

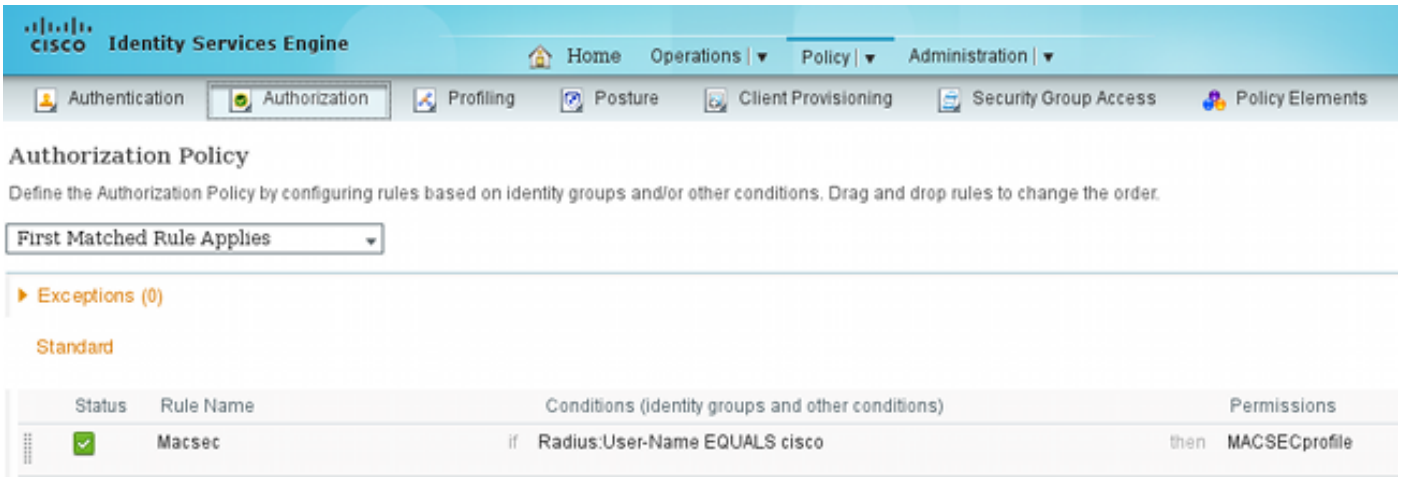
"cisco" 사용자를 로컬로 정의하려면 Administration(관리) > Identity Management(ID 관리) > Users(사용자)를 선택합니다.



권한 부여 프로파일에 암호화 정책이 포함될 수 있습니다.이 예와 같이 ISE가 링크 암호화가 필수인 스위치로 반환되는 정보를 보려면 **Policy > Results > Authorization Profiles**를 선택합니다.또한 VLAN 번호(10)가 구성되었습니다.



권한 **부여** 규칙에서 권한 부여 프로파일을 사용하려면 Policy > Authorization을 선택합니다.이 예에서는 "cisco" 사용자에 대해 구성된 프로필을 반환합니다. 802.1x가 성공하면 ISE는 Cisco AVPair linksec-policy=must-secure로 스위치에 Radius-Accept를 반환합니다.이 속성은 스위치가 MKA 세션을 시작하도록 강제합니다.해당 세션이 실패하면 스위치에서 802.1x 권한 부여도 실패합니다.



스위치

일반적인 802.1x 포트 설정은 다음과 같습니다(위쪽 부분 표시).

```
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
```

```
aaa group server radius ISE
 server name ISE

dot1x system-auth-control

interface GigabitEthernet1/0/2
 description windows7
 switchport mode access
 authentication order dot1x
 authentication port-control auto
 dot1x pae authenticator

radius server ISE
 address ipv4 10.48.66.74 auth-port 1645 acct-port 1646
 timeout 5
 retransmit 2
key cisco
```

로컬 MKA 정책이 생성되고 인터페이스에 적용됩니다.또한 인터페이스에서 MACsec이 활성화됩니다.

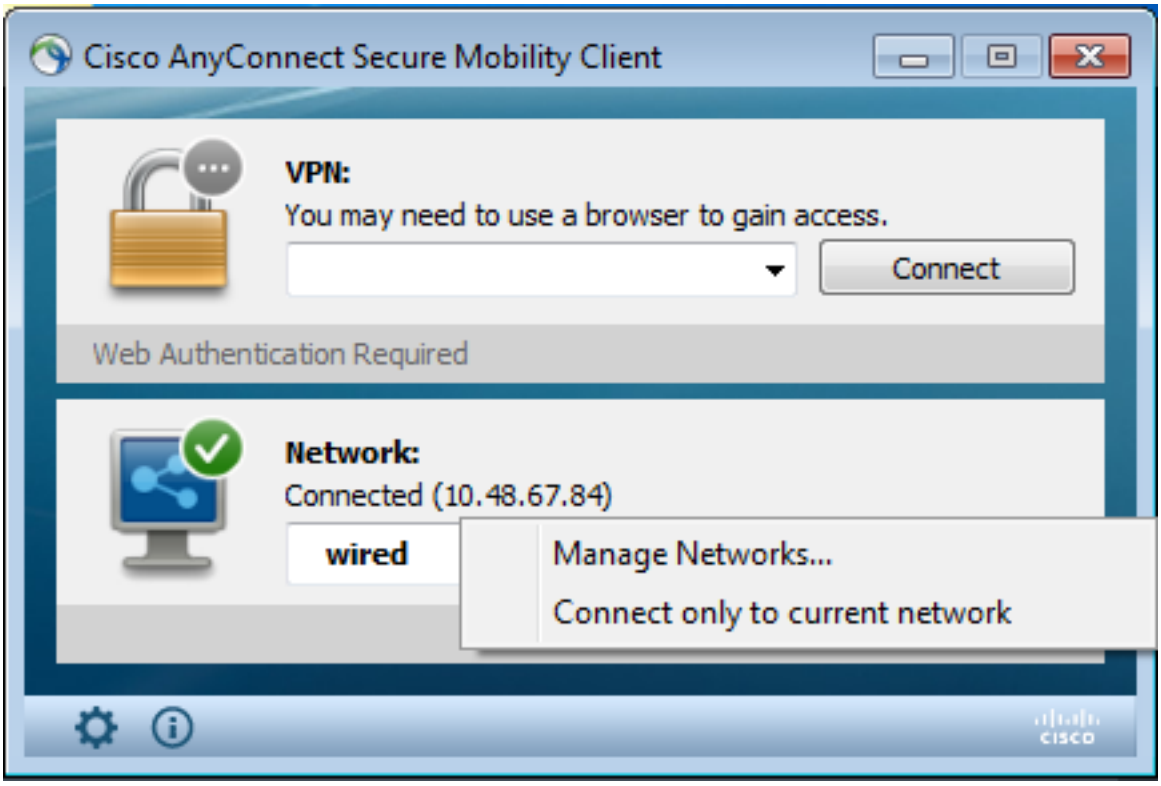
```
mka policy mka-policy
 replay-protection window-size 5000

interface GigabitEthernet1/0/2
 macsec
 mka policy mka-policy
```

로컬 MKA 정책을 사용하면 ISE에서 푸시할 수 없는 자세한 설정을 구성할 수 있습니다.로컬 MKA 정책은 선택 사항입니다.

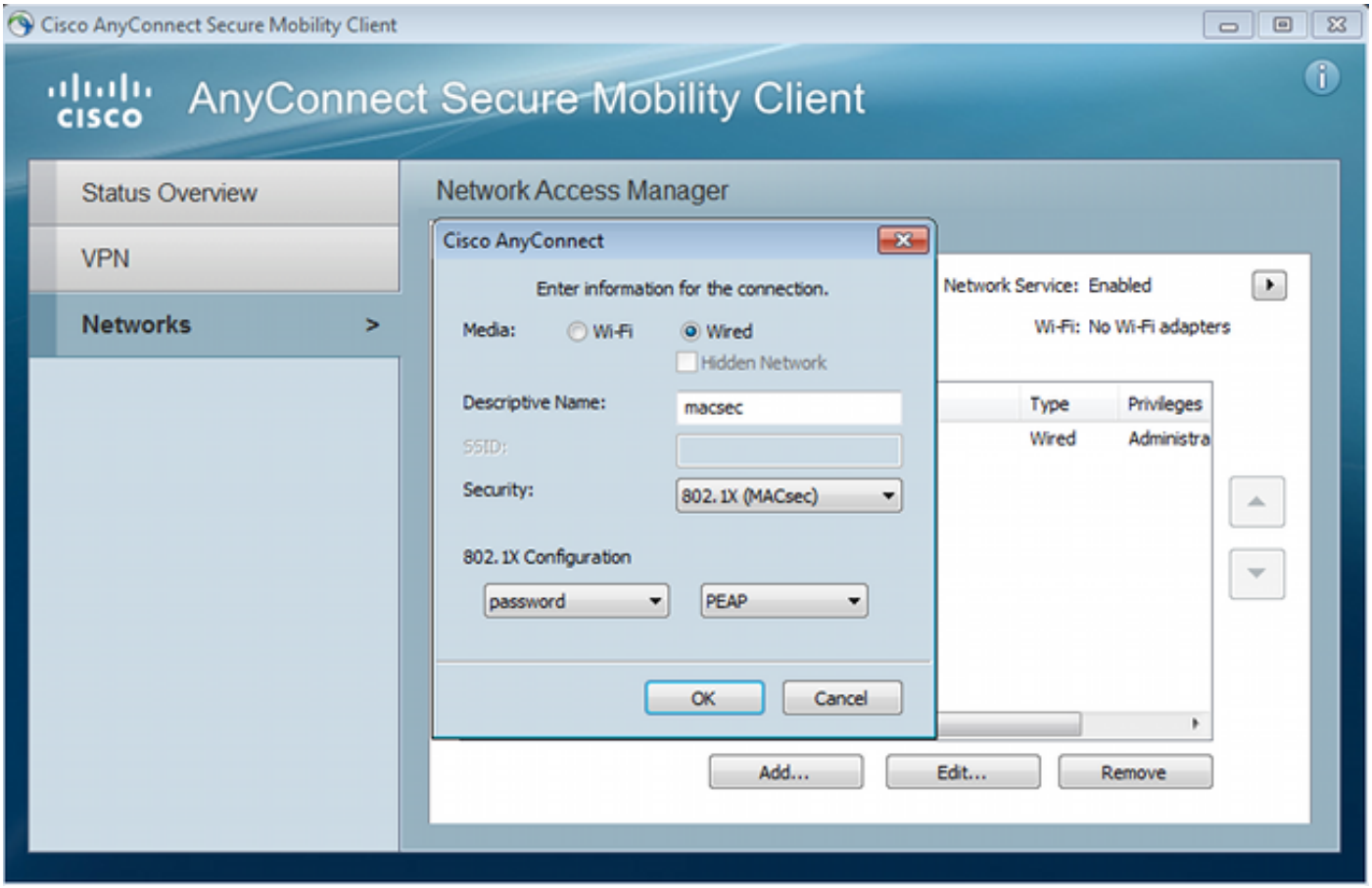
AnyConnect NAM

802.1x 신청자의 프로파일은 수동으로 구성하거나 Cisco ASA를 통해 푸시할 수 있습니다.다음 단계에서는 수동 컨피그레이션을 제공합니다.

NAM 프로파일을 관리하려면



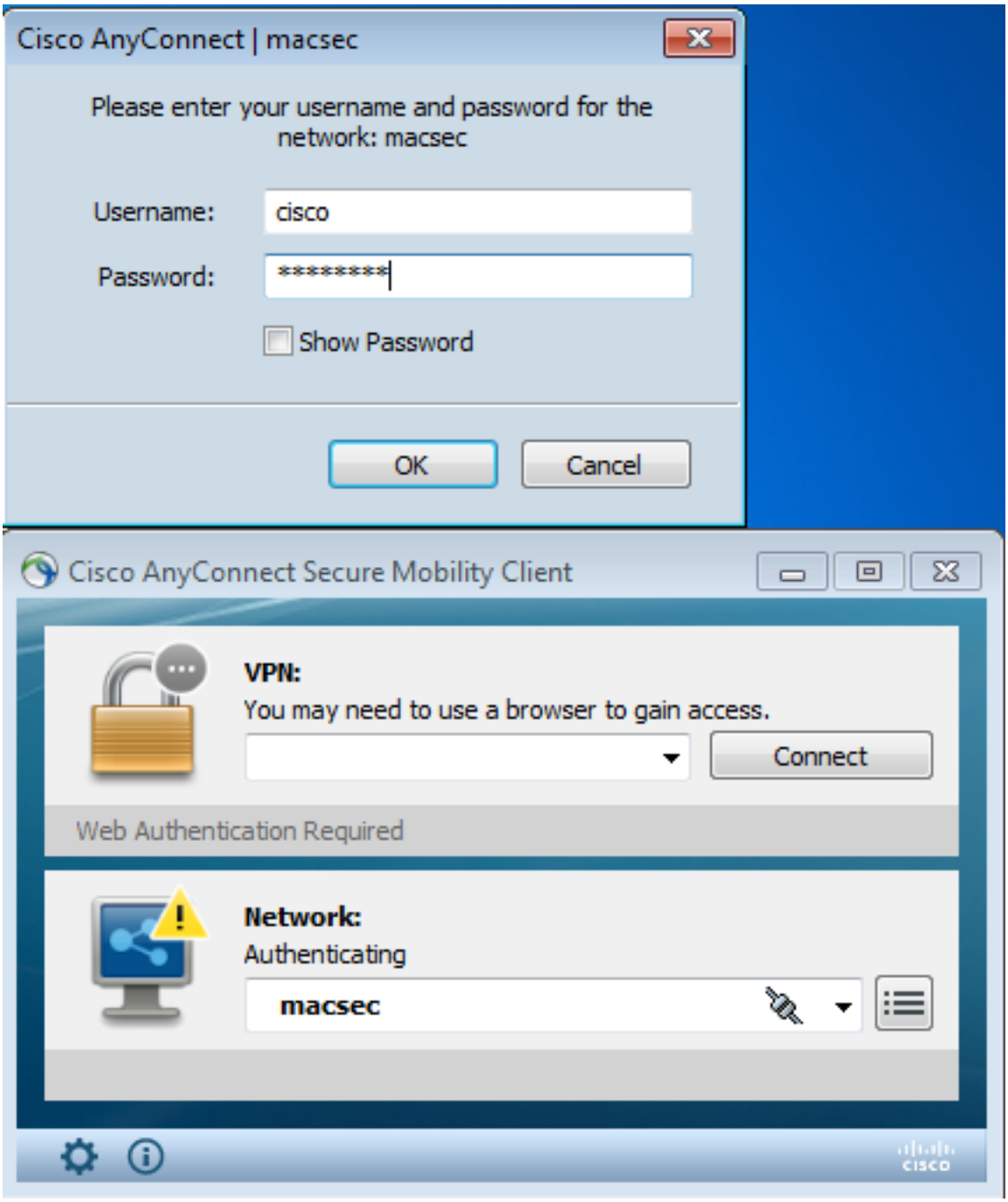
MACsec을 사용하여 새 802.1x 프로필을 추가합니다.802.1x의 경우 PEAP(Protected Extensible Authentication Protocol)가 사용됩니다(ISE에서 구성된 사용자 "cisco").



다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

EAP-PEAP에 대해 구성된 AnyConnect NAM에는 올바른 자격 증명이 필요합니다.



스위치의 세션은 인증되고 인증되어야 합니다.보안 상태는 "보안" 상태여야 합니다.

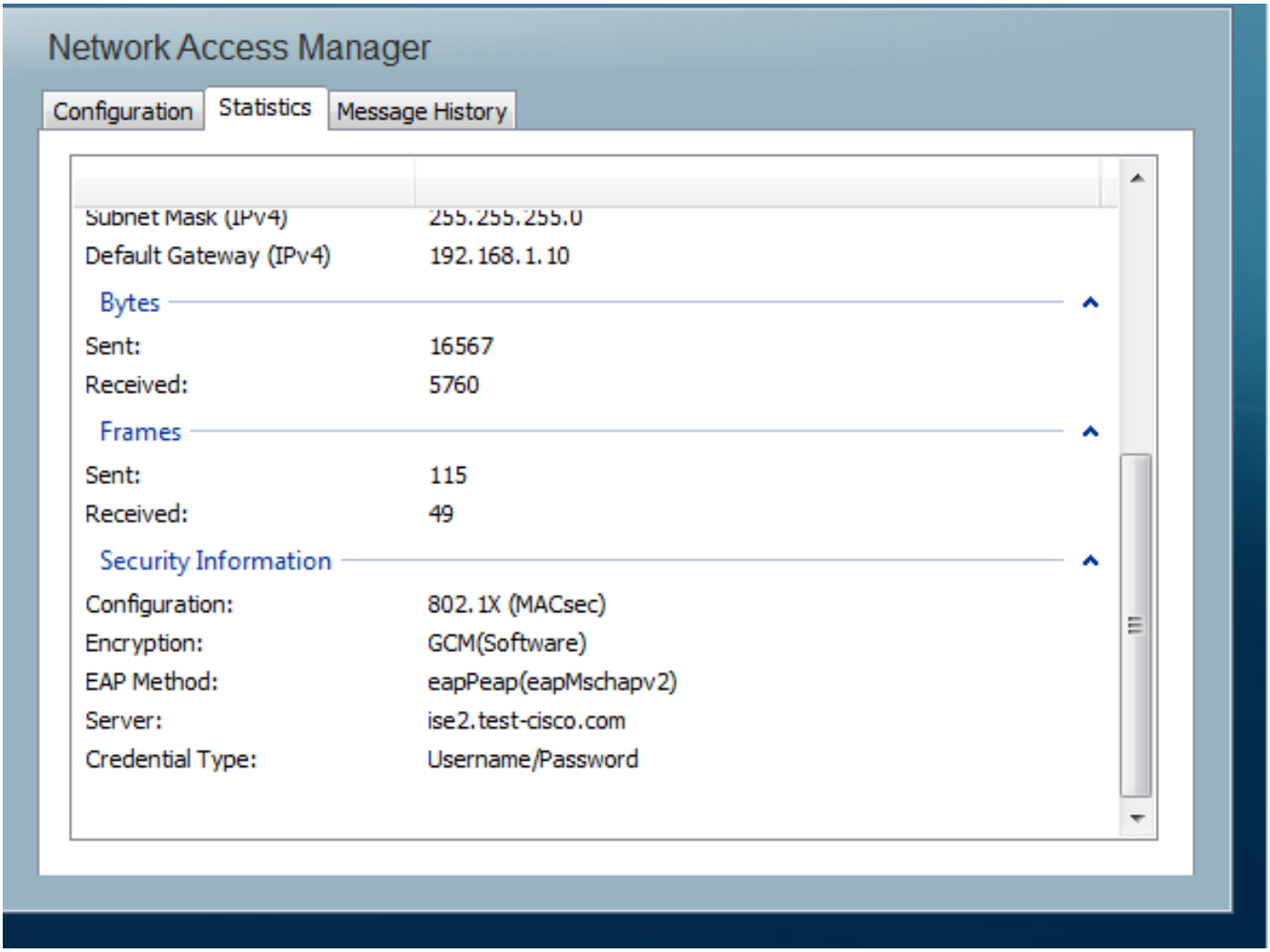
```
bsns-3750-5#show authentication sessions interface g1/0/2
            Interface:  GigabitEthernet1/0/2
          MAC Address:  0050.5699.36ce
           IP Address:  192.168.1.201
            User-Name:  cisco
               Status:  Authz Success
               Domain:  DATA
      Security Policy:  Must Secure
      Security Status:  Secured
       Oper host mode:  single-host
     Oper control dir:  both
        Authorized By:  Authentication Server
          Vlan Policy:  10
      Session timeout:  N/A
```

```
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D56FD55B3BF
     Acct Session ID:  0x00011CB4
              Handle:  0x97000D57

Runnable methods list:
      Method   State
       dot1x    Authc Success
```

스위치의 MACsec 통계는 로컬 정책 설정, 수신/전송 트래픽에 대한 SCI(Secure Channel Identifier), 포트 통계 및 오류와 관련된 세부 정보를 제공합니다.

```
bsns-3750-5#show macsec interface g1/0/2
MACsec is enabled
 Replay protect : enabled
 Replay window : 5000
 Include SCI : yes
 Cipher : GCM-AES-128
 Confidentiality Offset : 0
 Capabilities
 Max. Rx SA : 16
 Max. Tx SA : 16
 Validate Frames : strict
 PN threshold notification support : Yes
 Ciphers supported : GCM-AES-128
 Transmit Secure Channels
 SCI : BC166525A5020002
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Auth-only (0 / 0)
   Encrypt (2788 / 0)
 Receive Secure Channels
 SCI : 0050569936CE0000
  Elapsed time : 00:00:35
  Current AN: 0   Previous AN: -
  SC Statistics
   Notvalid pkts 0      Invalid pkts 0
   Valid pkts 76         Late pkts 0
   Uncheck pkts 0       Delay pkts 0
 Port Statistics
  Ingress untag pkts  0        Ingress notag pkts 2441
  Ingress badtag pkts 0        Ingress unknownSCI pkts 0
  Ingress noSCI pkts 0         Unused pkts 0
  Notusing pkts 0              Decrypt bytes 176153
  Ingress miss pkts 2437
```

AnyConnect에서 통계는 암호화 사용량 및 패킷 통계를 나타냅니다.



문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

작업 시나리오에 대한 디버깅

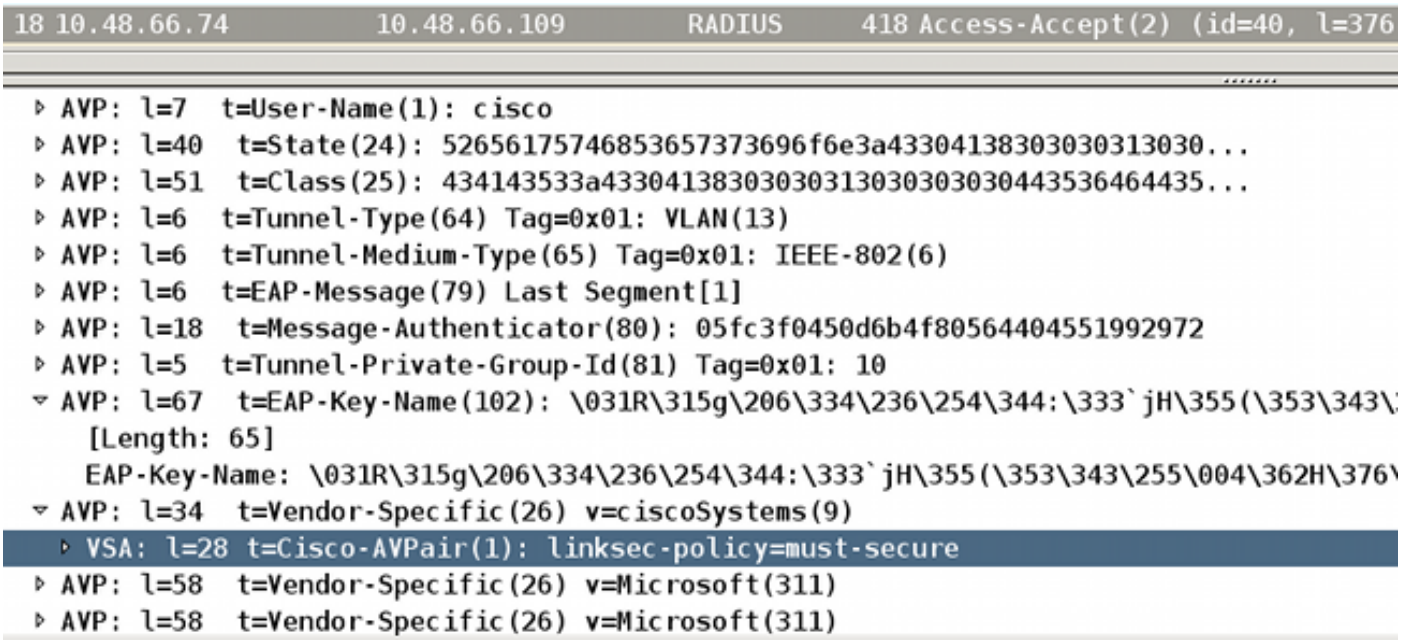
스위치에서 디버깅을 활성화합니다(일부 출력은 명확성을 위해 생략됨).

```
debug macsec event
debug macsec error
debug epm all
debug dot1x all
debug radius
debug radius verbose
```

802.1x 세션이 설정되면 EAPOL을 통해 여러 EAP 패킷이 교환됩니다.RADIUS-Accept 내에서 수행된 ISE(EAP 성공)의 마지막 성공 적 인 응답 또한 여러 Radius 특성을 포함 합니다.

```
RADIUS: Received from id 1645/40 10.48.66.74:1645, Access-Accept, len 376
RADIUS:  EAP-Key-Name          [102] 67  *
RADIUS:  Vendor, Cisco         [26]  34
RADIUS:   Cisco AVpair         [1]   28  "linksec-policy=must-secure"
RADIUS:  Vendor, Microsoft     [26]  58
RADIUS:   MS-MPPE-Send-Key     [16]  52  *
RADIUS:  Vendor, Microsoft     [26]  58
```

```
RADIUS:   MS-MPPE-Recv-Key   [17]  52  *
```
EAP-Key-Name은 MKA 세션에 사용됩니다.linksec-policy는 스위치에서 MACsec을 사용하도록 강제합니다(권한 부여가 완료되지 않으면 실패합니다). 이러한 특성은 패킷 캡처에서도 확인할 수 있습니다.



인증이 성공했습니다.

```
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```
스위치는 특성을 적용합니다(여기에는 또한 전송된 선택적 VLAN 번호가 포함됩니다).

```
%AUTHMGR-5-VLANASSIGN: VLAN 10 assigned to Interface Gi1/0/2 AuditSessionID
C0A8000100000D56FD55B3BF
```
그러면 스위치가 EAPOL 패킷을 보내고 받을 때 MKA 세션을 시작합니다.

```
%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,
AuditSessionID C0A8000100000D56FD55B3BF, AuthMgr-Handle 97000D57
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
EAPOL pak dump rx
dot1x-packet(Gi1/0/2): Received an EAPOL frame
dot1x-packet(Gi1/0/2): Received an MKA packet
```
4개의 패킷 교환 보안 식별자가 RX(Receive) 보안 연결과 함께 생성되면

```
HULC-MACsec: MAC: 0050.5699.36ce, Vlan: 10, Domain: DATA
HULC-MACsec: Process create TxSC i/f GigabitEthernet1/0/2 SCI BC166525A5020002
HULC-MACsec: Process create RxSC i/f GigabitEthernet1/0/2 SCI 50569936CE0000
HULC-MACsec: Process install RxSA request79F6630 for interface GigabitEthernet1/0/2
```
세션이 완료되고 전송(TX) 보안 연결이 추가됩니다.

```
%MKA-5-SESSION_SECURED: (Gi1/0/2 : 2) MKA Session was secured for
```

```
RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D56FD55B3BF,
CKN A2BDC3BE967584515298F3F1B8A9CC13
HULC-MACsec: Process install TxSA request66B4EEC for interface GigabitEthernet1/0/
```

"must-secure" 정책이 일치하고 권한 부여가 성공했습니다.

```
%AUTHMGR-5-SUCCESS: Authorization succeeded for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D56FD55B3BF
```

2초마다 MKA Hello 패킷이 교환되어 모든 참가자가 살아있는지 확인합니다.

```
dot1x-ev(Gi1/0/2): Received TX PDU (5) for the client 0x6E0001EC (0050.5699.36ce)
dot1x-packet(Gi1/0/2): MKA length: 0x0084 data&colon; ^A
dot1x-ev(Gi1/0/2): Sending EAPOL packet to group PAE address
EAPOL pak dump Tx
```

실패한 시나리오에 대한 디버깅

서 플리 컨 트가 MKA에 대해 구성되지 않았고 ISE가 성공 적 인 802.1x 인증 후 암호화를 요청 할 경우:

```
RADIUS: Received from id 1645/224 10.48.66.74:1645, Access-Accept, len 342
%DOT1X-5-SUCCESS: Authentication successful for client (0050.5699.36ce) on
Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
%AUTHMGR-7-RESULT: Authentication result 'success' from 'dot1x' for client
(0050.5699.36ce) on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

스위치는 5개의 EAPOL 패킷을 전송할 때 MKA 세션을 시작하려고 시도합니다.

```
%MKA-5-SESSION_START: (Gi1/0/2 : 2) MKA Session started for RxSCI 0050.5699.36ce/0000,
AuditSessionID C0A8000100000D55FD4D7529, AuthMgr-Handle A4000D56
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
dot1x-ev(Gi1/0/2): Sending out EAPOL packet
EAPOL pak dump Tx
```

그리고 마지막으로 시간 초과가 되고 권한 부여가 실패합니다.

```
 %MKA-4-KEEPALIVE_TIMEOUT: (Gi1/0/2 : 2) Peer has stopped sending MKPDUs for RxSCI
0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529, CKN
F8288CDF7FA56386524DD17F1B62F3BA
%MKA-4-SESSION_UNSECURED: (Gi1/0/2 : 2) MKA Session was stopped by MKA and not
secured for RxSCI 0050.5699.36ce/0000, AuditSessionID C0A8000100000D55FD4D7529,
CKN F8288CDF7FA56386524DD17F1B62F3BA
%AUTHMGR-5-FAIL: Authorization failed or unapplied for client (0050.5699.36ce)
on Interface Gi1/0/2 AuditSessionID C0A8000100000D55FD4D7529
```

802.1x 세션에서는 성공적인 인증을 보고하지만 권한 부여에 실패했습니다.

```
bsns-3750-5#show authentication sessions int g1/0/2
           Interface:  GigabitEthernet1/0/2
         MAC Address:  0050.5699.36ce
```

```
          IP Address:  192.168.1.201
           User-Name:  cisco
              Status:  Authz Failed
              Domain:  DATA
     Security Policy:  Must Secure
     Security Status:  Unsecure
      Oper host mode:  single-host
    Oper control dir:  both
     Session timeout:  N/A
        Idle timeout:  N/A
   Common Session ID:  C0A8000100000D55FD4D7529
     Acct Session ID:  0x00011CA0
              Handle:  0xA4000D56

Runnable methods list:
      Method   State
       dot1x    Authc Success
```

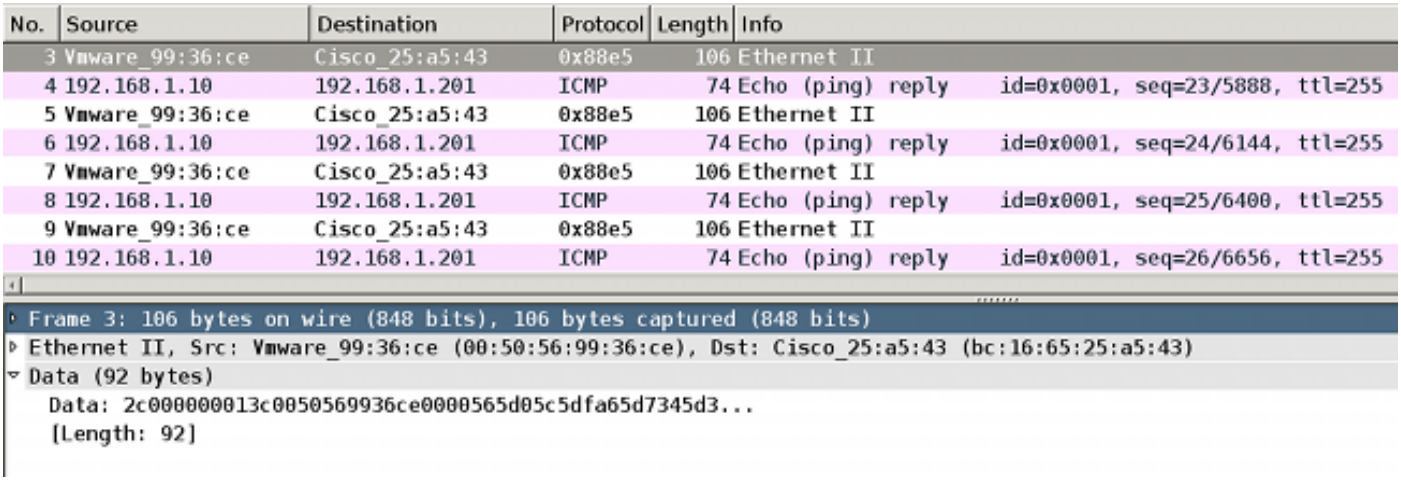
데이터 트래픽이 차단됩니다.

패킷 캡처

서 플리 컨 트 사이트 4 ICMP(Internet Control Message Protocol) 에코 요청/회신이 전송 및 수신되면 다음과 같은 트래픽이 있습니다.

- 스위치로 전송된 4개의 암호화된 ICMP 에코 요청(88e5는 802.1AE용으로 예약됨)
- 4개의 해독된 ICMP 에코 응답 수신

이는 AnyConnect가 Windows API에서 어떻게 후크(libpcap을 전송할 때 이전, 패킷을 수신할 때 libpcap 전) 처리되었기 때문입니다.



> **참고:**스위치드 포트 분석기(SPAN) 또는 EPC(Embedded Packet Capture) 등의 기능을 사용하여 스위치에서 MKA 또는 802.1AE 트래픽을 스니핑하는 기능은 지원되지 않습니다.

MACsec 및 802.1x 모드

모든 802.1x 모드가 MACsec에서 지원되지는 않습니다.

*Cisco TrustSec 3.0 방법 가이드:MACsec 및 NDAC의 소개*는 다음과 같습니다.

- **단일 호스트 모드**:**MACsec은** 단일 호스트 모드에서 **완전히 지원됩니다**.이 모드에서는 MACsec으로 단일 MAC 또는 IP 주소만 인증하고 보호할 수 있습니다.엔드포인트가 인증된 후

포트에서 다른 MAC 주소가 탐지되면 포트에서 보안 위반이 트리거됩니다.

- **MDA(Multi-Domain Authentication) 모드**:이 모드에서는 한 엔드포인트가 데이터 도메인에 있고 다른 엔드포인트가 음성 도메인에 있을 수 있습니다.**MACsec은 MDA 모드에서 완전히 지원됩니다**.두 엔드포인트가 모두 MACsec을 지원하는 경우 각각 독립적인 MACsec 세션에 의해 보호됩니다.하나의 엔드포인트만 MACsec을 지원하는 경우, 다른 엔드포인트는 트래픽을 일반 상태로 전송하는 동안 해당 엔드포인트를 보호할 수 있습니다.
- **다중 인증 모드**:이 모드에서는 단일 스위치 포트에서 거의 무제한의 엔드포인트를 인증할 수 있습니다.**이 모드에서는 MACsec이 지원되지 않습니다.**
- **다중 호스트 모드**:이 모드에서는 MACsec 사용이 기술적으로 가능하지만 **권장되지 않습니다**.멀티호스트 모드에서는 포트의 첫 번째 엔드포인트가 인증되고, 첫 번째 권한 부여를 통해 네트워크에 추가 엔드포인트가 허용됩니다.MACsec은 첫 번째 연결된 호스트에서 작동하지만, 다른 엔드포인트의 트래픽은 암호화 트래픽이 아니므로 실제로 전달되지 않습니다.

관련 정보

- 3750용 Cisco TrustSec 컨피그레이션 가이드
- ASA 9.1용 Cisco TrustSec 컨피그레이션 가이드
- ID 기반 네트워킹 서비스:MAC 보안
- TrustSec Cloud with 802.1x MACsec on Catalyst 3750X Series Switch 컨피그레이션 예
- ASA 및 Catalyst 3750X Series Switch TrustSec 컨피그레이션 예 및 문제 해결 가이드
- Cisco TrustSec 구축 및 로드맵
- 기술 지원 및 문서 – Cisco Systems