Catalyst 9000 Series 스위치의 Dot1x 문제 해결

목차

소개

사전 요구 사항

- 요구 사항
- 사용되는 구성 요소

배경 정보

기본 설정

구성 및 작업 확인

- 802.1x 소개
- 설정
- 인증 세션
- 인증 서버에 연결

문제 해결

- 방법론
- 증상의 예
- 플랫폼별 유틸리티
  - 추적 예

추가 정보

- 기본 설정
- 선택적 설정
- 순서도

관련 정보

소개

이 문서에서는 Catalyst 9000 Series 스위치에서 802.1x NAC(Network Access Control)를 구성, 검증 및 트러블슈팅하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 이러한 주제에 대해 알고 있는 것이 좋습니다.

- Catalyst 9000 시리즈 스위치
- Identity Services Engine(ISE)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Catalyst 9300
- Catalyst 9400
- Catalyst 9500
- Catalyst 9600
- Cisco IOS® XE 17.6.x 이상
- ISE-VM-K9 버전 3.0.0.458

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

참고: 다른 Cisco 플랫폼에서 이러한 기능을 활성화하는 데 사용되는 명령은 해당 설정 가이드를 참조하십시오.

배경 정보

802.1x 표준은 클라이언트-서버 기반 액세스 제어 및 인증 프로토콜을 정의하며, 이는 무단 클라이언트가 제대로 인증되지 않는 한 공개적으로 액세스 가능한 포트를 통해 LAN에 연결하는 것을 방지합니다. 인증 서버는 스위치 또는 LAN에서 제공하는 서비스를 사용하기 전에 스위치 포트에 연결된 각 클라이언트를 인증합니다.

802.1x 인증에는 3가지 구성 요소가 포함되어 있습니다.

신청자 - 인증을 위해 자격 증명을 제출하는 클라이언트
인증자 - 클라이언트와 네트워크 간의 네트워크 연결을 제공하고 네트워크 트래픽을 허용하거나 차단할 수 있는 네트워크 장치입니다.
인증 서버 - 네트워크 액세스 요청을 수신하고 응답할 수 있는 서버로, 인증자에게 연결을 허용할 수 있는지 여부 및 인증 세션에 적용될 기타 다양한 설정을 알려줍니다.

이 문서의 제공 대상은 반드시 보안에 중점을 둘 필요는 없는 엔지니어와 지원 담당자입니다.
802.1x 포트 기반 인증 및 ISE와 같은 구성 요소에 대한 자세한 내용은 해당 컨피그레이션 가이드를 참조하십시오.

참고: 가장 정확한 기본 802.1x 인증 컨피그레이션은 특정 플랫폼 및 코드 버전에 맞는 컨피그레이션 가이드를 참조하십시오.

기본 설정

이 섹션에서는 802.1x 포트 기반 인증을 구현하는 데 필요한 기본 컨피그레이션에 대해 설명합니다. 추가 기능 설명은 이 문서의 "추가 사항" 탭에 있습니다. 버전마다 컨피그레이션 표준이 조금씩 다릅니다. 현재 버전 컨피그레이션 가이드를 기준으로 컨피그레이션을 검증합니다.

802.1x 사후 기반 인증을 구성하기 전에 AAA(Authentication, Authorization, and Account)를 활성화해야 하며 방법 목록을 설정해야 합니다.

- 방법 목록은 사용자 인증을 위해 쿼리할 시퀀스 및 인증 방법을 설명합니다.
- 802.1x도 전역적으로 활성화해야 합니다.

<#root>

```
C9300>
enable

C9300#
configure terminal

C9300(config)#
aaa new-model

C9300(config)#
aaa authentication dot1x default group radius

C9300(config)#
dot1x system-auth-control
```

스위치에서 RADIUS 서버 정의

<#root>

```
C9300(config)#
radius server RADIUS_SERVER_NAME

C9300(config-radius-server)#
address ipv4 10.0.1.12

C9300(config-radius-server)#
key rad123

C9300(config-radius-server)#
exit
```

클라이언트 인터페이스에서 802.1x를 활성화합니다.

<#root>

```
C9300(config)#
interface TenGigabitEthernet 1/0/4

C9300(config-if)#
switchport mode access

C9300(config-if)#
authentication port-control auto

C9300(config-if)#
dot1x pae authenticator

C9300(config-if)#
end
```

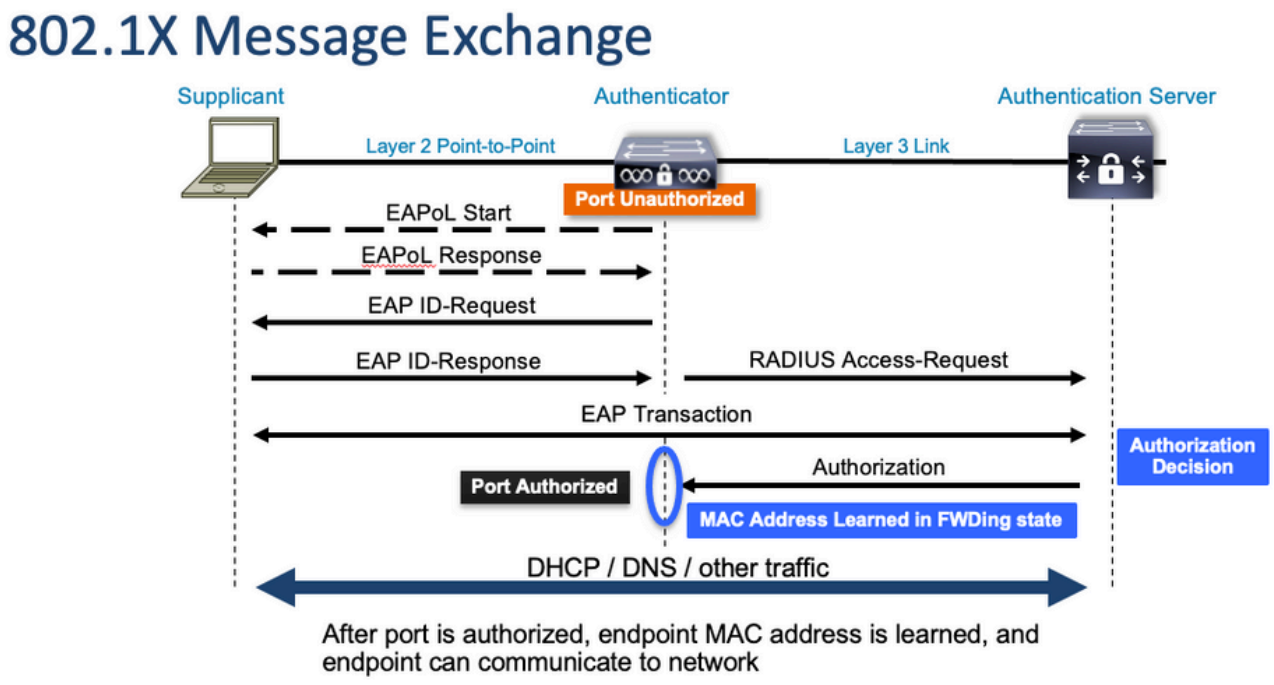
구성 및 작업 확인

이 섹션에서는 801.1x에 대한 배경 정보와 컨피그레이션 및 운영을 확인하는 방법을 제공합니다.

802.1x 소개

802.1x에는 EAPoL(LAN을 통한 확장 가능 인증 프로토콜)을 통한 클라이언트-인증자(point-to-point) 트래픽과 RADIUS를 통해 캡슐화되는 인증 서버-인증자 트래픽의 두 가지 고유한 트래픽 유형이 포함됩니다.

이 다이어그램은 간단한 dot1x 트랜잭션에 대한 데이터 흐름을 나타냅니다



인증자(스위치) 및 인증 서버(예: ISE)는 종종 레이어 3으로 구분됩니다. RADIUS 트래픽은 인증자와 서버 간에 네트워크를 통해 라우팅됩니다. EAPoL 트래픽은 신청자(클라이언트)와 인증자 간의 직접 링크에서 교환됩니다.

MAC 학습은 인증 및 권한 부여 후에 발생합니다.

다음은 802.1x와 관련된 문제에 접근할 때 염두에 두어야 할 몇 가지 질문입니다.

- 올바르게 구성되었습니까?
- 인증 서버에 연결할 수 있습니까?
- 인증 관리자의 상태는 어떻습니까?
- 클라이언트와 인증자 간 또는 인증자와 인증 서버 간 패킷 전달에 문제가 있습니까?

설정

일부 컨피그레이션은 주요 릴리스마다 조금씩 다릅니다. 플랫폼/코드별 지침은 관련 컨피그레이션 가이드를 참조하십시오.

802.1x 포트 기반 인증을 활용하도록 AAA를 구성해야 합니다.

- "dot1x"에 대한 인증 방법 목록을 설정해야 합니다. 이는 802.1X가 활성화된 일반적인 AAA 컨피그레이션을 나타냅니다.

<#root>

```
C9300#

show running-config | section aaa

aaa new-model

<-- This enables AAA.

aaa group server radius ISEGROUP

<-- This block establishes a RADIUS server group named "ISEGROUP".
 server name DOT1x

 ip radius source-interface Vlan1
aaa authentication dot1x default group ISEGROUP

<-- This line establishes the method list for 802.1X authentication. Group ISEGROUP is be used.
aaa authorization network default group ISEGROUP

aaa accounting update newinfo periodic 2880
aaa accounting dot1x default start-stop group ISEGROUP

C9300#

show running-config | section radius

aaa group server radius ISEGROUP
 server name DOT1x
 ip radius source-interface Vlan1

<-- Notice 'ip radius source-interface' configuration exists in both global configuration and the aaa se

ip radius source-interface Vlan1
```

```
radius server DOT1x
 address ipv4 10.122.141.228 auth-port 1812 acct-port 1813
<-- 1812 and 1813 are default auth-port and acct-port, respectively.
 key secretKey
```

이는 802.1x가 활성화된 인터페이스 컨피그레이션의 예입니다. MAB (MAC 인증 우회) 는 dot1x 서플리 컨 트를 지원 하지 않는 클라이언트를 인증 하기 위한 일반 적 인 백업 방법입니다.

<#root>

```
C9300#
show running-config interface te1/0/4
Building configuration...

Current configuration : 148 bytes
!
interface TenGigabitEthernet1/0/4
 switchport access vlan 50
 switchport mode access
 authentication order dot1x mab
<-- Specifies authentication order, dot1x and then mab

 authentication priority dot1x mab
<-- Specifies authentication priority, dot1x and then mab

 authentication port-control auto
<-- Enables 802.1x dynamic authentication on the port

 mab
<-- Enables MAB
 dot1x pae authenticator
<-- Puts interface into "authenticator" mode.
end
```

"show mac address-table interface <interface>"를 사용하여 인터페이스에서 MAC 주소를 학습했는지 확인합니다. 인터페이스는 성공적으로 인증될 때만 MAC 주소를 인식합니다.

<#root>

```
C9300#
show mac address-table interface te1/0/4
```

```
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
  50    0800.2766.efc7    STATIC      Te1/0/4

<-- The "type" is STATIC and the MAC persists until the authentication session is cleared.

Total Mac Addresses for this criterion: 1
```

인증 세션

Show 명령은 802.1x 인증 검증에 사용할 수 있습니다.

현재 인증 세션에 대한 정보를 표시하려면 "show authentication sessions" 또는 "show authentication sessions <interface>"를 사용하십시오. 이 예에서는 Te1/0/4만 활성 인증 세션이 설정되어 있습니다.

```
<#root>

C9300#

show authentication sessions interface te1/0/4

Interface                MAC Address    Method  Domain  Status Fg  Session ID
-----------------------------------------------------------------------------------------
Te1/0/4                  0800.2766.efc7 dot1x   DATA    Auth        13A37A0A0000011DC85C34C5

<-- "Method" and "Domain" in this example are dot1x and DATA, respectfully. Multi-domain authentication


Key to Session Events Blocked Status Flags:

  A - Applying Policy (multi-line status for details)
  D - Awaiting Deletion
  F - Final Removal in progress
  I - Awaiting IIF ID allocation
  P - Pushed Session
  R - Removing User Profile (multi-line status for details)
  U - Applying User Profile (multi-line status for details)
  X - Unknown Blocker

Runnable methods list:
  Handle  Priority  Name
      13         5  dot1xSup
       1         5  dot1x
       2        10  webauth
      14        15  mab
```

"Show authentication sessions interface <interface> details"는 특정 인터페이스 인증 세션에 대한 추가 세부 정보를 제공합니다.

<#root>

C9300#

show authentication session interface te1/0/4 details

```
            Interface:  TenGigabitEthernet1/0/4
               IIF-ID:  0x14D66776
          MAC Address:  0800.2766.efc7
         IPv6 Address:  Unknown
         IPv4 Address:  Unknown
            User-Name:  alice
               Status:  Authorized
               Domain:  DATA
       Oper host mode:  multi-auth
     Oper control dir:  both
      Session timeout:  N/A
  Acct update timeout:  172800s (local), Remaining: 152363s
    Common Session ID:  13A37A0A0000011DC85C34C5
      Acct Session ID:  0x00000002
               Handle:  0xe8000015
       Current Policy:  POLICY_Te1/0/4
```

<-- If a post-authentication ACL is applied, it is listed here.

```
Local Policies:
    Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
      Security Policy:  Should Secure

Server Policies:


Method status list:
       Method           State
        dot1x           Authc Success
```

<-- This example shows a successful 801.1x authentication session.

인터페이스에서 인증이 활성화되었지만 활성 세션이 없는 경우 실행 가능한 방법 목록이 표시됩니다. "제공된 기준과 일치하는 세션 없음"도 표시됩니다.

<#root>

C9300#

show authentication sessions interface te1/0/5

```
No sessions match supplied criteria.

Runnable methods list:
  Handle  Priority  Name
      13         5  dot1xSup
       1         5  dot1x
       2        10  webauth
      14        15  mab
```

인터페이스에서 활성화된 인증이 없으면 인터페이스에서 탐지된 인증 관리자 프레즌스가 없습니다. "제공된 기준과 일치하는 세션 없음"도 표시됩니다.

<#root>

C9300#

show authentication sessions interface te1/0/6

No sessions match supplied criteria.
No Auth Manager presence on this interface

인증 서버에 연결

802.1x 인증에 성공하려면 인증 서버에 연결해야 합니다.

연결을 빠르게 테스트하려면 "ping <server_ip>"을 사용하십시오. RADIUS 소스 인터페이스에서 ping이 제공되는지 확인합니다.

<#root>

C9300#

ping 10.122.141.228 source vlan 1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.122.141.228, timeout is 2 seconds:
Packet sent with a source address of 10.122.163.19
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

"show aaa servers" 명령은 서버 상태를 식별하고 구성된 모든 AAA 서버와의 트랜잭션에 대한 통계를 제공합니다.

<#root>

C9300#

show aaa servers

RADIUS: id 3, priority 1, host 10.122.141.228, auth-port 1812, acct-port 1813, hostname DOT1x <-- Speci
     State: current UP, duration 84329s, previous duration 0s <-- Current State
     Dead: total time 0s, count 1
     Platform State from SMD: current UP, duration 24024s, previous duration 0s
     SMD Platform Dead: total time 0s, count 45
     Platform State from WNCD (1) : current UP
     Platform State from WNCD (2) : current UP
     Platform State from WNCD (3) : current UP
     Platform State from WNCD (4) : current UP
     Platform State from WNCD (5) : current UP

```
    Platform State from WNCD (6) : current UP
    Platform State from WNCD (7) : current UP
    Platform State from WNCD (8) : current UP, duration 0s, previous duration 0s
    Platform Dead: total time 0s, count 0UP
    Quarantined: No


Authen: request 510, timeouts 468, failover 0, retransmission 351   <-- Authentication Statistics

            Response: accept 2, reject 2, challenge 38
            Response: unexpected 0, server error 0, incorrect 12, time 21ms
            Transaction: success 42, failure 117
            Throttled: transaction 0, timeout 0, failure 0
            Malformed responses: 0
            Bad authenticators: 0
            Dot1x transactions:
            Response: total responses: 42, avg response time: 21ms
            Transaction: timeouts 114, failover 0
            Transaction: total 118, success 2, failure 116
            MAC auth transactions:
            Response: total responses: 0, avg response time: 0ms
            Transaction: timeouts 0, failover 0
            Transaction: total 0, success 0, failure 0
    Author: request 0, timeouts 0, failover 0, retransmission 0
            Response: accept 0, reject 0, challenge 0
            Response: unexpected 0, server error 0, incorrect 0, time 0ms
            Transaction: success 0, failure 0
            Throttled: transaction 0, timeout 0, failure 0
            Malformed responses: 0
            Bad authenticators: 0
            MAC author transactions:
            Response: total responses: 0, avg response time: 0ms
            Transaction: timeouts 0, failover 0
            Transaction: total 0, success 0, failure 0
    Account: request 3, timeouts 0, failover 0, retransmission 0
            Request: start 2, interim 0, stop 1
            Response: start 2, interim 0, stop 1
            Response: unexpected 0, server error 0, incorrect 0, time 11ms
            Transaction: success 3, failure 0
            Throttled: transaction 0, timeout 0, failure 0
            Malformed responses: 0
            Bad authenticators: 0
    Elapsed time since counters last cleared: 1d3h4m
    Estimated Outstanding Access Transactions: 0
    Estimated Outstanding Accounting Transactions: 0
    Estimated Throttled Access Transactions: 0
    Estimated Throttled Accounting Transactions: 0
    Maximum Throttled Transactions: access 0, accounting 0
    Consecutive Response Failures: total 115
            SMD Platform : max 113, current 0 total 113
            WNCD Platform: max 0, current 0 total 0
            IOSD Platform : max 2, current 2 total 2
    Consecutive Timeouts: total 466
            SMD Platform : max 455, current 0 total 455
            WNCD Platform: max 0, current 0 total 0
            IOSD Platform : max 11, current 11 total 11
    Requests per minute past 24 hours:
            high - 23 hours, 25 minutes ago: 4
            low  - 3 hours, 4 minutes ago: 0
            average: 0
```

"test aaa" 유틸리티를 사용하여 스위치에서 인증 서버로의 연결을 확인합니다. 이 유틸리티는 더 이상 사용되지 않으며 무기한 사용할 수 없습니다.

```
<#root>

C9300#

debug radius <-- Classic Cisco IOS debugs are only useful in certain scenarios. See "Cisco IOS XE Debugs


C9300#

test aaa group ISE username password new-code <-- This sends a RADIUS test probe to the identified serve


User rejected

<-- This means that the RADIUS server received our test probe, but rejected our user. We can conclude th


*Jul 16 21:05:57.632: %PARSER-5-HIDDEN: Warning!!! ' test platform-aaa group server-group ISE user-name
*Jul 16 21:05:57.644: RADIUS/ENCODE(00000000):Orig. component type = Invalid
*Jul 16 21:05:57.644: RADIUS/ENCODE(00000000): dropping service type, "radius-server attribute 6 on-for
*Jul 16 21:05:57.644: RADIUS(00000000): Config NAS IP: 10.122.161.63
*Jul 16 21:05:57.644: vrfid: [65535] ipv6 tableid : [0]
*Jul 16 21:05:57.644: idb is NULL
*Jul 16 21:05:57.644: RADIUS(00000000): Config NAS IPv6: ::
*Jul 16 21:05:57.644: RADIUS(00000000): sending
*Jul 16 21:05:57.644: RADIUS/DECODE(00000000): There is no General DB. Want server details may not be s
*Jul 16 21:05:57.644: RADIUS(00000000): Send Access-Request to 10.122.141.199:1812 id 1645/8, len 50

<-- Sending Access-Request to RADIUS server


RADIUS: authenticator 3B 65 96 37 63 E3 32 41 - 3A 93 63 B6 6B 6A 5C 68
*Jul 16 21:05:57.644: RADIUS: User-Password [2] 18 *
*Jul 16 21:05:57.644: RADIUS: User-Name [1] 6 "username"
*Jul 16 21:05:57.644: RADIUS: NAS-IP-Address [4] 6 10.122.161.63
*Jul 16 21:05:57.644: RADIUS(00000000): Sending a IPv4 Radius Packet
*Jul 16 21:05:57.644: RADIUS(00000000): Started 5 sec timeout
*Jul 16 21:05:57.669: RADIUS: Received from id 1645/8 10.122.141.199:1812, Access-Reject, len 20

<-- Receiving the Access-Reject from RADIUS server


RADIUS: authenticator 1A 11 32 19 12 F9 C3 CC - 6A 83 54 DF 0F DB 00 B8
*Jul 16 21:05:57.670: RADIUS/DECODE(00000000): There is no General DB. Reply server details may not be
*Jul 16 21:05:57.670: RADIUS(00000000): Received from id 1645/8
```

문제 해결

이 섹션에서는 Catalyst 스위치의 대부분의 802.1x 문제를 해결하는 방법에 대한 지침을 제공합니다.

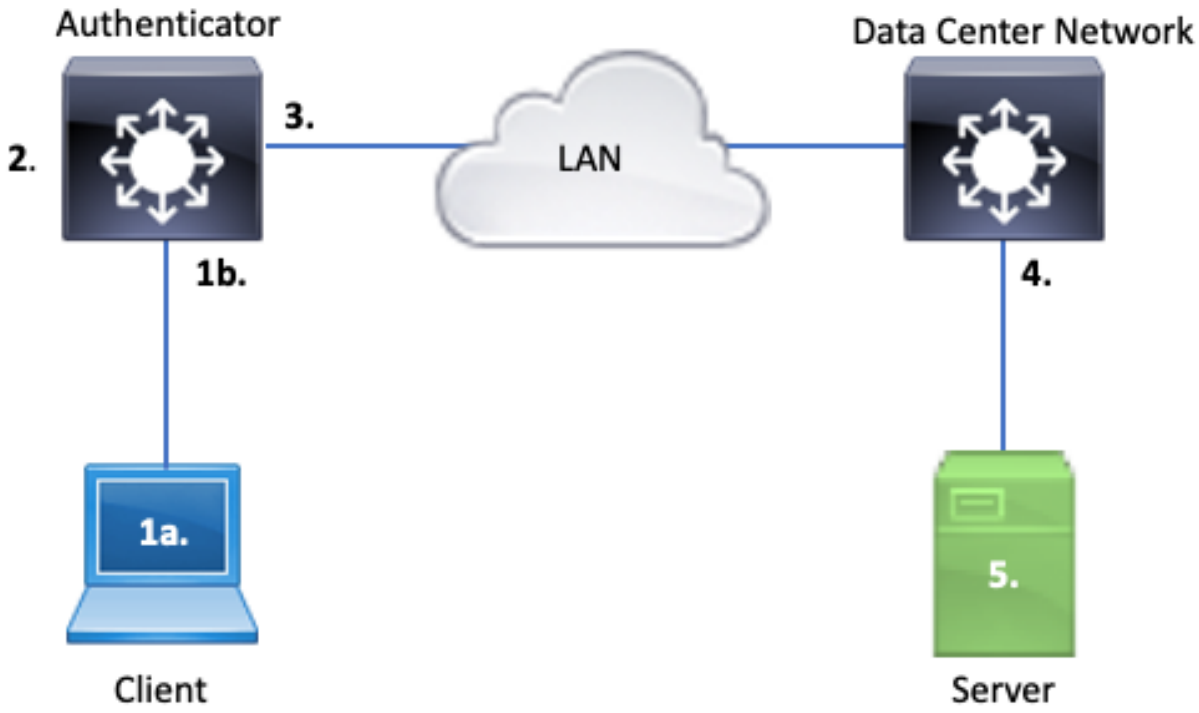
방법론

최상의 결과를 위해 802.1x 및 인증과 관련된 문제를 체계적으로 접근합니다. 몇 가지 좋은 질문에

답해 주십시오.

- 문제가 단일 스위치로 분리되었습니까? 단일 포트? 단일 클라이언트 유형?
- 구성이 검증되었습니까? 인증 서버에 연결할 수 있습니까?
- 매번 문제가 발생합니까, 아니면 간헐적으로 발생합니까? 재인증 또는 권한 부여 변경에서만 발생합니까?

명백한 문제가 배제된 후에도 문제가 지속되는 경우 실패한 단일 트랜잭션을 끝까지 면밀히 검토하십시오. 클라이언트에서 서버로의 802.1x 트랜잭션을 조사하는 가장 완벽한 데이터 집합에는 다음이 포함됩니다.



1a. 클라이언트 및/또는

10억 클라이언트가 연결되는 액세스 인터페이스에서

이 참조 지점은 dot1x가 활성화된 액세스 포트와 클라이언트 간에 교환되는 EAPoL 패킷에 대한 통찰력을 제공하는 데 중요합니다. SPAN은 클라이언트와 인증자 간의 트래픽을 보는 데 가장 신뢰할 수 있는 도구입니다.

2. 인증자에 대한 디버깅

디버그를 통해 인증자를 통해 트랜잭션을 추적할 수 있습니다.

- 인증자는 수신된 EAPoL 패킷을 펀트하고 인증 서버로 향하는 유니캐스트 RADIUS 캡슐화 트래픽을 생성해야 합니다.

- 최대 효과를 위해 적절한 디버그 수준이 설정되었는지 확인합니다.

3. 인증자 옆의 캡처

이 캡처를 사용하면 인증자와 인증 서버 간의 대화를 볼 수 있습니다.

- 이 캡처는 인증자의 관점에서 전체 대화를 정확하게 표시합니다.
- 포인트 4의 캡처와 페어링하면 인증 서버와 인증자 간에 손실이 있는지 확인할 수 있습니다.

4. 인증 서버 옆의 캡처

이 캡처는 포인트 3에서 캡처의 동반자입니다.

- 이 캡처는 인증 서버의 관점에서 전체 대화를 제공합니다.
- 포인트 3의 캡처와 페어링하면 인증자와 인증 서버 간에 손실이 있는지 확인할 수 있습니다.

5. 인증 서버에서 캡처, 디버깅, 로그

퍼즐의 마지막 조각, 서버 디버그는 서버가 우리의 거래에 대해 무엇을 알고 있는지 우리에게 알려줍니다.

- 네트워크 엔지니어는 이 엔드 투 엔드 데이터 집합을 사용하여 트랜잭션이 중단된 위치를 확인하고 문제에 기여하지 않는 구성 요소를 제외할 수 있습니다.

증상의 예

이 섹션에서는 일반적인 증상 및 문제 시나리오의 목록을 제공합니다.

- 클라이언트에서 응답 없음

스위치에 의해 생성된 EAPoL 트래픽이 응답을 유도하지 않으면 다음과 같은 syslog가 표시됩니다.

```
Aug 23 11:23:46.387 EST: %DOT1X-5-FAIL: Switch 1 R0/0: sessmgrd: Authentication failed for client (aaaa
```

이유 코드 "No Response from Client(클라이언트에서 응답 없음)"는 스위치가 dot1x 프로세스를 시작했지만 시간 제한 내에 클라이언트에서 응답을 받지 못했음을 나타냅니다.
즉, 클라이언트가 스위치 포트에서 전송한 인증 트래픽을 수신하지 않았거나 이해하지 못했거나, 클라이언트의 응답이 스위치 포트에서 수신되지 않았습니다.

- 클라이언트 포기 세션

인증 세션이 시작되었지만 완료되지 않은 경우 인증 서버(예: ISE)는 클라이언트가 세션을 시작했지만 완료되기 전에 세션을 취소했음을 보고합니다.
종종 이는 인증 프로세스가 부분적으로만 완료할 수 있음을 의미합니다.

인증자 스위치와 인증 서버 간의 전체 트랜잭션이 엔드 투 엔드로 전달되고 인증 서버에서 올바르게 해석되는지 확인합니다.

RADIUS 트래픽이 네트워크에서 손실되거나 제대로 어셈블할 수 없는 방식으로 전달되는 경우 트랜잭션이 완료되지 않고 클라이언트가 인증을 재시도합니다. 서버는 클라이언트가 세션을 취소했음을 보고합니다.

- MAB 클라이언트가 DHCP 실패/APIPA로 폴백

MAB(MAC Authentication Bypass)는 MAC 주소를 기반으로 인증을 허용합니다. 신청자 소프트웨어를 지원하지 않는 클라이언트는 MAB를 통해 인증하는 경우가 많습니다.

MAB가 인증을 위한 폴백 방법으로 사용되는 반면 dot1x가 스위치 포트에서 실행되는 기본 방법인 경우 클라이언트가 DHCP를 완료할 수 없는 시나리오가 발생할 수 있습니다.

그 문제는 결국 운영 질서로 귀결된다. dot1x가 실행되는 동안 스위치 포트는 인증이 완료되거나 dot1x가 시간 초과될 때까지 EAPoL 이외의 패킷을 사용합니다. 그러나 클라이언트는 즉시 IP 주소 가져오기를 시도하고 DHCP 검색 메시지를 브로드캐스트합니다. 이러한 검색 메시지는 dot1x가 구성된 시간 초과 값을 초과하고 MAB를 실행할 수 있을 때까지 스위치 포트에서 소비됩니다. 클라이언트 DHCP 시간 초과 기간이 dot1x 시간 초과 기간보다 작으면 DHCP가 실패하고 클라이언트는 APIPA 또는 해당 폴백 전략에 의해 지시되는 어떤 것으로도 폴백됩니다.

이 문제는 여러 가지 방법으로 방지됩니다. MAB 인증 클라이언트가 연결되는 인터페이스의 MAB를 선호합니다. dot1x를 먼저 실행해야 하는 경우 클라이언트 DHCP 동작을 주의하고 시간 초과 값을 적절하게 조정하십시오.

dot1x 및 MAB를 사용 할 때 클라이언트 동작을 고려 하십시오. 유효한 구성은 전술한 바와 같이 기술적 문제를 야기할 수 있다.

플랫폼별 유틸리티

이 섹션에서는 Catalyst 9000 스위치 제품군에서 dot1x 문제를 해결하는 데 유용한 플랫폼별 유틸리티에 대해 설명합니다.

- 스위치 포트 분석기(SPAN)

SPAN을 사용하면 캡처 및 분석을 위해 하나 이상의 포트에서 대상 포트로 트래픽을 미러링할 수 있습니다. 로컬 SPAN은 가장 '신뢰할 수 있는' 캡처 유틸리티입니다.

컨피그레이션 및 구현에 대한 자세한 내용은 이 컨피그레이션 가이드를 참조하십시오.

SPAN 및 RSPAN 구성, Cisco IOS XE Bengaluru 17.6.x(Catalyst 9300)

- EPC(Embedded Packet Capture)

EPC는 CPU 및 메모리 리소스를 활용하여 온보드 로컬 패킷 캡처 기능을 제공합니다.

EPC가 특정 문제를 조사하는 데 미치는 영향은 제한적입니다. EPC는 초당 1,000패킷으로 속도 제한됩니다. 또한 EPC는 물리적 인터페이스의 이그레스(egress)에서 CPU 주입 패킷을 안정적으로 캡처할 수 없습니다. 이는 인증자 스위치와 인증 서버 간의 RADIUS 트랜잭션에 초점을 맞출 때 중요합니다. 종종 서버를 향하는 인터페이스의 트래픽 속도는 초당 1,000개의 패킷을 크게 초과합니다. 또한 서버에 대한 인터페이스의 이그레스(egress)에 있는 EPC는 인증자 스위치에서 생성된 트

래픽을 캡처할 수 없습니다.

초당 1000 패킷 제한으로 인한 영향을 방지하려면 양방향 액세스 목록을 사용하여 EPC를 필터링합니다. 인증자와 서버 간의 RADIUS 트래픽에 관심이 있는 경우 인증자 RADIUS 소스 인터페이스 주소와 서버 주소 간의 트래픽에 초점을 맞춥니다.

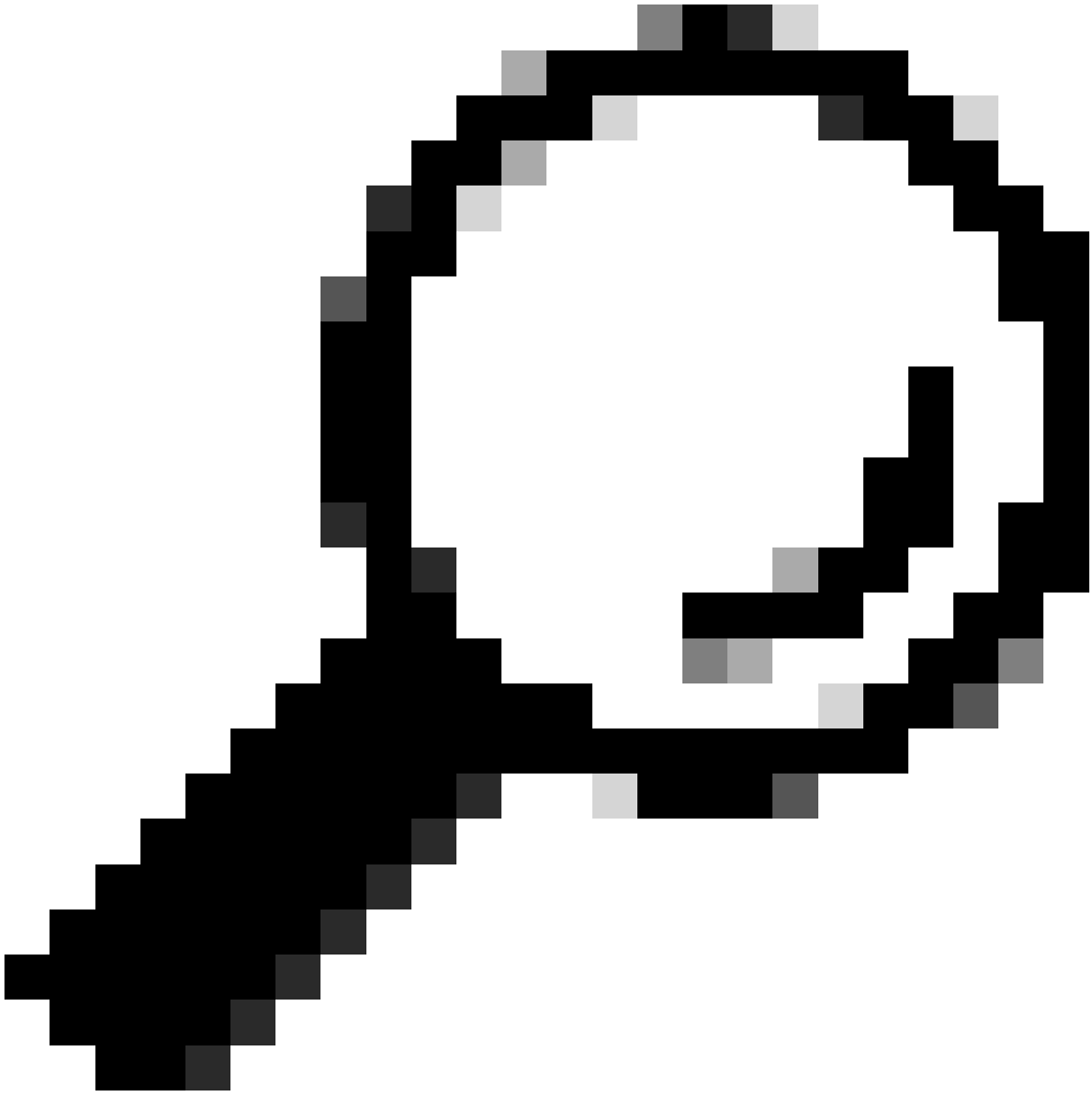
인증 서버를 향하는 다음 업스트림 디바이스가 Catalyst 스위치인 경우 최상의 결과를 얻으려면 인증자 스위치로 향하는 다운링크에서 필터링된 EPC를 사용합니다.

컨피그레이션 및 구현에 대한 자세한 내용은 이 컨피그레이션 가이드를 참조하십시오.

패킷 캡처 구성, Cisco IOS Bengaluru 17.6.x(Catalyst 9300)

- Cisco IOS XE 디버그

Cisco IOS XE 버전 16.3.2부터 시작되는 소프트웨어 아키텍처 변경으로 AAA 구성 요소가 별도의 Linux 데몬으로 이동했습니다. 친숙한 디버깅은 더 이상 로깅 버퍼에서 볼 수 있는 디버그를 활성화하지 않습니다. 대신,



팁: 기존 IOS AAA 디버그는 더 이상 syslog 버퍼 내의 전면 패널 포트 인증을 위해 시스템 로그에 출력을 제공하지 않습니다

dot1x 및 RADIUS에 대한 이러한 클래식 Cisco IOS 디버그는 더 이상 스위치의 스위치 로깅 버퍼 내에서 볼 수 있는 디버그를 활성화하지 않습니다.

```
debug radius
debug access-session all
debug dot1x all
```

이제 SMD(Session Manager Daemon) 아래의 시스템 추적을 통해 AAA 구성 요소 디버깅에 액세스할 수 있습니다.

- 기존 syslog와 마찬가지로 Catalyst 시스템 추적 보고서는 기본 수준으로, 더 심층적인 로그를 수집하도록 지시해야 합니다.
- "set platform software trace smd switch active r0 <component> debug" 명령을 사용하여 원하는 하위 구성 요소에 대한 루틴 추적 수준을 변경합니다.

<#root>

```
Switch#

set platform software trace smd switch active R0 auth-mgr debug

 <<<--- This sets the "auth-mgr" subcomponent to "debug" log level.
```

이 표에서는 기존 IOS 디버그를 해당 추적에 매핑합니다.

이전 스타일 명령	새 스타일 명령
#debug 반지름	#set 플랫폼 소프트웨어 추적 smd 스위치 활성 R0 radius 디버그
#debugx 모두 표시	#set 플랫폼 소프트웨어 추적 smd 스위치 활성 R0 dot1x-all 디버그
#debug 액세스 세션 모두	#set 플랫폼 소프트웨어 추적 smd 스위치 활성 R0 auth-mgr-all 디버그
#debug 모두 표시	#set 플랫폼 소프트웨어 추적 smd 스위치 활성 R0 epm-all 디버그

클래식 디버그는 모든 관련 구성 요소 추적을 'debug' 수준으로 활성화합니다. 필요에 따라 특정 추적을 활성화하는 데 플랫폼 명령도 사용됩니다.

SMD 하위 구성 요소의 현재 추적 수준을 표시하려면 "show platform software trace level smd switch active R0" 명령을 사용합니다.

<#root>

```
Switch#

show platform software trace level smd switch active R0


Module Name                      Trace Level
----------------------------------------------
aaa

Notice


<--- Default level is "Notice"


aaa-acct                         Notice
aaa-admin                        Notice
aaa-api                          Notice
aaa-api-attr                     Notice
<snip>
auth-mgr
```

```
Debug <--- Subcomponent "auth-mgr" traces at "debug" level


auth-mgr-all                    Notice
<snip>
```

하위 구성 요소 추적 레벨은 두 가지 방법으로 기본값으로 복원할 수 있습니다.

- 복원하려면 "모두 디버그 해제" 또는 "플랫폼 소프트웨어 추적 smd 스위치 활성 R0 <하위 구성 요소> 알림 설정"을 사용하십시오.
- 디바이스가 다시 로드되면 추적 레벨도 기본값으로 복원됩니다.

<#root>

```
Switch#

undebug all


All possible debugging has been turned off

or

Switch#

set platform software trace smd switch active R0 auth-mgr notice


<--- Sets sub-component "auth-mgr" to trace level "Notice", the system default.
```

구성 요소 추적 로그는 콘솔에서 보거나, 아카이브에 기록하여 오프라인으로 볼 수 있습니다. 추적은 디코딩이 필요한 압축된 이진 아카이브에 보관됩니다. 보관된 추적을 처리할 때 디버그 지원이 필요하면 TAC에 문의하십시오. 이 워크플로에서는 CLI에서 추적을 보는 방법에 대해 설명합니다.

"show platform software trace message smd switch active R0" 명령을 사용하여 SMD 구성 요소에 대한 메모리에 저장된 추적 로그를 확인합니다.

<#root>

```
Switch#

show platform software trace message smd switch active R0


2016/11/26 03:32:24.790 [auth-mgr]: [1422]: UUID: 0, ra: 0 (info): [0000.0000.0000:unknown] Auth-mgr aa
2016/11/26 03:32:29.678 [btrace]: [1422]: UUID: 0, ra: 0 (note): Single message size is greater than 10
2016/11/26 03:32:24.790 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Delay-Time [41] 6 0 RADI
2016/11/26 03:32:24.790 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1646/52 10.4
2016/11/26 03:32:24.758 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeo
2016/11/26 03:32:24.758 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radi
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Output-Packets [48] 6 0
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Input-Packets [47] 6 8
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Output-Octets [43] 6 0
```

```
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Input-Octets [42] 6 658
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Session-Time [46] 6 125
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Event-Timestamp [55] 6 148013
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Status-Type [40] 6 Stop
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: 36 36 33 36 36 39 30 30 2f 33
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: 68 72 65 6e 65 6b 2d 69 73 65
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: 30 30 30 32 41 39 45 41 45 46
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Class [25] 63
RADIUS: 43 41 43 53 3a 30 41 30 30 30 41 46 45 30 30 30 [CACS:0A000AFE000]
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Terminate-Cause[49] 6 ad
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Authentic [45] 6 Remote
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Acct-Session-Id [44] 10 "0000
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50108
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitE
2016/11/26 03:32:24.757 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 17 "C3850
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 10.48.44
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "0
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Called-Station-Id [30] 19 "00
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 12 "method=m
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 18
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-se
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 19 "00-50-56-99
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Framed-IP-Address [8] 6 10.0.
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 205 "cts-pac
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 211
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 95 52 40 05 8f
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Accounting-Req
2016/11/26 03:32:24.756 [radius]: [1422]: UUID: 0, ra: 0 (debug): abcdefghijklmno:NO EAP-MESSAGE
2016/11/26 03:32:24.755 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): sending
2016/11/26 03:32:24.755 [radius]: [1422]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Config NAS IP: 10.4
2016/11/26 03:32:24.755 [radius]: [1422]: UUID: 0, ra: 0 (debug): Config for source interface found in
<snip>
```

출력은 자세히 표시되므로 출력을 파일로 리디렉션하는 것이 유용합니다.

- "more" 유틸리티를 사용하여 CLI를 통해 파일을 읽거나 텍스트 편집기에서 보기 위해 오프라인으로 이동할 수 있습니다.

<#root>

```
Switch#

show platform software trace message smd switch active R0 | redirect flash:SMD_debugs.txt

Switch#more flash:SMD_debugs.txt

This command is being deprecated. Please use 'show logging process' command.
executing cmd on chassis 1 ...



2022/12/02 15:04:47.434368 {smd_R0-0}{2}: [auth-mgr] [16908]: (debug): [0800.27dd.3016:Gi2/0/11] Starte
2022/12/02 15:04:47.434271 {smd_R0-0}{2}: [auth-mgr] [16908]: (info): [0800.27dd.3016:Gi2/0/11] Account
2022/12/02 15:04:43.366688 {smd_R0-0}{2}: [auth-mgr] [16908]: (debug): [5057.a8e1.6f49:Gi2/0/11] Starte
2022/12/02 15:04:43.366558 {smd_R0-0}{2}: [auth-mgr] [16908]: (info): [5057.a8e1.6f49:Gi2/0/11] Account
2022/12/02 15:01:03.629116 {smd_R0-0}{2}: [smd] [16908]: (warn): Setting trace for 52:7
```

```
2022/12/02 15:00:19.350560 {smd_RO-0}{2}: [smd] [16908]: (warn): Setting trace for 52:7
2022/12/02 01:28:39.841376 {smd_RO-0}{2}: [auth-mgr] [16908]: (ERR): [0000.0000.0000:unknown] sm ctx un
<snip>
```

"Show logging process"는 추적을 위한 업데이트된 유틸리티이며 Cisco IOS XE 17.9.x 이상 버전의 표준입니다.

<#root>

```
C9300#

show logging process smd ?

  <0-25>            instance number
  end               specify log filtering end location
  extract-pcap      Extract pcap data to a file
  filter            specify filter for logs
  fru               FRU specific commands
  internal          select all logs. (Without the internal keyword only
                    customer curated logs are displayed)
  level             select logs above specific level
  metadata          CLI to display metadata for every log message
  module            select logs for specific modules
  reverse           show logs in reverse chronological order
  start             specify log filtering start location
  switch            specify switch number
  to-file           decode files stored in disk and write output to file
  trace-on-failure  show the trace on failure summary
  |                 Output modifiers
```

"로깅 프로세스 표시"는 "플랫폼 소프트웨어 추적 표시"와 동일한 기능을 보다 우아하고 액세스 가능한 형식으로 제공합니다.

<#root>

```
C9300#

clear auth sessions

C9300#

show logging process smd reverse

Logging display requested on 2023/05/02 16:44:04 (UTC) for Hostname: [C9300], Model: [C9300X-24HX], Ver

Displaying logs from the last 0 days, 0 hours, 10 minutes, 0 seconds
executing cmd on chassis 1 ...
============================================================
 UTM [LUID NOT FOUND] ..... 0
 UTM [PCAP] ..... 0
 UTM [MARKER] ..... 0
 UTM [APP CONTEXT] ..... 0
 UTM [TDL TAN] ..... 5
 UTM [MODULE ID] ..... 0
```

```
 UTM [DYN LIB] ..................... 0
 UTM [PLAIN TEXT] .................. 6
 UTM [ENCODED] ..................... 85839
 UTM [Skipped / Rendered / Total] .. 85128 / 722 / 85850
 Last UTM TimeStamp ................ 2023/05/02 16:44:03.775663010
 First UTM TimeStamp ............... 2023/05/02 15:52:18.763729918
============================================================
---------------- Decoder Output Information --------------
============================================================
 MRST Filter Rules ...... 1
 UTM Process Filter ..... smd
 Total UTM To Process ... 85850
 Total UTF To Process ... 1
 Num of Unique Streams .. 1
============================================================
---------------- Decoder Input Information ---------------
============================================================
======= Unified Trace Decoder Information/Statistics ======
============================================================
2023/05/02 16:44:03.625123675 {smd_R0-0}{1}: [radius] [22624]: (ERR): Failed to mark Identifier for reu
2023/05/02 16:44:03.625123382 {smd_R0-0}{1}: [radius] [22624]: (ERR): RSPE-  Set Identifier Free for Re
2023/05/02 16:44:03.625116747 {smd_R0-0}{1}: [radius] [22624]: (info): Valid Response Packet, Free the
2023/05/02 16:44:03.625091040 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  authenticator 2b f4 ea
2023/05/02 16:44:03.625068520 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Received from id 1813/9
2023/05/02 16:44:03.610151863 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Started 5 sec timeout
2023/05/02 16:44:03.610097362 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Delay-Time     [41]
2023/05/02 16:44:03.610090044 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Event-Timestamp     [55]
2023/05/02 16:44:03.610085857 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Status-Type    [40]
2023/05/02 16:44:03.610040912 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Class              [25]
2023/05/02 16:44:03.610037444 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Authentic     [45]
2023/05/02 16:44:03.610032802 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Acct-Session-Id    [44]
2023/05/02 16:44:03.610028677 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Called-Station-Id  [30]
2023/05/02 16:44:03.610024641 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Nas-Identifier     [32]
2023/05/02 16:44:03.610020641 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Calling-Station-Id [31]
2023/05/02 16:44:03.610016809 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-Port           [5]
2023/05/02 16:44:03.610012487 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-Port-Type      [61]
2023/05/02 16:44:03.610007504 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-Port-Id        [87]
2023/05/02 16:44:03.610003581 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  NAS-IP-Address     [4]
2023/05/02 16:44:03.609998136 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Calling-Station-Id  [31]
2023/05/02 16:44:03.609994109 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Called-Station-Id   [30]
2023/05/02 16:44:03.609989329 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:   Cisco AVpair      [1]
2023/05/02 16:44:03.609985171 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Vendor, Cisco      [26]
2023/05/02 16:44:03.609981606 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:   Cisco AVpair      [1]
2023/05/02 16:44:03.609976961 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  Vendor, Cisco      [26]
2023/05/02 16:44:03.609969166 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  User-Name          [1]
2023/05/02 16:44:03.609963241 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS:  authenticator 0b 99 e3
2023/05/02 16:44:03.609953614 {smd_R0-0}{1}: [radius] [22624]: (info): RADIUS: Send Accounting-Request
2023/05/02 16:44:03.609863172 {smd_R0-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Handl
2023/05/02 16:44:03.609695649 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAPOL pa
2023/05/02 16:44:03.609689224 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:unknown] Pkt body
2023/05/02 16:44:03.609686794 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] EAP Pack
2023/05/02 16:44:03.609683919 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Sent EAP
2023/05/02 16:44:03.609334292 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Sending
2023/05/02 16:44:03.609332867 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0000.0000.0000:Te1/0/4] Setting
2023/05/02 16:44:03.609310820 {smd_R0-0}{1}: [dot1x] [22624]: (info): [0800.2766.efc7:Te1/0/4] Posting
2023/05/02 16:44:03.609284841 {smd_R0-0}{1}: [auth-mgr] [22624]: (info): [0800.2766.efc7:Te1/0/4] Raisi
```

추적 예

이 섹션에는 실패한 전체 트랜잭션(서버에서 클라이언트 자격 증명을 거부함)에 대한 dot1x 및 radius 구성 요소에 대한 세션 관리자 추적이 포함되어 있습니다. 전면 패널 인증과 관련된 시스템 추적을 탐색하기 위한 기본 지침을 제공하고자 한다.

- 테스트 클라이언트가 GigabitEthernet1/0/2에 연결하려고 시도하지만 거부됩니다.

이 예에서는 SMD 구성 요소 추적이 "debug"로 설정됩니다.

<#root>

C9300#

set platform software trace smd sw active r0 dot1x-all

C9300#

set platform software trace smd sw active r0 radius debug

EAPoL: 시작

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on l2 s
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] queuing an EAPOL pkt on Auth Q
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE= 0,TYPE= 0,LEN= 0
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr = 0040.E93E.0000 ,
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Couldn't find the supplicant in the l
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] New client detected, sending session
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: initialising
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: disconnected
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: entering restart
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Sending create new context event to E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: entering init state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering idle state
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Created a client entry (0x0A00000E)
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Dot1x authentication started for 0x0A
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting !EAP_RESTART on Client 0x0A0
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:enter connecting state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: restart connecting
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting RX_REQ on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: authenticating state ent
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:connecting authenticating
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting AUTH_START for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state
```

EAPoL: EAP 요청 ID

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:idle request action
```

EAPoL: EAP 응답

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on l2 s
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Queuing an EAPOL pkt on Authenticator
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE= 2,TYPE= 1,LEN= 14
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr = 0040.E93E.0000 ,
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAPOL_EAP for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering response state
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Response sent to the server from 0x0A
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:request response action
[aaa-authen]: [16498]: UUID: 0, ra: 0 (debug): AAA/AUTHEN/8021X (00000000): Pick method list 'default'
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Best Local IP-Address 172.28.99.147 for Radiu
[radius-failover]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Nas-Identifier "C9300"
[aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: ACCESS-REQUEST

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Access-Request to 172.28.99.252:1645
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 59 c9 e0 be 4d b5 1c 11 - 02 cb 5b eb
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 11 "ixia_data"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Service-Type [6] 6 Framed [2]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 27
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 21 "service-type=Framed"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Framed-MTU [12] 6 1500
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "00-40-E9-3E-00-00"
0e 01 69 78 69 61 5f 64 61 74 61 [ ixia_data]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 16
69 87 3c 61 80 3a 31 a8 73 2b 55 76 f4 [ Ei<a:1s+Uv]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Key-Name [102] 2 *
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-session-id=AC1C6393000000
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 20
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 14 "method=dot1x"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 172.28.99.147
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 8 "C9300"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/2"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radius Packet
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeout
```

RADIUS: ACCESS-CHALLENGE

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1645/82 172.28.99.252:0, Access-Cha
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50014 RADIUS: authenticator 82 71 61
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
```

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID=
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
RADIUS: 01 f9 00 06 0d 20 [ ]
02/15 14:01:28.986 [radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 8
RADIUS: 78 66 ec be 2c a4 af 79 5e ec c6 47 8b da 6a c2 [ xf,y^Gj]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS:rad_code 11, suppress reject flag 0
[radius-authen]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Received from id 1645/82
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAP_REQ for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting response state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state###
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response request action
```

EAPoL: EAP 응답

```
02/15 14:01:28.988 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pk
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Queuing an EAPOL p
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE=
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAPOL_EAP
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:enteri
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Response sent to t
02/15 14:01:28.989 [dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:reques
02/15 14:01:28.989 [aaa-authen]: [16498]: UUID: 0, ra: 0 (debug): AAA/AUTHEN/8021X (00000000): Pick met
02/15 14:01:28.990 [radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Best Local IP-Address 172.
02/15 14:01:28.990 [radius-failover]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Nas-Identifier "C
02/15 14:01:28.990 [aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: ACCESS-REQUEST

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Access-Request to 172.28.99.252:1645
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 3d 31 3f ee 14 b8 9d 63 - 7a 8b 52 90
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 11 "ixia_data"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Service-Type [6] 6 Framed [2]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 27
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 21 "service-type=Framed"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Framed-MTU [12] 6 1500
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "00-40-E9-3E-00-00"
RADIUS: 02 f9 00 06 03 04
02/15 14:01:28.991 [radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 8
RADIUS: 8b 2a 2e 75 90 a2 e1 c9 06 84 c9 fe f5 d0 98 39 [ *.u9]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Key-Name [102] 2 *
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-session-id=AC1C6393000000
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 20
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 14 "method=dot1x"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 172.28.99.147
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 8 "C9300"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/2"
```

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50014
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID=
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radius Packet
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeout
```

RADIUS: ACCESS-CHALLENGE

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1645/83 172.28.99.252:0, Access-Cha
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 0c 8d 49 80 0f 51 89 fa - ba 22 2f 96
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID=
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
RADIUS: 01 fa 00 21 04 10 5b d0 b6 4e 68 37 6b ca 5e 6f 5a 65 78 04 77 bf 69 73 65 2d [![Nh7k^oZexwise-]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 35
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 70 6f 6c 2d 65 73 63 [ pol-esc]
RADIUS: a3 0d b0 02 c8 32 85 2c 94 bd 03 b3 22 e6 71 1e [ 2,"q]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS:rad_code 11, suppress reject flag 0
[radius-authen]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Received from id 1645/83
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAP_REQ for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting response state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state
```

EAPoL: EAP 요청

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response request action
```

EAPoL: EAP 응답

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0000.0000.0000:unknown] Received EAPOL pkt (size=92) on l2 s
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Queuing an EAPOL pkt on Authenticator
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Dequeued pkt: CODE= 2,TYPE= 4,LEN= 31
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Received pkt saddr = 0040.E93E.0000 ,
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAPOL_EAP for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering response state
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Response sent to the server from 0x0A
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:request response action
```

```
[aaa-authen]: [16498]: UUID: 0, ra: 0 (debug): AAA/AUTHEN/8021X (00000000): Pick method list 'default'
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Best Local IP-Address 172.28.99.147 for Radiu
[radius-failover]: [16498]: UUID: 0, ra: 0 (debug): RADIUS/ENCODE: Nas-Identifier "C9300"
[aaa-author]: [16498]: UUID: 0, ra: 0 (debug): VALID SG handle
```

RADIUS: ACCESS-REQUEST

```
radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Send Access-Request to 172.28.99.252:1645 i
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator 41 4d 76 8e 03 93 9f 05 - 5e fa f1 d6
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: User-Name [1] 11 "ixia_data"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Service-Type [6] 6 Framed [2]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 27
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 21 "service-type=Framed"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Framed-MTU [12] 6 1500
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Calling-Station-Id [31] 19 "00-40-E9-3E-00-00"
RADIUS: 02 fa 00 1f 04 10 02 b6 bc aa f4 91 2b d6 cf 9e 3b d5 44 96 78 d5 69 78 69 61 5f 64 61 74 61 [
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 33
RADIUS: 3b 70 b1 dd 97 ac 47 ae 81 ca f8 78 5b a3 7b fe [ ;pGx[{]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Key-Name [102] 2 *
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 49
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 43 "audit-session-id=AC1C6393000000
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Vendor, Cisco [26] 20
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Cisco AVpair [1] 14 "method=dot1x"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-IP-Address [4] 6 172.28.99.147
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Nas-Identifier [32] 8 "C9300"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Id [87] 22 "GigabitEthernet1/0/2"
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port-Type [61] 6 Ethernet [15]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: NAS-Port [5] 6 50014
RADIUS: 33 37 43 50 4d 53 65 73 73 69 6f 6e 49 44 3d 41 [37CPMSessionID=A]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: State [24] 81
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 43 31 43 36 33 39 33 30 30 30 30 30 30 31 37 45 [C1C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 35 33 43 36 45 38 45 3b 33 36 53 65 73 73 69 6f [53C
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 6e 49 44 3d 69 73 65 2d 70 6f 6c 2d 65 73 63 2f [nID=
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: 32 34 30 31 39 38 34 32 39 2f 38 39 32 34 3b [ 24019
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Sending a IPv4 Radius Packet
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Started 5 sec timeout
```

RADIUS: 액세스 거부

```
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Received from id 1645/84 172.28.99.252:0, Access-Rej
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: authenticator d1 a3 eb 43 11 45 6b 8f - 07 a7 34 dd
RADIUS: 04 fa 00 04
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: EAP-Message [79] 6
RADIUS: 80 77 07 f7 4d f8 a5 60 a6 b0 30 e4 67 85 ae ba [ wM`0g]
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS: Message-Authenticator[80] 18
[radius]: [16498]: UUID: 0, ra: 0 (debug): RADIUS:rad_code 3, suppress reject flag 0
[radius-authen]: [16498]: UUID: 0, ra: 0 (debug): RADIUS(00000000): Received from id 1645/84
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Received an EAP Fail
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting EAP_FAIL for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting response state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering fail state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:response fail action
```

```
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering idle state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting AUTH_FAIL on Client 0x0A0000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:exiting authenticating st
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering authc result sta
[errmsg]: [16498]: UUID: 0, ra: 0 (note): %DOT1X-5-FAIL: Authentication failed for client (0040.E93E.00
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Added username in dot1x
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Dot1x did not receive any key data
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Received Authz fail (result: 2) for t
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting_AUTHZ_FAIL on Client 0x0A000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: held
```

EAPoL: EAP 거부

```
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0000.0000.0000:Gi1/0/2] Sending out EAPOL packet
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] EAPOL packet sent to client 0x0A00000
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting FAILOVER_RETRY on Client 0x0A
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: exiting held state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: entering restart
[dot1x]: [16498]: UUID: 0, ra: 0 (info): [0040.E93E.0000:Gi1/0/2] Sending create new context event to EA
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:restart action called
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting RESTART on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting !EAP_RESTART on Client 0x0A0
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:enter connecting state
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: restart connecting
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting RX_REQ on Client 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E: authenticating state ent
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:connecting authenticating
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] Posting AUTH_START for 0x0A00000E
[dot1x]: [16498]: UUID: 0, ra: 0 (debug): [0040.E93E.0000:Gi1/0/2] 0x0A00000E:entering request state
```

추가 정보

기본 설정

기능	기본 설정
스위치 802.1x 활성화 상태	비활성화됨.
포트당 802.1x 활성화 상태	사용 안 함(강제 인증) 포트는 클라이언트의 802.1x 기반 인증 없이 일반 트래픽을 보내고 받습니다.
AAA	비활성화됨.

기능	기본 설정
RADIUS 서버 • IP 주소 • UDP 인증 포트 • 기본 계정 관리 포트 • 키	• 지정되지 않았습니다. • 1645 . • 1646 . • 지정되지 않았습니다.
호스트 모드	단일 호스트 모드.
제어 방향	양방향 제어.
주기적인 재인증	비활성화됨.
재인증 시도 간격(초)	3600초
재인증 번호	2회(포트가 인증되지 않은 상태로 변경되기 전에 스위치가 인증 프로세스를 다시 시작하는 횟수)
조용한 시기	60초(클라이언트와 인증 교환에 실패한 후 스위치가 자동 상태로 유지되는 시간(초))
재전송 시간	30초(스위치가 요청을 다시 전송하기 전에 클라이언트에서 EAP 요청/ID 프레임에 대한 응답을 기다리는 시간(초))
최대 재전송 수	2회(인증 프로세스를 다시 시작하기 전에 스위치에서 EAP-request/identity 프레임을 전송하는 횟수).
클라이언트 시간 초과 기간	30초(인증 서버에서 클라이언트로 요청을 릴레이할 때 스위치에서 클라이언트로 요청을 다시 보내기 전에 응답을 기다리는 시간)
인증 서버 시간 초과 기간	30초(클라이언트에서 인증 서버로 응답을 릴레이할 경우 스위치에서 응답을 서버에 다시 보내기 전에 응답을 기다리는 시간)

기능	기본 설정
	dot1x timeout server-timeout interface 컨피그레이션 명령을 사용하여 이 시간 제한 기간을 변경할 수 있습니다.
비활성 시간 초과	비활성화됨.
게스트 VLAN	지정되지 않았습니다.
액세스할 수 없는 인증 우회	비활성화됨.
제한된 VLAN	지정되지 않았습니다.
인증자(스위치) 모드	지정되지 않았습니다.
MAC 인증 우회	비활성화됨.
음성 인식 보안	비활성화됨.

선택적 설정

정기 재인증

주기적인 802.1x 클라이언트 재인증을 활성화하고 발생 빈도를 지정할 수 있습니다.

- authentication periodic - 클라이언트의 주기적인 재인증을 활성화합니다.
- inactivity - 클라이언트에서 아무런 활동이 없는 경우 인증되지 않은 상태가 될 때까지의 간격(초)입니다
- reauthenticate - 자동 재인증 시도가 시작된 이후의 시간(초)입니다.
- restartvalue — 인증되지 않은 포트를 인증하려고 시도하는 간격(초)
- unauthorizedvalue— 권한이 없는 세션이 삭제되기 전까지 경과해야 하는 간격(초)입니다

```
authentication periodic
authentication timer {{[inactivity | reauthenticate | restart | unauthorized]} {value}}
```

위반 모드

디바이스가 802.1x 지원 포트에 연결되거나 디바이스에서 허용되는 최대 디바이스 수가 포트에서 인증된 경우 802.1x 포트를 종료하거나 syslog 오류를 생성하거나 새 디바이스에서 패킷을 폐기하도록 구성할 수 있습니다.

- shutdown - 포트를 비활성화하는 동안 오류가 발생했습니다.
- restrict - syslog 오류를 생성합니다.
- protect - 포트로 트래픽을 전송하는 모든 새 디바이스에서 패킷을 삭제합니다.
- replace - 현재 세션을 제거하고 새 호스트로 인증합니다.

```
authentication violation {shutdown | restrict | protect | replace}
```

자동 기간 변경

authentication timer restart interface configuration 명령은 유휴 기간을 제어하며, 이는 스위치가 클라이언트를 인증할 수 없는 후 스위치가 유휴 상태로 유지되는 설정 기간을 나타냅니다. 값의 범위는 1~65535초입니다.

```
authentication timer restart {seconds}
```

스위치-클라이언트 재전송 시간 변경

클라이언트는 EAP-응답/ID 프레임으로 스위치에서 EAP-요청/ID 프레임에 응답합니다. 스위치가 이 응답을 받지 못하면, 설정된 시간(재전송 시간이라고 함)을 기다린 다음 프레임을 다시 전송합니다.

```
authentication timer reauthenticate {seconds}
```

스위치-클라이언트 프레임 재전송 번호 설정

인증 프로세스를 다시 시작하기 전에 스위치에서 클라이언트에 EAP-request/identity 프레임을 보내는 횟수(응답이 수신되지 않은 것으로 가정)를 변경할 수 있습니다. 범위는 1~10입니다.

```
dot1x max-reauth-req {count}
```

호스트 모드 구성

802.1x 인증 포트에서 여러 호스트(클라이언트)를 허용할 수 있습니다.

- multi-auth - 음성 VLAN과 데이터 VLAN 모두에서 인증된 여러 클라이언트를 허용합니다.
- multi-host- 단일 호스트가 인증된 후 802.1x 인증 포트에서 여러 호스트를 허용합니다.
- multi-domain- IEEE 802.1x 인증 포트에서 호스트 및 음성 디바이스(예: IP 전화(Cisco 또는 Cisco 이외의 전화) 모두 인증할 수 있습니다.

```
authentication host-mode [multi-auth | multi-domain | multi-host | single-host]
```

MAC 이동 활성화

MAC 이동을 사용하면 인증된 호스트가 디바이스의 한 포트에서 다른 포트로 이동할 수 있습니다.

```
authentication mac-move permit
```

MAC 교체 활성화

MAC replace를 사용하면 호스트가 포트의 인증된 호스트를 교체할 수 있습니다.

- protect - 포트는 시스템 메시지를 생성하지 않고 예기치 않은 MAC 주소가 포함된 패킷을 삭제합니다.
- restrict - 위반 패킷이 CPU에 의해 삭제되고 시스템 메시지가 생성됩니다.
- shutdown - 예기치 않은 MAC 주소를 수신하는 경우 포트가 error disable됩니다.

```
authentication violation {protect | replace | restrict | shutdown}
```

재인증 번호 설정

포트가 인증되지 않은 상태로 변경되기 전에 디바이스가 인증 프로세스를 다시 시작하는 횟수를 변경할 수도 있습니다. 범위는 0~10입니다

```
dot1x max-req {count}
```

게스트 VLAN 구성

게스트 VLAN을 구성할 때 802.1x를 지원하지 않는 클라이언트는 서버에서 EAP 요청/ID 프레임에 대한 응답을 받지 못할 때 게스트 VLAN에 배치됩니다.

```
authentication event no-response action authorize vlan {vlan-id}
```

제한된 VLAN 구성

디바이스에서 제한된 VLAN을 구성할 때, 인증 서버가 유효한 사용자 이름 및 비밀번호를 수신하지 못할 경우 IEEE 802.1x 호환 클라이언트가 제한된 VLAN으로 이동됩니다.

```
authentication event fail action authorize vlan {vlan-id}
```

제한된 VLAN에 대한 인증 시도 횟수 구성

authentication event fail retryretry countinterface 컨피그레이션 명령을 사용하여 사용자가 제한된 VLAN에 할당되기 전에 허용되는 최대 인증 시도 횟수를 구성할 수 있습니다. 허용되는 인증 시도의 범위는 1~3입니다.

```
authentication event fail retry {retry count}
```

중요 음성 VLAN을 사용하여 802.1x 액세스 불가 인증 우회 구성

포트에서 중요한 음성 VLAN을 구성하고 액세스 불가능한 인증 우회 기능을 활성화할 수 있습니다.

- authorize - 인증을 시도하는 모든 새 호스트를 사용자 지정 중요 VLAN으로 이동합니다.
- reinitialize - 포트의 모든 권한 있는 호스트를 사용자가 지정한 중요 VLAN으로 이동합니다.

```
authentication event server dead action {authorize | reinitialize} vlanvlan-id]
authentication event server dead action authorize voice
```

WoL을 사용하여 802.1x 인증 구성

WoL(Wake on LAN)을 사용하여 802.1x 인증을 활성화할 수 있습니다

```
authentication control-direction both
```

MAC 인증 우회 구성

```
mab
```

유연한 인증 순서 구성

```
authentication order [ dot1x | mab ] | {webauth}
authentication priority [ dot1x | mab ] | {webauth}
```

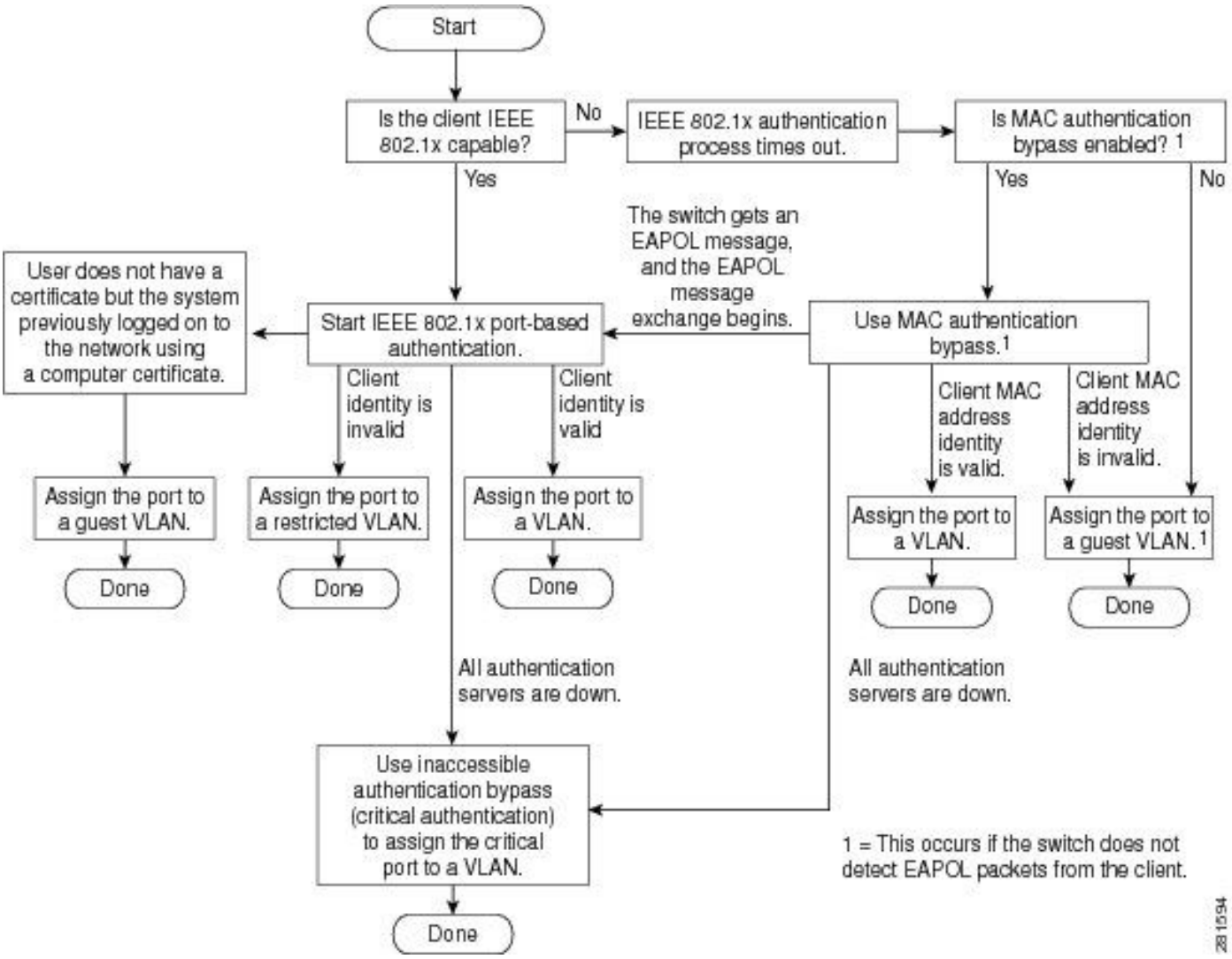
음성 인식 802.1x 보안 구성

디바이스에서 음성 인식 802.1x 보안 기능을 사용하여 데이터 또는 음성 VLAN이든 관계없이 보안 위반이 발생한 VLAN만 비활성화할 수 있습니다. 데이터 VLAN에서 보안 위반이 발견되면 데이터 VLAN만 종료됩니다. 전역 컨피그레이션입니다.

```
errdisable detect cause security-violation shutdown vlan
errdisable recovery cause security-violation
```

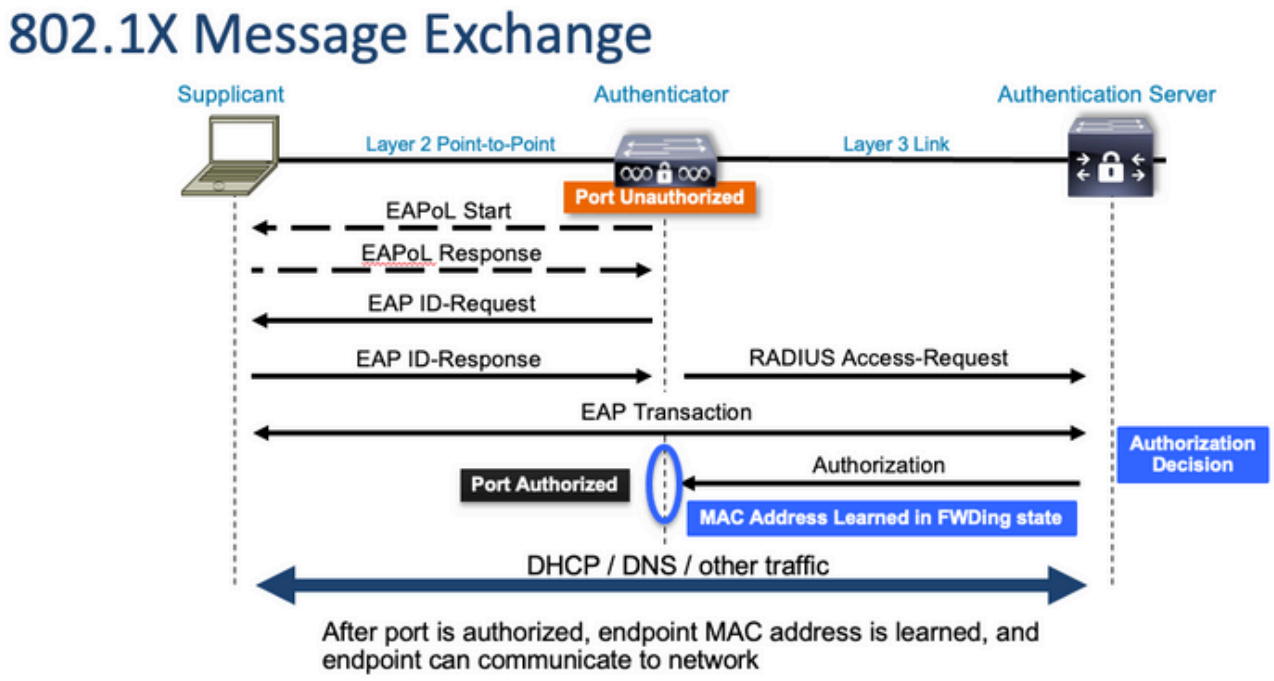
순서도

인증 흐름도



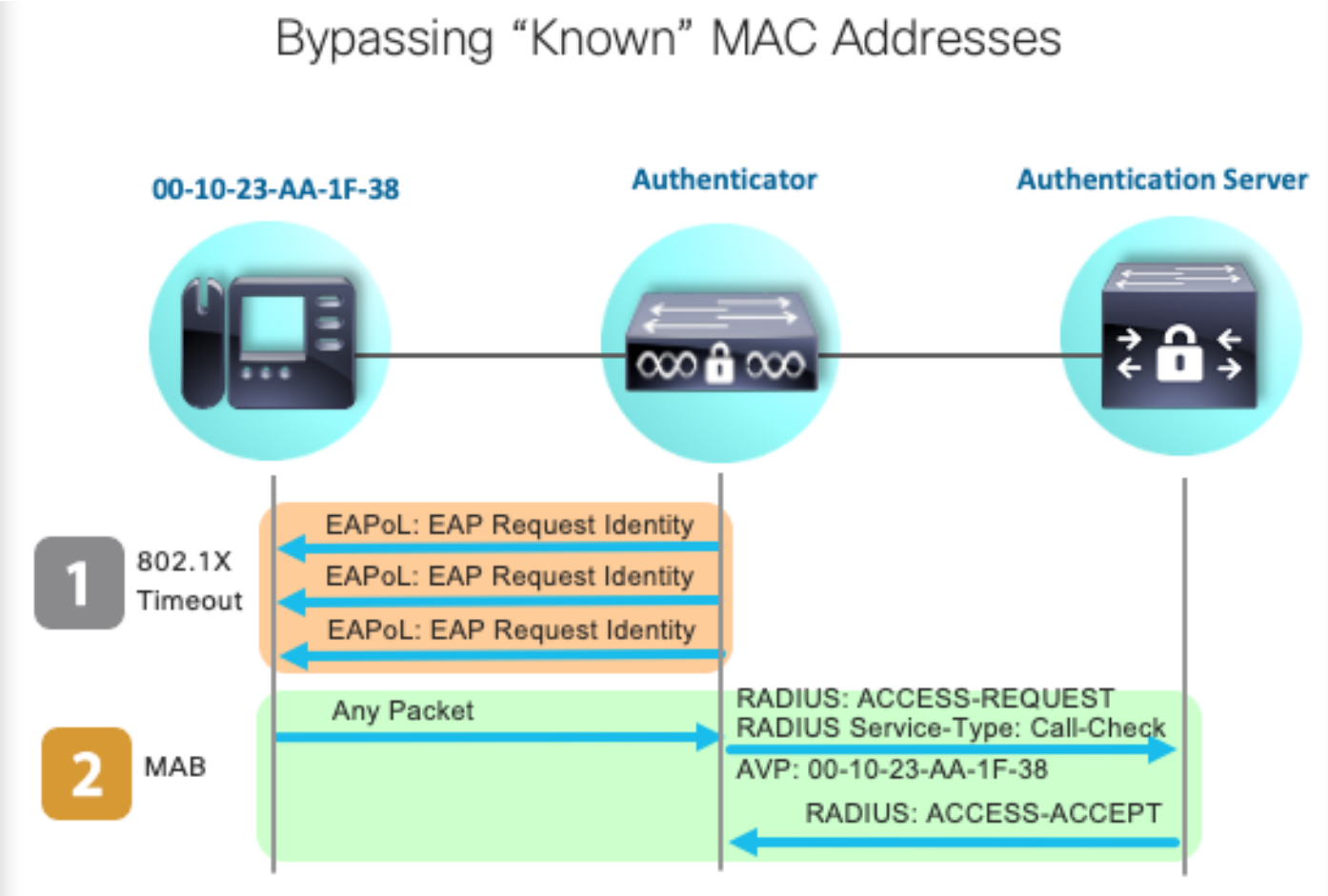
포트 기반 인증 시작 및 메시지 교환

이 그림에서는 클라이언트가 RADIUS 서버와의 메시지 교환을 시작하는 것을 보여줍니다.



MAB 인증 시작 및 메시지 교환

이 그림에서는 MAB(MAC 인증 우회) 중 메시지 교환을 보여줍니다



관련 정보

- RADIUS 서버 컨피그레이션 식별
- MAC 인증 우회 구축 가이드
- 유선 802.1x 구축 설명서
- Catalyst 9300 SPAN 컨피그레이션 가이드
- Catalyst 9300 EPC 컨피그레이션 가이드

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.