네트워크에서 APIPA 주소 오류 트러블슈팅

목차

소개

이 문서에서는 APIPA 주소와 관련된 문제에 대해 설명하고 동일한 문제에 대한 해결책을 제공합니다.

사용되는 구성 요소

- Catalyst 9000 스위치.
- ASA 방화벽(예: 5516)
- 모든 종류의 DHCP 서버
- SDA 설정의 Catalyst 9300
- 소프트웨어: 해당 없음

이유

최종 사용자는 이러한 상황에서 APIPA를 할당하며

- DHCP 서버를 사용할 수 없습니다.
- DHCP Offer(DHCP 제공)는 현재 홉(hop) 이전 또는 이전 단계에서 삭제됩니다.
- ARP 프로브는 중복 IP를 나타내는 응답을 받습니다.

시나리오 및 문제 해결

시나리오 1 - 방화벽 프록시 컨피그레이션

ASA 5516

문제 설명:

- 사용자 시스템은 APIPA IP 주소 및 사용자 연결에 영향을 받습니다.

문제 증상

1. 특정 VLAN의 사용자는 APIPA IP 주소를 받고 네트워크에 대한 연결이 끊기는 간헐적인 문제가 발생합니다.
2. 방화벽에는 다음과 같이 단일 최종 사용자 MAC 주소에 대한 여러 ARP 항목이 있습니다.

<#root>

```
Firewall/pri/act# show arp | include abcd.abcd.abcd


inside 10.1.1.12 abcd.abcd.abcd 30


inside 10.1.1.13 abcd.abcd.abcd 40


inside 10.1.1.14 abcd.abcd.abcd 51


inside 10.1.1.15 abcd.abcd.abcd 53
```

문제 해결 단계

1. 방화벽에 대한 디버깅은 최종 사용자 ARP 프로브에 응답을 보내는 방화벽을 가리킵니다.

<#root>

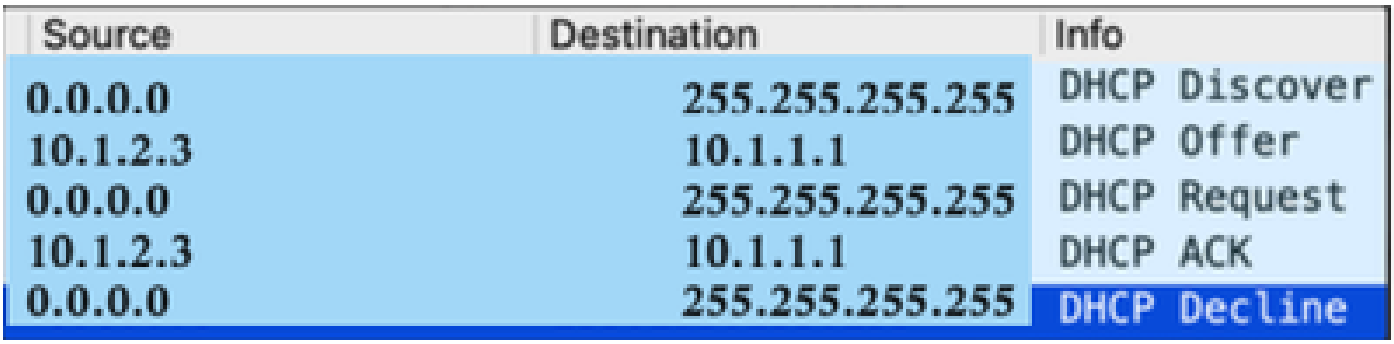
```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).


DHCPRA: Adding rule to allow client to respond using offered address 10.1.1.12
```

이렇게 하면 최종 디바이스가 중복된 주소로 인식됩니다.

2. 엔드 디바이스 또는 방화벽에서 캡처

DORA 프로세스가 완료되면 DHCP 거부 패킷을 전송하는 엔드 디바이스를 캡처합니다.



Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

격리

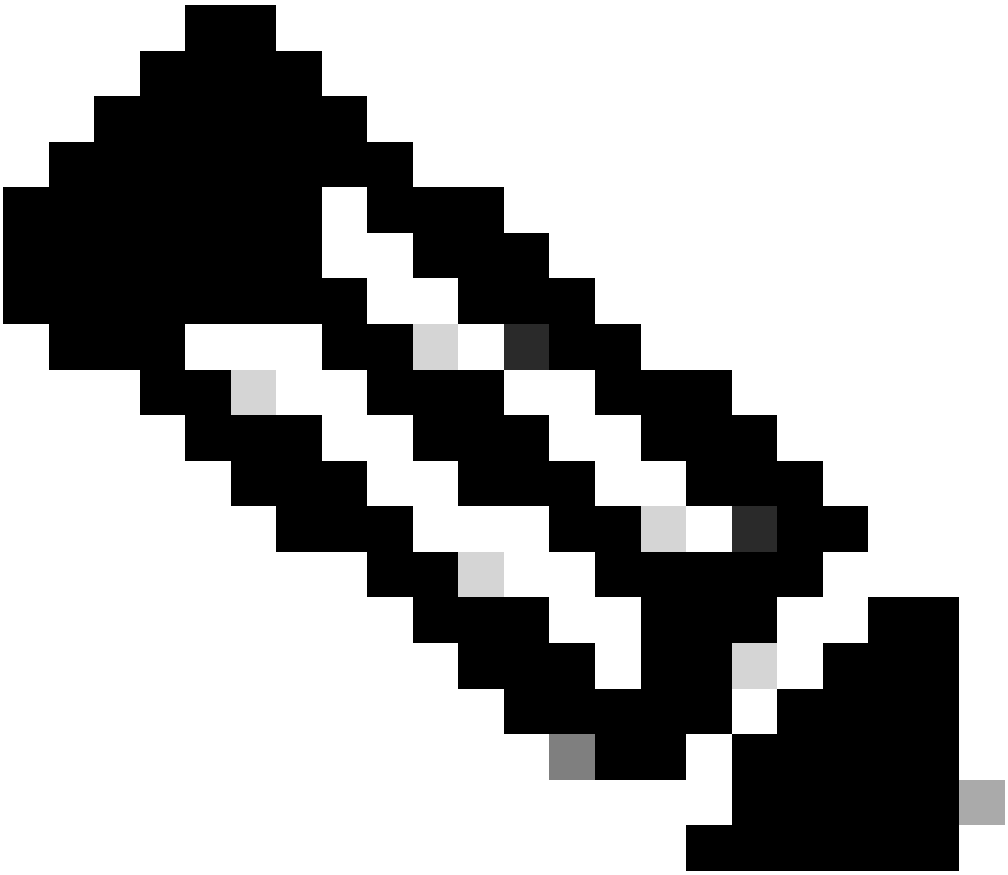
- 방화벽 내부 인터페이스는 DORA 프로세스가 완료되면 프록시 역할을 하여 ARP 프로브에 응답합니다. 이렇게 하면 PC에서 DHCP를 전송할 수 없습니다.

행동 계획

- "sysopt noproxyarp inside" 명령을 사용하여 방화벽 내부 인터페이스에서 프록시 arp를 비활성화합니다.

해결/확인

- 프록시 ARP를 비활성화한 후 엔드 디바이스가 IP 주소를 수신합니다.



- 참고: 디바이스가 프록시 역할을 하거나 최종 사용자 ARP 프로브에 대한 응답을 전송하지 않는지 확인하십시오.

.

시나리오 2 - DHCP 서버 범위

문제 설명:

- 사용자 시스템은 APIPA IP 주소 및 사용자 연결에 영향을 받습니다.

증상

1. 특정 VLAN의 사용자는 APIPA IP 주소만 가져오고 네트워크에 대한 연결이 끊어집니다.

트러블슈팅 수행

- DHCP 거부가 최종 사용자에게 전송되었으며 APIPA 주소로 구성되었습니다.

격리

- DHCP 서버는 범위 A에서 하나의 IP 주소를 할당하고, 범위 B의 범위가 동일하기 때문에 동일한 IP 주소가 다른 랩탑에 할당됩니다. 이로 인해 DHCP가 거부됩니다.

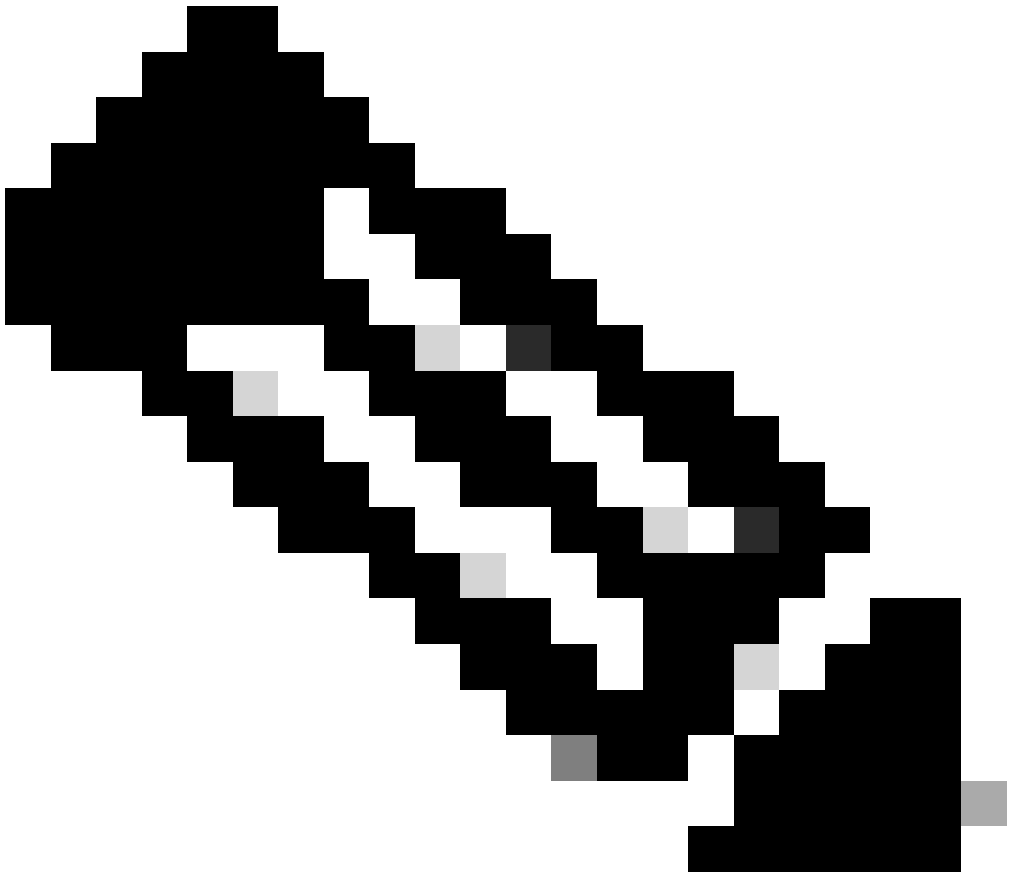
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

행동 계획

- 고유한 DHCP 범위 범위 할당

해결/확인

- 범위 변경 후 엔드 디바이스가 IP 주소를 수신합니다.



- 참고: DHCP 서버에 중복 범위가 구성되어 있지 않은지 확인하십시오.

시나리오 3 - C9300 SDA 컨피그레이션

Cat9300 in SDA

문제 설명:

- 사용자 시스템은 APIPA IP 주소 및 사용자 연결에 영향을 받습니다.

사용자 증상

1. 특정 VLAN의 일부 사용자는 무선 AP를 통해 DHCP 주소를 가져올 수 없습니다.
2. 방화벽에 단일 최종 사용자 mac 주소에 대한 여러 arp 항목이 있음

<#root>

```
Firewall# show arp | i abcd


Inside 10.1.1.22 abcd.abcd.abcd 48


Inside 10.1.1.23 abcd.abcd.abcd 49


Inside 10.1.1.24 abcd.abcd.abcd 50
```

트러블슈팅 수행

- DHCP 오퍼가 스위치에 의해 삭제되었습니다.
- FTD는 DHCP 서버에서 제공되는 DHCP 오퍼에 따라 ARP를 채웁니다.

<#root>

```
***DROP*** Broadcast to Access-Tunnel disallowed (accessTunnelBroadcastDrop)
```

격리

- L2 전용 VLAN이 SDA 무선 설정에 대해 구성된 경우 브로드캐스트 플래그가 있는 오퍼가 AP에 도달하지 않습니다. Access-tunnel은 기본적으로 브로드캐스트 패킷을 허용하지 않으므로

행동 계획

- LISP 환경 내에서 "플러드 기능"을 허용합니다.

<#root>

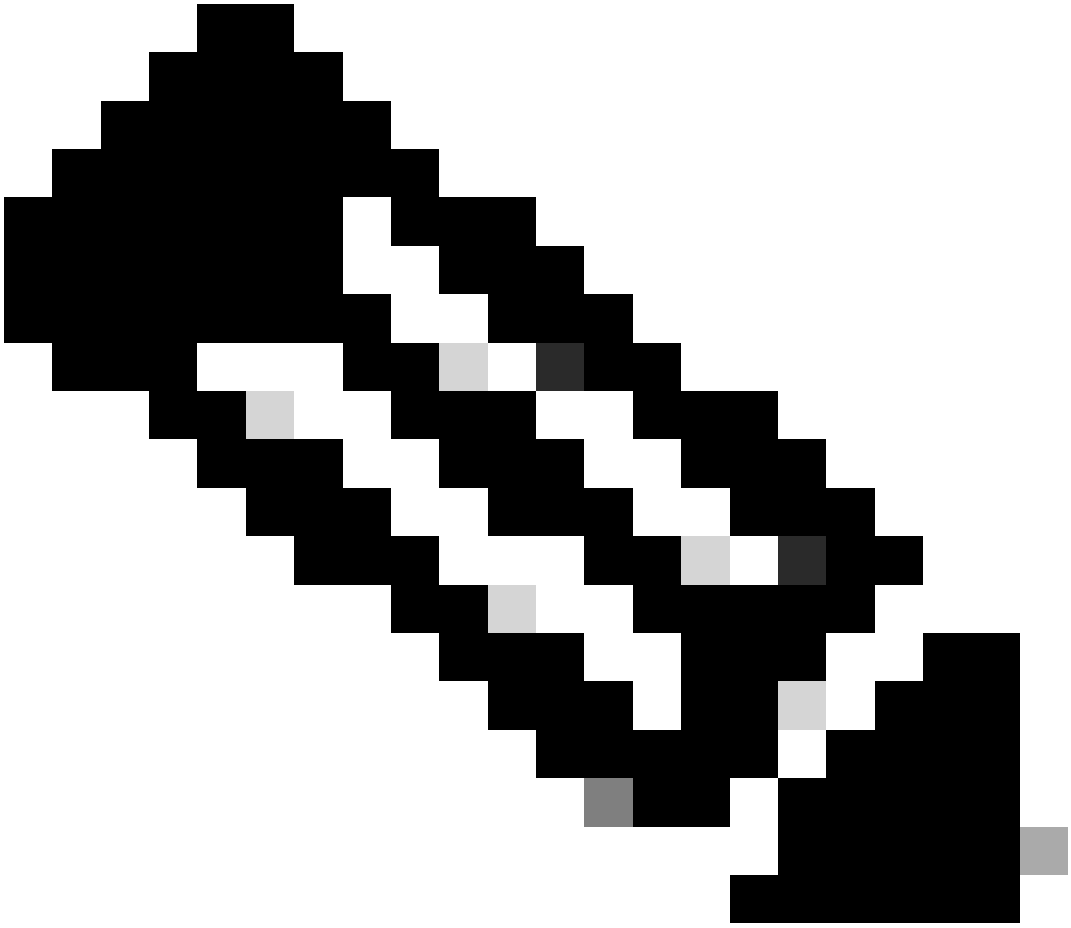
```
router lisp


instance-id 8456


flood access-tunnel
```

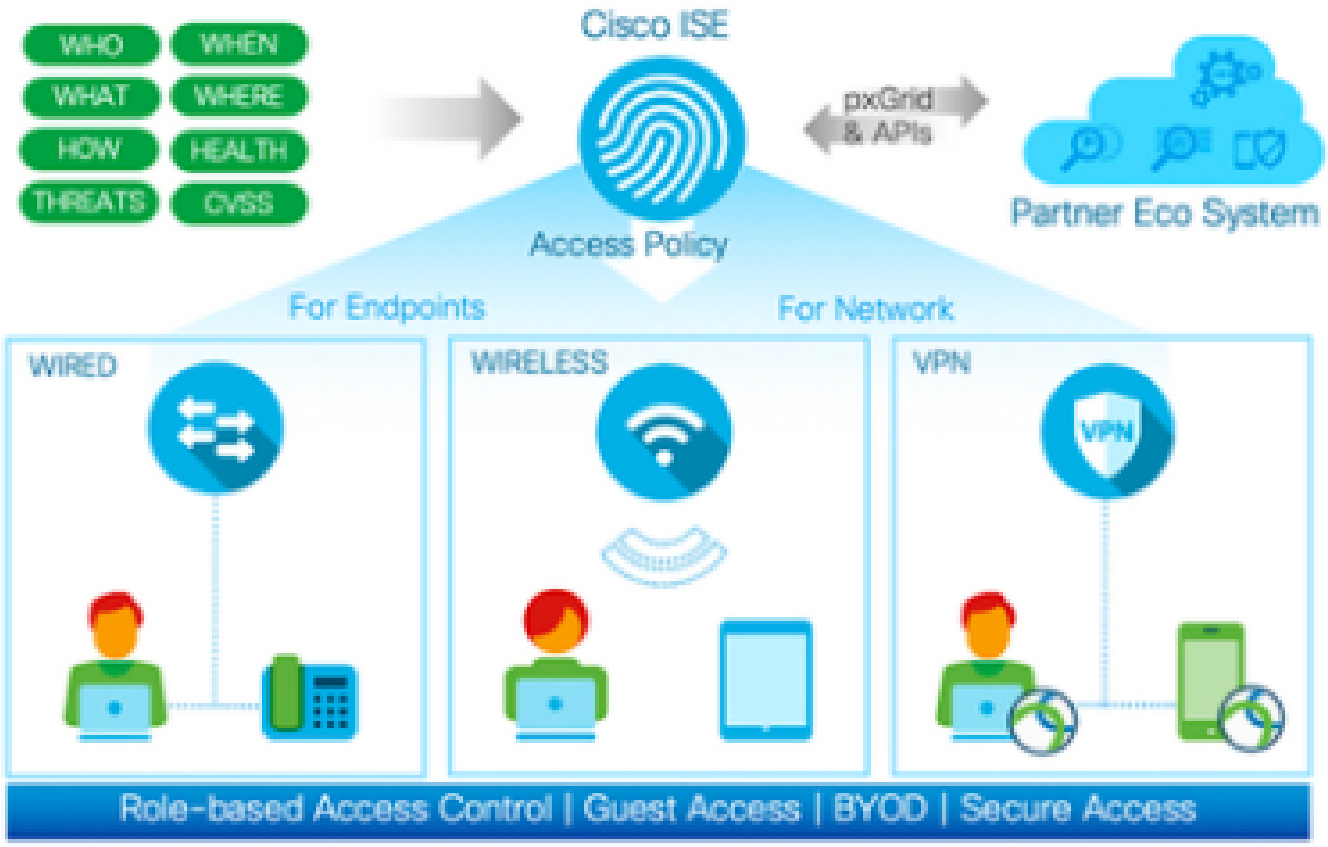
해결/확인

- 내부 인터페이스에 연결된 C9300에서 `flood access-tunnel`을 구성하면 클라이언트는 DHCP 주소를 받습니다.



참고: 엔드 디바이스가 브로드캐스트 오퍼를 수신하도록 구성된 경우 lisp에서 플러드 액세스 터널을 활성화해야 합니다.

시나리오 4 - LAN 어댑터 문제



cisco ISE

문제 설명:

- 사용자 시스템은 APIPA IP 주소 및 사용자 연결에 영향을 받습니다.

증상

1. Mac address-table에는 "drop"이 포함된 항목이 표시됩니다.

<#root>

```
#show mac address-table interface gigabitethernet1/0/20


Mac Address Table


-------------------------------------------


Vlan    Mac Address       Type        Ports


----    -----------       --------    -----
```

```
10    0000.0001.000a    DYNAMIC     Drop
```

2. Show Authentication 세션에 2000 또는 10000을 초과할 수 있는 많은 항목이 표시됩니다.

<#root>

```
switch2#show authentication sessions

Gi1/0/1  0000.0001.1234 N/A   UNKNOWN Unauth  0AFF0B8D000000EC000000AF

Gi1/0/1  0000.0001.2345 N/A   UNKNOWN Unauth  0AFF0B8D000000F00016B7D7

Gi1/0/1  0000.0001.3456 N/A   UNKNOWN Unauth  0AFF0B8D0028DE3500000000
```

문제 해결 단계

- 패킷 캡처는 서로 다른 소스 MAC 주소를 가진 최종 디바이스에서 들어오는 여러 패킷을 표시합니다.
- 인증 세션 한도는 2000이며, 한도가 초과되면 네트워크에서 예기치 않은 문제가 발생합니다
- https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3650/software/release/16-12/configuration_guide/sec/b_1612_sec_3650_cg/configuring_ieee_802_1x_port_based_authenticati

격리

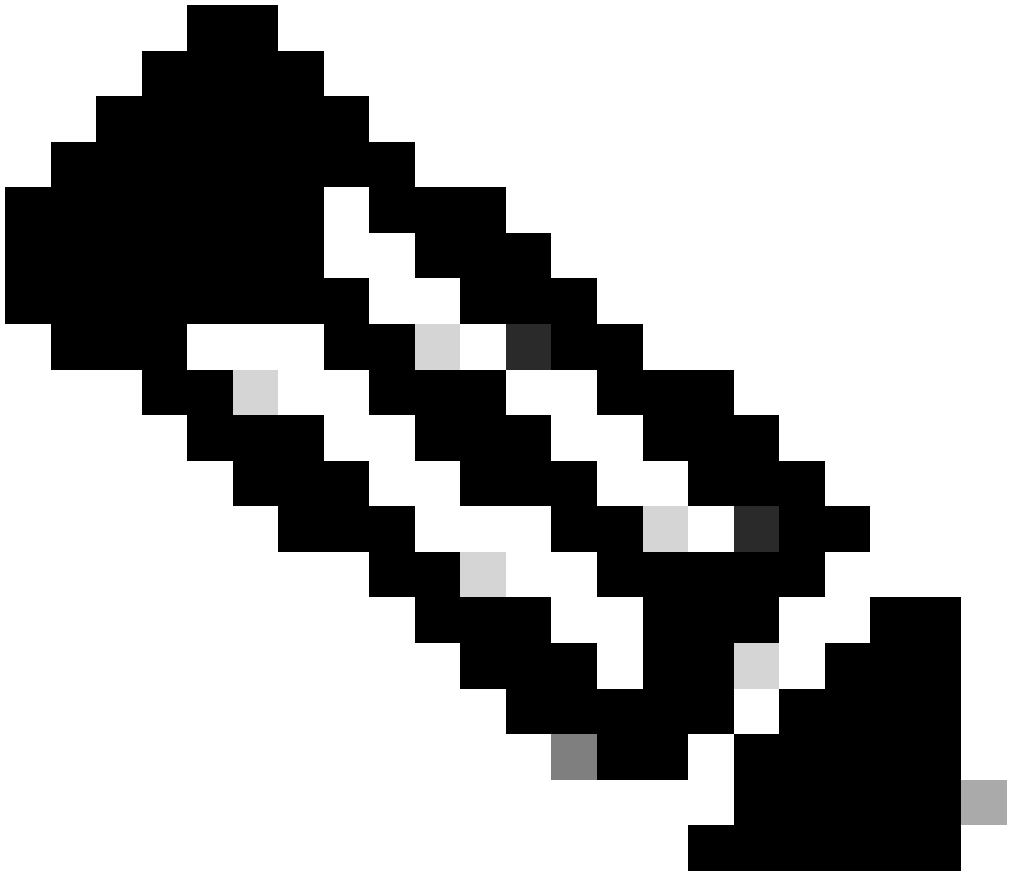
- 이것은 엔드 유저 어댑터 문제를 나타냅니다. 스위치가 임의 소스 mac 주소로 인식하는 잘못된 형식의 패킷을 보냅니다.

행동 계획

- 2개의 mac 주소만 허용하는 "authentication host-mode multi-domain"을 구성합니다.
- 원인 디바이스를 식별하고 격리합니다.

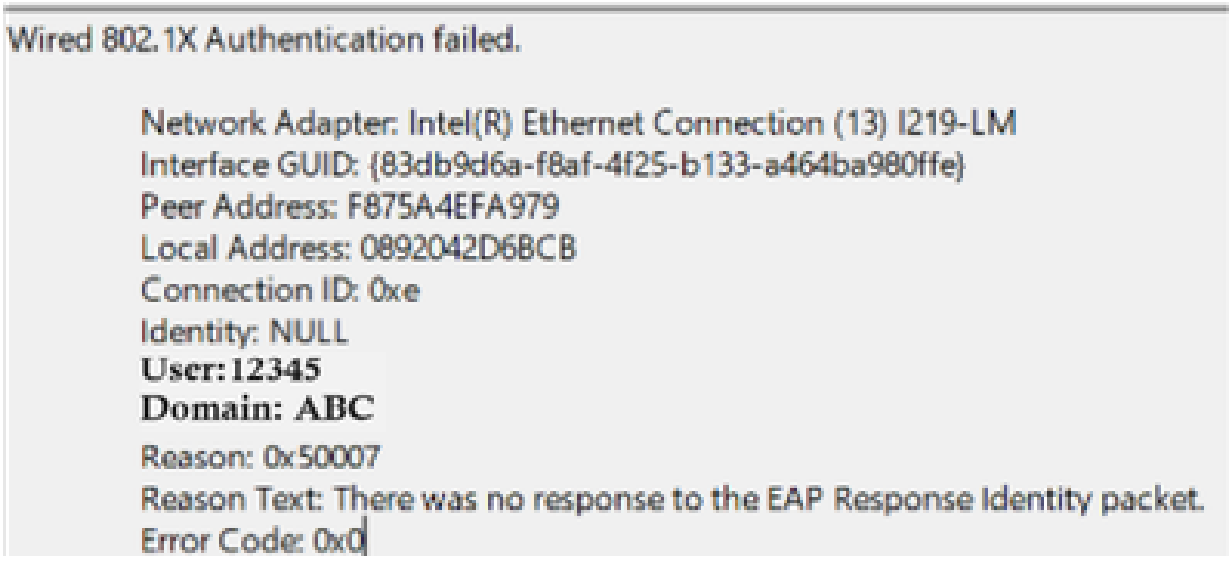
해결/확인

- 이 해결 방법을 구성한 후에는 문제가 발견되지 않습니다.



- 참고: 포트 보안 또는 Dot1x 인증 세션 호스트 모드 멀티 도메인을 활성화해야 합니다 .

시나리오 5 - MTU 불일치



ISE는 서버에서 이 오류를 나타냅니다.

문제 설명:

- 사용자 시스템은 APIPA IP 주소 및 사용자 연결에 영향을 받습니다.

사용자 증상

1. 최종 클라이언트는 실제 예상 패킷 길이(1492)보다 큰 패킷 길이(예: 3736)로 EAP 응답을 보냅니다.

```
Extensible Authentication Protocol
Code: Response (2)
Id: 4
Length: 1492
Type: TLS EAP (EAP-TLS) (13)
• EAP-TLS Flags: 0xc0
..0. .... = Start: False
EAP-TLS Length: 3736
```

트러블슈팅 수행

- MTU는 시스템 전체 항목으로 스위치에서 더 작은 크기로 설정됩니다. (예:1998바이트)
- 더 큰 크기로 구성된 이그레스 인터페이스. (예: 9198바이트)

격리

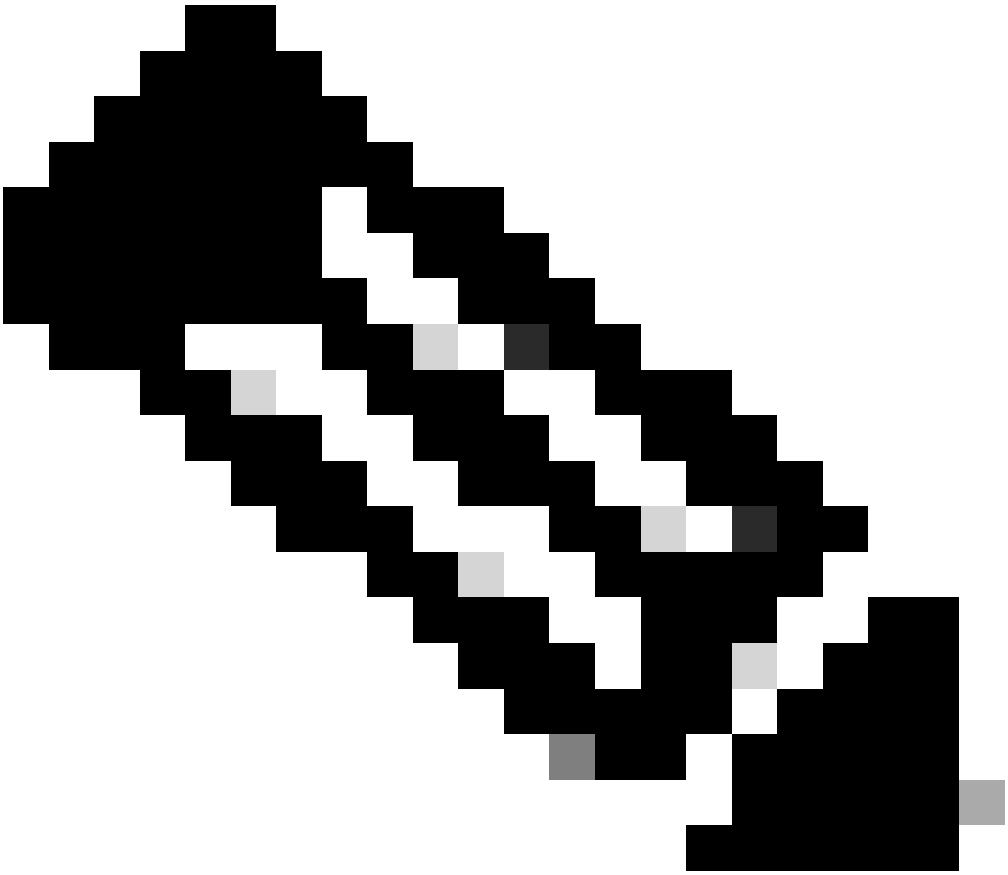
- 경로 전체에서 MTU가 일치하지 않으면 문제가 발생합니다.

행동 계획

- 시스템 MTU를 1500으로 변경하고 스위치 다시 로드

해결/확인

- 이 설정을 구성하면 인증에 성공합니다.



- 참고: 패킷 흐름의 경로 전체에서 동일한 MTU를 활성화해야 합니다.

시나리오 6 - IPDT Guard

문제 설명:

- 사용자 시스템은 APIPA IP 주소 및 사용자 연결에 영향을 받습니다.

사용자 증상

- HA에 VM이 있는 경우, 인터페이스에 이 정책이 적용된 경우:

장치 추적 정책 IPDT_POLICY

프로토콜 udp 없음

추적 사용

- 장애 조치 후 ARP 응답이 액세스 스위치에 의해 삭제됩니다.

트러블슈팅 수행

1. 프로브에 대한 ARP 응답은 스위치에 의해 삭제됩니다.
2. 스위치가 IPDT Guard로 구성되었습니다.
3. IPDT - ARP 프로브를 삭제하는 보호자 및 APIPA를 가져오는 최종 디바이스

격리

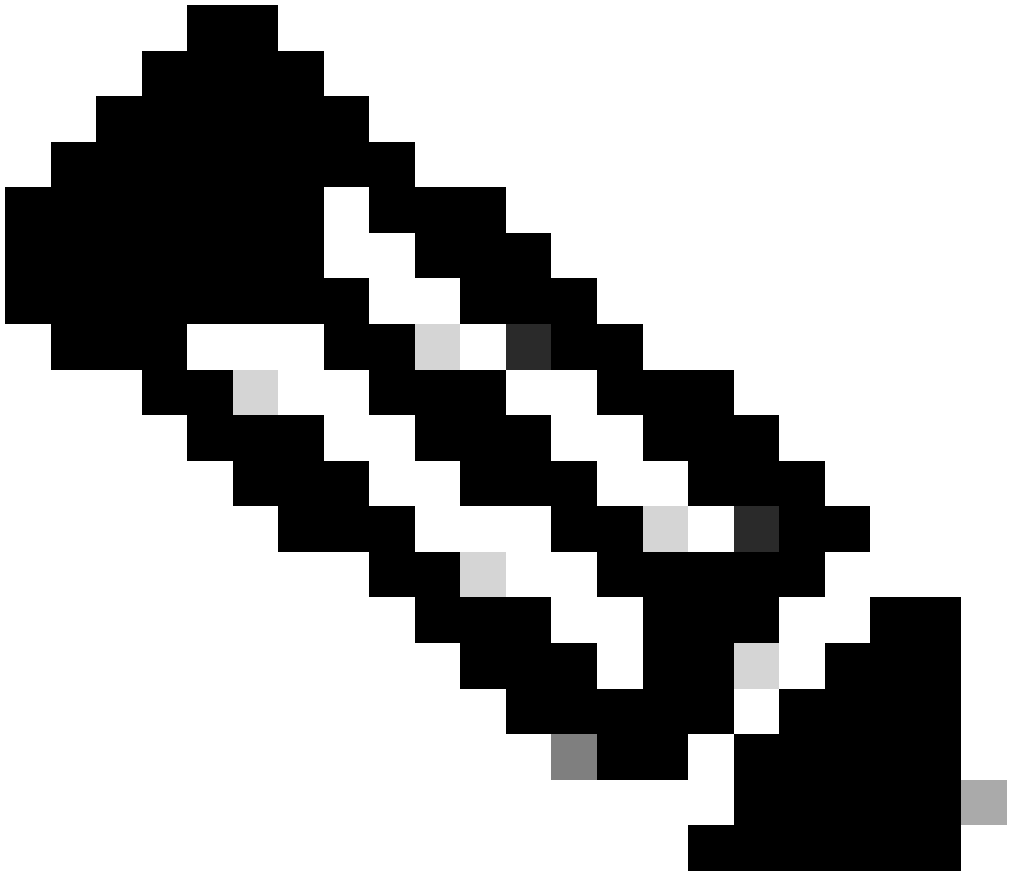
- ARP 프로브 패킷은 IPDT에 도달하고 보호 기능 때문에 삭제됩니다.
- '보안 레벨 가드' 구성으로 구성된 IPDT 정책이 ARP 패킷을 삭제하여 일부 또는 모든 엔드 디바이스에 연결할 수 없게 만듭니다.

행동 계획

- Guard에서 Glean으로 설정을 변경합니다.
  IPDT 정책에서 '보안 수준의 청소' 구성

해결/확인

- 일반 설정을 구성하면 ARP 프로브가 ARP 프로세스에 의해 처리되고 문제가 해결됩니다.



- 참고: 이는 잘 알려진 결함이며 17.15.1 버전 이상에서 수정됩니다.

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.