Probleemoplossing voor APIPA-adresfout in het netwerk

Inhoud

Inleiding

In dit document worden de kwesties met betrekking tot APIPA-adressen beschreven en worden resoluties voor hetzelfde onderwerp verstrekt.

Gebruikte componenten

- Catalyst 9000 switches.
- ASA firewalls zoals 5516
- DHCP-server van elke soort
- Catalyst 9300 in installatie van SDA
- Software: nvt

Redenen

Eindgebruikers wijzen APIPA toe tijdens deze scenario's.

- DHCP-server is niet beschikbaar.
- DHCP-aanbieding is voor of op dit moment ingetrokken.
- ARP sonde krijgt een reactie die Dubbele IP vertegenwoordigt.

Scenario's en probleemoplossing

Scenario 1 - Firewall-proxyconfiguratie

ASA 5516

Probleembeschrijving:

- Gebruikersmachines ontvangen APIPA IP-adres en de gebruikersconnectiviteit is erdoor beïnvloed.

Probleemsymptomen

1. Gebruikers op een specifiek VLAN ervaren intermitterende problemen waar ze een APIPA IP-adres ontvangen en connectiviteit met het netwerk verliezen.
2. Firewalls hebben meerdere ARP-vermeldingen voor één MAC-adres van de eindgebruiker, zoals dit:

<#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
```

Stappen voor probleemoplossing

1. Debugs op Firewall wijst naar de firewall die het antwoord naar eindgebruikers ARP sonde verzendt.

<#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
```

Dit maakt het eindapparaat om zijn een dubbel adres te denken.

2. Opname op eindapparaat of firewall

Capture toont eindapparaat verzenden DHCP Decline-pakketten zodra het DORA-proces is voltooid.

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

Isolatie

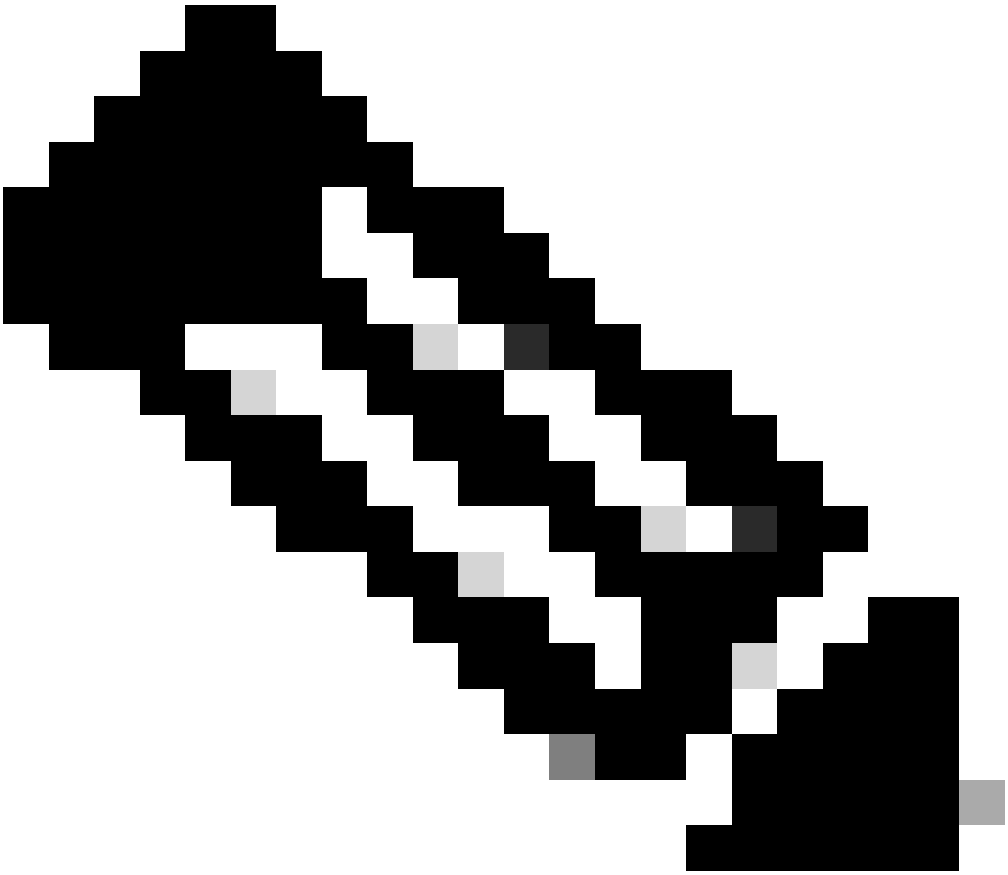
- Firewall in interface reageert op de ARP-sonde door als proxy te fungeren, zodra het DORA-proces is voltooid. Dit maakt de PC om DHCP te verzenden afnemen.

Actieplan

- Schakel de proxy-arp in de interface van Firewall uit met behulp van de opdracht "sysopt noproxyarp inside"

Resolutie/verificatie

- Eindapparaten ontvangen IP-adres nadat proxy-arp is uitgeschakeld.



- Opmerking: Zorg ervoor dat geen apparaat fungeert als proxy of een reactie verstuurt voor eindgebruiker ARP-probes.

.

Scenario 2 - DHCP-serverbereik

DHCP Server

Probleembeschrijving:

- Gebruikersmachines ontvangen APIPA IP-adres en de gebruikersconnectiviteit is erdoor beïnvloed.

Symptomen

1. Gebruikers op specifieke VLAN krijgen alleen APIPA IP-adres en verliezen verbinding met het netwerk.

Probleemoplossing uitgevoerd

- DHCP-afname verzonden naar eindgebruikers en het is geconfigureerd met APIPA-adres

Isolatie

- DHCP-server wijst één IP-adres toe van scope A en hetzelfde IP-adres dat wordt

toegewezen aan een ander Laptop omdat scope B hetzelfde bereik heeft. Dit veroorzaakt DHCP-afname:

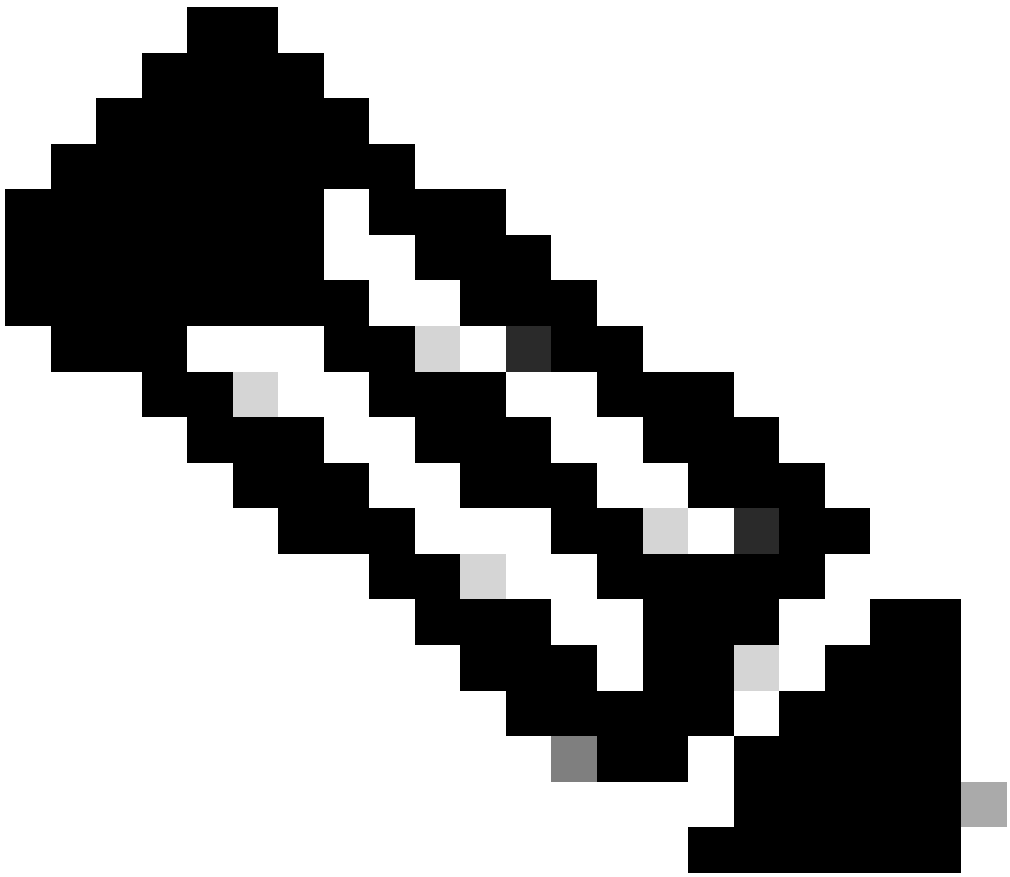
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

Actieplan

- Wijs een uniek DHCP-bereik toe

Resolutie/verificatie

- Eindapparaten ontvangen IP-adres na wijziging van bereik.



Opmerking: Zorg ervoor dat DHCP-server geen duplicaat van scènes heeft geconfigureerd.

Scenario 3 - C9300 SDA-configuratie

Cat9300 in SDA

Probleembeschrijving:

- Gebruikersmachines ontvangen APIPA IP-adres en de gebruikersconnectiviteit is erdoor beïnvloed.

Gebruikerssymptomen

1. Sommige gebruikers in een specifiek VLAN kunnen geen DHCP-adressen verkrijgen via de draadloze AP.
2. Firewall had meerdere arp-vermeldingen voor één eindgebruiker mac-adres

<#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
```

Probleemoplossing uitgevoerd

- DHCP-aanbieding is door switch ingetrokken
- FTD bevolkt ARP op basis van DHCP OFFER terugkomend van DHCP server.

<#root>

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

Isolatie

- Als L2-only VLAN is geconfigureerd voor draadloze SDA-instelling, bieden pakketondersteuning met broadcast-vlag niet op AP. Aangezien de toegangstunnel geen uitzendingspakketten standaard toestaat.

Actieplan

- Laat "flood mogelijkheid" toe in LISP omgeving.

<#root>

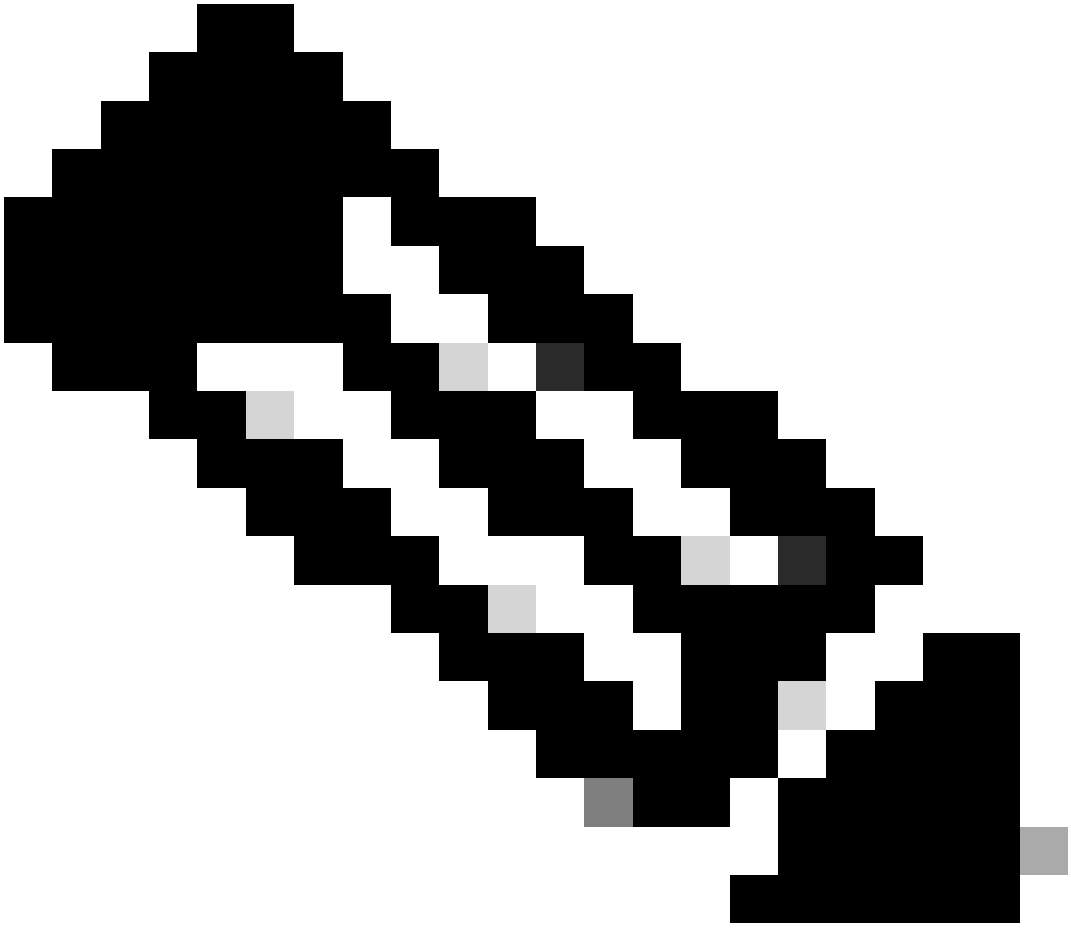
```
router lisp


instance-id 8456


flood access-tunnel
```

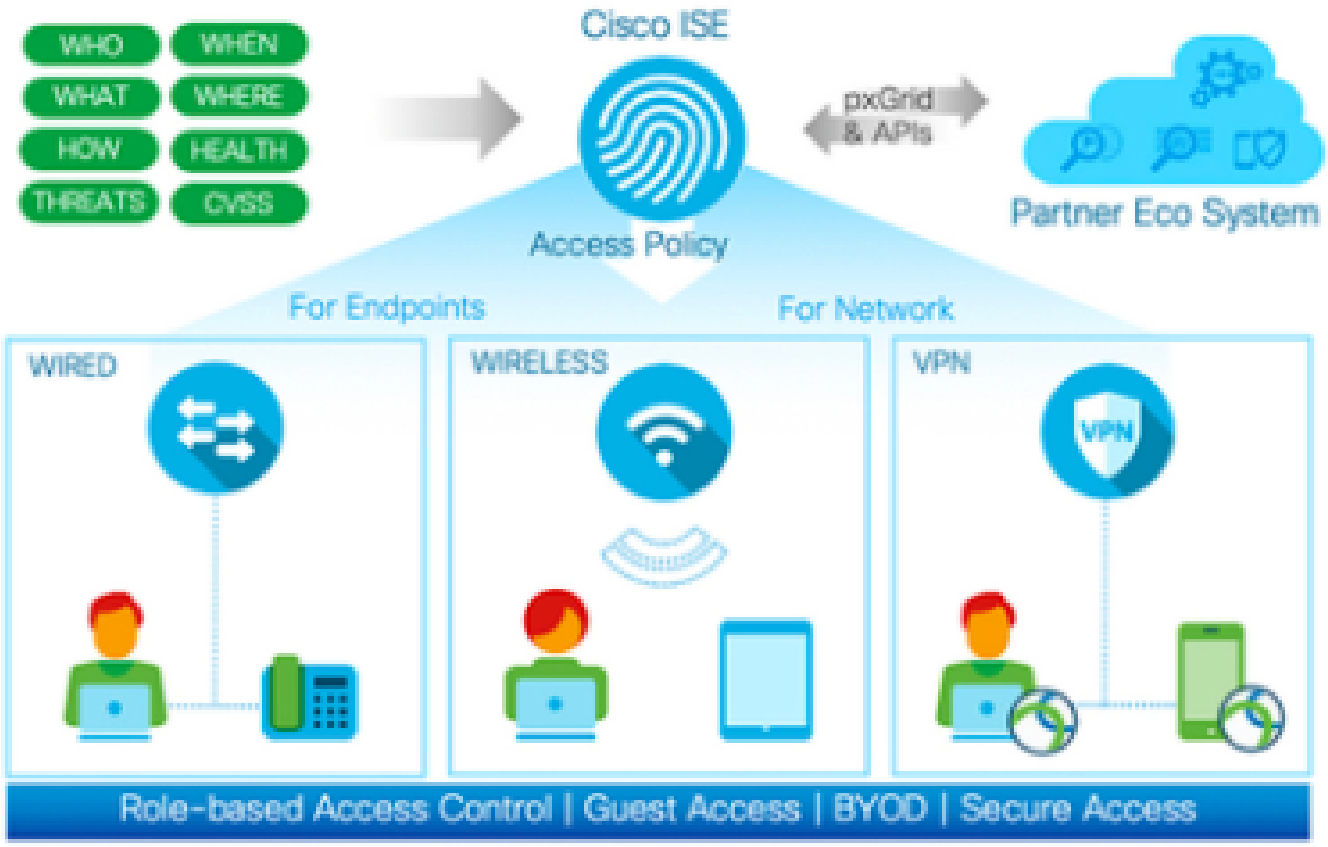
Resolutie/verificatie

- Na het configureren van de ‘flood access tunnel’ in de C9300 aangesloten op de binneninterface, ontvangen clients DHCP-adressen.



Opmerking: Zorg ervoor dat de Flood Access-tunnel onder lisp is ingeschakeld als het eindapparaat is geconfigureerd om broadcast-aanbod te ontvangen.

Scenario 4 - LAN-adapterprobleem



cisco ISE

Probleembeschrijving:

- Gebruikersmachines ontvangen APIPA IP-adres en de gebruikersconnectiviteit is erdoor beïnvloed.

Symptomen

1. Mac adrestabel toont ingangen met "drop".

<#root>

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


Mac Address Table


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


Vlan    Mac Address       Type        Ports
```

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

10    0000.0001.000a    DYNAMIC     Drop
```

2. De Show Authenticatiesessie toont vele inzendingen, mogelijk boven 2000 of zelfs 10000.

<#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
```

Stappen voor probleemoplossing

- Packet Capture toont veel inkomende pakketten van een eindapparaat met verschillende Source MAC-adressen.
- De sessielimiet is 2000 en zodra de limiet is overschreden, ontstaan er onverwachte problemen in het netwerk
- 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

Isolatie

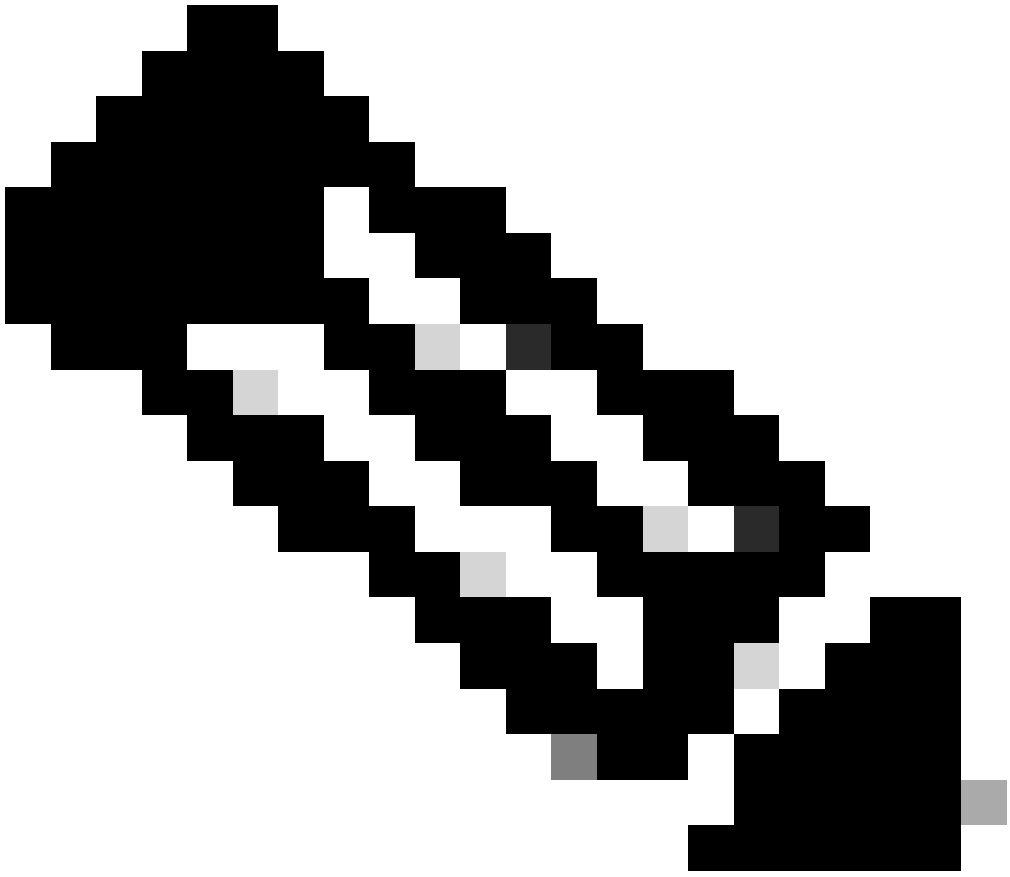
- Dit is een indicatie van het probleem van de eindgebruikeradapter.Hiermee worden misvormde pakketten verzonden die de switch als willekeurige bronmac-adressen begrijpt.

Actieplan

- Configureer "authenticatie host-mode multi-domain" wat slechts 2 mac adressen toestaat.
- Identificeer en isoleer de schuldige.

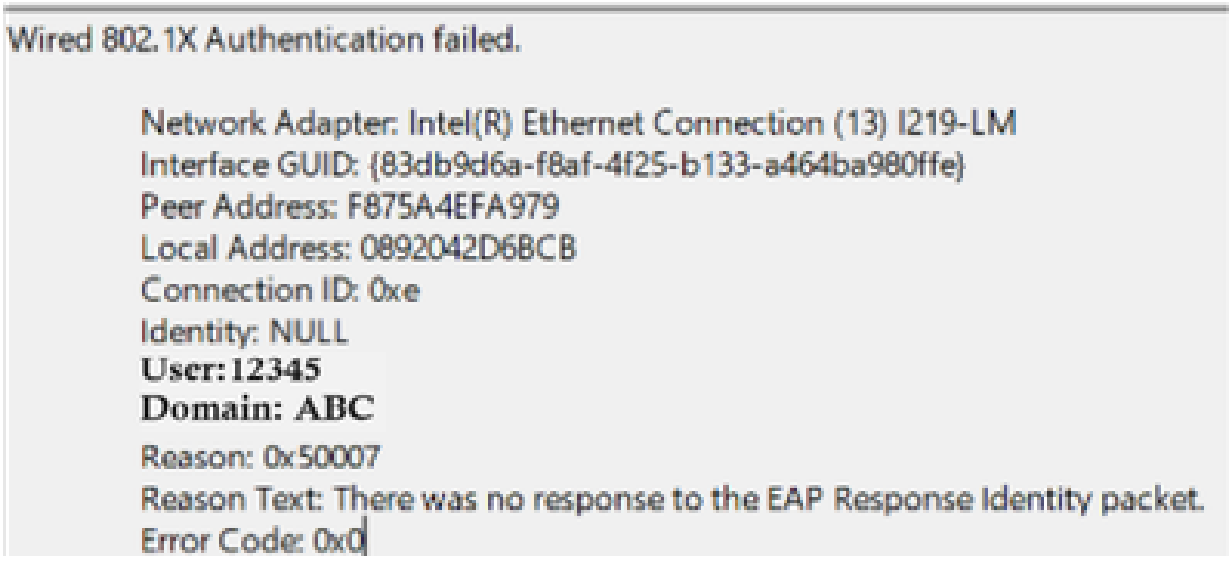
Resolutie/verificatie

- Na het configureren van deze tijdelijke oplossing wordt geen probleem geobserveerd.



- Opmerking: zorg ervoor dat poortbeveiliging of Dot1x auth-sessie host-mode multi-domein is ingeschakeld.

Scenario 5 - MTU Mismatch



ISE geeft deze fout op de server weer.

Probleembeschrijving:

- Gebruikersmachines ontvangen APIPA IP-adres en de gebruikersconnectiviteit is erdoor beïnvloed.

Gebruikerssymptomen

1. De eindclient verzendt een EAP-respons met een pakketlengte die groter is dan (Voorbeeld: 3736) de feitelijke verwachte pakketlengte 1492.

```
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
```

Probleemoplossing uitgevoerd

- MTU is ingesteld op minder formaat op switch als een systeembrede ingang. (Voorbeeld:1998bytes)
- Uitgaande interface geconfigureerd met hogere grootte. (Voorbeeld: 9198bytes)

Isolatie

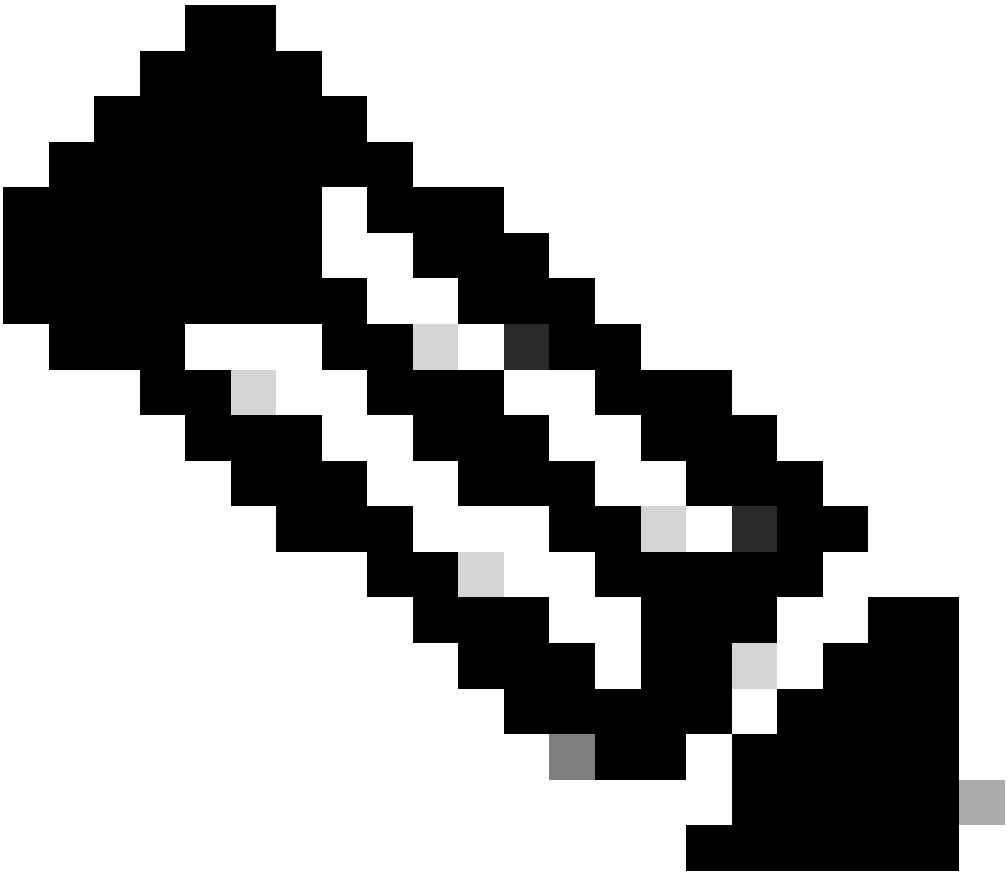
- Mismatch in MTU op het pad veroorzaakt het probleem.

Actieplan

- Verander het systeem MTU in 1500 en herlaad de switch

Resolutie/verificatie

- Nadat u deze instellingen hebt geconfigureerd, wordt de verificatie succesvol.



- Opmerking: Zorg ervoor dat dezelfde MTU op het pad van pakketstroom staat.

Scenario 6 - IPDT Guard

Probleembeschrijving:

- Gebruikersmachines ontvangen APIPA IP-adres en de gebruikersconnectiviteit is erdoor beïnvloed.

Gebruikerssymptomen

- Als u VM's in HA hebt, als dit beleid in de interface wordt toegepast:

apparaat-volgende beleid IPDT_POLICY

geen protocol-dup

volgen inschakelen

- Na een failover, wordt ARP antwoord gelaten vallen door de access switch.

Probleemoplossing uitgevoerd

1. ARP reacties op de sondes zou door switch worden gelaten vallen.
2. Switch is geconfigureerd met IPDT Guard.
3. IPDT - Guard laat vallen ARP sonde & eindapparaat krijgt APIPA.

Isolatie

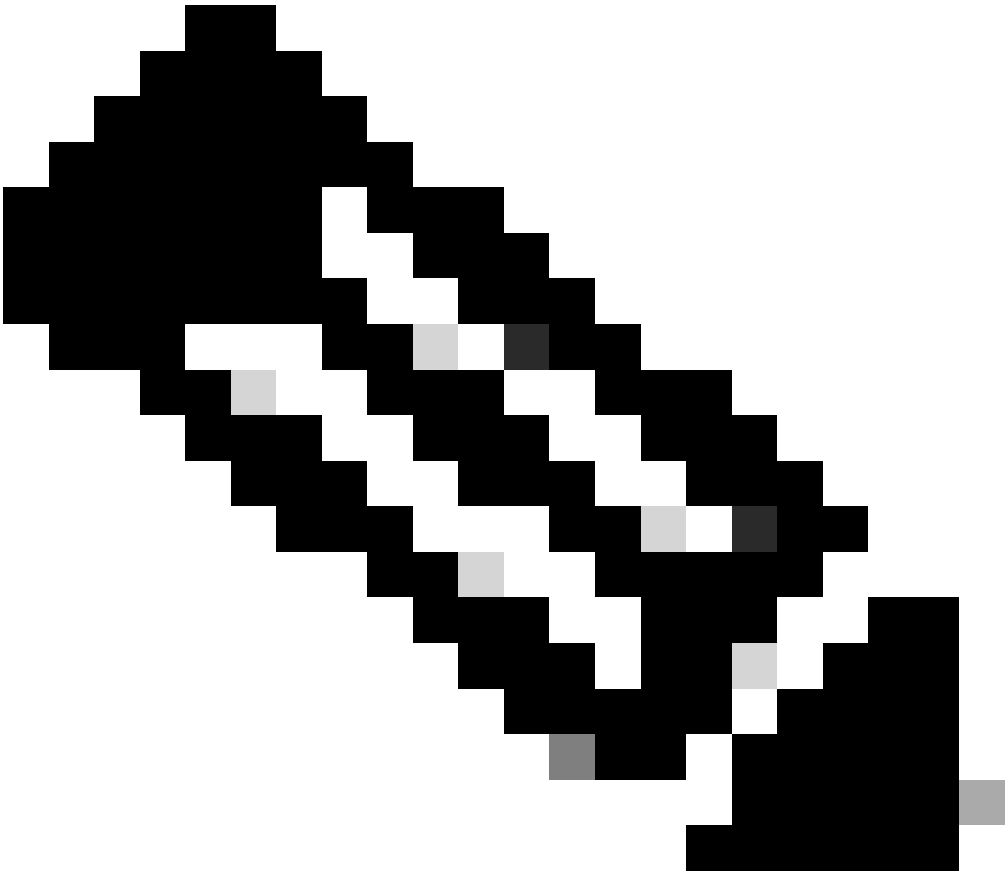
- ARP sonde pakketten die IPDT bereiken en wegens de eigenschap van de Garde worden gelaten vallen.
- IPDT-beleid geconfigureerd met 'security-level guard' configuratie laat ARP-pakketten vallen waardoor weinig of alle eindapparaten onbereikbaar zijn

Actieplan

- Verander de instelling van Guard naar Glean.
  Configureer 'glean op veiligheidsniveau' in het IPDT-beleid

Resolutie/verificatie

- Na het configureren van glean instellingen worden de ARP-sondes verwerkt door het ARP-proces & Probleem wordt opgelost.



- Opmerking: dit is een bekend defect dat in versie 17.15.1 en later zal worden verholpen.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.