Fehlerbehebung bei APIPA-Adressfehlern im Netzwerk

Inhalt

Einleitung

In diesem Dokument werden die Probleme im Zusammenhang mit den APIPA-Adressen beschrieben und entsprechende Lösungen vorgestellt.

Verwendete Komponenten

- Catalyst 9000 Switches
- ASA-Firewalls wie 5516
- DHCP-Server aller Art
- Catalyst 9300 in SDA-Konfiguration
- Software: k. A.

Gründe

Endbenutzer weisen in diesen Szenarien APIPA zu.

- DHCP-Server nicht verfügbar.
- Das DHCP-Angebot wird vor oder im aktuellen Hop verworfen.
- Der ARP-Prüfpunkt erhält eine Antwort, die "Duplicate IP" (Doppelte IP) darstellt.

Szenarien und Fehlerbehebung

Szenario 1 - Firewall-Proxy-Konfiguration

ASA 5516

Problembeschreibung:

- Die Benutzercomputer erhalten die APIPA-IP-Adresse, und die Benutzerkonnektivität wurde beeinträchtigt.

Symptome des Problems

1. Benutzer in einem bestimmten VLAN haben unregelmäßig Probleme, wenn sie eine APIPA-IP-Adresse erhalten und die Verbindung zum Netzwerk unterbrochen wird.
2. Firewalls verfügen über mehrere ARP-Einträge für eine MAC-Adresse eines Endbenutzers:

<#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
```

Schritte zur Fehlerbehebung

1. Die Debugging-Funktion der Firewall verweist auf die Firewall und sendet die Antwort an die ARP-Anfrage des Endbenutzers.

<#root>

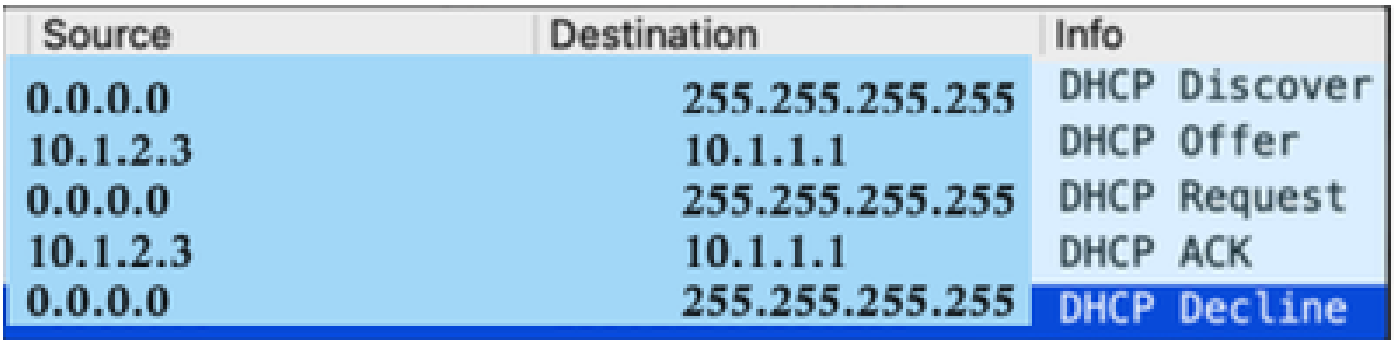
```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).


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

Dies macht das Endgerät zu denken, seine eine doppelte Adresse.

2. Erfassung auf Endgerät oder Firewall

Die Erfassungen zeigen, dass das Endgerät DHCP-Ablehnungspakete sendet, sobald der DORA-Prozess abgeschlossen ist.



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

Isolierung

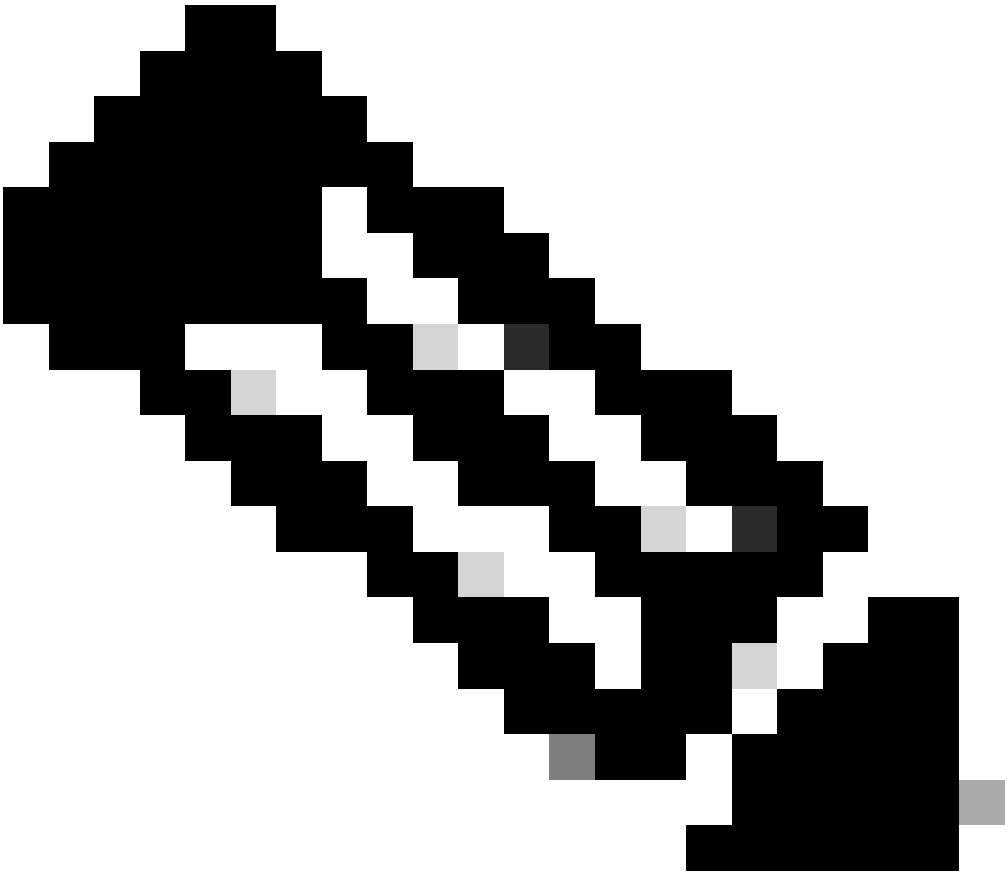
- Die interne Firewall-Schnittstelle reagiert auf die ARP-Anfrage, indem sie als Proxy fungiert, sobald der DORA-Prozess abgeschlossen ist. Dadurch wird der PC zum Senden von DHCP gezwungen.

Aktionsplan

- Deaktivieren Sie den Proxy-ARP auf der Firewall innerhalb der Schnittstelle mit dem Befehl "sysopt noproxyarp inside".

Auflösung/Verifizierung

- Endgeräte erhalten nach der Deaktivierung von Proxy-arp eine IP-Adresse.



- Hinweis: Vergewissern Sie sich, dass kein Gerät als Proxy fungiert und keine Antwort für Endbenutzer-ARP-Tests sendet.

.

Szenario 2 - DHCP-Serverbereich

DHCP Server

Problembeschreibung:

- Die Benutzercomputer erhalten die APIPA-IP-Adresse, und die Benutzerkonnektivität wurde beeinträchtigt.

Symptome

1. Benutzer eines bestimmten VLANs erhalten nur die APIPA-IP-Adresse, und die Verbindung zum Netzwerk wird unterbrochen.

Fehlerbehebung durchgeführt

- DHCP-Deaktivierung wurde an Endbenutzer gesendet und mit einer APIPA-Adresse konfiguriert

Isolierung

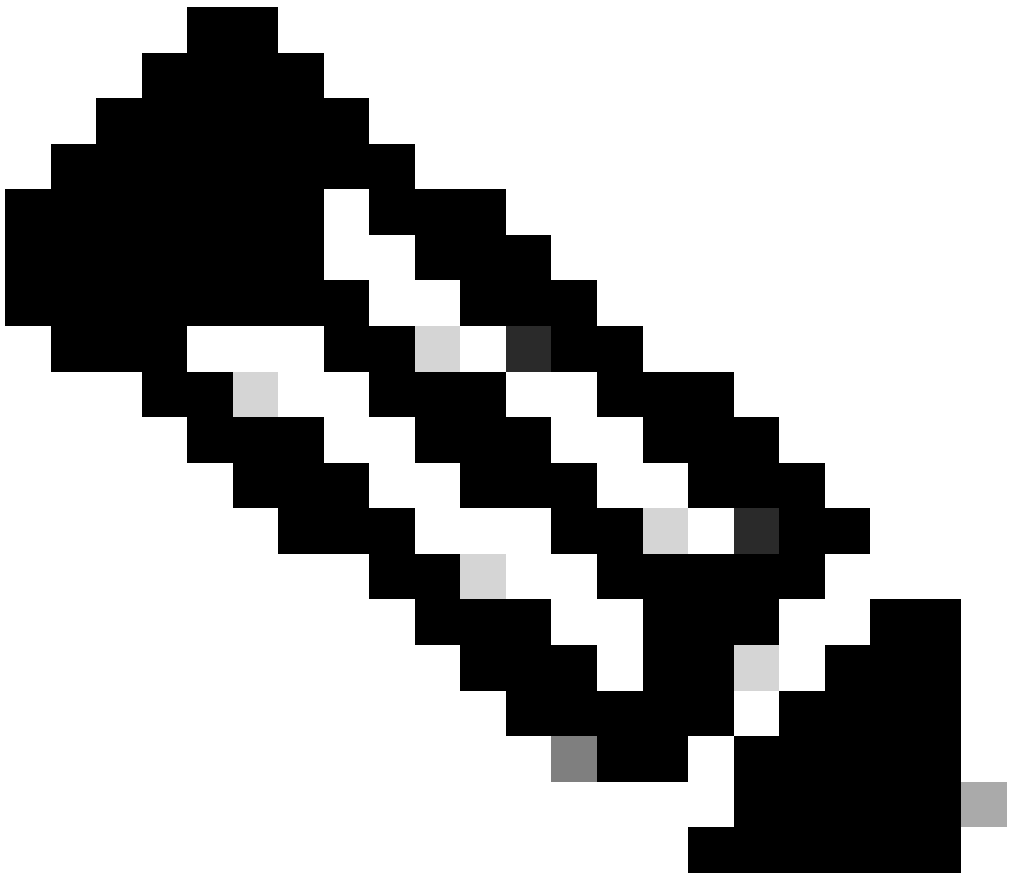
- Der DHCP-Server weist einem anderen Laptop eine IP-Adresse aus Bereich A und dieselbe IP-Adresse zu, da Bereich B denselben Bereich aufweist. Dies führt zu einem DHCP-Ausfall:
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

Aktionsplan

- Eindeutigen DHCP-Bereichsbereich zuweisen

Auflösung/Verifizierung

- Endgeräte erhalten nach der Bereichsänderung eine IP-Adresse.



Hinweis: Stellen Sie sicher, dass auf dem DHCP-Server keine doppelten Bereiche konfiguriert sind.

Szenario 3 - C9300 SDA-Konfiguration

Cat9300 in SDA

Problembeschreibung:

- Die Benutzercomputer erhalten die APIPA-IP-Adresse, und die Benutzerkonnektivität wurde beeinträchtigt.

Benutzersymptome

1. Einige Benutzer in einem bestimmten VLAN können keine DHCP-Adressen über den WAP abrufen.
2. Die Firewall verfügte über mehrere ARP-Einträge für eine MAC-Adresse eines Endbenutzers

<#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
```

Fehlerbehebung durchgeführt

- DHCP-Angebot wurde vom Switch gelöscht.
- FTD füllt ARP basierend auf dem DHCP-ANGEBOT aus, das vom DHCP-Server zurückgesendet wird.

<#root>

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

Isolierung

- Wenn für die SDA-Wireless-Einrichtung ein reines L2-VLAN konfiguriert ist, erreichen Pakete mit Broadcast-Flag den AP nicht. Da der Access-Tunnel standardmäßig keine Broadcast-Pakete zulässt,

Aktionsplan

- Überflutungsfähigkeit innerhalb der LISP-Umgebung zulassen.

<#root>

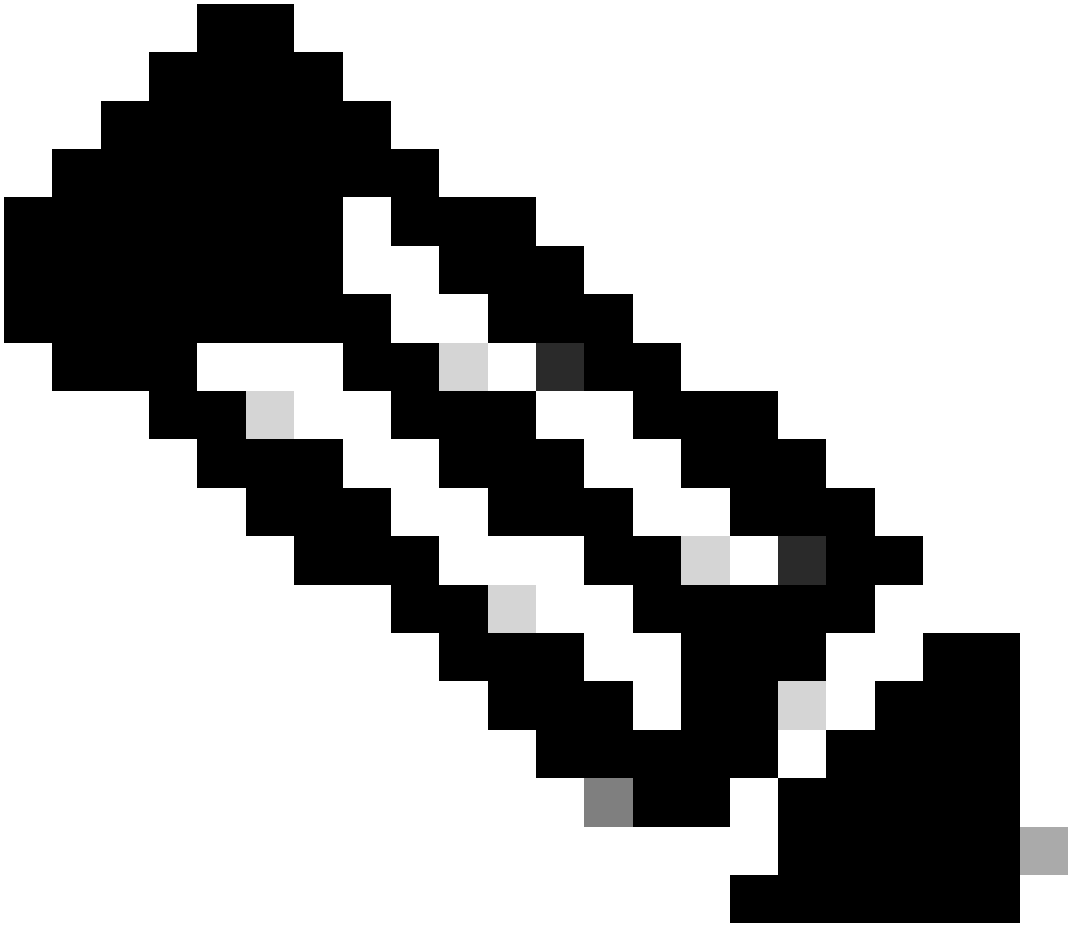
```
router lisp


instance-id 8456


flood access-tunnel
```

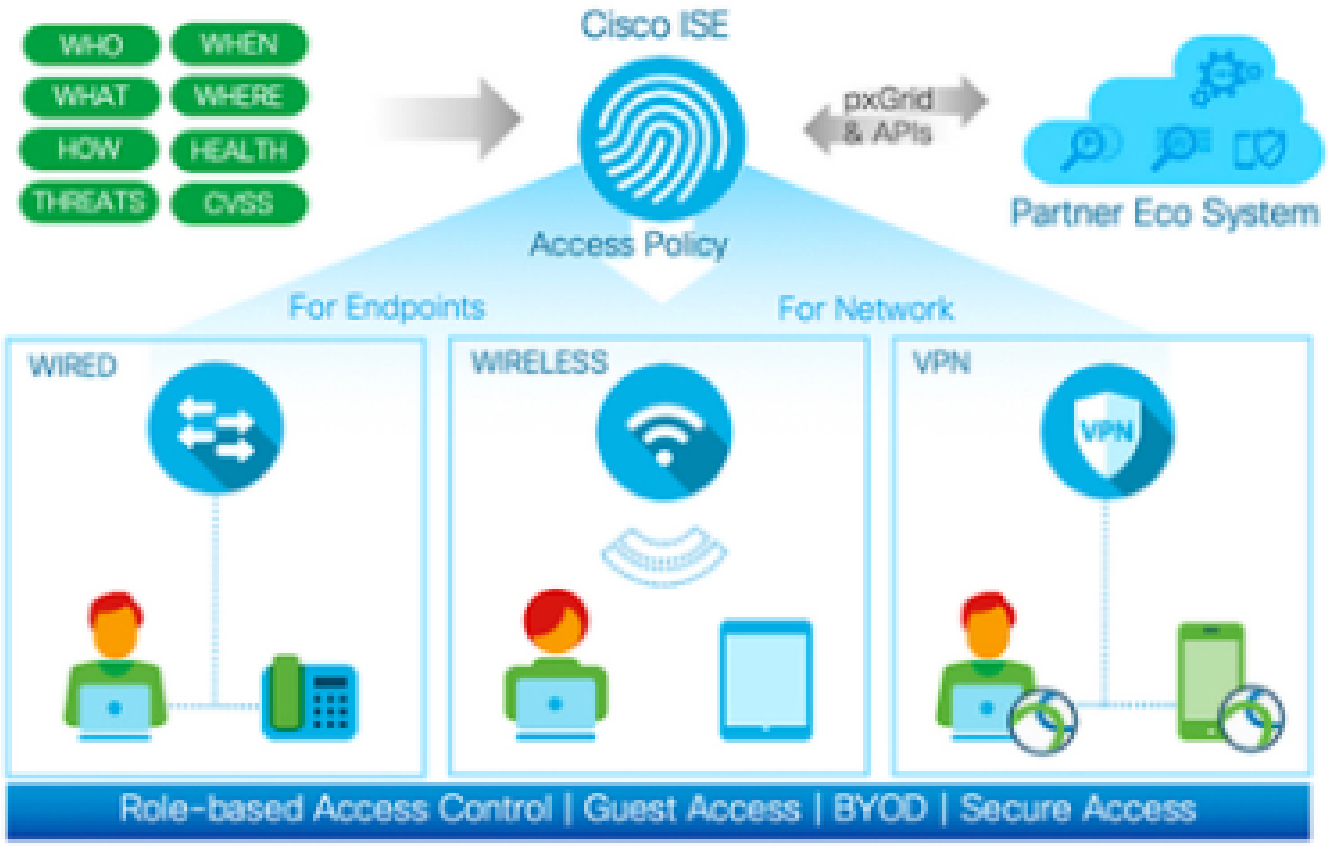
Auflösung/Verifizierung

- Nach der Konfiguration des "Flood Access-Tunnels" auf dem an der internen Schnittstelle angeschlossenen C9300 erhalten die Clients DHCP-Adressen.



Hinweis: Stellen Sie sicher, dass Sie den Zugriffstunnel unter lisp aktivieren, wenn das Endgerät für den Empfang des Broadcast-Angebots konfiguriert ist.

Szenario 4 - Problem mit dem LAN-Adapter



cisco ISE

Problembeschreibung:

- Die Benutzercomputer erhalten die APIPA-IP-Adresse, und die Benutzerkonnektivität wurde beeinträchtigt.

Symptome

1. Die MAC-Adresstabelle zeigt Einträge mit "drop" an.

<#root>

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


Mac Address Table


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


Vlan    Mac Address       Type        Ports
```

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

10    0000.0001.000a    DYNAMIC     Drop
```

2. Die Show Authentication Session zeigt viele Einträge an, möglicherweise mehr als 2000 oder sogar 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
```

Schritte zur Fehlerbehebung

- Bei der Paketerfassung werden viele eingehende Pakete von Endgeräten mit unterschiedlichen Quell-MAC-Adressen angezeigt.
- Das Authentifizierungssitzungslimit beträgt 2000, und sobald das Limit überschritten wird, treten unerwartete Probleme im Netzwerk auf.
- 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

Isolierung

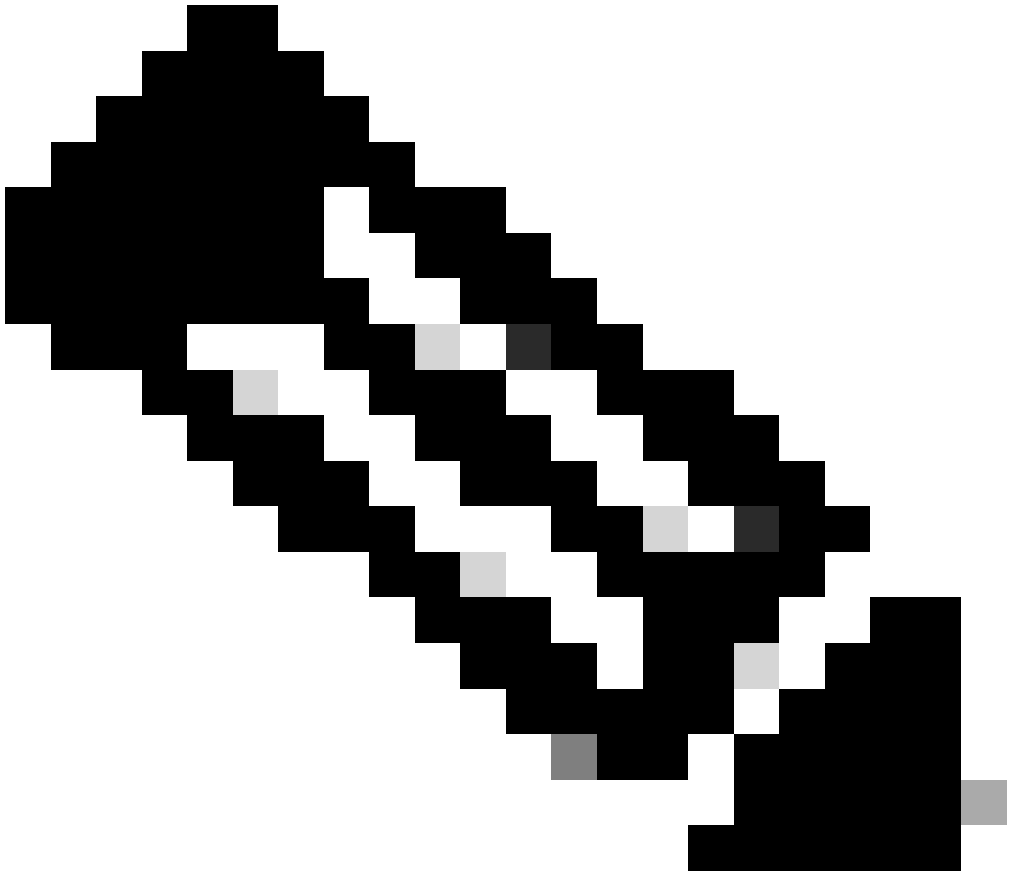
- Dies ist ein Hinweis auf ein Endbenutzer-Adapterproblem. Dies sendet fehlerhafte Pakete, die der Switch als zufällige Quell-MAC-Adressen versteht.

Aktionsplan

- Konfigurieren Sie "authentication host-mode multi-domain", die nur 2 MAC-Adressen zulässt.
- Identifizierung und Isolierung des verantwortlichen Geräts

Auflösung/Verifizierung

- Nach der Konfiguration dieser Problemumgehung konnte kein Problem festgestellt werden.



- Hinweis: Stellen Sie sicher, dass Sie entweder "port-security" oder "Dot1x auth session host-mode multi-domain" aktivieren.

Szenario 5 - MTU-Abweichung

Wired 802.1X Authentication failed.

Network Adapter: Intel(R) Ethernet Connection (13) I219-LM
Interface GUID: {83db9d6a-f8af-4f25-b133-a464ba980ffe}
Peer Address: F875A4EFA979
Local Address: 0892042D6BCB
Connection ID: 0xe
Identity: NULL
User: 12345
Domain: ABC
Reason: 0x50007
Reason Text: There was no response to the EAP Response Identity packet.
Error Code: 0x0

ISE stellt diesen Fehler auf dem Server dar.

Problembeschreibung:

- Die Benutzercomputer erhalten die APIPA-IP-Adresse, und die Benutzerkonnektivität wurde beeinträchtigt.

Benutzersymptome

1. Der Endclient sendet eine EAP-Antwort, deren Paketlänge größer ist als die tatsächliche erwartete Paketlänge von 1492 (Beispiel: 3736).

```
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
```

Fehlerbehebung durchgeführt

- Die MTU wird auf dem Switch als systemweiter Eintrag auf eine geringere Größe festgelegt. (Beispiel: 1998 Byte)
- Für die Ausgangsschnittstelle wurde eine höhere Größe konfiguriert. (Beispiel: 9198 Byte)

Isolierung

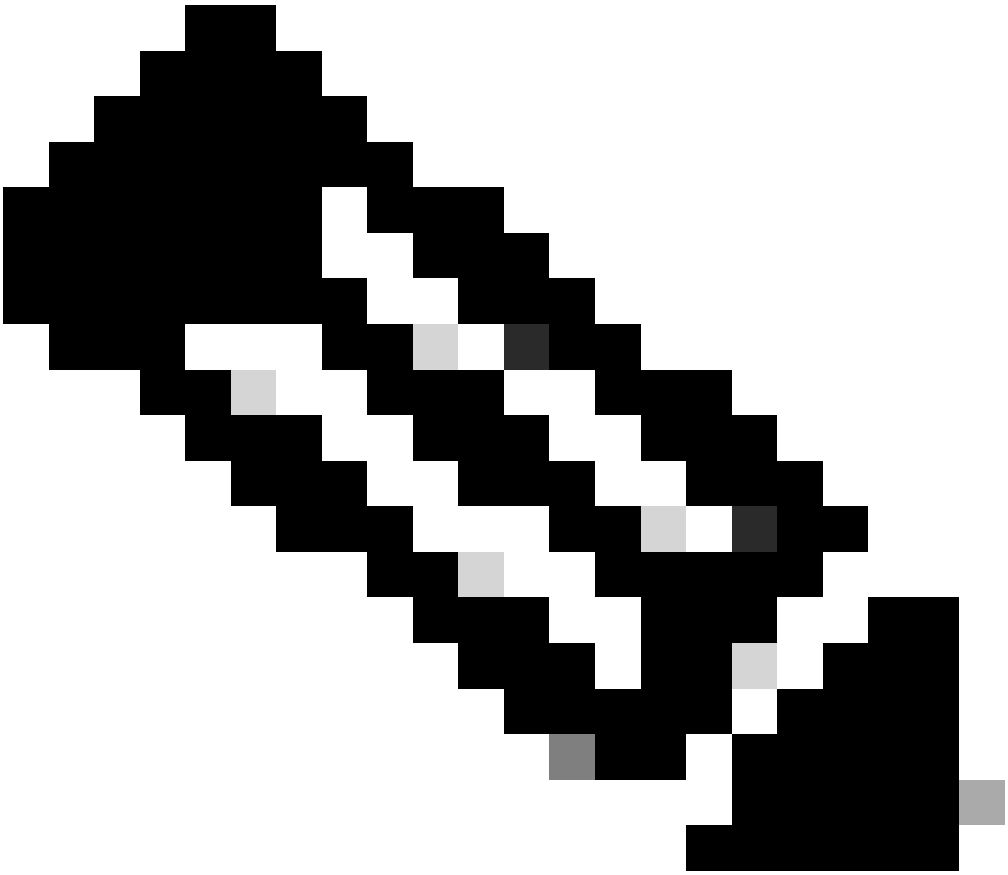
- Diskrepanzen in der MTU im gesamten Pfad verursachen das Problem.

Aktionsplan

- Ändern Sie die System-MTU auf 1500, und laden Sie den Switch neu.

Auflösung/Verifizierung

- Nach der Konfiguration dieser Einstellungen ist die Authentifizierung erfolgreich.



- Hinweis: Stellen Sie sicher, dass Sie im gesamten Pfad des Paketflusses dieselbe MTU aktivieren.

Szenario 6 - IPDT-Schutz

Problembeschreibung:

- Die Benutzercomputer erhalten die APIPA-IP-Adresse, und die Benutzerkonnektivität wurde beeinträchtigt.

Benutzersymptome

- Wenn VMs in HA sind und Sie diese Richtlinie in der Schnittstelle angewendet haben:

Richtlinie zur Geräteverfolgung IPDT_POLICY

Kein Protokoll-UDP

Nachverfolgung aktivieren

- Nach einem Failover wird die ARP-Antwort vom Access Switch gelöscht.

Fehlerbehebung durchgeführt

1. Die ARP-Antworten auf die Tests werden per Switch verworfen.
2. Der Switch wird mit IPDT Guard konfiguriert.
3. IPDT - Guard fallen ARP-Sonde und Endgerät APIPA zu erhalten.

Isolierung

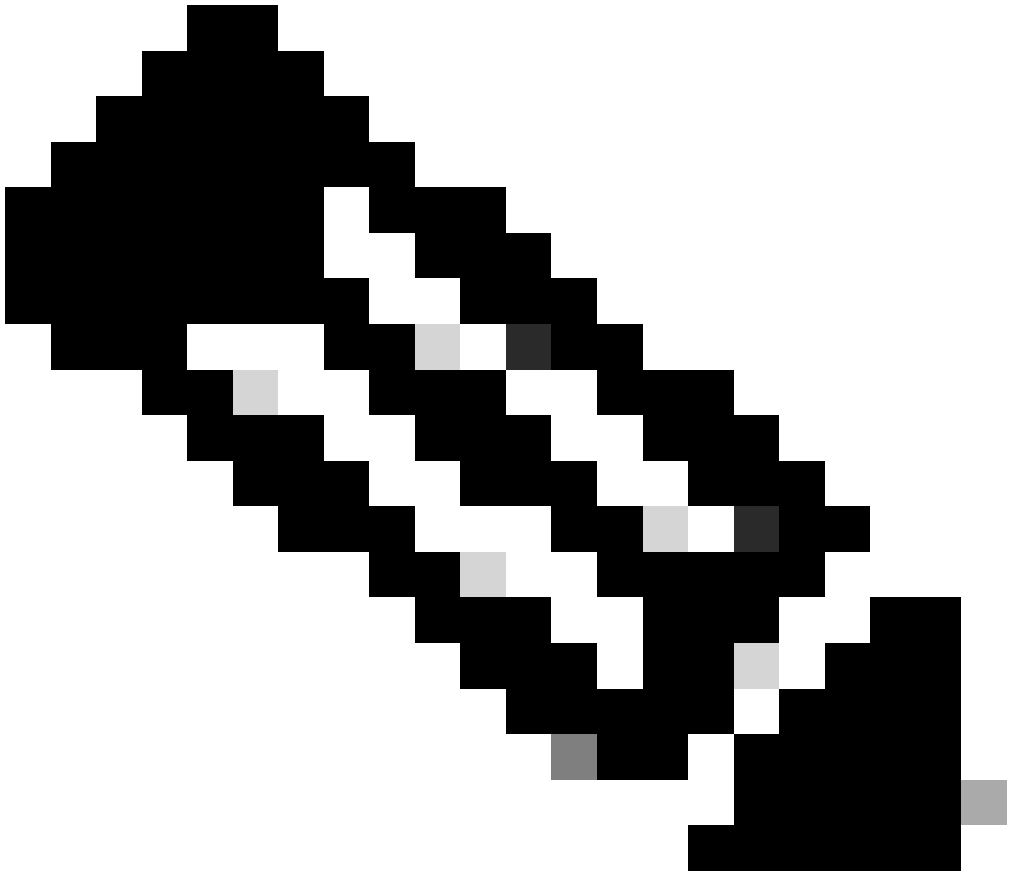
- ARP-Testpakete erreichen IPDT und werden aufgrund der Guard-Funktion verworfen.
- Bei Konfiguration der IPDT-Richtlinie mit der Konfiguration "Security Level Guard" werden ARP-Pakete verworfen, sodass nur wenige oder alle Endgeräte nicht erreichbar sind.

Aktionsplan

- Ändern Sie die Einstellung von Guard in Glean.
  Konfigurieren Sie "security-level glean" in der IPDT-Richtlinie.

Auflösung/Verifizierung

- Nach der Konfiguration der Glean-Einstellungen werden die ARP-Tests vom ARP-Prozess verarbeitet, und das Problem wird behoben.



- Hinweis: Dies ist ein bekannter Fehler, der in der Version 17.15.1 und höher behoben wird.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.