Resolución de problemas de falla de dirección APIPA en la red

Contenido

Introducción

Este documento describe los problemas relacionados con las direcciones de APIPA y proporciona resoluciones para el mismo.

Componentes Utilizados

- switches Catalyst 9000.
- Firewalls ASA como el 5516
- Servidor DHCP de cualquier tipo
- Catalyst 9300 en configuración SDA
- Software: N/D

Motivos

Los usuarios finales asignan APIPA en estos casos,

- Servidor DHCP no disponible.
- La oferta de DHCP se suprime antes o antes del salto actual.
- La sonda ARP obtiene una respuesta que representa la IP duplicada.

Escenarios y resolución de problemas

Situación 1: configuración de proxy de firewall

ASA 5516

Descripción de problemas:

- Las máquinas de usuario reciben la dirección IP de APIPA y la conectividad de usuario se ve afectada.

Indicios de problema

1. Los usuarios de una VLAN específica experimentan problemas intermitentes cuando reciben una dirección IP APIPA y pierden la conectividad con la red.
2. Los firewalls tienen múltiples entradas ARP para una sola dirección MAC de usuario final como esta:

<#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
```

Pasos para la resolución de problemas

1. Las depuraciones del firewall apuntan al firewall que envía la respuesta a la sonda ARP de los usuarios finales.

<#root>

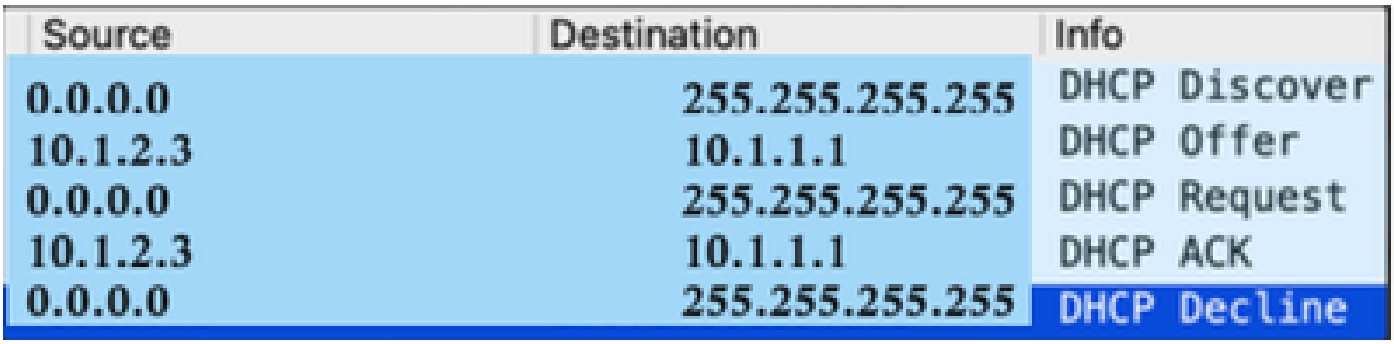
```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).


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

Esto hace que el dispositivo final piense que es una dirección duplicada.

2. Capturas en el dispositivo final o firewall

Las capturas muestran el dispositivo final que envía paquetes de rechazo DHCP una vez que se completa el proceso DORA.



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

Aislamiento

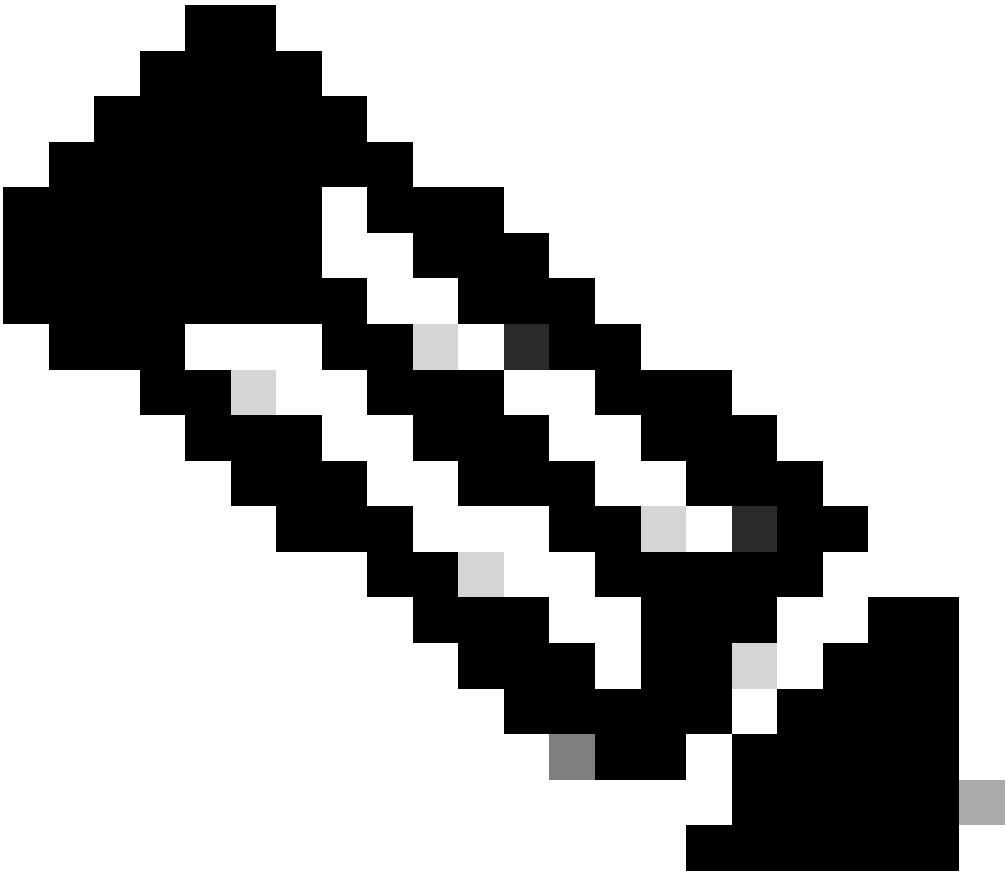
- La interfaz interna del firewall responde a la sonda ARP actuando como proxy, una vez que se completa el proceso DORA. Esto hace que el PC que envía DHCP se rechace.

Plan de acción

- Inhabilite el proxy arp en la interfaz interna del Firewall mediante el comando "sysopt noproxyarp inside"

Resolución/Verificación

- Los dispositivos finales reciben la dirección IP después de inhabilitar proxy-arp.



- Nota: Asegúrese de que ningún dispositivo actúe como proxy o envíe una respuesta para las sondas ARP del usuario final.

.

Situación 2: ámbito del servidor DHCP

DHCP Server

Descripción de problemas:

- Las máquinas de usuario reciben la dirección IP de APIPA y la conectividad de usuario se ve afectada.

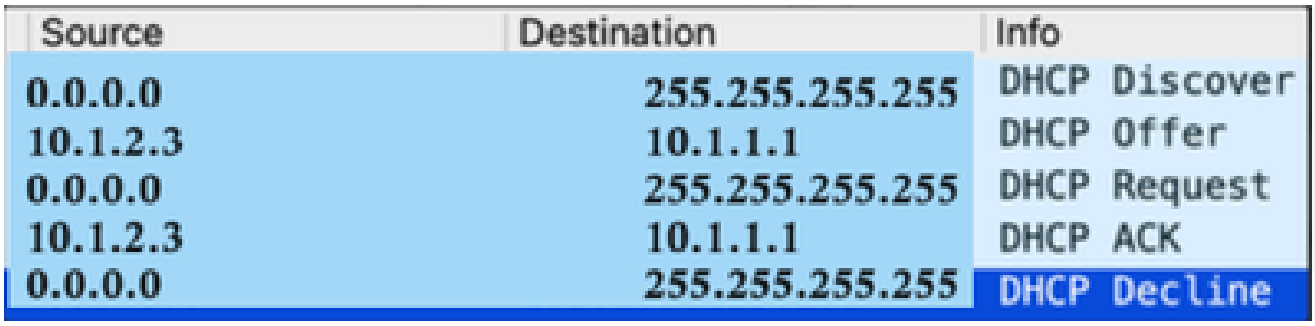
Síntomas

1. Los usuarios de una vlan específica obtienen solo la dirección IP de APIPA y pierden la conexión a la red.

Resolución de problemas realizada

- La declinación de DHCP se envió a los usuarios finales y se configuró con la dirección APIPA

Aislamiento

- El servidor DHCP asigna una dirección IP del ámbito A y la misma dirección IP se asigna a otro ordenador portátil porque el ámbito B tiene el mismo intervalo. Esto provoca el rechazo de DHCP:
- 

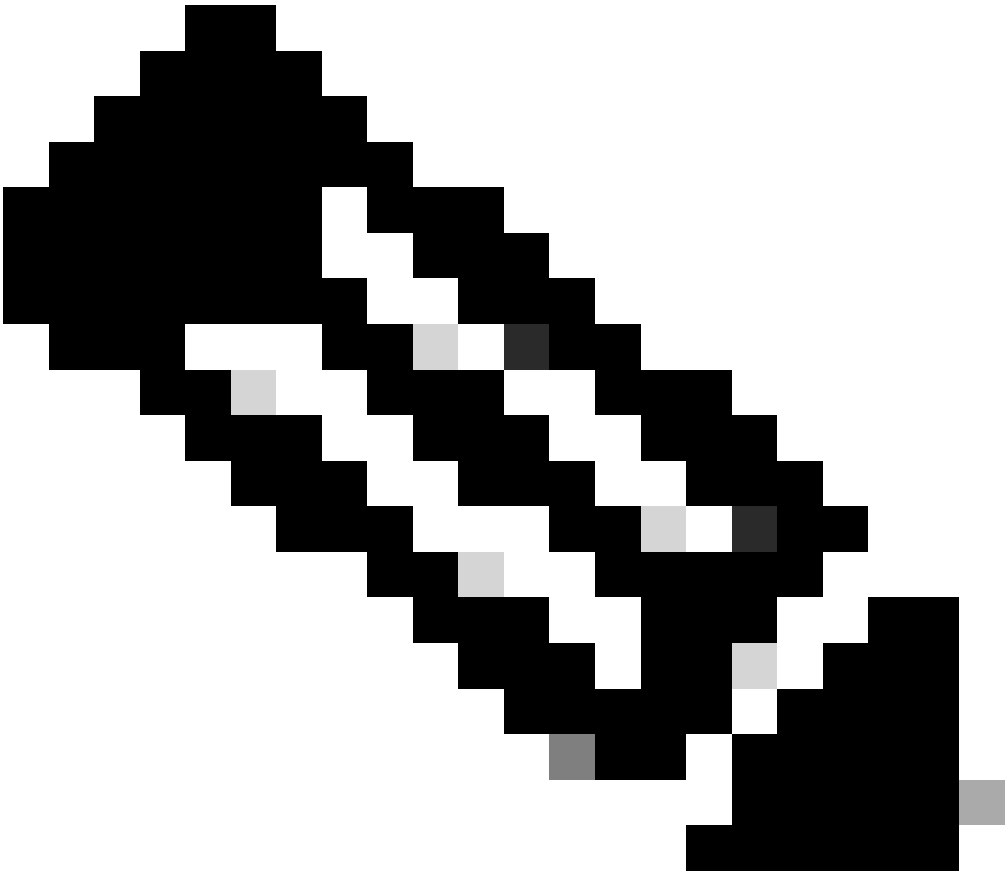
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

Plan de acción

- Asignar un intervalo de alcance DHCP único

Resolución/Verificación

- Los dispositivos finales reciben la dirección IP después de cambiar el alcance.



- Nota: Asegúrese de que el servidor DHCP no tiene ámbitos duplicados configurados.

Situación 3: configuración SDA del C9300

Cat9300 in SDA

Descripción de problemas:

- Las máquinas de usuario reciben la dirección IP de APIPA y la conectividad de usuario se ve afectada.

Síntomas del usuario

1. Algunos usuarios en una VLAN específica no pueden obtener direcciones DHCP a través del AP inalámbrico.
2. El firewall tenía varias entradas arp para una única dirección mac de usuario final

<#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
```

Resolución de problemas realizada

- La oferta de DHCP se ha eliminado por switch
- El FTD rellena el ARP basándose en la OFERTA DHCP que vuelve del servidor DHCP.

<#root>

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

Aislamiento

- Si la VLAN solo de L2 está configurada para la configuración inalámbrica SDA, el paquete de oferta con el indicador de difusión no alcanza el AP. Dado que el túnel de acceso no permite paquetes de difusión de forma predeterminada.

Plan de acción

- Permitir la "capacidad de saturación" dentro del entorno LISP.

<#root>

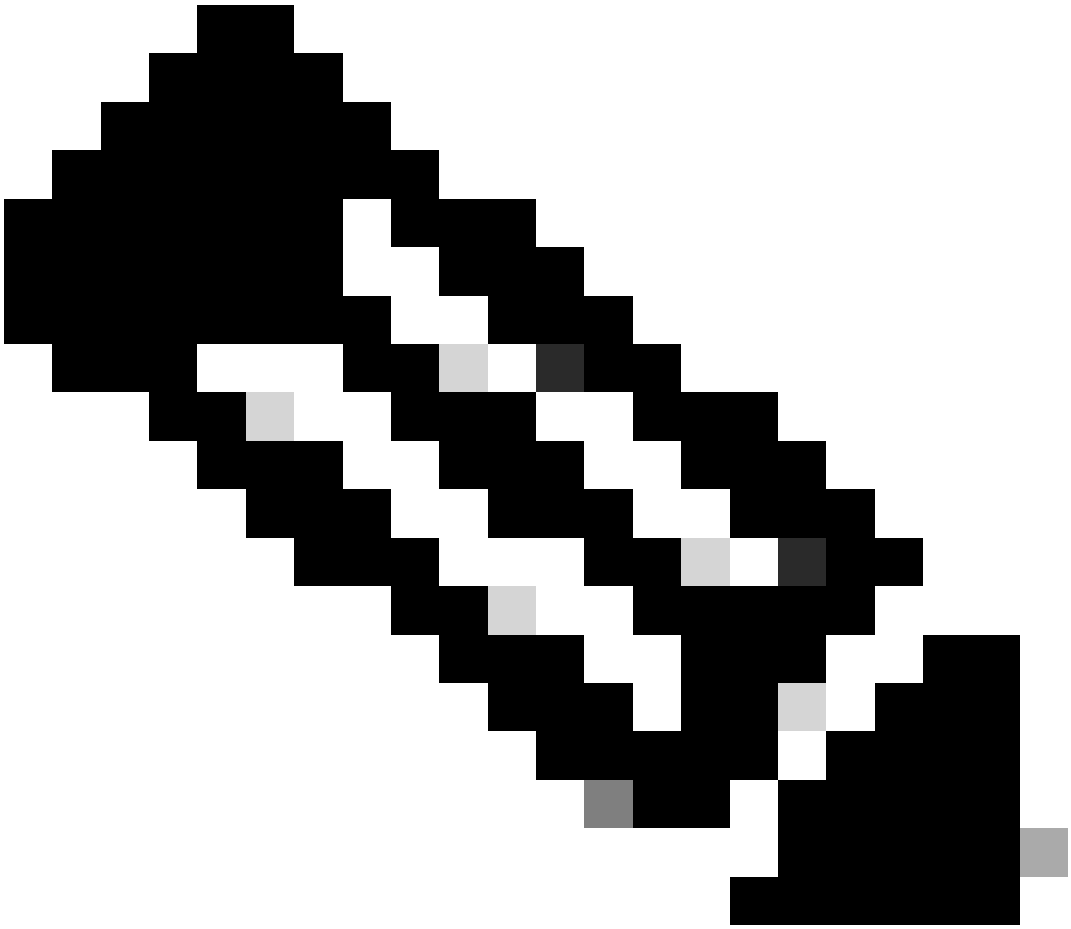
```
router lisp

instance-id 8456

flood access-tunnel
```

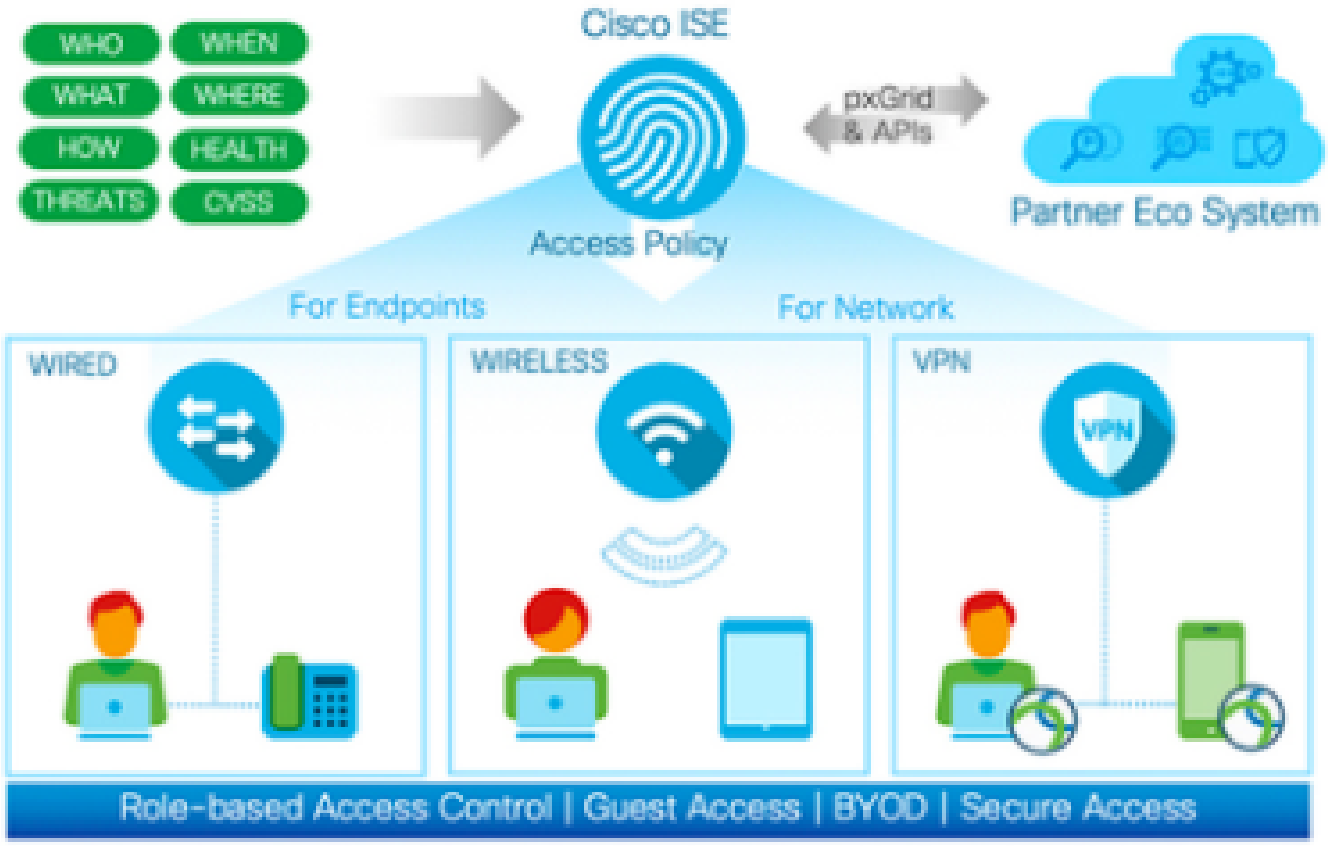
Resolución/Verificación

- Después de configurar `flood access-tunnel` en el C9300 conectado en la interfaz interna, los clientes reciben las direcciones DHCP.



Nota: Asegúrese de habilitar flood access-tunnel bajo lisp, si el dispositivo final está configurado para recibir la oferta de broadcast.

Situación 4: problema del adaptador LAN



cisco ISE

Descripción de problemas:

- Las máquinas de usuario reciben la dirección IP de APIPA y la conectividad de usuario se ve afectada.

Síntomas

1. La tabla de direcciones MAC muestra las entradas con "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. La sesión Show Authentication muestra muchas entradas, posiblemente excediendo 2000 o incluso 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
```

Pasos para la resolución de problemas

- La captura de paquetes muestra muchos paquetes entrantes del dispositivo final con diferentes direcciones MAC de origen.
- El límite de sesiones de autenticación es 2000 y una vez que se supera el límite, surgen problemas inesperados en la red
- 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

Aislamiento

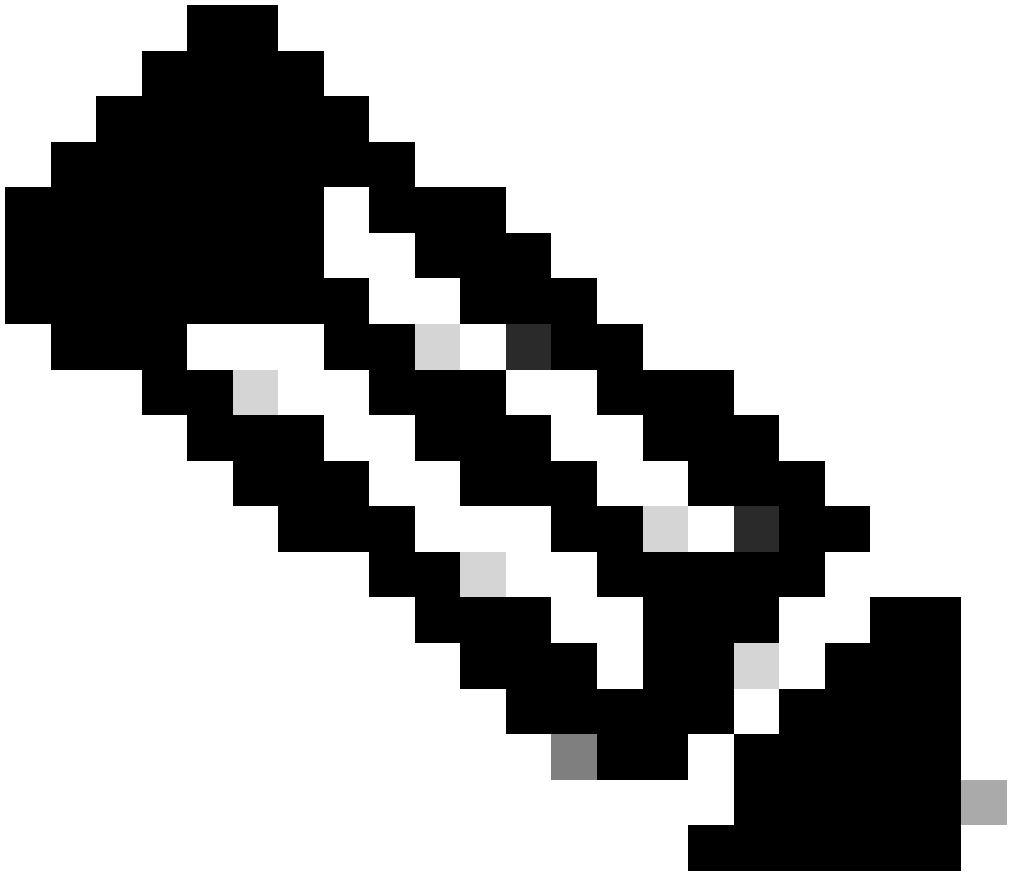
- Esto es una indicación del problema del adaptador del usuario final. Esto envía paquetes mal formados que el switch entiende como direcciones MAC de origen aleatorias.

Plan de acción

- Configure el "modo de host de autenticación multidominio" que permite sólo 2 direcciones MAC.
- Identifique y aísle el dispositivo culpable.

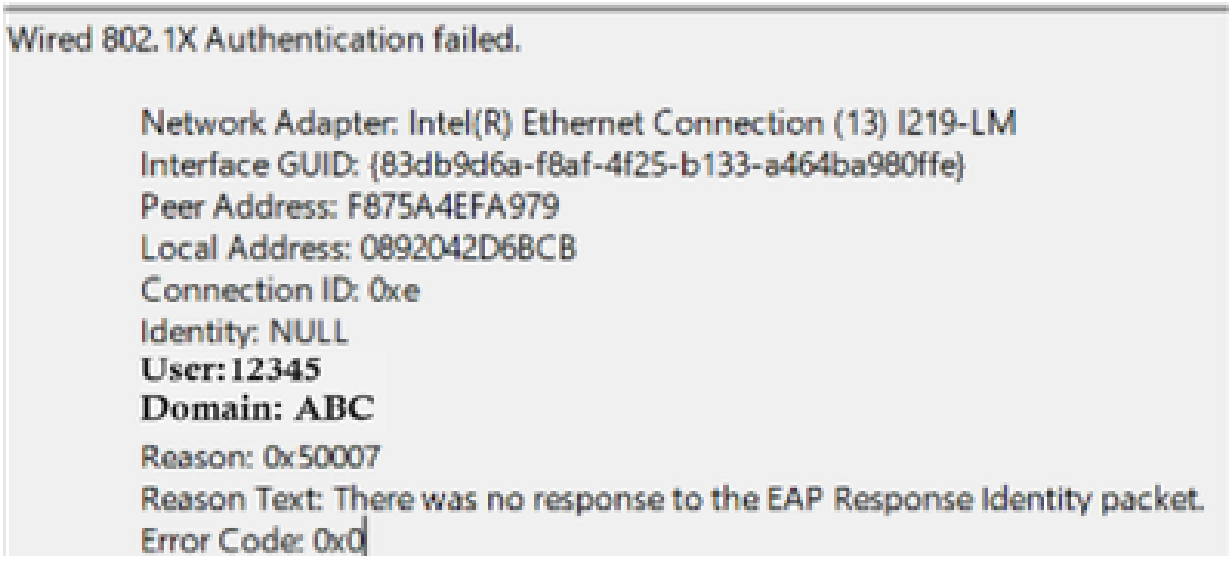
Resolución/Verificación

- Después de configurar esta solución alternativa, no se observará ningún problema.



- Nota: Asegúrese de habilitar port-security o Dot1x auth session host-mode multi-domain.

Situación 5: discordancia de MTU



ISE representa este error en el servidor.

Descripción de problemas:

- Las máquinas de usuario reciben la dirección IP de APIPA y la conectividad de usuario se ve afectada.

Síntomas del usuario

1. El cliente final envía una respuesta EAP con una longitud de paquete superior a (ejemplo: 3736) la longitud de paquete real esperada 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
```

Resolución de problemas realizada

- MTU establecida en menor tamaño en el switch como entrada para todo el sistema. (Ejemplo: 1998 bytes)
- Interfaz de salida configurada con un tamaño mayor. (Ejemplo: 9198 bytes)

Aislamiento

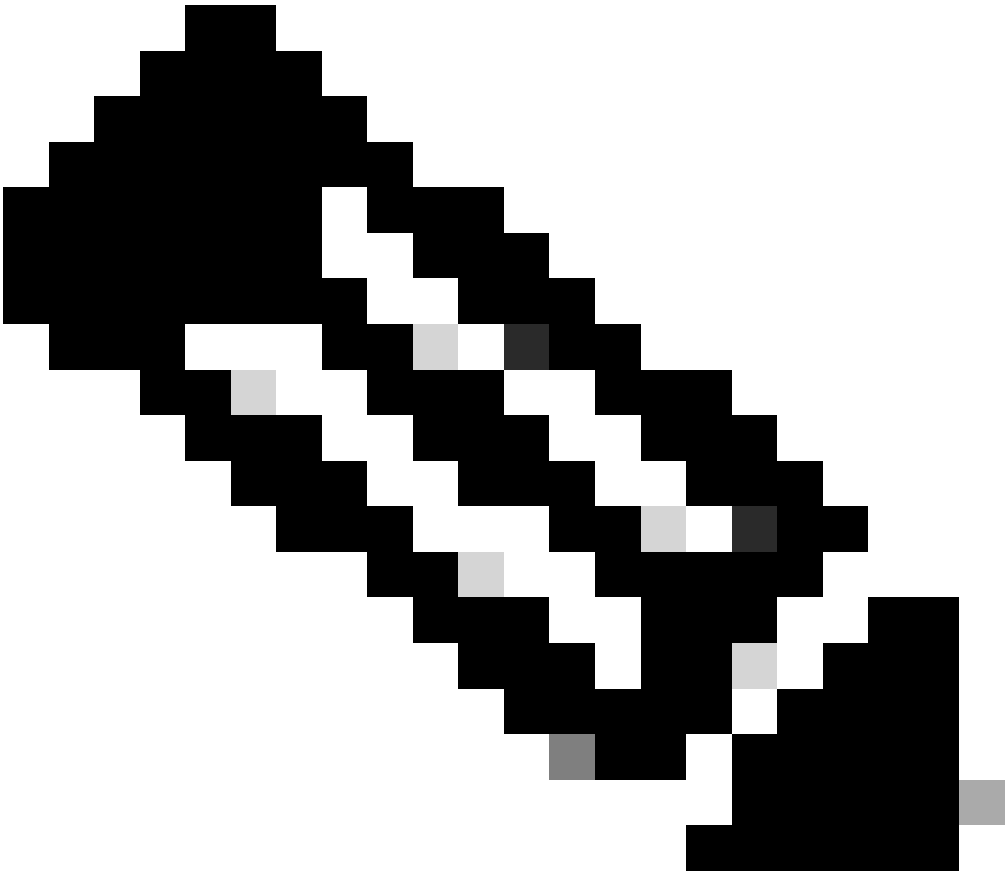
- La discordancia en la MTU a lo largo de la trayectoria causa el problema.

Plan de acción

- Cambie la MTU del sistema a 1500 y recargue el switch

Resolución/Verificación

- Después de configurar esta configuración, la autenticación se realiza correctamente.



- Nota: Asegúrese de habilitar la misma MTU en toda la trayectoria del flujo de paquetes.

Situación 6: protección IPDT

Descripción de problemas:

- Las máquinas de usuario reciben la dirección IP de APIPA y la conectividad de usuario se ve afectada.

Síntomas del usuario

- Al tener VM en HA, si tiene esta política aplicada en la interfaz:

política de seguimiento de dispositivos IPDT_POLICY

no protocol udp

tracking enable

- Después de una conmutación por fallas, el switch de acceso descarta la respuesta ARP.

Resolución de problemas realizada

1. Las respuestas ARP a las sondas se descartarían por el switch.
2. El switch está configurado con protección IPDT.
3. IPDT - Proteja la sonda ARP y el dispositivo final que recibe APIPA.

Aislamiento

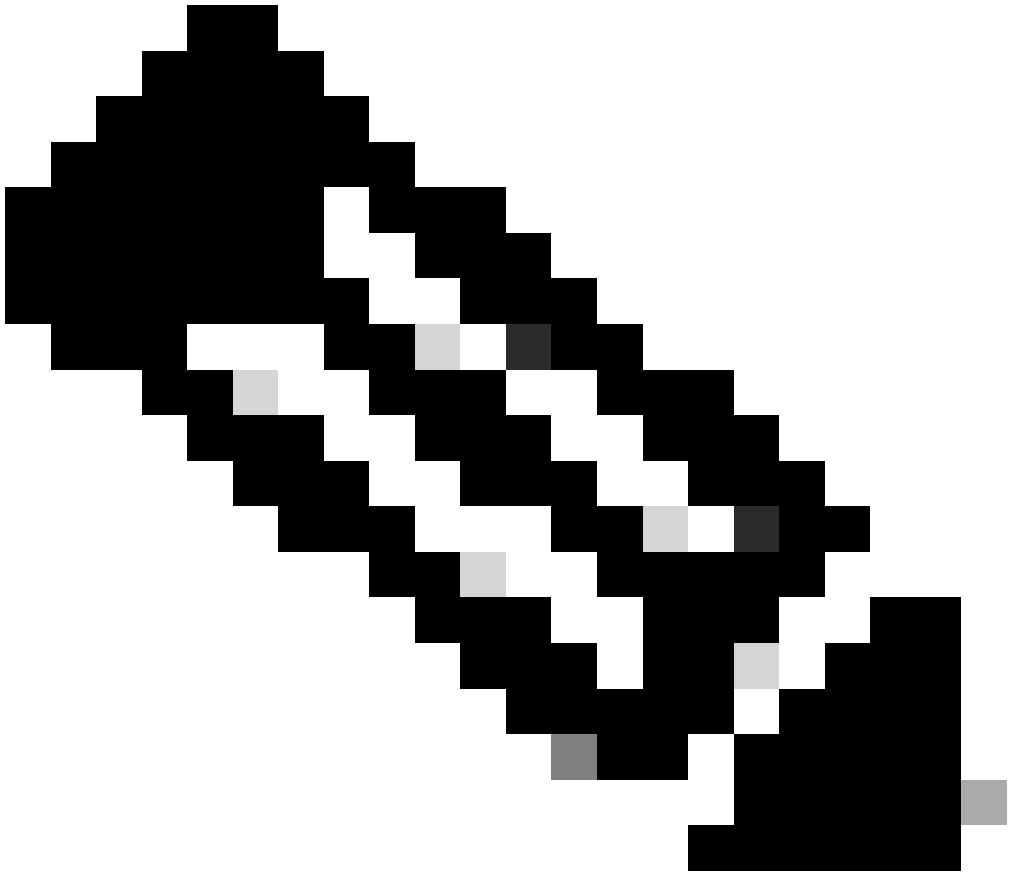
- Los paquetes de sondeo ARP que llegan a IPDT se descartan debido a la función Guard.
- La política IPDT configurada con la configuración 'security-level guard' descarta paquetes ARP que hacen que unos o todos los dispositivos finales sean inalcanzables

Plan de acción

- Cambie el ajuste de Guard (Protector) a Glean.
  Configure 'security-level glean' en la política IPDT

Resolución/Verificación

- Después de configurar los ajustes de recolección, las sondas ARP son procesadas por el proceso ARP y el problema se resuelve.



- Nota: Este es un defecto bien conocido y se corregiría en la versión 17.15.1 y posteriores.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).