Identificar e Solucionar Falhas de Endereço APIPA na Rede

Contents

Introdução

Este documento descreve os problemas relacionados aos endereços APIPA e fornece soluções para os mesmos.

Componentes Utilizados

- Catalyst 9000 Switches.
- Firewalls ASA como o 5516
- Servidor DHCP de qualquer tipo
- Catalyst 9300 na configuração SDA
- Software: N/A

Motivos

Os usuários finais atribuem APIPA durante esses cenários,

- Servidor DHCP não disponível.
- A oferta DHCP é descartada antes do salto atual.
- A sonda ARP obtém uma resposta que representa IP duplicado.

Cenários e solução de problemas

Cenário 1 - Configuração de proxy do firewall

ASA 5516

Descrição do problema:

- As máquinas do usuário recebem o endereço IP APIPA e a conectividade do usuário afetada.

Sintomas do problema

1. Os usuários em uma VLAN específica enfrentam problemas intermitentes quando recebem um endereço IP APIPA e perdem a conectividade com a rede.
2. Os firewalls têm várias entradas ARP para um único endereço MAC de usuário final como este:

<#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
```

Passos de Troubleshooting

1. As depurações no Firewall apontam para o firewall que envia a resposta para a sonda ARP dos usuários finais.

<#root>

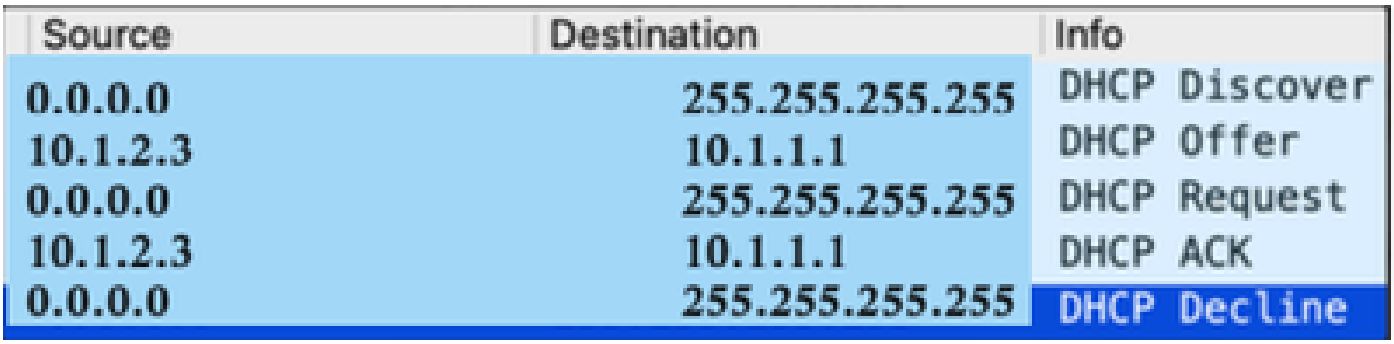
```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).


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

Isso faz com que o dispositivo final pense que é um endereço duplicado.

2. Capturas no dispositivo final ou Firewall

Capturas mostram o dispositivo final enviando pacotes DHCP Decline uma vez que o processo DORA é concluído.



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

Isolamento

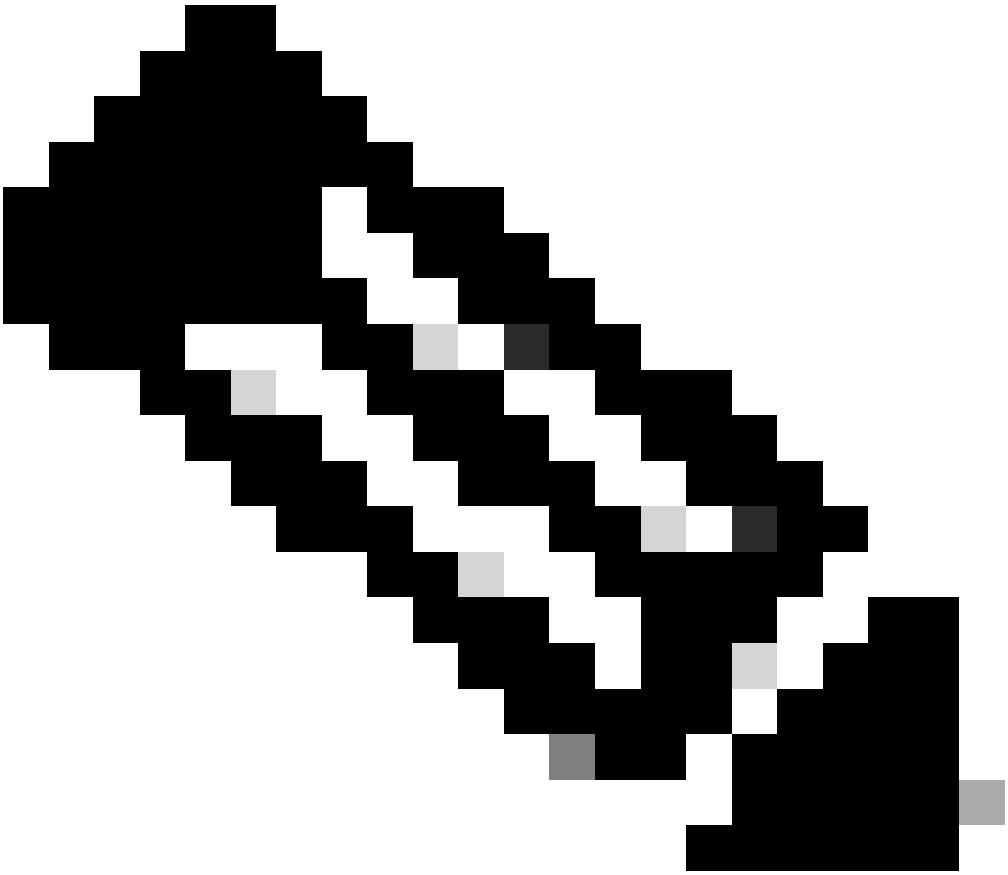
- A interface interna do firewall responde à sonda ARP atuando como proxy, uma vez que o processo DORA é concluído. Isso faz com que o PC envie a recusa de DHCP.

Plano de ação

- Desative o proxy arp na interface interna do Firewall usando o comando "sysopt noproxyarp inside"

Resolução/Verificação

- Os dispositivos finais recebem o endereço IP após desativar o proxy-arp.



- Observação: certifique-se de que nenhum dispositivo atue como proxy ou envie resposta para testes ARP do usuário final.

.

Cenário 2 - Escopo do servidor DHCP

DHCP Server

Descrição do problema:

- As máquinas do usuário recebem o endereço IP APIPA e a conectividade do usuário afetada.

Sintomas

1. Os usuários em uma vlan específica obtêm apenas o endereço IP APIPA e perdem a conexão com a rede.

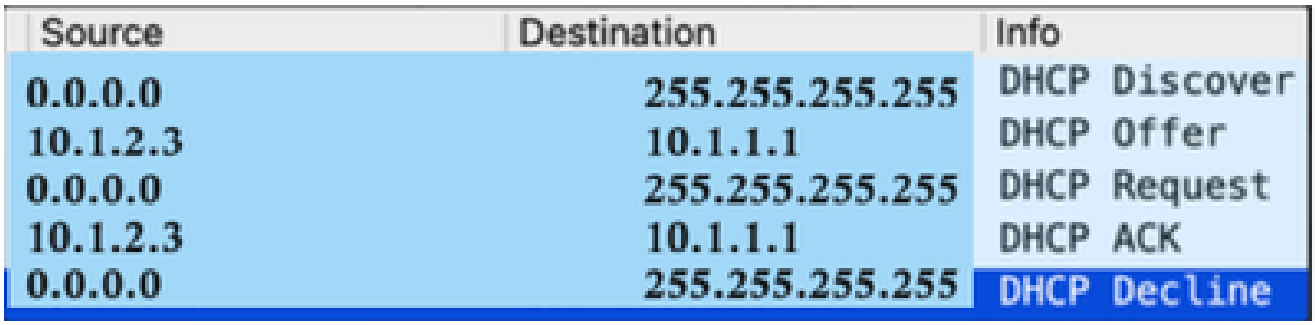
Solução de problemas realizada

- Recusa de DHCP enviada aos usuários finais e foi configurada com o endereço APIPA

Isolamento

- O servidor DHCP atribui um endereço IP do escopo A e o mesmo endereço IP sendo

atribuído a outro Laptop porque o escopo B tem o mesmo intervalo. Isso causa a recusa de DHCP:

- 

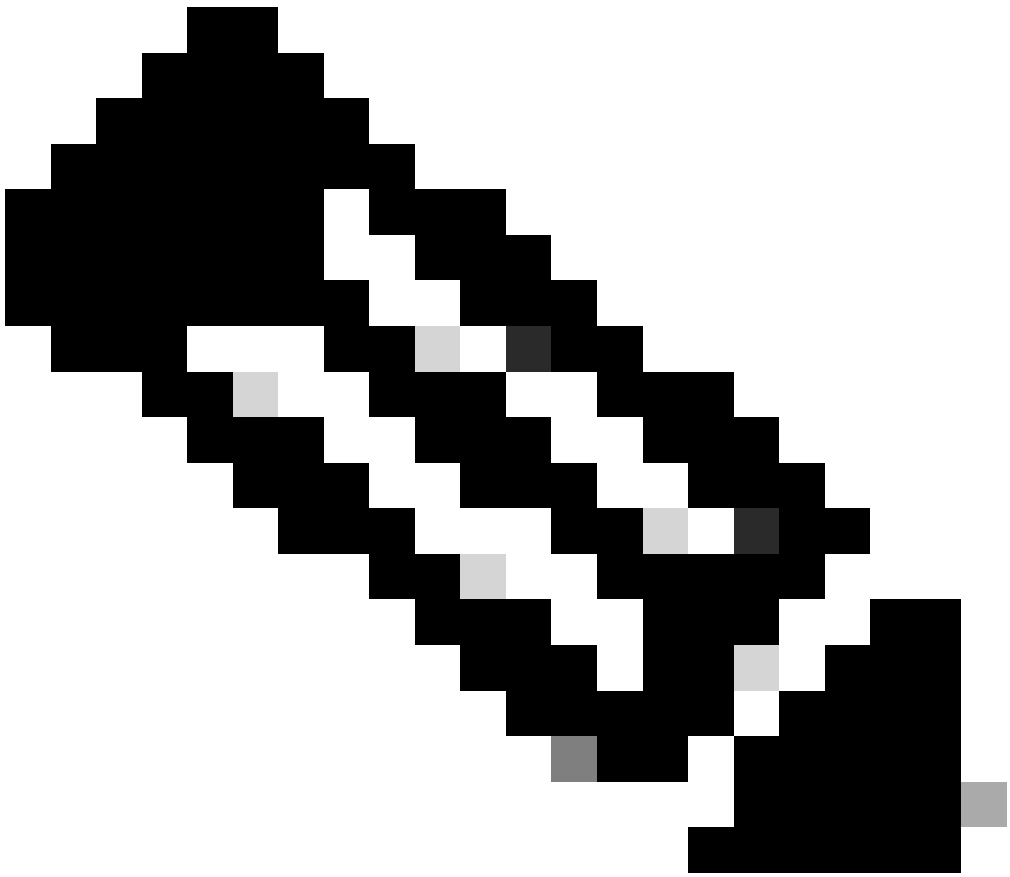
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

Plano de ação

- Atribuir intervalo de escopo de DHCP exclusivo

Resolução/Verificação

- Os dispositivos finais recebem o endereço IP após a alteração do escopo.

- 

Observação: verifique se o servidor DHCP não tem escopos duplicados configurados.

Cenário 3 - Configuração do SDA C9300

Cat9300 in SDA

Descrição do problema:

- As máquinas do usuário recebem o endereço IP APIPA e a conectividade do usuário afetada.

Sintomas do usuário

1. Alguns usuários em uma VLAN específica não podem obter endereços DHCP através do AP sem fio.
2. O firewall tinha várias entradas arp para um único endereço mac de usuário 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
```

Solução de problemas realizada

- A oferta DHCP foi descartada pelo switch
- O FTD preenche o ARP com base na OFERTA DHCP que volta do servidor DHCP.

<#root>

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

Isolamento

- Se a VLAN somente L2 estiver configurada para a configuração sem fio do SDA, o pacote de oferta com flag de broadcast não alcançará o AP. Como o túnel de acesso não permite pacotes de broadcast por padrão.

Plano de ação

- Permitir "capacidade de inundação" dentro do ambiente LISP.

<#root>

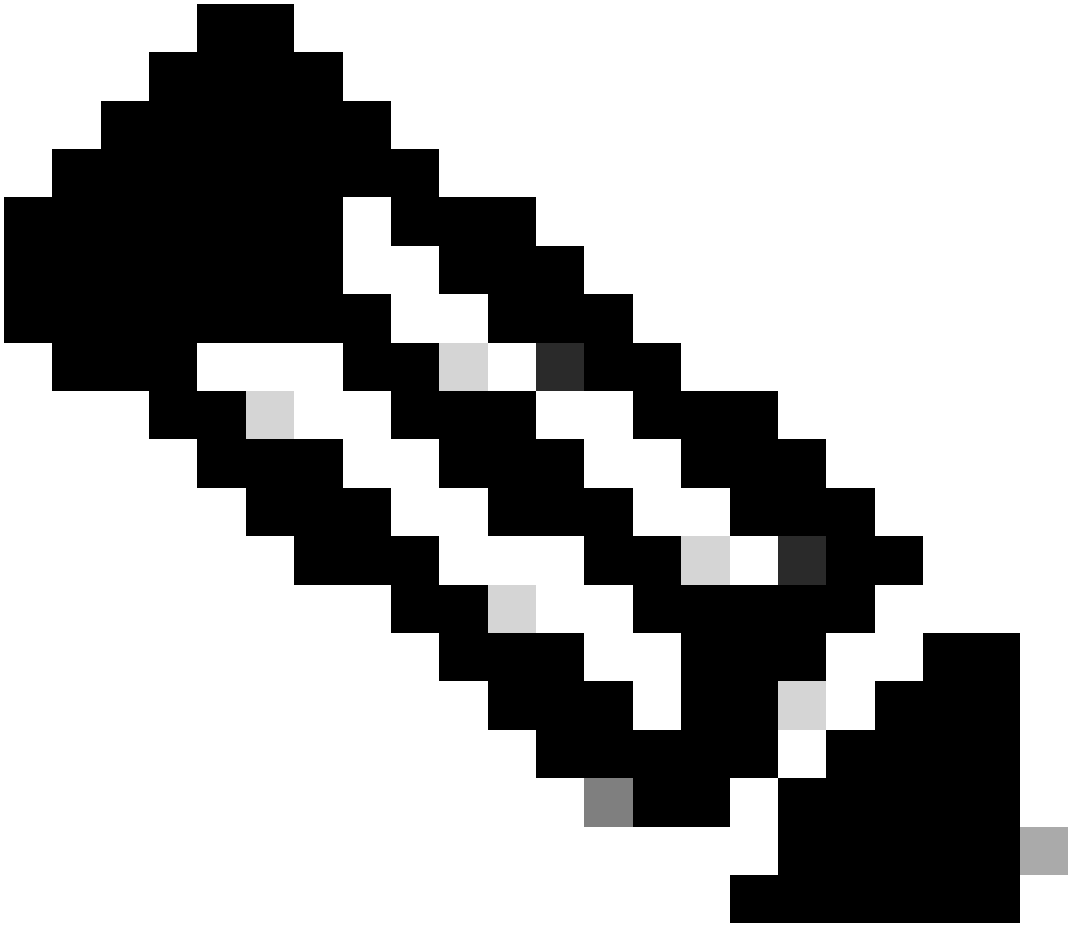
```
router lisp


instance-id 8456


flood access-tunnel
```

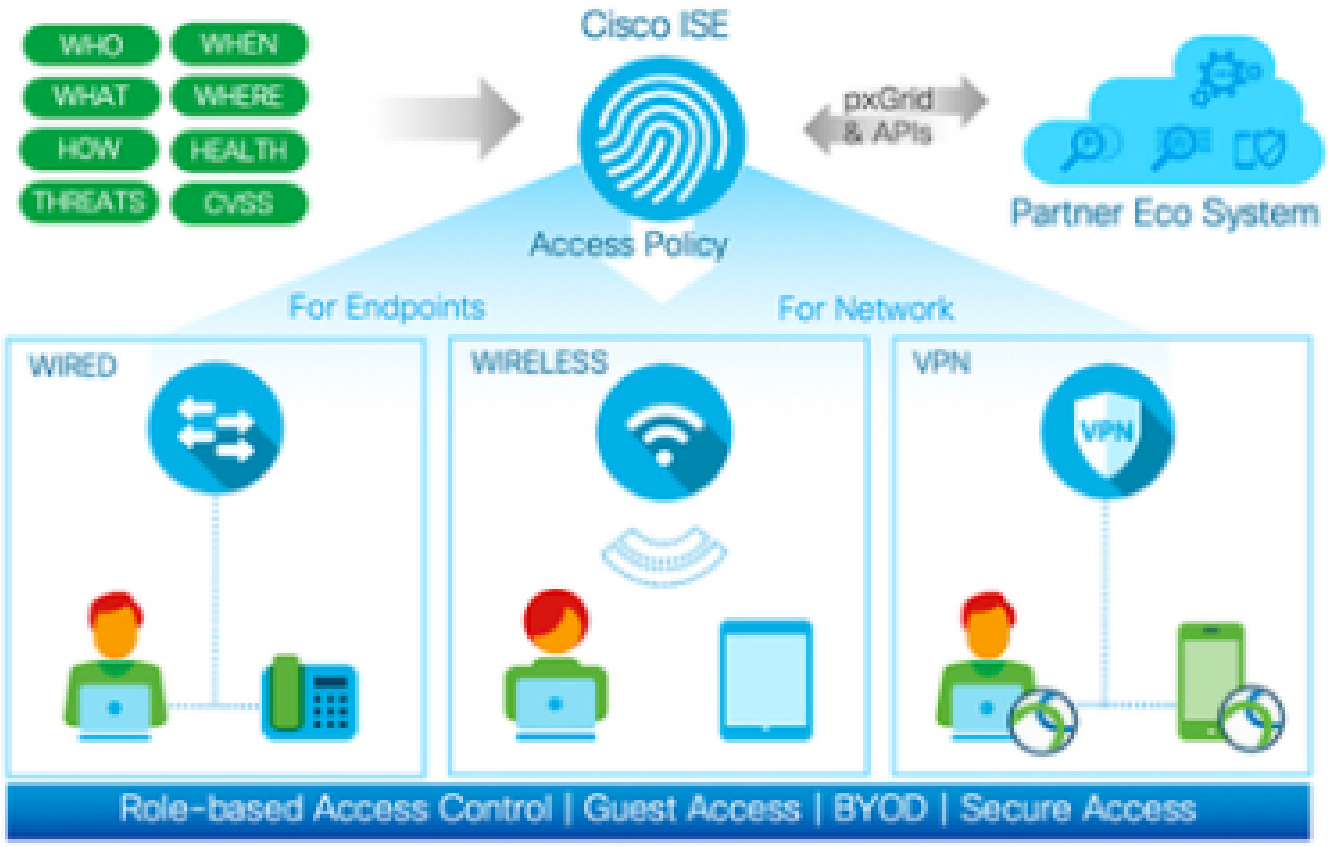
Resolução/Verificação

- Após configurar o "flood access-tunnel" no C9300 conectado à interface interna, os clientes recebem endereços DHCP.



Observação: certifique-se de habilitar flood access-tunnel em lisp, se o dispositivo final estiver configurado para receber a oferta de broadcast.

Cenário 4 - Problema com o adaptador de LAN



cisco ISE

Descrição do problema:

- As máquinas do usuário recebem o endereço IP APIPA e a conectividade do usuário afetada.

Sintomas

1. A tabela de endereços MAC mostra as entradas com "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. A sessão Mostrar Autenticação mostra muitas entradas, possivelmente excedendo 2000 ou mesmo 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
```

Passos de Troubleshooting

- A captura de pacotes mostra muitos pacotes de entrada do dispositivo final com endereços MAC de origem diferentes.
- O limite da sessão de autenticação é 2000 e, quando o limite for ultrapassado, problemas inesperados surgirão na rede
- 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

Isolamento

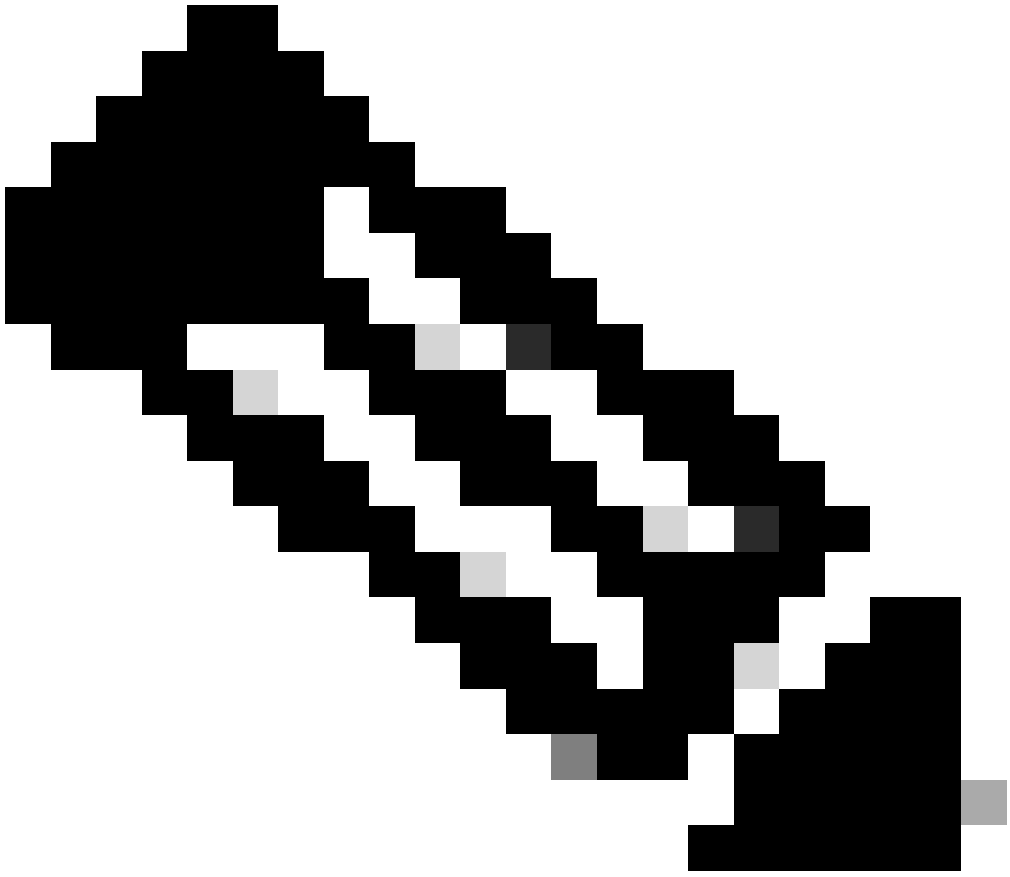
- Essa é uma indicação do problema do Adaptador do usuário final.Isso envia pacotes malformados que o switch entende como endereços MAC de origem aleatória.

Plano de ação

- Configure "authentication host-mode multi-domain", que permite apenas 2 endereços mac.
- Identifique e isole o dispositivo culpado.

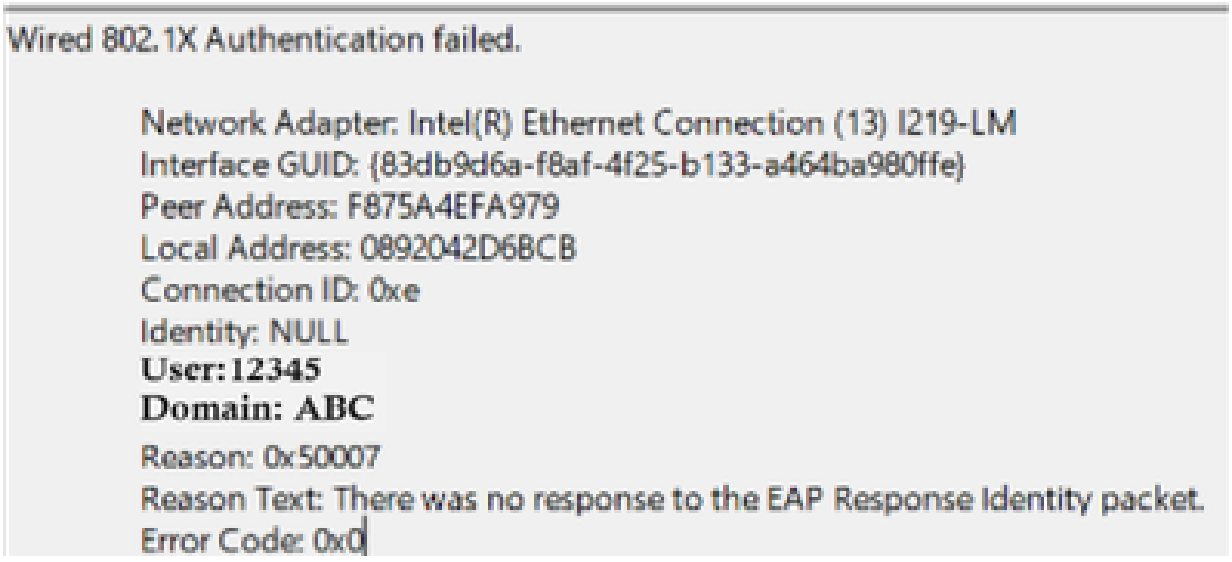
Resolução/Verificação

- Depois de configurar essa solução, nenhum problema será observado.



- Observação: certifique-se de habilitar a segurança de porta ou a sessão de autenticação Dot1x no modo host multidomínio.

Cenário 5 - Incompatibilidade de MTU



O ISE representa esse erro no servidor.

Descrição do problema:

- As máquinas do usuário recebem o endereço IP APIPA e a conectividade do usuário afetada.

Sintomas do usuário

1. O cliente final envia a resposta EAP com um comprimento de pacote maior que (Exemplo: 3736) o comprimento de pacote real esperado 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
```

Solução de problemas realizada

- MTU definido para um tamanho menor no switch como uma entrada do sistema. (Exemplo:1998bytes)
- Interface de saída configurada com tamanho maior. (Exemplo: 9198 bytes)

Isolamento

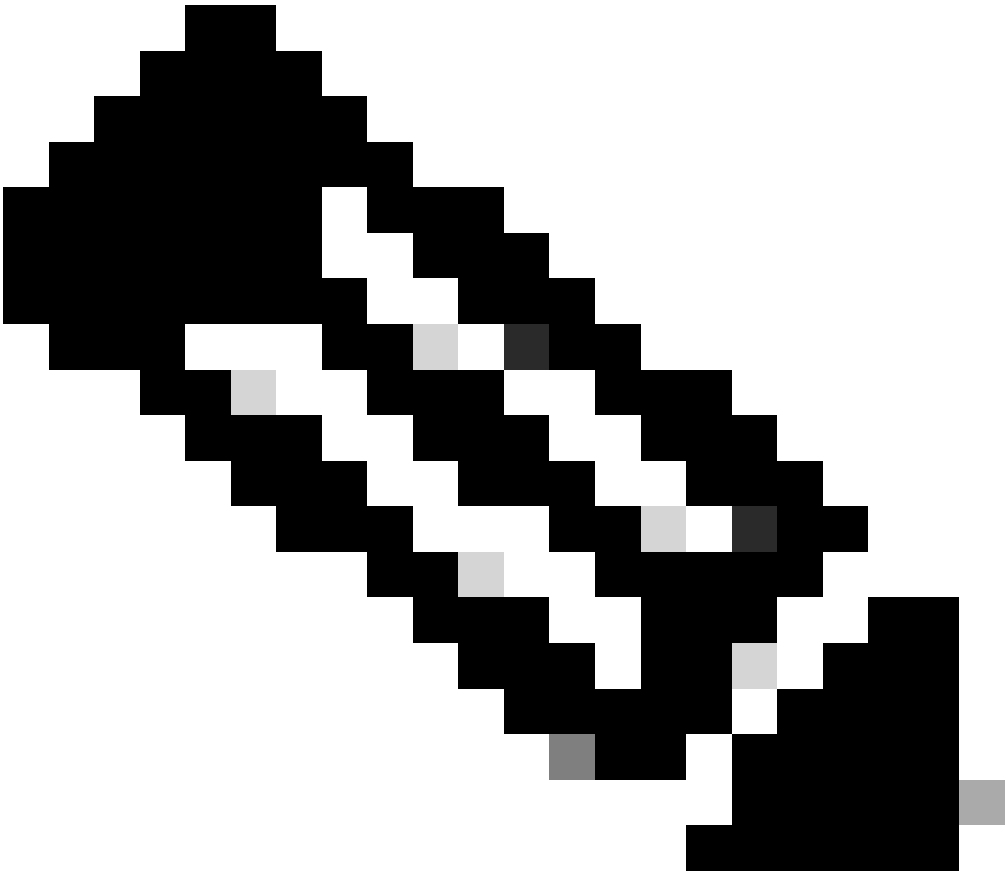
- A incompatibilidade na MTU em todo o caminho causa o problema.

Plano de ação

- Altere a MTU do sistema para 1500 e recarregue o switch

Resolução/Verificação

- Depois de definir essas configurações, a autenticação será bem-sucedida.



- Observação: certifique-se de ativar o mesmo MTU em todo o caminho do fluxo de pacotes.

Cenário 6 - Protetor de IPDT

Descrição do problema:

- As máquinas do usuário recebem o endereço IP APIPA e a conectividade do usuário afetada.

Sintomas do usuário

- Ao ter VMs em HA, se você tiver essa política aplicada na interface:

device-tracking policy IPDT_POLICY

no protocol udp

tracking enable

- Após um failover, a resposta ARP é descartada pelo switch de acesso.

Solução de problemas realizada

1. As respostas ARP aos testadores seriam descartadas pelo switch.
2. O switch está configurado com IPDT Guard.
3. IPDT - Protege a queda da sonda ARP e o dispositivo final obtém APIPA.

Isolamento

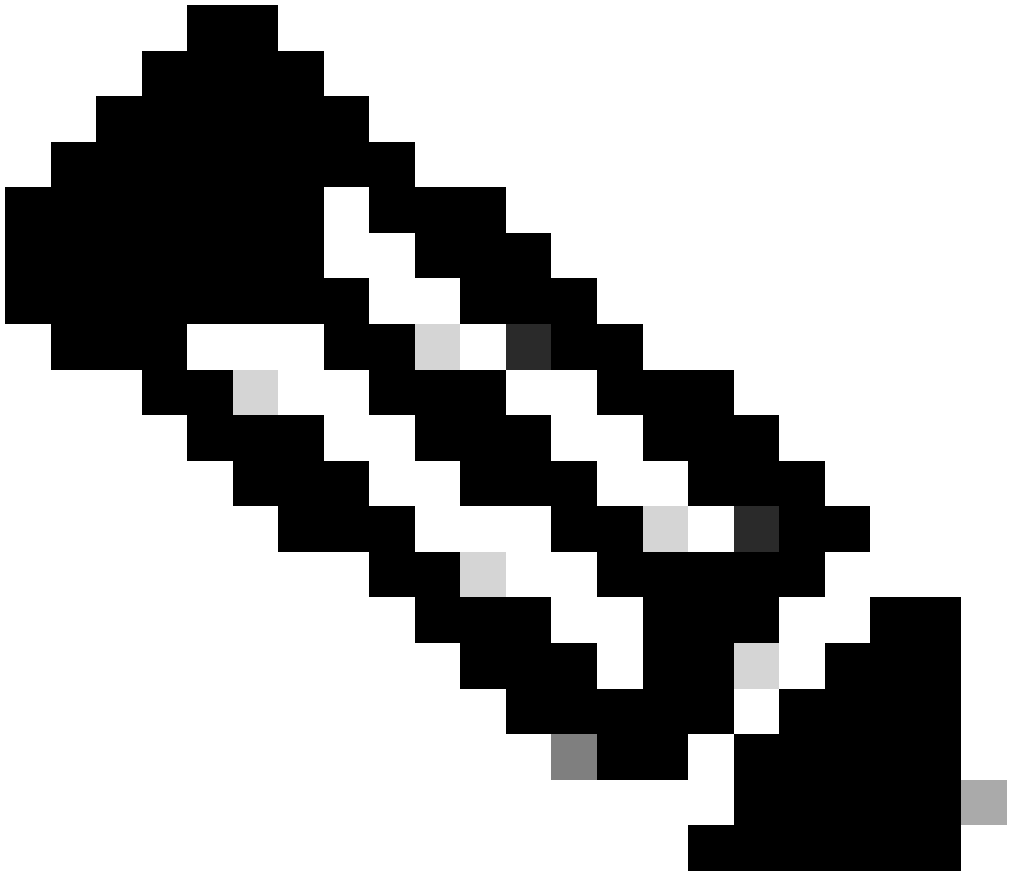
- Pacotes de prova ARP atingindo o IPDT e são descartados devido ao recurso Guard.
- A política IPDT configurada com a configuração 'security-level guard' descarta pacotes ARP, fazendo com que alguns ou todos os dispositivos finais fiquem inacessíveis

Plano de ação

- Altere a configuração de Guarda para Limpar.
  Configure 'security-level glean' na política IPDT

Resolução/Verificação

- Depois de definir as configurações de limpeza, os testes ARP são processados pelo processo ARP e o problema é resolvido.



- Observação: este é um defeito bem conhecido e seria corrigido na versão 17.15.1 e posterior.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.