排除网络中的APIPA地址故障

目录

简介

本文档介绍与APIPA地址相关的问题，并提供解决这些问题的方法。

使用的组件

- Catalyst 9000 交换机.
- 类似5516的ASA防火墙
- 任何类型的DHCP服务器
- SDA设置中的Catalyst 9300
- 软件：N/A

原因

在这些情况下，最终用户分配APIPA，

- DHCP服务器不可用。
- DHCP提供在跳之前或当前跳被丢弃。
- ARP探测功能会收到代表重复IP的响应。

场景和故障排除

方案1 -防火墙代理配置

ASA 5516

问题说明:

- 用户设备收到APIPA IP地址，并且用户连接受到影响。

问题症状

1. 特定VLAN上的用户会遇到间歇性问题，他们会收到APIPA IP地址并失去与网络的连接。
2. 防火墙具有单个最终用户MAC地址的多个ARP条目，如下所示：

<#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
```

故障排除步骤

1. 防火墙上的调试指向将响应发送到最终用户ARP探测的防火墙。

<#root>

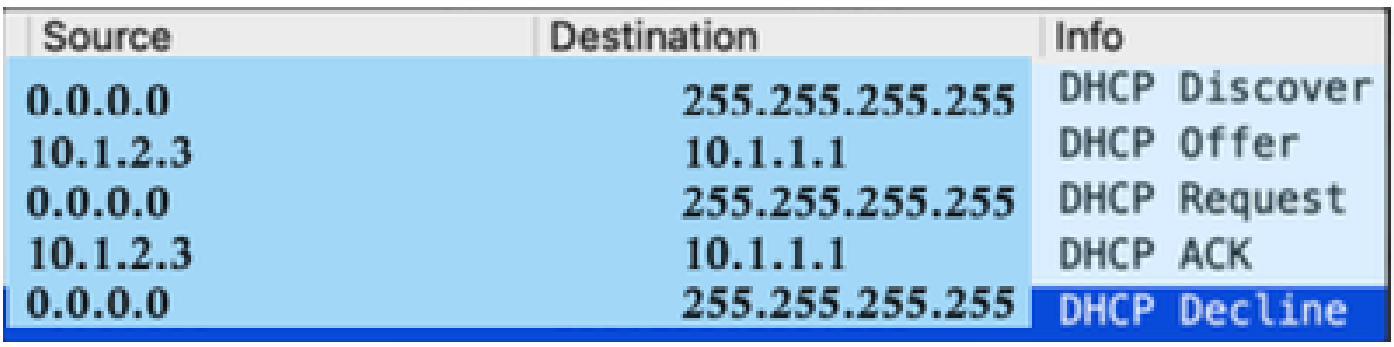
```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).


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

这使终端设备认为其地址重复。

2. 捕获终端设备或防火墙

在DORA过程完成之后，捕获show end device sending DHCP Decline packets。



隔离

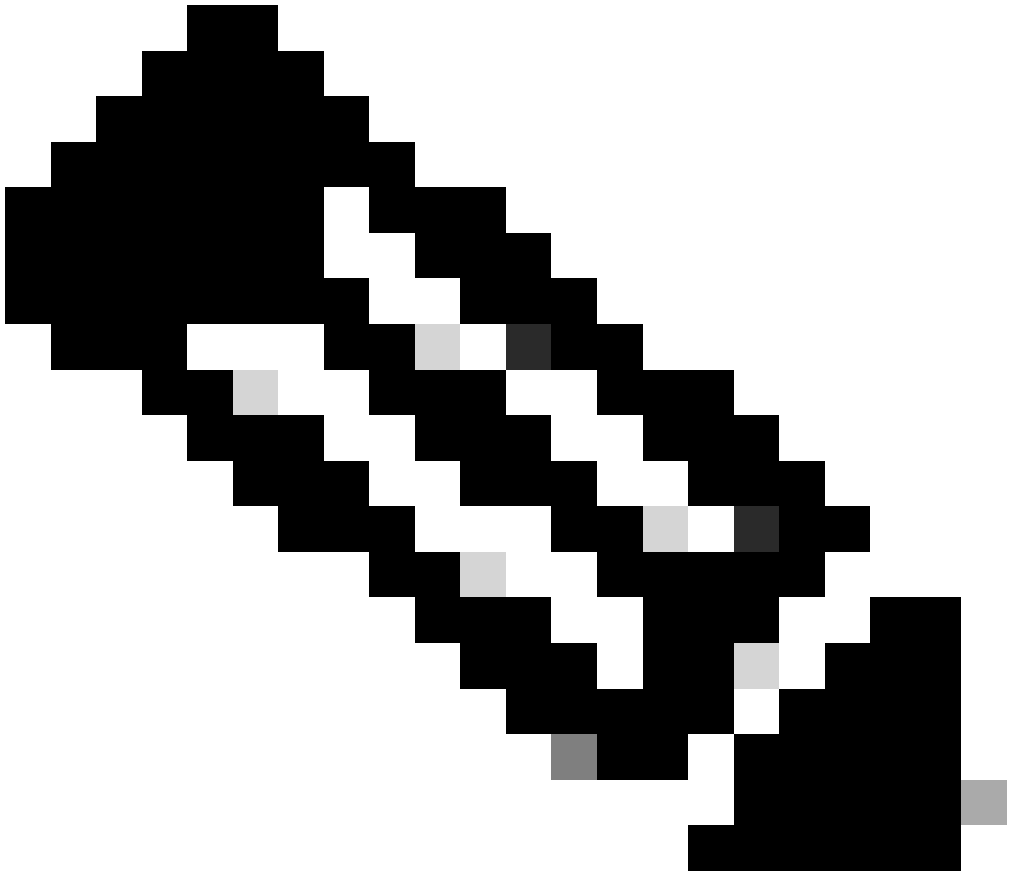
- 一旦DORA过程完成，防火墙内部接口通过代理响应ARP探测。这使PC发送DHCP失败。

行动计划

- 使用命令“sysopt noproxyarp inside”在防火墙内部接口上禁用代理arp

解决/验证

- 终端设备在禁用proxy-arp后接收IP地址。



- 注意：请确保没有任何设备充当最终用户ARP探测的代理或发送响应。

.

场景2 - DHCP服务器范围

问题说明:

- 用户设备收到APIPA IP地址，并且用户连接受到影响。

症状

1. 特定vlan上的用户仅获得APIPA IP地址并失去与网络的连接。

已执行故障排除

- DHCP拒绝发送给最终用户，并且已为其配置了APIPA地址

隔离

- DHCP服务器从作用域A分配一个IP地址，并将同一IP地址分配给另一台笔记本电脑，因为作用域B的范围相同。这会导致DHCP下降：

-

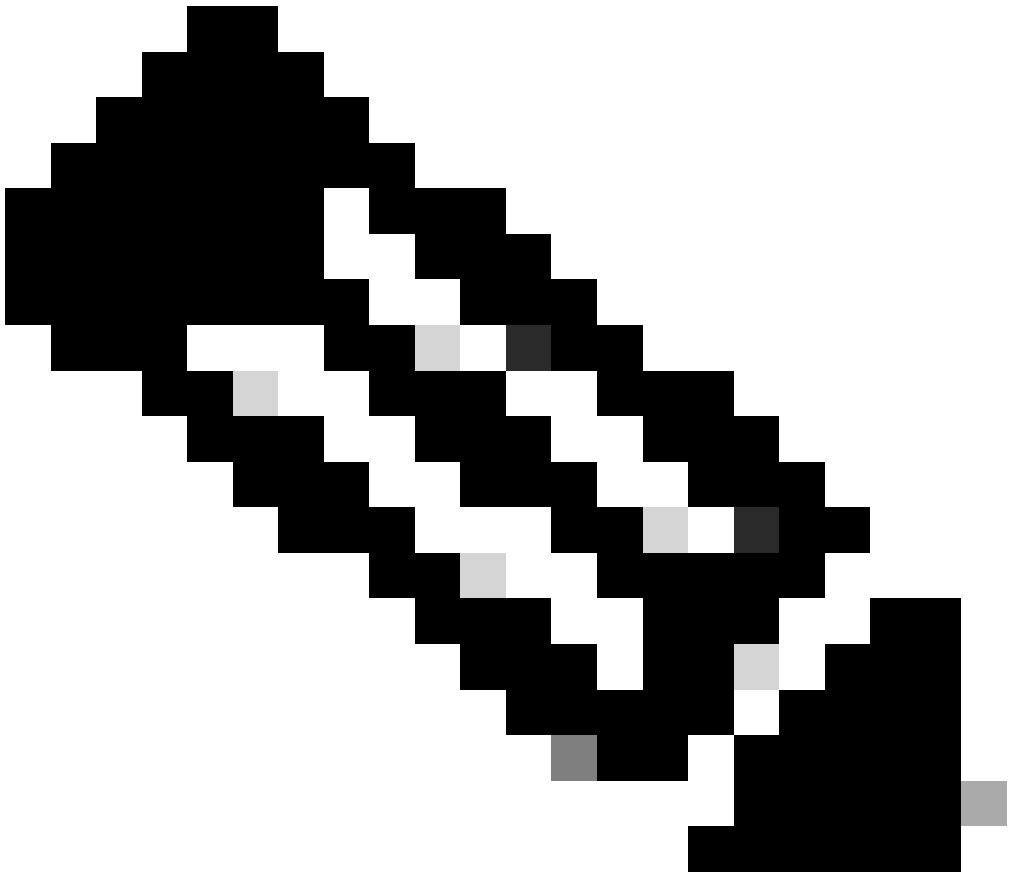
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

行动计划

- 分配唯一的DHCP作用域范围

解决/验证

- 范围更改后，终端设备会收到IP地址。



- 注意：请确保DHCP服务器未配置重复的作用域。

方案3 -C9300 SDA配置

Cat9300 in SDA

问题说明:

- 用户设备收到APIPA IP地址，并且用户连接受到影响。

用户症状

1. 特定VLAN中的某些用户无法通过无线AP获取DHCP地址。
2. 防火墙为单个最终用户MAC地址提供了多个ARP条目

<#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
```

已执行故障排除

- DHCP提供已被交换机丢弃
- FTD根据DHCP服务器返回的DHCP提供填充ARP。

<#root>

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

隔离

- 如果为SDA无线设置配置了仅L2 VLAN，则具有广播标记的数据包无法到达AP。因为默认情况下Access-tunnel不允许广播数据包。

行动计划

- 在LISP环境中允许“泛洪功能”。

<#root>

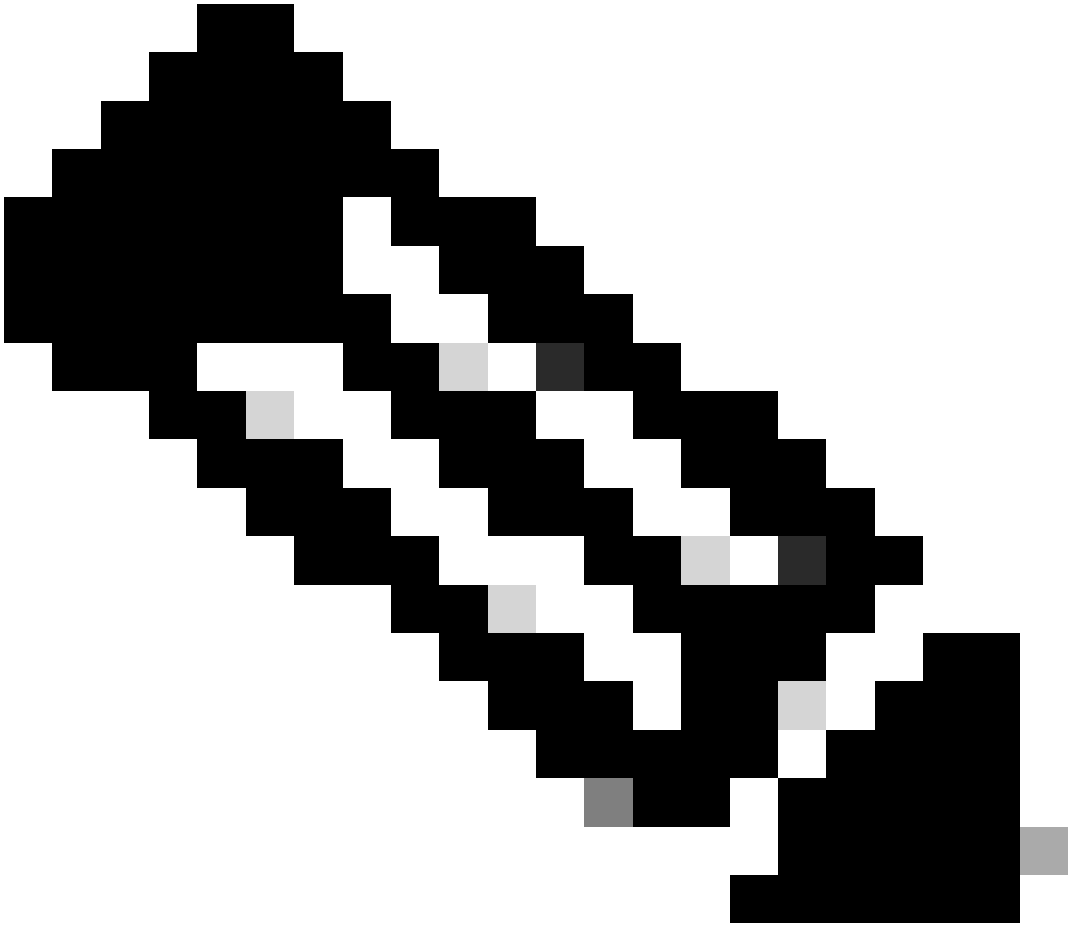
```
router lisp


instance-id 8456


flood access-tunnel
```

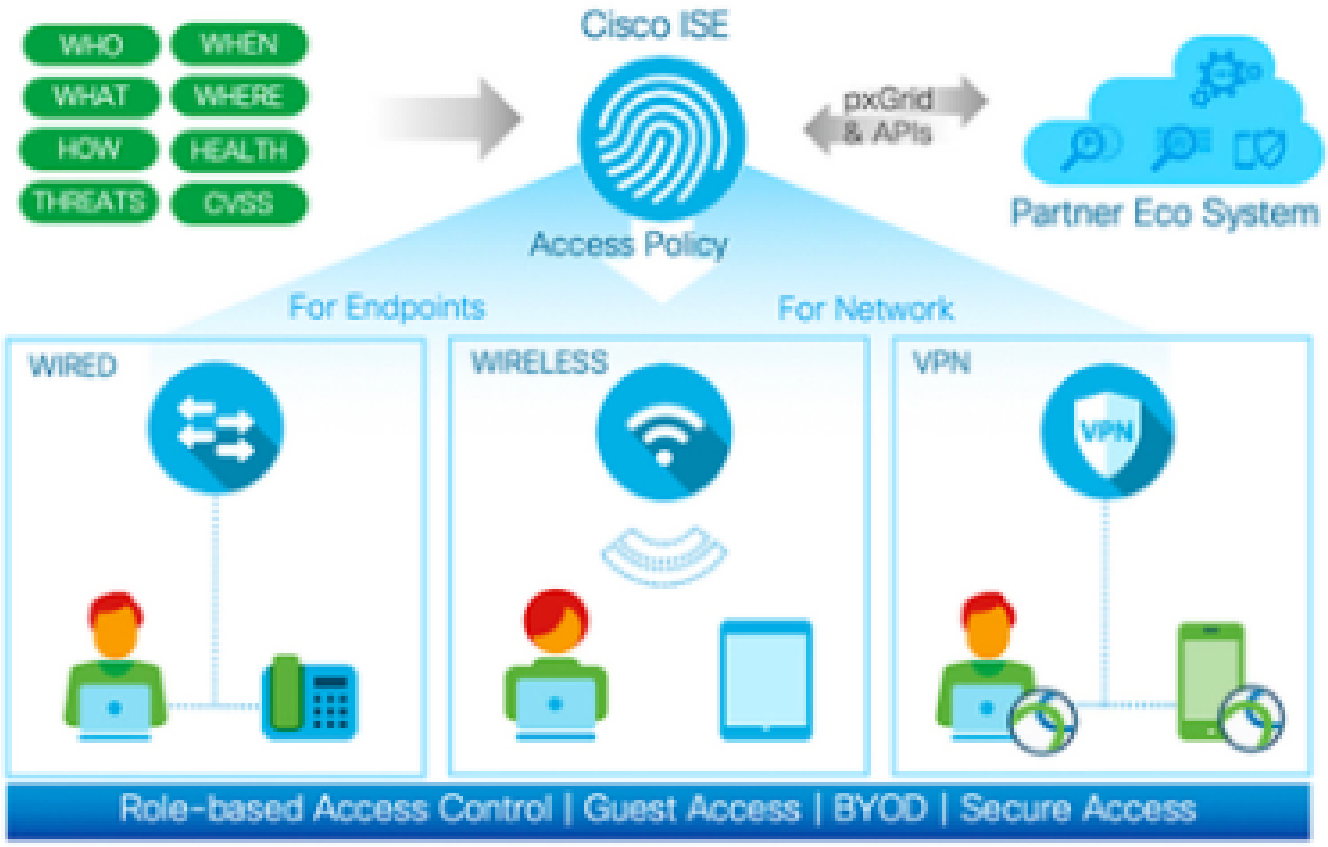
解决/验证

- 在内部接口上连接的C9300中配置“泛洪接入隧道”后，客户端接收DHCP地址。



注意：如果终端设备配置为接收广播提议，请确保在lisp下启用泛洪访问隧道。

场景4 - LAN适配器问题



cisco ISE

问题说明:

- 用户设备收到APIPA IP地址，并且用户连接受到影响。

症状

1. Mac address-table显示带有“drop”的条目。

<#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会话显示许多条目，可能超过2000甚至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
```

故障排除步骤

- 数据包捕获显示来自具有不同源MAC地址的终端设备的许多传入数据包。
- 身份验证会话限制为2000，一旦超过该限制，网络中就会出现意外问题
- 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

隔离

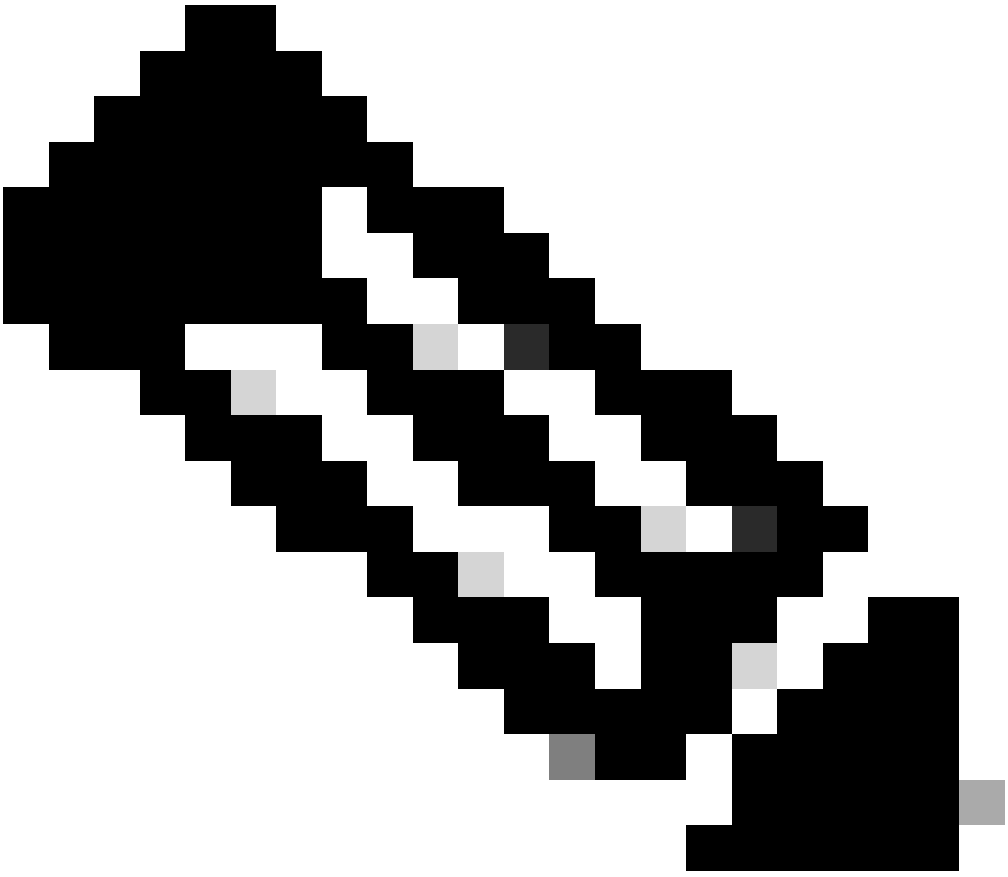
- 这表示存在最终用户适配器问题。这会发送交换机理解为随机源mac地址的格式错误的数据包。

行动计划

- 配置仅允许2个mac地址的“身份验证主机模式多域”。
- 识别并隔离故障设备。

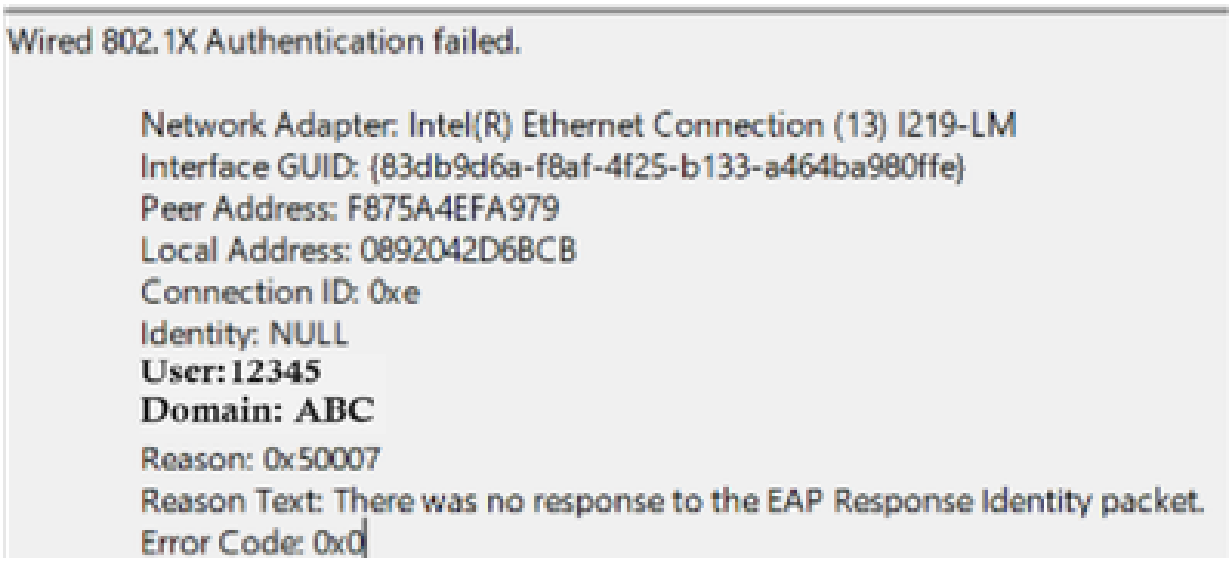
解决/验证

- 配置此解决方法后，未发现任何问题。



- 注意：请确保启用port-security或Dot1x auth session host-mode multi-domain。

方案5 - MTU不匹配



ISE在服务器上代表此错误。

问题说明:

- 用户设备收到APIPA IP地址，并且用户连接受到影响。

用户症状

1. 终端客户端发送的EAP响应的数据包长度大于（示例：3736）实际预期数据包长度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
```

已执行故障排除

- 作为系统范围条目，交换机上的MTU设置为更小的大小。（示例：1998字节）
- 出口接口配置了更大的大小。（示例：9198字节）

隔离

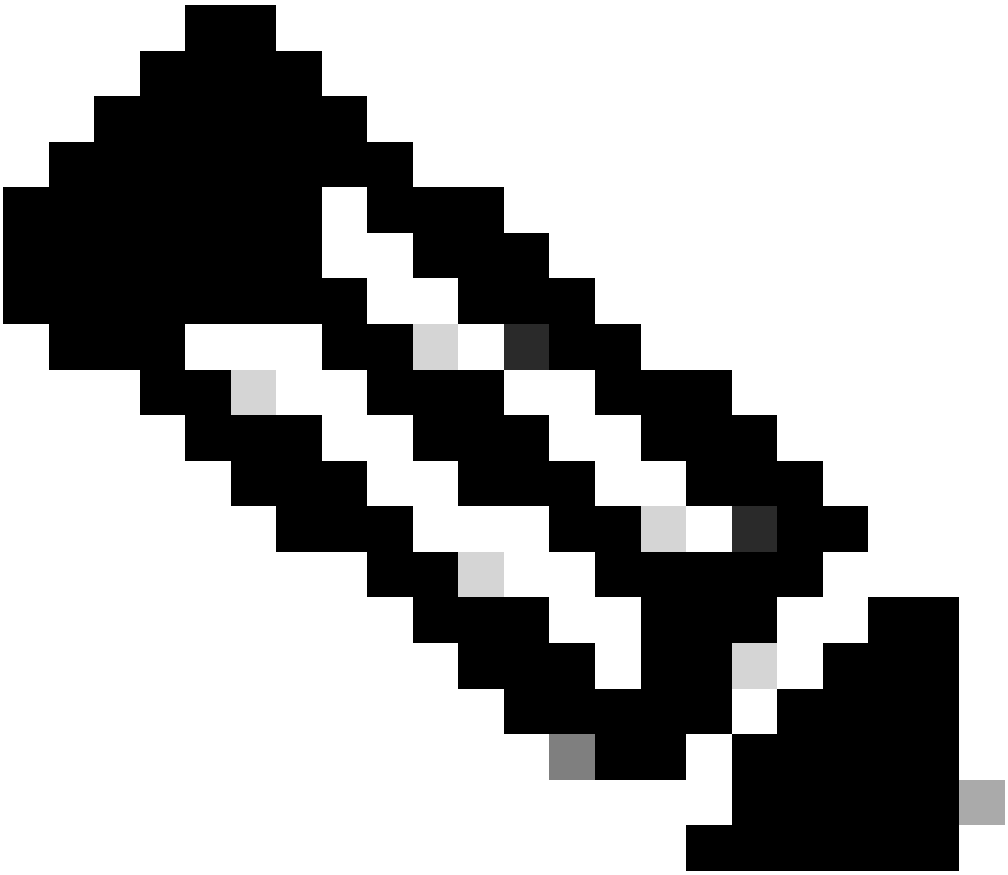
- 整个路径的MTU不匹配导致此问题。

行动计划

- 将系统MTU更改为1500并重新加载交换机

解决/验证

- 配置此设置后，身份验证成功。



- 注意：请确保在数据包流的整个路径中启用相同的MTU。

场景6 - IPDT防护

问题说明:

- 用户设备收到APIPA IP地址，并且用户连接受到影响。

用户症状

- 在HA中具有VM时，如果已在接口中应用此策略：

设备跟踪策略IPDT_POLICY

no protocol udp

tracking enable

- 故障转移后，接入交换机丢弃ARP应答。

已执行故障排除

1. 交换机将丢弃对探测功能的ARP响应。
2. 交换机配置了IPDT防护。
3. IPDT -保护丢弃ARP探测和终端设备获取APIPA。

隔离

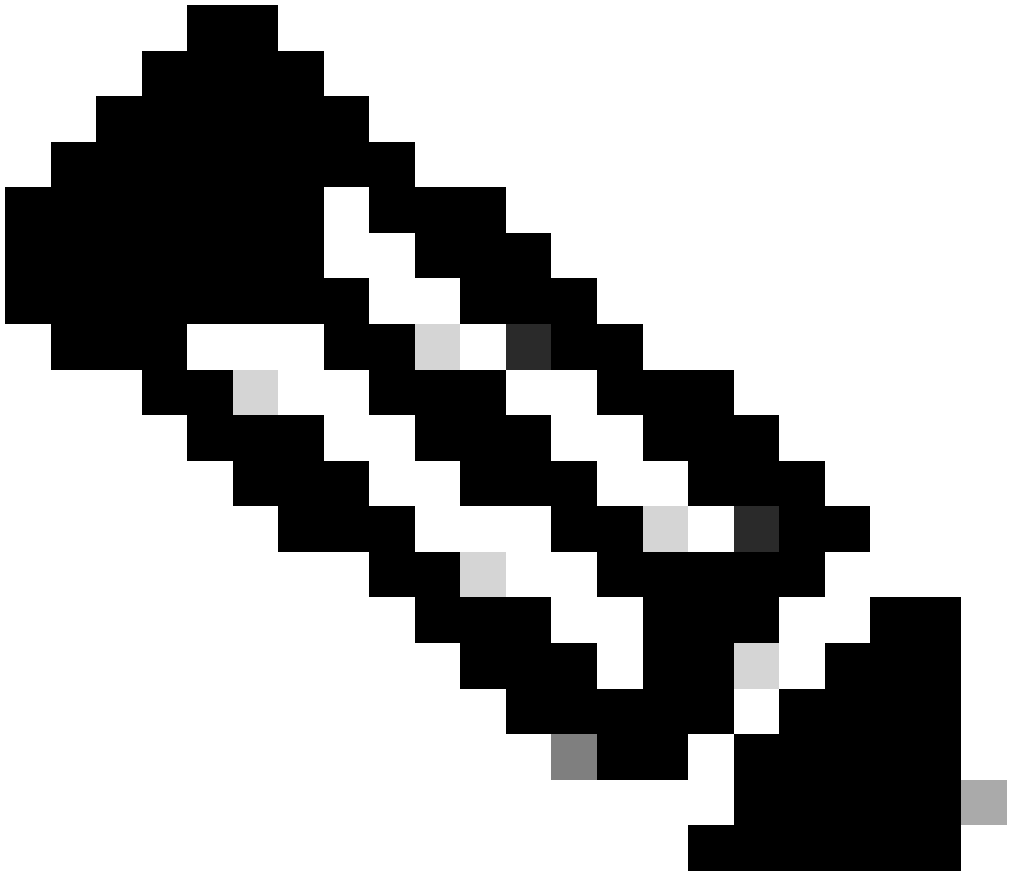
- ARP探测数据包到达IPDT并且由于防护功能而被丢弃。
- 配置了“安全级别防护”配置的IPDT策略丢弃ARP数据包，导致少量或所有终端设备无法访问

行动计划

- 将设置从“防护”更改为“收集”。
  在IPDT策略中配置“security-level glean”

解决/验证

- 配置收集设置后，ARP探测功能将由ARP进程进行处理，问题将得到解决。



- 注意：这是一个已知的缺陷，在17.15.1版本及更高版本中会修复。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。