排除網路中的APIPA地址故障

目錄

簡介

本文檔介紹了與APIPA地址相關的問題，並提供了相關解決方案。

採用元件

- Catalyst 9000交換機。
- ASA防火牆（如5516）
- 任何型別的DHCP伺服器
- SDA設定中的Catalyst 9300
- 軟體：N/A

原因

在這些情況下，終端使用者分配APIPA，

- DHCP伺服器不可用。
- DHCP Offer在跳之前或當前跳之前被丟棄。
- ARP探測功能會獲得代表重複IP的響應。

案例與疑難排解

方案1 -防火牆代理配置

ASA 5516

問題描述：

- 使用者電腦收到APIPA IP地址，並且使用者連線受到影響。

問題症狀

1. 特定VLAN上的使用者會間歇性地遇到問題，他們收到APIPA IP地址並失去與網路的連線。
2. 防火牆針對單一終端使用者MAC地址具有多個ARP條目，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
```

疑難排解步驟

1. 防火牆上的調試指向將響應傳送到終端使用者ARP探測的防火牆。

<#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
```

這使得終端裝置認為其地址重複。

2. 捕獲終端裝置或防火牆

在DORA進程完成後捕獲show end device sending DHCP Decline packets。

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

隔離

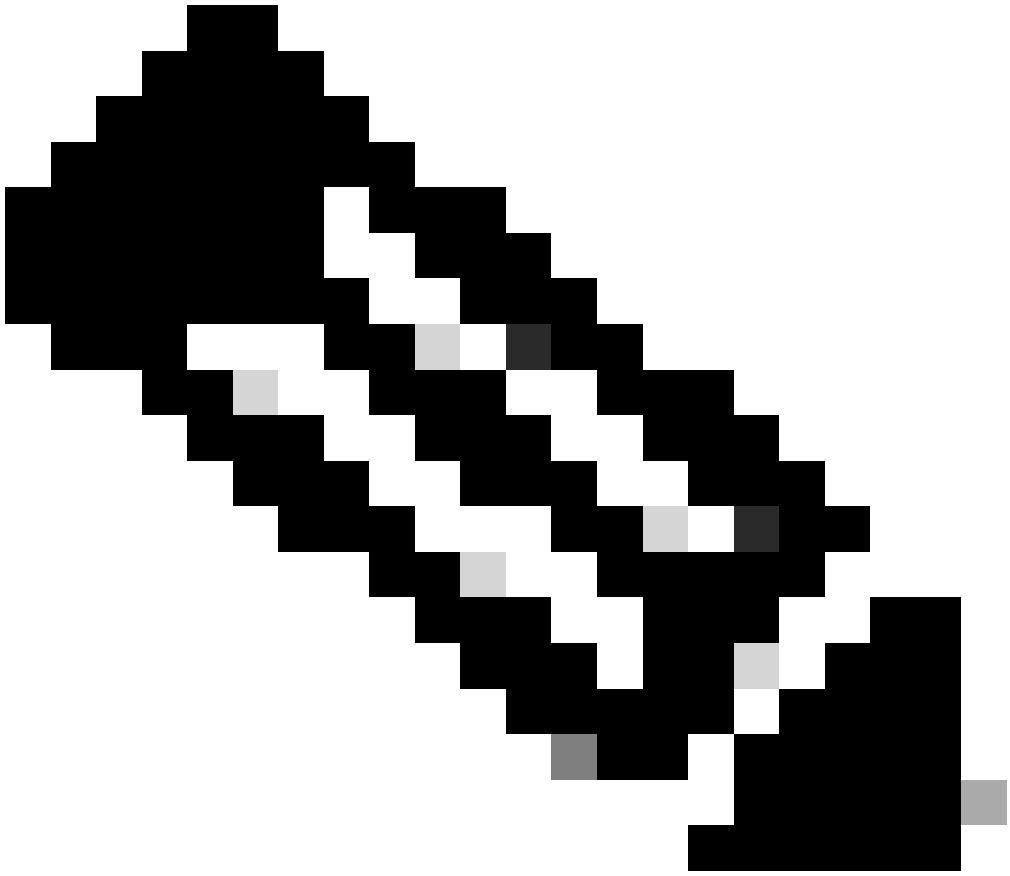
- 一旦DORA進程完成，防火牆內部介面透過充當代理來響應ARP探測。這使PC傳送DHCP拒絕。

行動計畫

- 使用命令「sysopt noproxyarp inside」在防火牆內部介面上停用代理arp

解決方案/驗證

- 終端裝置在停用proxy-arp後接收IP地址。



- 注意：請確保沒有任何裝置充當代理或傳送響應以響應終端使用者ARP探測。

.

方案2 - DHCP伺服器作用域

問題描述：

- 使用者電腦收到APIPA IP地址，並且使用者連線受到影響。

症狀

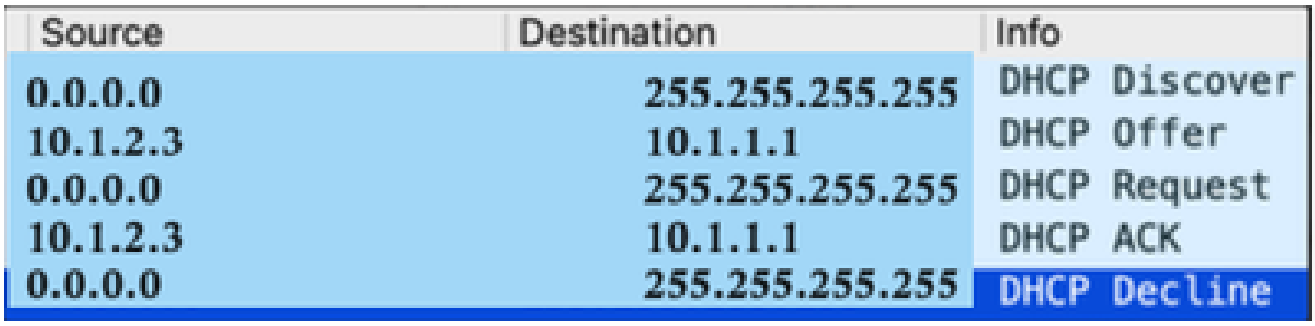
1. 特定vlan上的使用者僅獲得APIPA IP地址並失去與網路的連線。

已執行疑難排解

- DHCP拒絕傳送給終端使用者，並且已使用APIPA地址進行配置

隔離

- DHCP伺服器從作用域A分配一個IP地址，並將相同的IP地址分配給另一檯筆記型電腦，因為作用域B的範圍相同。這會導致DHCP拒絕：

- 

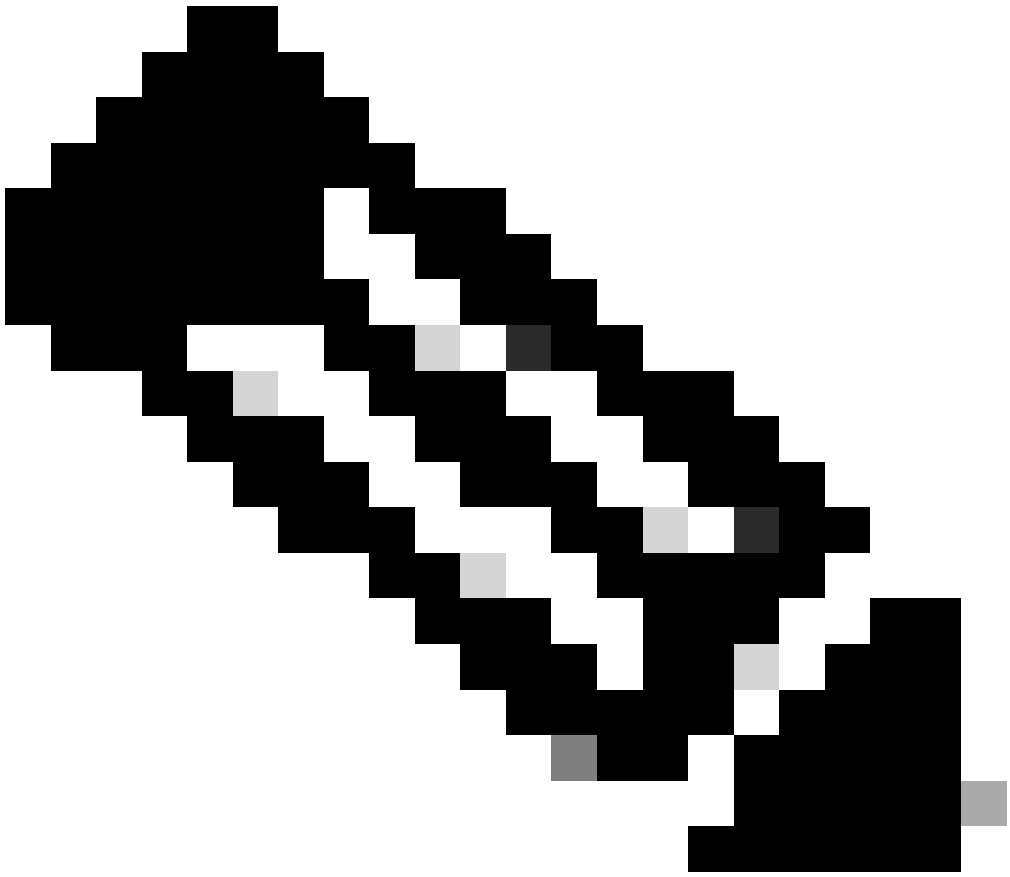
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

行動計畫

- 分配唯一的DHCP作用域範圍

解決方案/驗證

- 終端裝置在範圍更改後接收IP地址。



- 注意：請確保DHCP伺服器未配置重複的作用域。

方案3 -C9300 SDA配置

Cat9300 in SDA

問題描述：

- 使用者電腦收到APIPA IP地址，並且使用者連線受到影響。

使用者症狀

1. 特定VLAN中的某些使用者無法通過無線AP獲取DHCP地址。
2. 防火牆為單個終端使用者MAC地址提供了多個ARP條目

<#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
```

已執行疑難排解

- DHCP Offer被交換機丟棄
- FTD會根據DHCP伺服器傳回的DHCP OFFER植入ARP。

<#root>

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

隔離

- 如果為SDA無線設定配置僅L2的VLAN，則提供帶有廣播標籤的資料包不會到達AP。因為預設情況下Access-tunnel不允許廣播資料包。

行動計畫

- 在LISP環境中允許「泛洪功能」。

<#root>

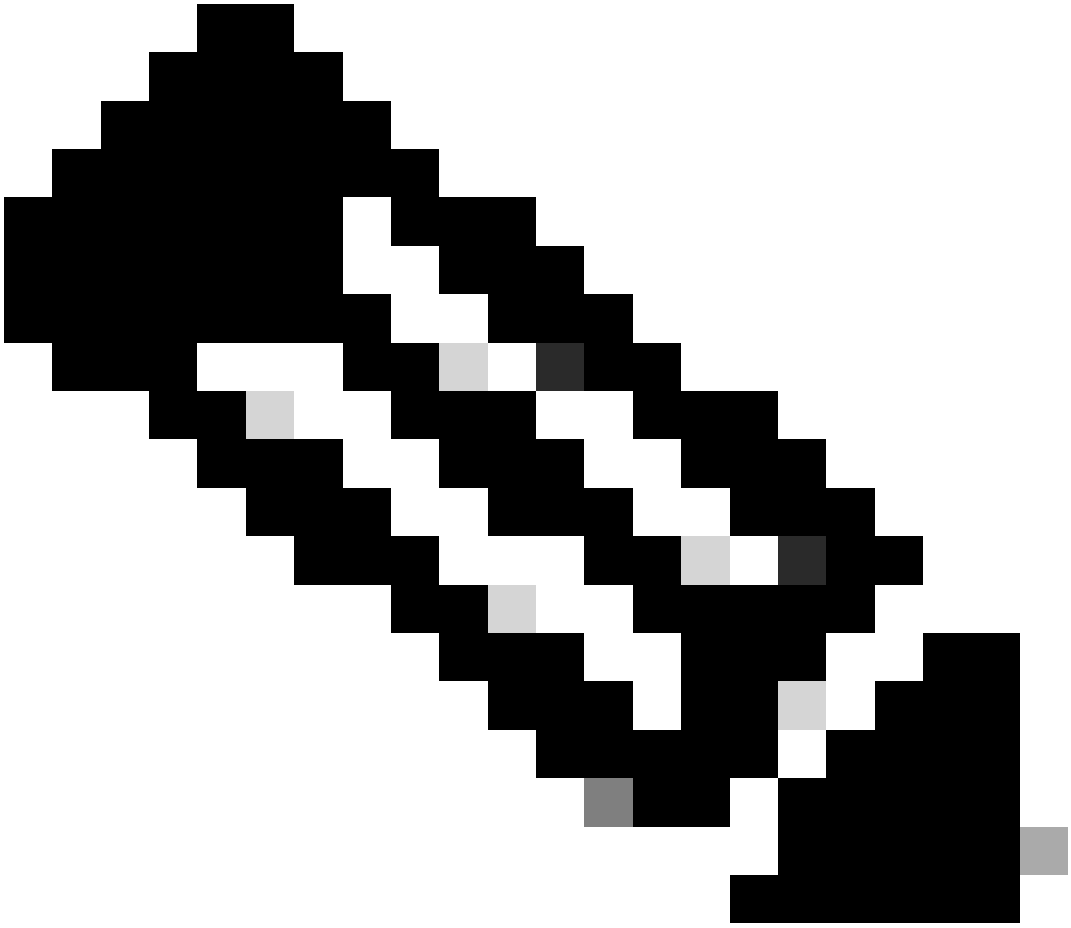
```
router lisp


instance-id 8456


flood access-tunnel
```

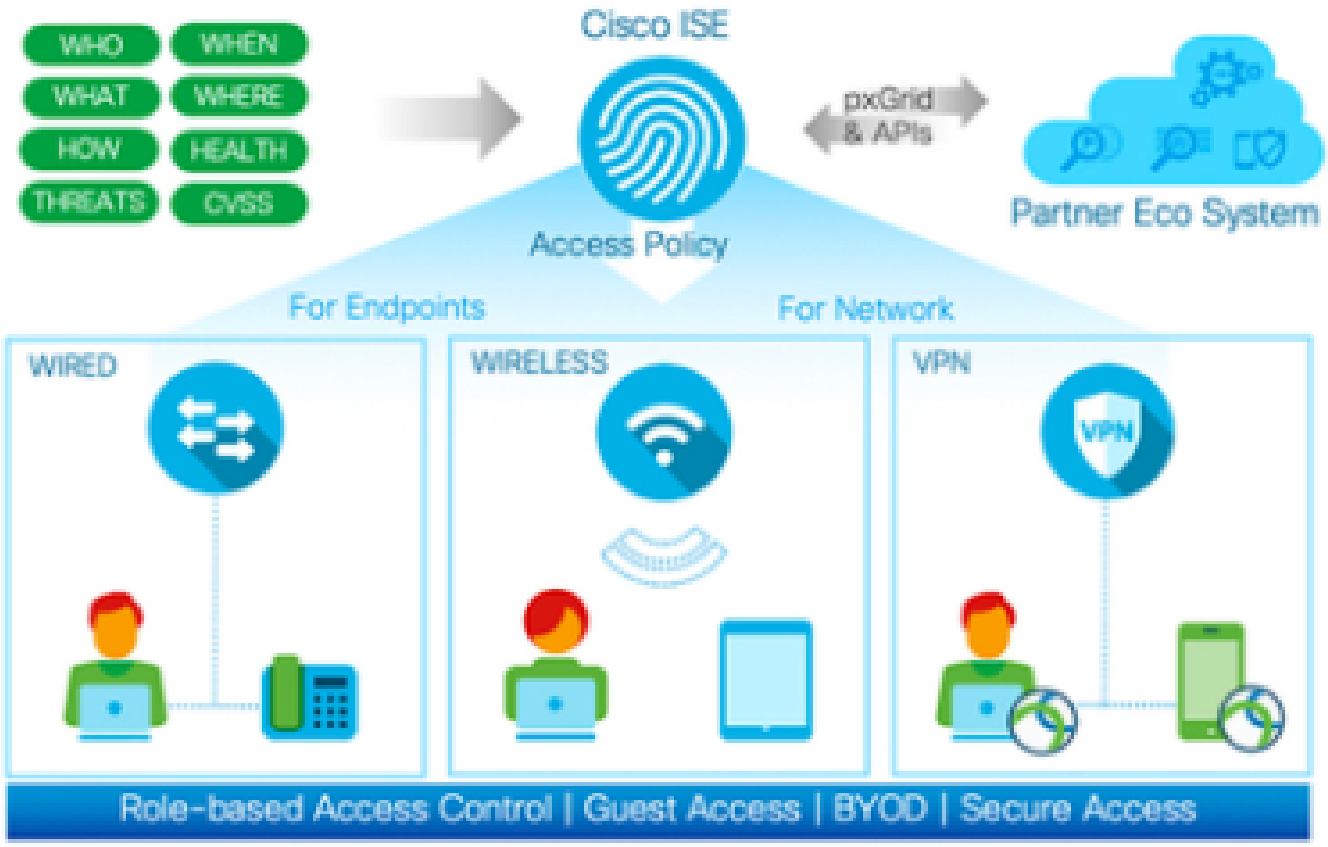
解決方案/驗證

- 在內部介面上連線的C9300中配置「泛洪接入隧道」後，客戶端接收DHCP地址。



注意：如果終端裝置配置為接收廣播提議，請確保在lisp下啟用泛洪接入隧道。

場景4 - LAN介面卡問題



cisco ISE

問題描述：

- 使用者電腦收到APIPA IP地址，並且使用者連線受到影響。

症狀

1. Mac address-table顯示帶有「drop」的條目。

<#root>

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


Mac Address Table


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


Vlan    Mac Address       Type        Ports


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

```
10    0000.0001.000a    DYNAMIC     Drop
```

2.「顯示認證」作業階段會顯示許多專案，可能會超過2000個甚至10000個。

<#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
```

疑難排解步驟

- 資料包捕獲顯示來自具有不同源MAC地址的終端裝置的許多傳入資料包。
- 身份驗證會話限制為2000，一旦超過此限制，網路中就會出現意外問題
- 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

隔離

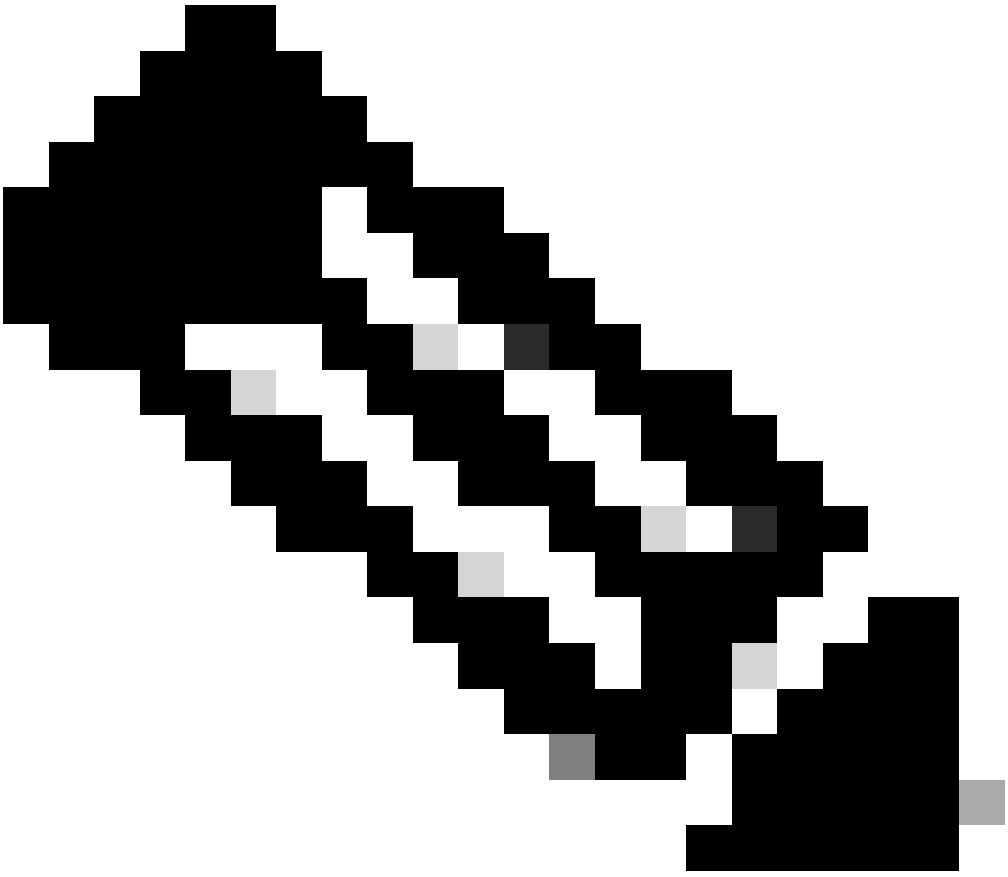
- 這表示終端使用者介面卡問題。這會傳送交換機理解為隨機源MAC地址的格式錯誤的資料包。

行動計畫

- 配置僅允許2個mac地址的「身份驗證主機模式多域」。
- 辨識並隔離肇事裝置。

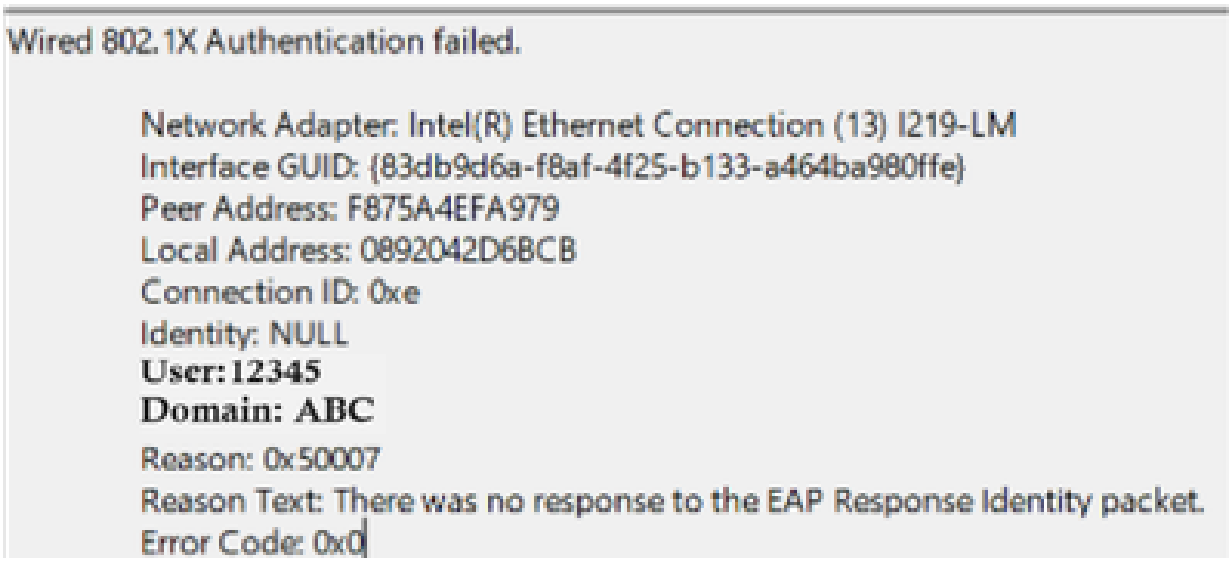
解決方案/驗證

- 配置此解決方法後，未發現任何問題。



- 注意：請確保啟用port-security或Dot1x auth session host-mode multi-domain。

方案5 - MTU不匹配



ISE在伺服器上表示此錯誤。

問題描述：

- 使用者電腦收到APIPA IP地址，並且使用者連線受到影響。

使用者症狀

1. 終端使用者端傳送的EAP回應封包長度大於（範例： 3736）實際預期封包長度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
```

已執行疑難排解

- 作為系統範圍條目，交換機上的MTU設定為較小的大小。（範例：1998位元組）
- 輸出介面配置了更大的大小。（範例： 9198位元組）

隔離

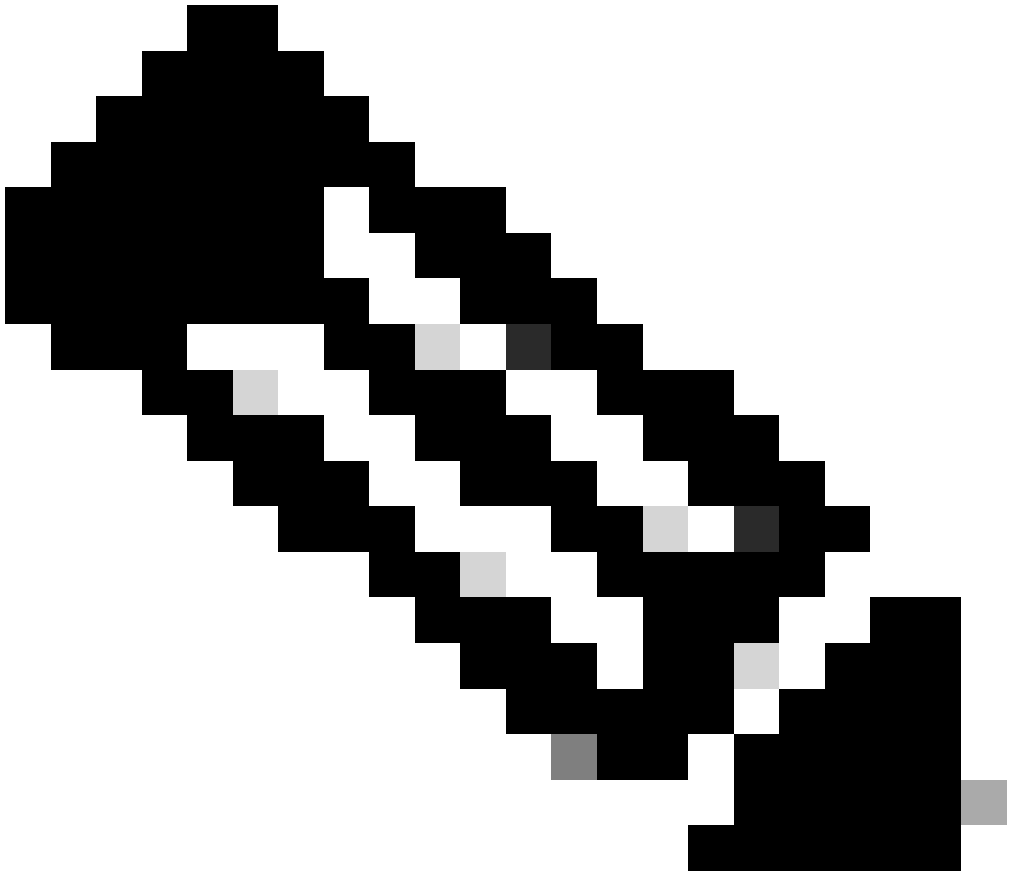
- 整個路徑的MTU不相符就會造成問題。

行動計畫

- 將系統MTU更改為1500並重新載入交換機

解決方案/驗證

- 配置此設定後，身份驗證將成功。



- 注意：請確保在資料包流的整個路徑中啟用相同的MTU。

案例6 - IPDT防護

問題描述：

- 使用者電腦收到APIPA IP地址，並且使用者連線受到影響。

使用者症狀

- 在HA中部署VM時，如果在介面中應用了以下策略：

裝置跟蹤策略IPDT_POLICY

無協定udp

追蹤啟用

- 故障切換後，接入交換機丟棄ARP應答。

已執行疑難排解

1. 交換機將丟棄對探查的ARP響應。
2. 交換機配置了IPDT防護。
3. IPDT -保護丟棄ARP探測器和終端裝置獲得APIPA。

隔離

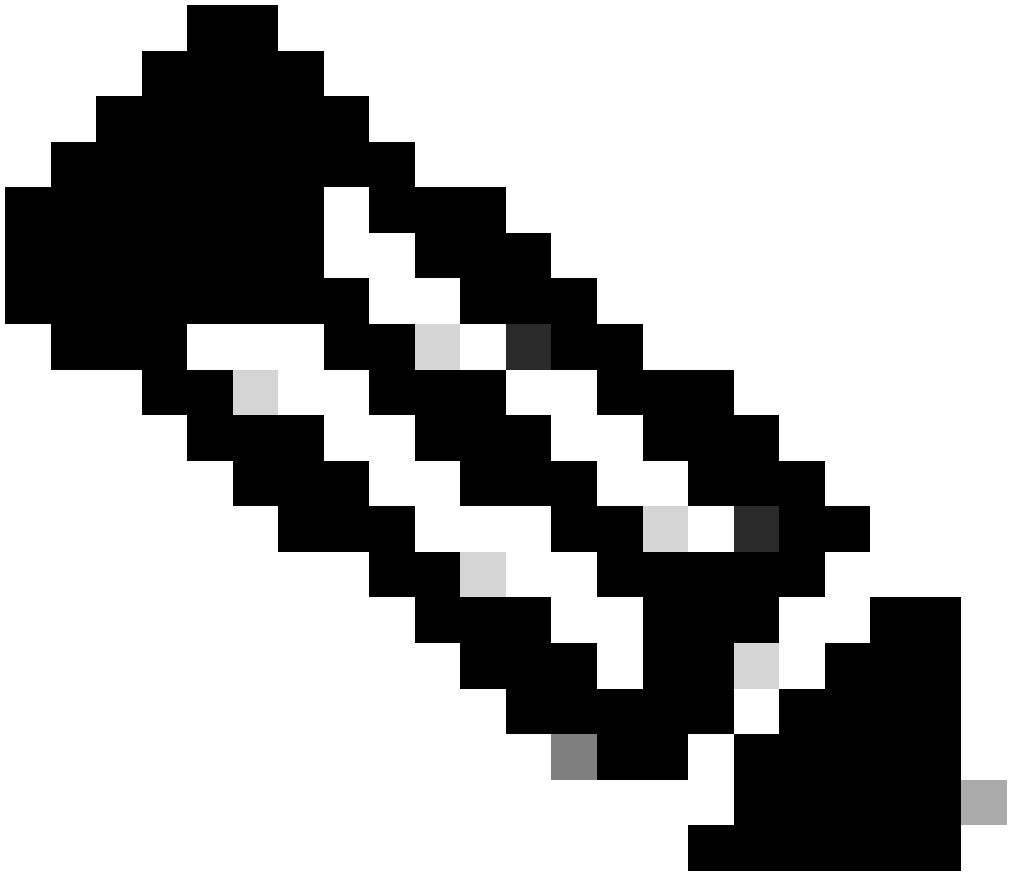
- ARP探測資料包到達IPDT並且由於防護功能而被丟棄。
- 配置了「安全級別防護」配置的IPDT策略丟棄ARP資料包，導致少數或所有終端裝置無法訪問

行動計畫

- 將設定從「防護」變更為「收集」。
  在IPDT策略中配置「security-level glean」

解決方案/驗證

- 配置收集設定後，ARP探測將由ARP進程進行處理，問題將得到解決。



- 注意：這是一個已知的缺陷，可以在17.15.1版及更高版本中修復。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。