ネットワークのAPIPAアドレス障害のトラブルシューティング

内容

はじめに

このドキュメントでは、APIPAアドレスに関連する問題について説明し、その解決策を示します。

使用するコンポーネント

- Catalyst 9000 スイッチ
- 5516などのASAファイアウォール
- あらゆる種類のDHCPサーバ
- SDA設定のCatalyst 9300
- ソフトウェア：該当なし

理由

エンドユーザがAPIPAを割り当てるのは、次のような場合です。

- DHCPサーバが使用できません。
- DHCPオファーは、現在のホップの前にドロップされます。
- ARPプローブは、重複IPを表す応答を取得します。

シナリオとトラブルシューティング

シナリオ1:ファイアウォールプロキシの設定

ASA 5516

事象の説明:

- ユーザマシンがAPIPA IPアドレスを受け取り、ユーザ接続に影響があります。

問題の症状

1. 特定のVLAN上のユーザで、APIPA IPアドレスを受信してネットワークへの接続が失われるといった、断続的な問題が発生します。
2. ファイアウォールには、次のような単一のエンドユーザMACアドレスに対する複数のARPエントリがあります。

<#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
```

トラブルシューティングの手順

1. ファイアウォールのデバッグは、エンドユーザのARPプローブに応答を送信するファイアウォールをポイントします。

<#root>

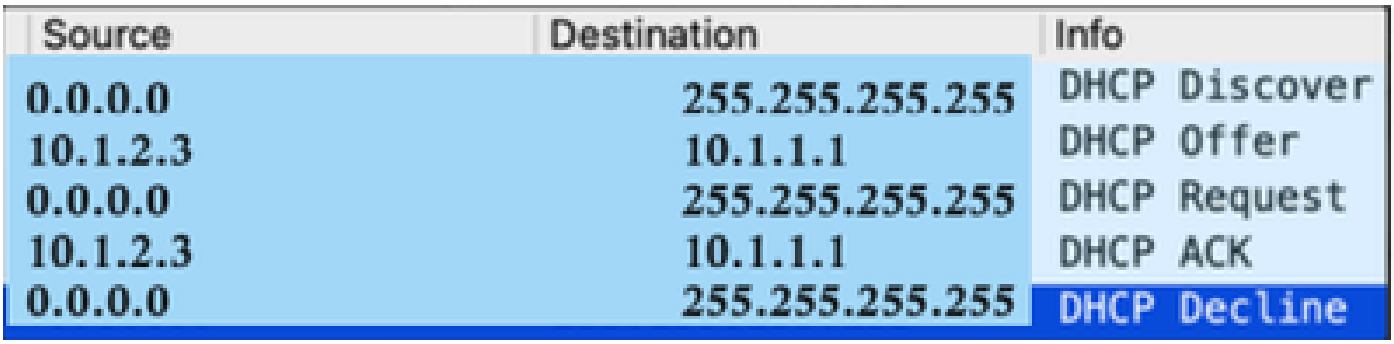
```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).


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

これにより、エンドデバイスは重複アドレスであると認識します。

2. エンドデバイスまたはファイアウォール上のキャプチャ

DORAプロセスが完了すると、キャプチャはDHCP拒否パケットを送信しているエンドデバイスを示します。



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

分離

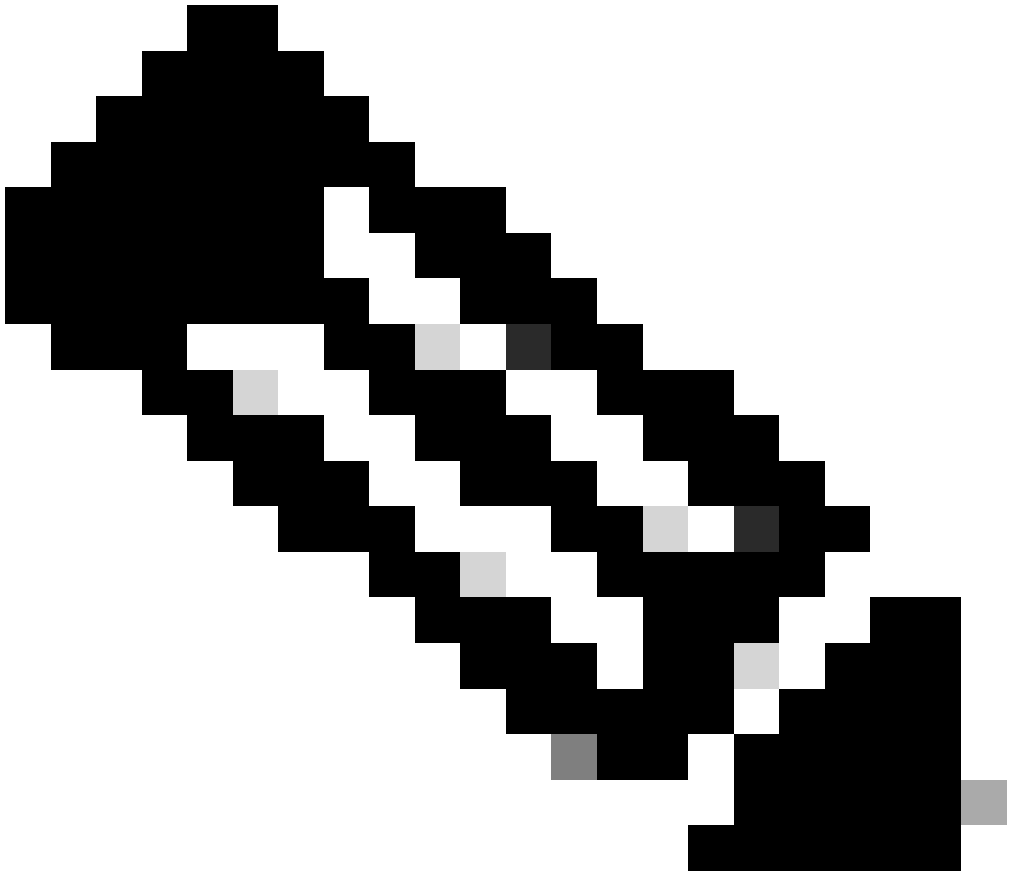
- DORAプロセスが完了すると、ファイアウォールの内部インターフェイスはプロキシとして動作してARPプローブに応答します。これにより、PCはDHCP拒否を送信するようになります。

アクションプラン

- コマンド「sysopt noproxyarp inside」を使用して、ファイアウォール内部インターフェイスのプロキシarpを無効にします。

解決/検証

- エンドデバイスは、proxy-arpを無効にした後でIPアドレスを受け取ります。



- 注：エンドユーザのARPプローブで、プロキシとして動作したり、応答を送信したりするデバイスがないことを確認してください。

.

シナリオ2:DHCPサーバスコープ

事象の説明:

- ユーザマシンがAPIPA IPアドレスを受け取り、ユーザ接続に影響があります。

症状

1. 特定のVLAN上のユーザが取得するのはAPIPA IPアドレスだけで、ネットワークへの接続は失われます。

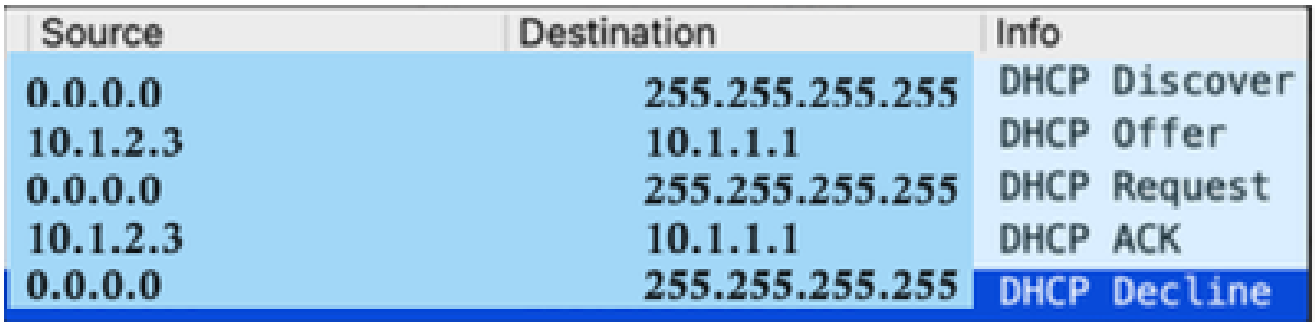
実施したトラブルシューティング

- DHCP拒否がエンドユーザに送信され、APIPAアドレスが設定されました

分離

- スコープBの範囲は同じであるため、DHCPサーバはスコープAから1つのipアドレスを割り当て、同じipアドレスを別のラップトップに割り当てます。これにより、DHCPの拒否が発

生します。

- 

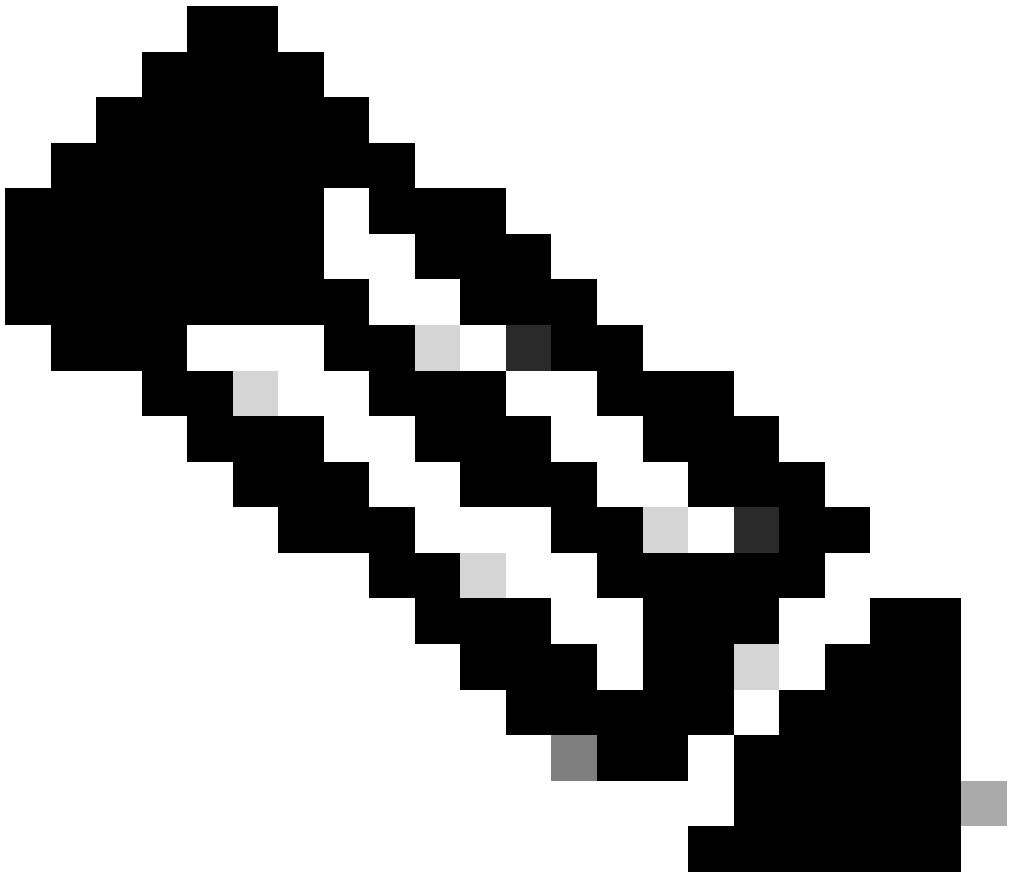
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

アクションプラン

- 固有のDHCPスコープ範囲の割り当て

解決/検証

- エンドデバイスは、スコープの変更後にIPアドレスを受け取ります。



- 注： DHCPサーバーに重複するスコープが構成されていないことを確認してくださ

い。

シナリオ3:C9300 SDAの設定

Cat9300 in SDA

事象の説明:

- ユーザマシンがAPIPA IPアドレスを受け取り、ユーザ接続に影響があります。

ユーザの症状

1. 特定のVLAN内の一部のユーザが、ワイヤレスAPを介してDHCPアドレスを取得できません。
2. ファイアウォールには、単一のエンドユーザMACアドレスに対する複数のARPエントリがある

<#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
```

実施したトラブルシューティング

- DHCPオファーがスイッチによってドロップされました
- FTDは、DHCPサーバから戻されるDHCP OFFERに基づいてARPを入力します。

<#root>

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

分離

- L2専用VLANがSDAワイヤレス設定用に設定されている場合、ブロードキャストフラグ付きのオファーパケットはAPに到達しません。デフォルトでは、Access-tunnelはブロードキャストパケットを許可しません。

アクションプラン

- LISP環境内で「フラッディング機能」を許可します。

<#root>

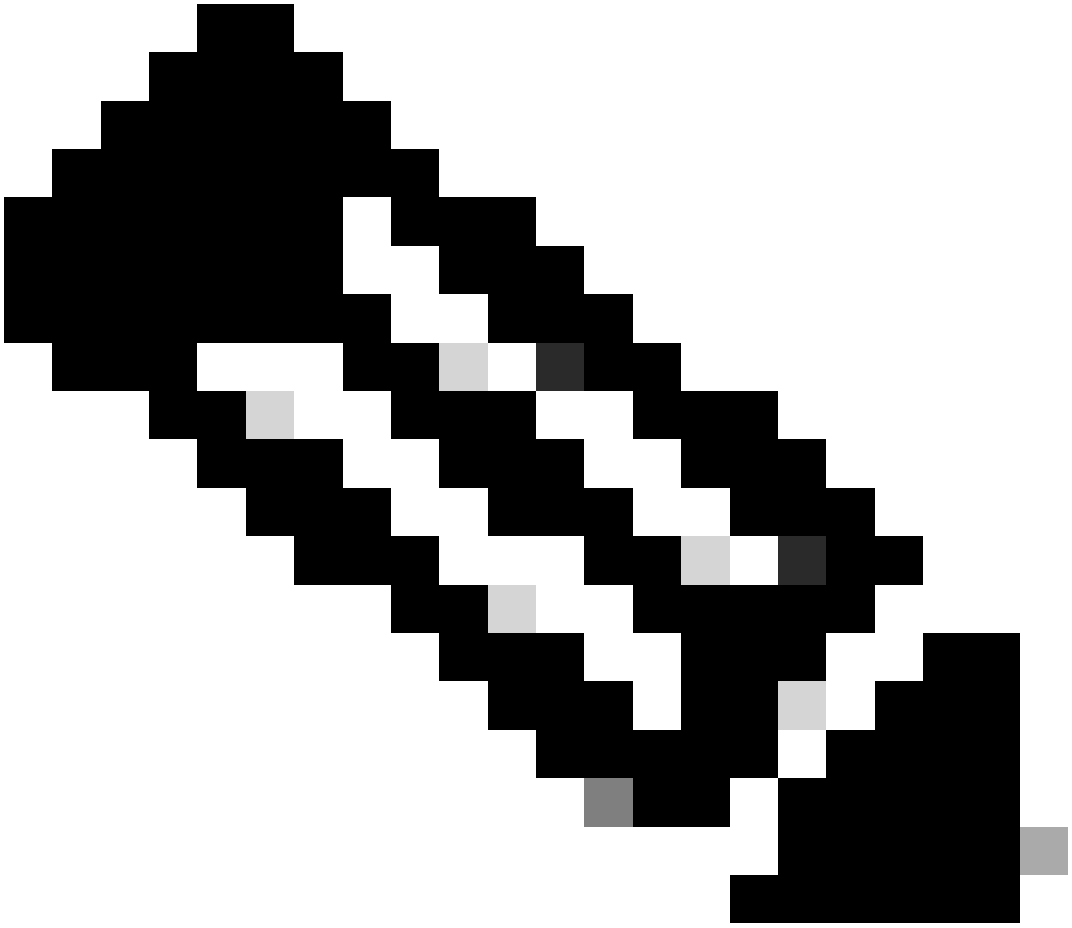
```
router lisp


instance-id 8456


flood access-tunnel
```

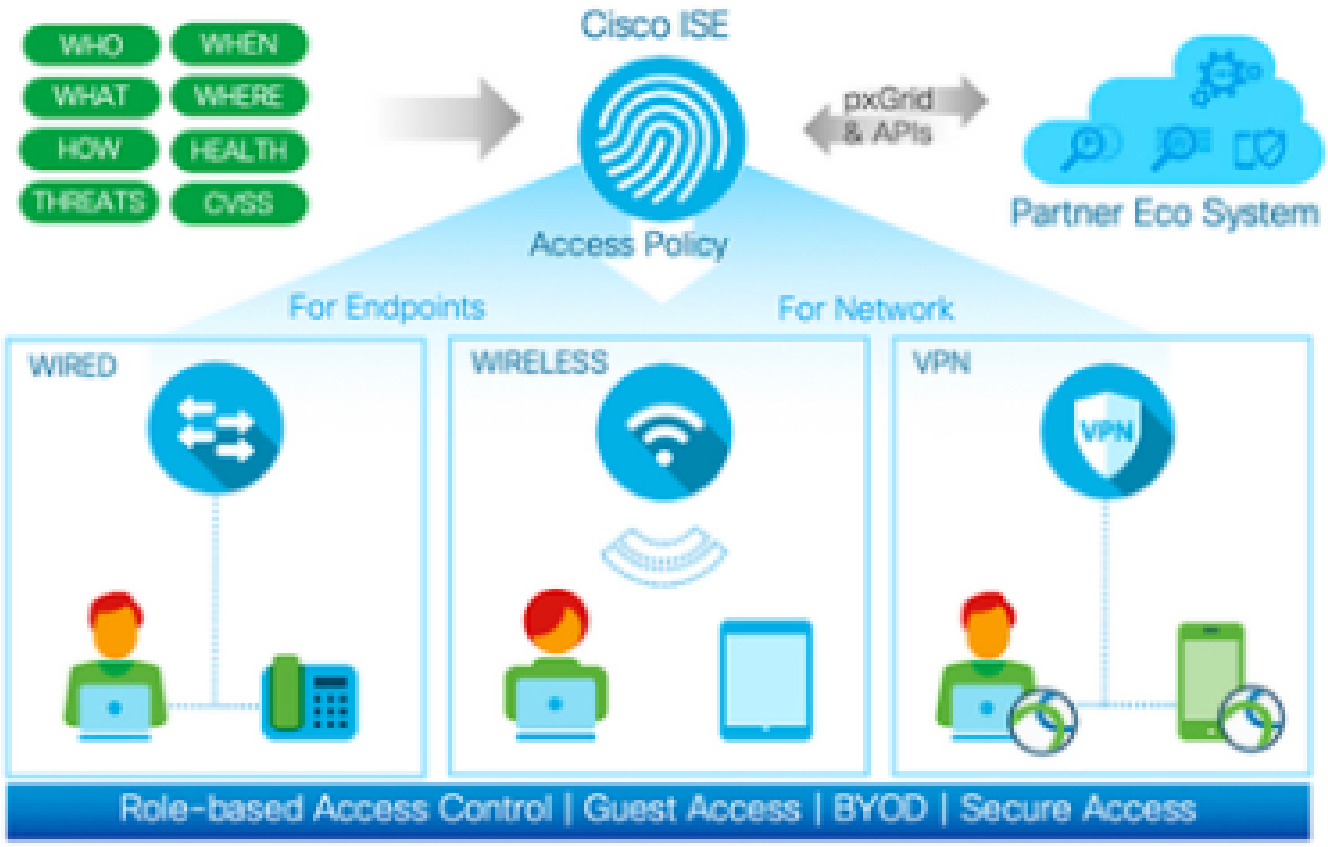
解決/検証

- 内部インターフェイスに接続されたC9300で「フラッドアクセストンネル」を設定した後、クライアントはDHCPアドレスを受信します。



注：エンドデバイスがブロードキャストオファーを受信するように設定されている場合は、lispでフラッドアクセストンネルを有効にしてください。

シナリオ4:LANアダプタの問題



cisco ISE

事象の説明:

- ユーザマシンがAPIPA IPアドレスを受け取り、ユーザ接続に影響があります。

症状

1. Macアドレステーブルは、「drop」を含むエントリを表示します。

<#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セッションで多数のエントリが表示され、2000を超える可能性があり、10000の場合もあります。

<#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
```

トラブルシューティングの手順

- パケットキャプチャは、異なる送信元MACアドレスを持つエンドデバイスからの多数の着信パケットを示します。
- 認証セッションの制限は2000で、制限を超えると、ネットワークで予期しない問題が発生します
- 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

分離

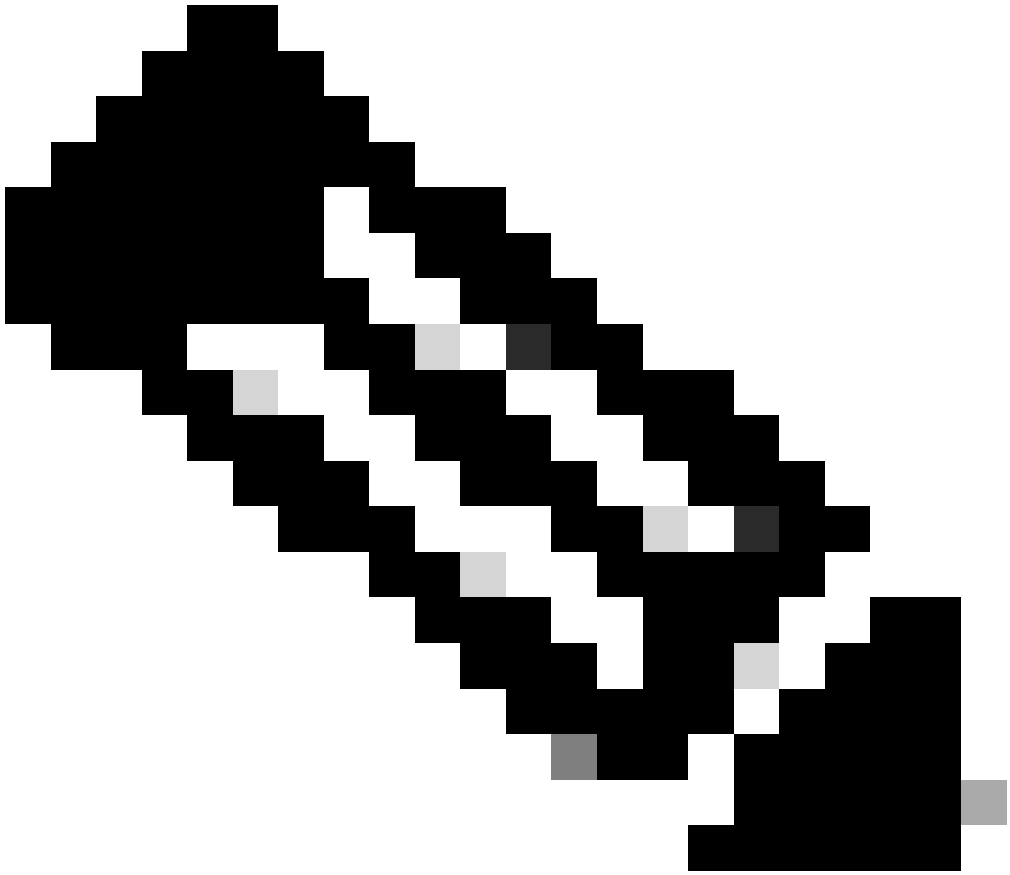
- これは、エンドユーザアダプタの問題を示しています。これにより、スイッチがランダムな送信元MACアドレスとして認識する不正なパケットが送信されます。

アクションプラン

- 2つのmacアドレスだけを許可するように「authentication host-mode multi-domain」を設定します。
- 問題を引き起こしているデバイスを特定して切り分けます。

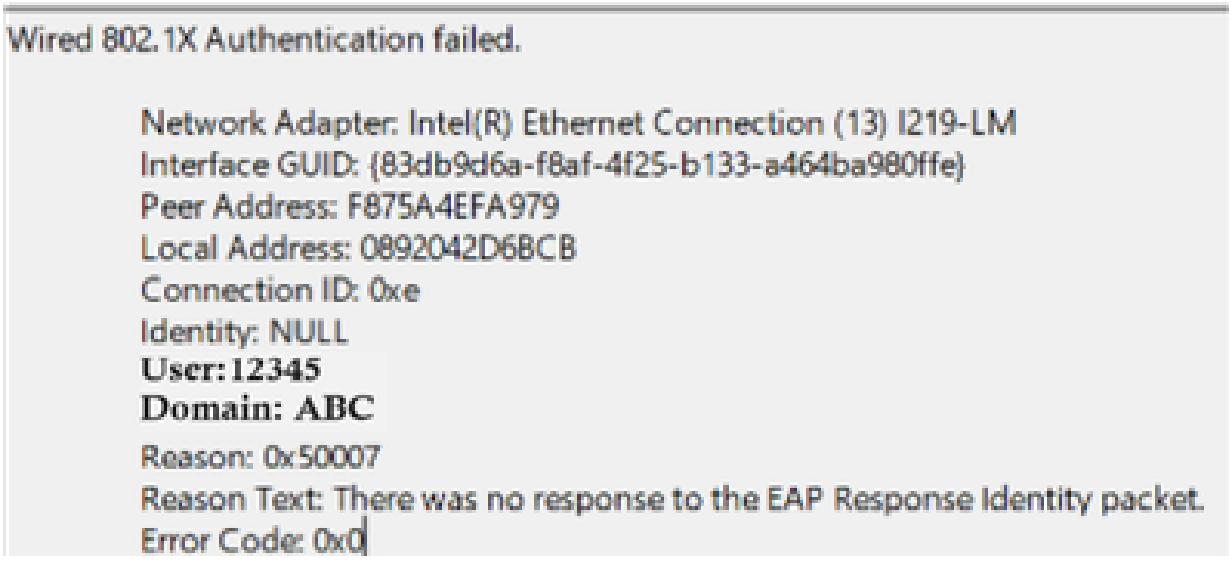
解決/検証

- この回避策を設定しても、問題は発生しません。



- 注：ポートセキュリティまたはDot1x auth session host-mode multi-domainのいずれかを有効にしてください。

シナリオ5 - MTUの不一致



ISEはサーバでこのエラーを示します。

事象の説明:

- ユーザマシンがAPIPA IPアドレスを受け取り、ユーザ接続に影響があります。

ユーザの症状

1. エンドクライアントが、実際の予想パケット長である1492よりも長いパケット長（例：3736）でEAP応答を送信する。

```
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
```

実施したトラブルシューティング

- システム全体のエントリとして、スイッチのMTUをより小さいサイズに設定する。（例：1998bytes）
- より大きいサイズで設定された出力インターフェイス。（例：9198バイト）。

分離

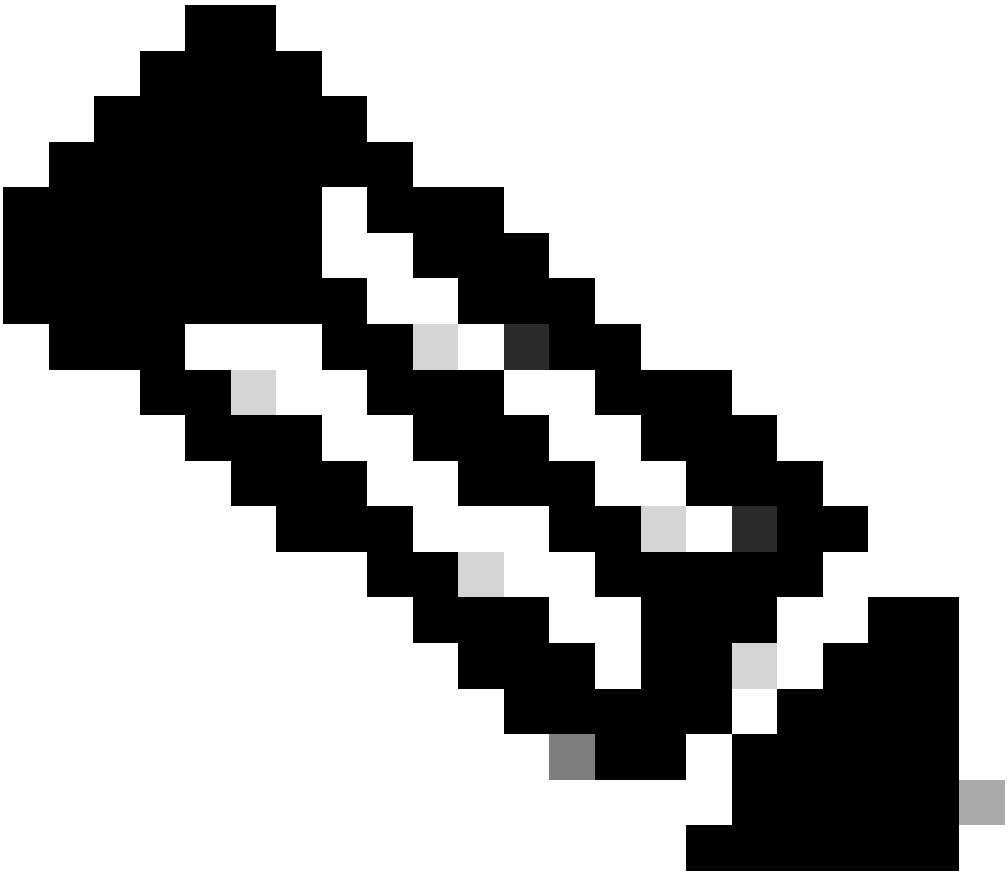
- パス全体でのMTUの不一致が問題の原因です。

アクションプラン

- システムMTUを1500に変更し、スイッチをリロードします

解決/検証

- この設定を行うと、認証は成功します。



- 注：パケットフローのパス全体で同じMTUを有効にしてください。

シナリオ6:IPDTガード

事象の説明:

- ユーザマシンがAPIPA IPアドレスを受け取り、ユーザ接続に影響があります。

ユーザの症状

- VMをHAにしているとき、インターフェイスに次のポリシーが適用されている場合：

デバイストラッキングポリシーIPDT_POLICY

プロトコルUDPなし

トラッキングの有効化

- フェールオーバーの後、ARP応答はアクセススイッチによってドロップされます。

実施したトラブルシューティング

1. プローブに対するARP応答がスイッチによって廃棄される。
2. スイッチにIPDTガードが設定されている。
3. IPDT - ARPプローブのガードドロップとエンドデバイスによるAPIPAの取得

分離

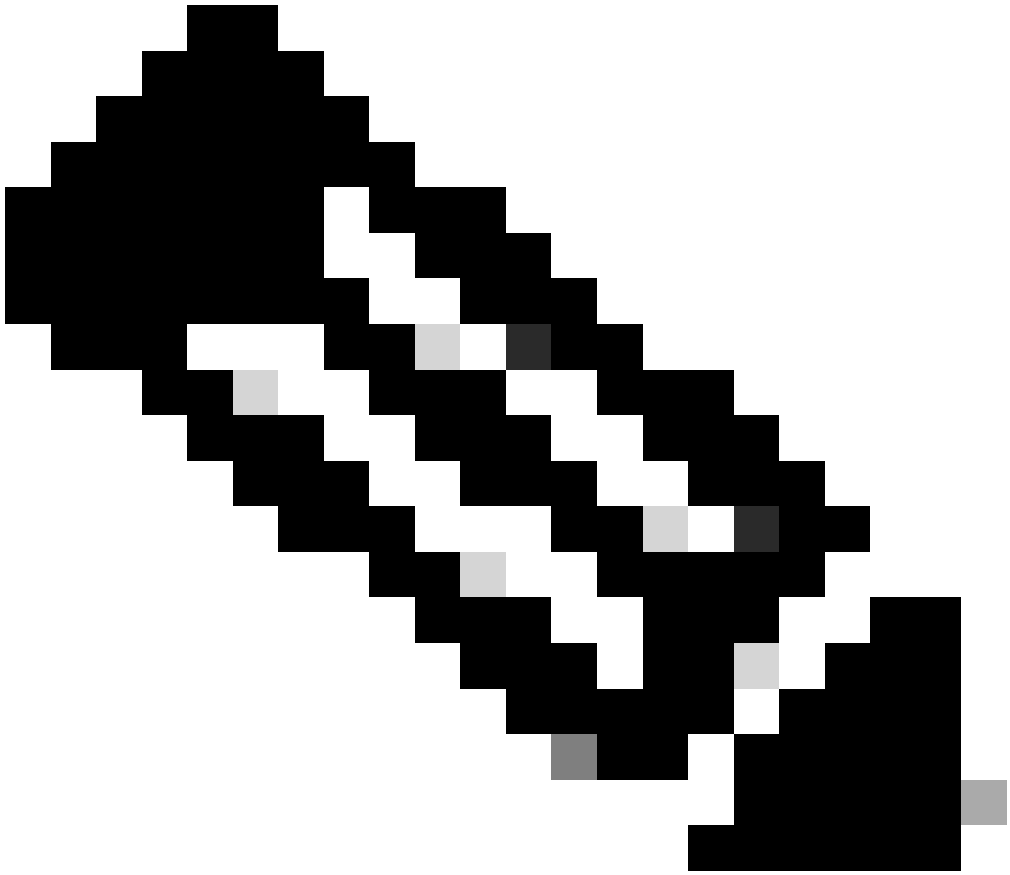
- ARPプローブパケットがIPDTに到達し、ガード機能によってドロップされる。
- 「security-level guard」設定で設定されたIPDTポリシーがARPパケットをドロップするため、少数またはすべてのエンドデバイスが到達不能になる

アクションプラン

- 設定をガードからグリーニングに変更します。
  IPDTポリシーで「security-level glean」を設定します

解決/検証

- 収集の設定を行うと、ARPプローブがARPプロセスによって処理され、問題が解決されます。



- 注：これは既知の不具合であり、17.15.1以降で修正される予定です。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。