# Dépannage d'une défaillance d'adresse APIPA sur le réseau

## Table des matières

# Introduction

Ce document décrit les problèmes liés aux adresses APIPA et fournit des solutions pour les mêmes.

# Composants utilisés

- Commutateurs Catalyst 9000
- Pare-feu ASA comme 5516
- Serveur DHCP de toute nature
- Configuration du Catalyst 9300 dans SDA
- Logiciels : S/O

# Motifs

Les utilisateurs finaux attribuent l'APIPA dans ces scénarios,

- Serveur DHCP non disponible.
- L'offre DHCP est abandonnée avant le saut actuel.
- La sonde ARP obtient une réponse qui représente l'adresse IP dupliquée.

# Scénarios et dépannage

## Scénario 1 : configuration du proxy du pare-feu

ASA 5516

Description du problème :

- Les ordinateurs des utilisateurs reçoivent l'adresse IP APIPA et la connectivité des utilisateurs est affectée.

Symptômes du problème

1. Les utilisateurs d’un VLAN spécifique rencontrent des problèmes intermittents lorsqu’ils reçoivent une adresse IP APIPA et perdent la connectivité au réseau.
2. Les pare-feu possèdent plusieurs entrées ARP pour une adresse MAC d'utilisateur final unique, comme suit :

<#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
```

Étapes de dépannage

1. Les débogages sur le pare-feu indiquent que le pare-feu envoie la réponse à la sonde ARP des utilisateurs finaux.

<#root>

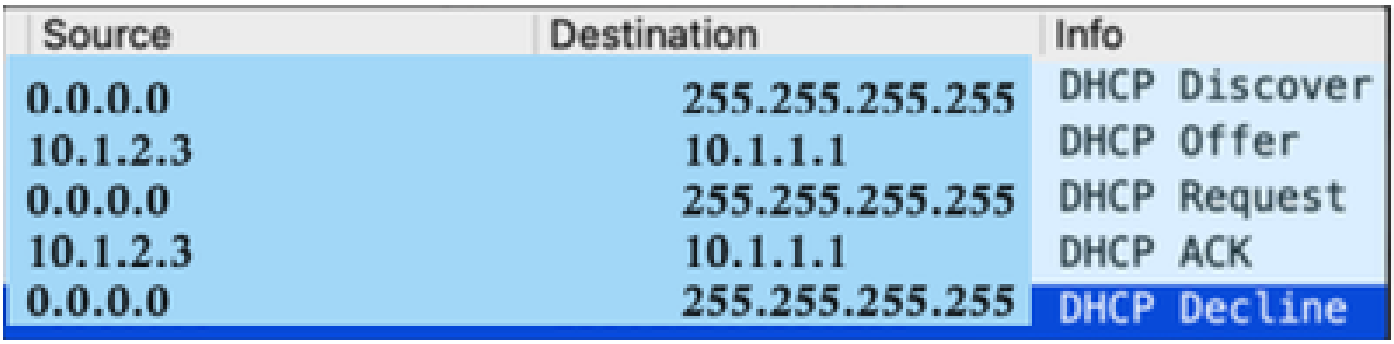
```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).


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

Le périphérique final peut ainsi penser que son adresse est dupliquée.

2. Captures sur le périphérique final ou le pare-feu

Les captures montrent le périphérique final envoyant des paquets DHCP Refuser une fois le processus DORA terminé.



| 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 |

Isolement

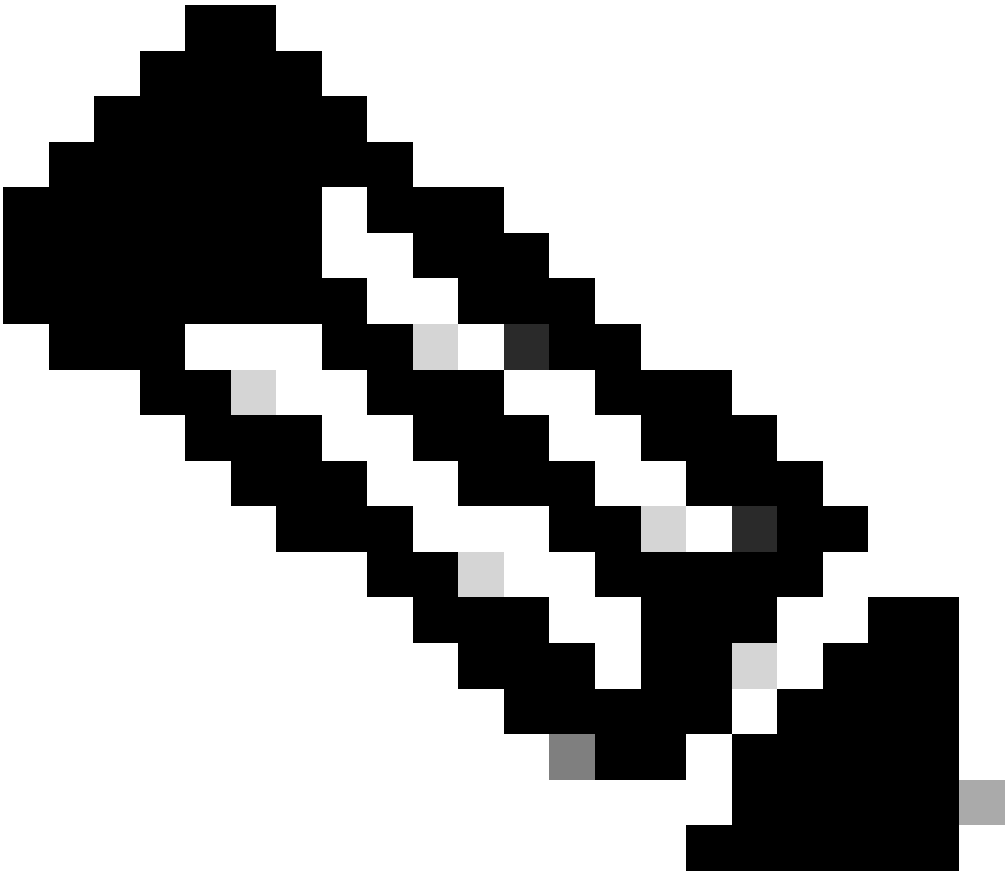
- L'interface interne du pare-feu répond à la sonde ARP en agissant comme proxy, une fois le processus DORA terminé. Le PC doit alors envoyer un refus DHCP.

Plan d'action

- Désactivez le proxy arp sur l'interface interne du pare-feu en utilisant la commande « sysopt noproxyarp inside »

Résolution/vérification

- Les périphériques finaux reçoivent une adresse IP après la désactivation de proxy-arp.



- Remarque : assurez-vous qu'aucun périphérique n'agit en tant que proxy ou n'envoie de réponse pour les sondes ARP des utilisateurs finaux.

.

## Scénario 2 : étendue du serveur DHCP

DHCP Server

Description du problème :

- Les ordinateurs des utilisateurs reçoivent l'adresse IP APIPA et la connectivité des utilisateurs est affectée.

Symptômes

1. Les utilisateurs d’un VLAN spécifique obtiennent uniquement l’adresse IP APIPA et perdent la connexion au réseau.

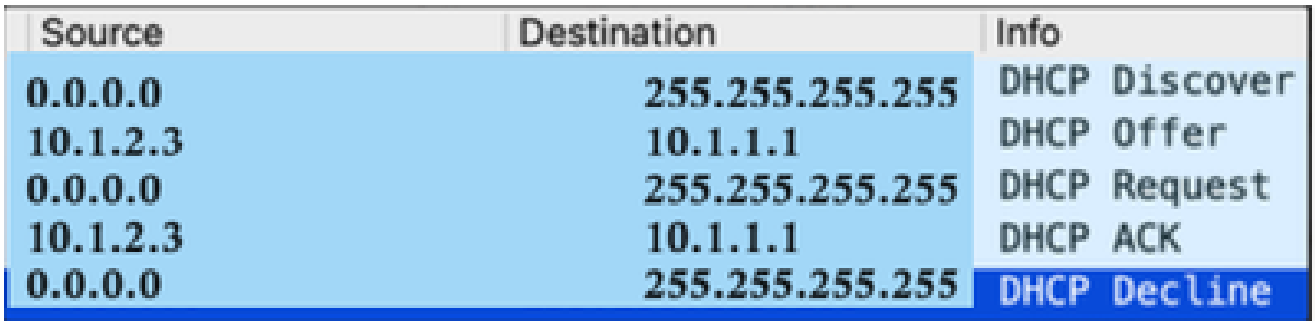
Dépannage effectué

- Refus DHCP envoyé aux utilisateurs finaux et configuré avec l'adresse APIPA

Isolement

- Le serveur DHCP attribue une adresse IP de l'étendue A et la même adresse IP est

attribuée à un autre ordinateur portable, car l'étendue B a la même plage. Cela entraîne un refus 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 |

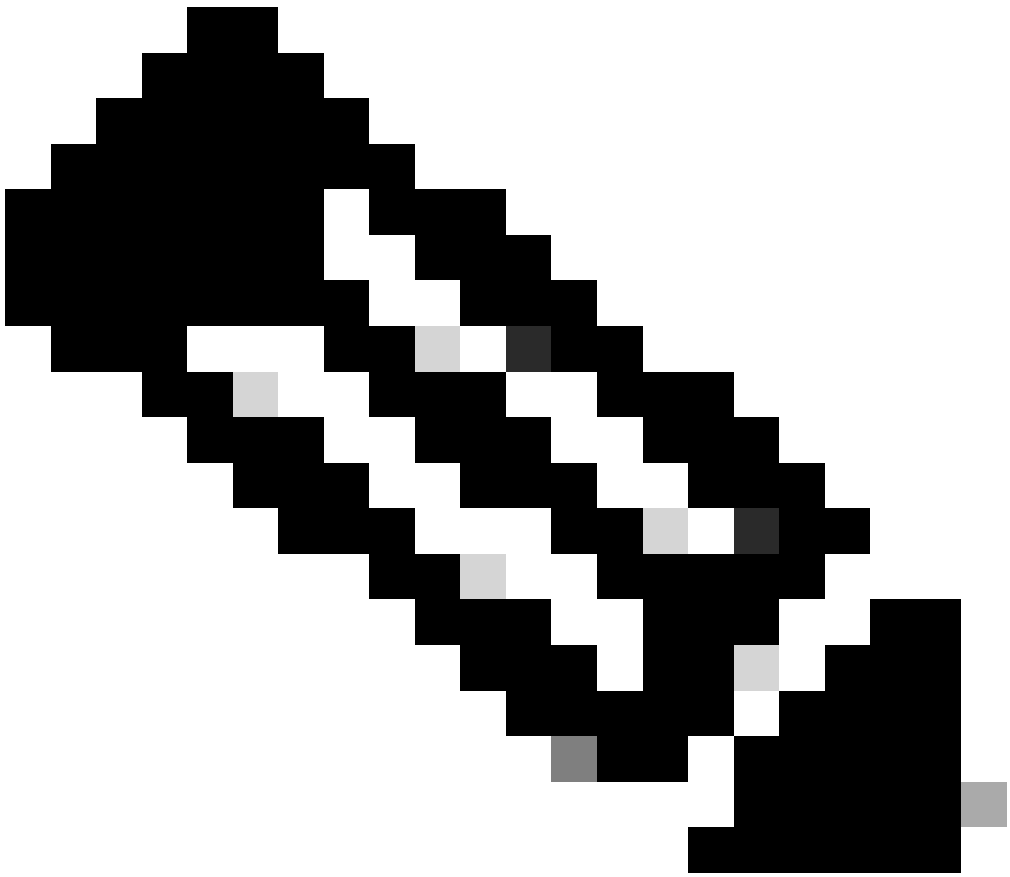
Plan d'action

- Attribuer une plage d'étendues DHCP unique

Résolution/vérification

- Les périphériques finaux reçoivent une adresse IP après modification de l'étendue.

---



-

---

Remarque : assurez-vous que le serveur DHCP n'a pas d'étendues en double configurées.

## Scénario 3 : configuration SDA C9300

Cat9300 in SDA

Description du problème :

- Les ordinateurs des utilisateurs reçoivent l'adresse IP APIPA et la connectivité des utilisateurs est affectée.

Symptômes utilisateur

1. Certains utilisateurs d'un VLAN spécifique ne peuvent pas obtenir d'adresses DHCP via le point d'accès sans fil.
2. Le pare-feu possède plusieurs entrées arp pour une adresse MAC d'utilisateur final unique

<#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
```

Dépannage effectué

- L'offre DHCP a été abandonnée par le commutateur
- FTD remplit le protocole ARP en fonction de l'OFFRE DHCP reçue du serveur DHCP.

<#root>

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

Isolement

- Si le VLAN L2-only est configuré pour la configuration sans fil SDA, le paquet d'offre avec l'indicateur de diffusion n'atteint pas le point d'accès. Puisque le tunnel d'accès n'autorise pas les paquets de diffusion par défaut.

Plan d'action

- Autoriser la capacité d'inondation dans l'environnement LISP.

<#root>

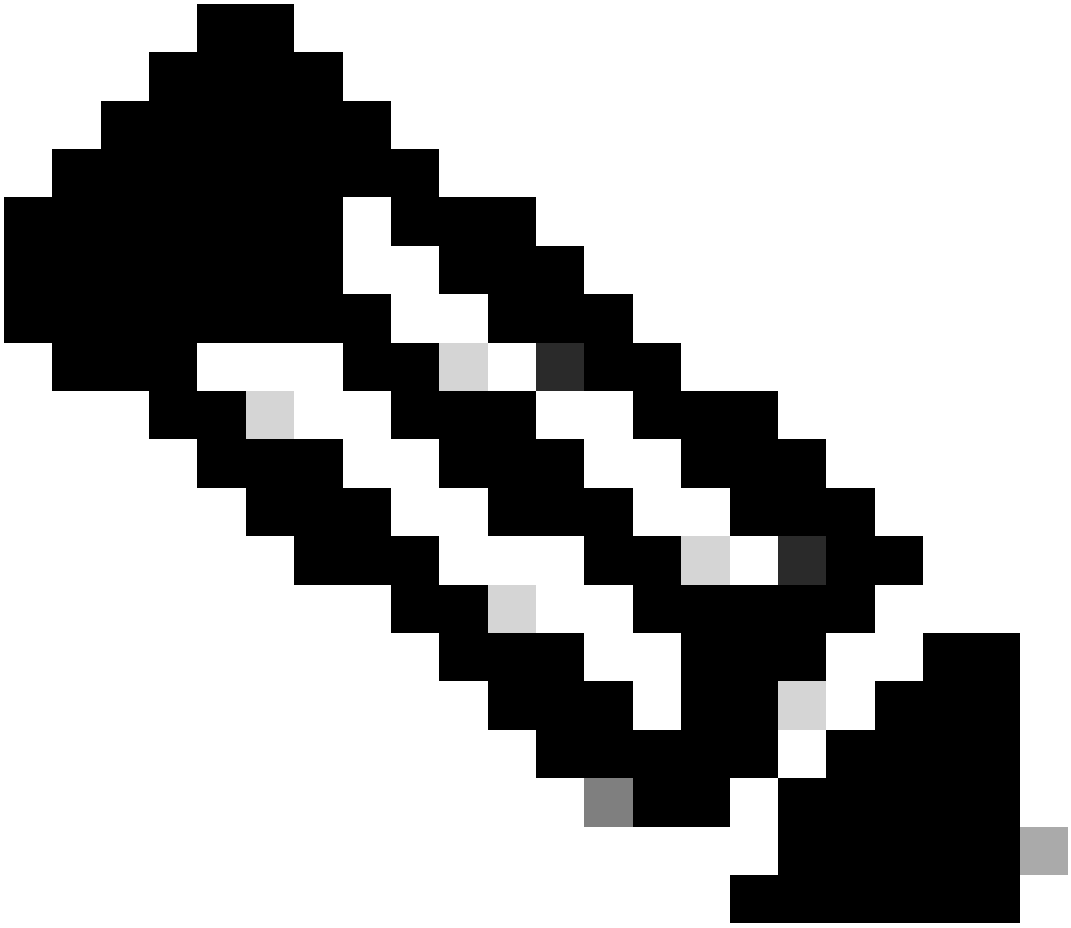
```
router lisp


instance-id 8456


flood access-tunnel
```

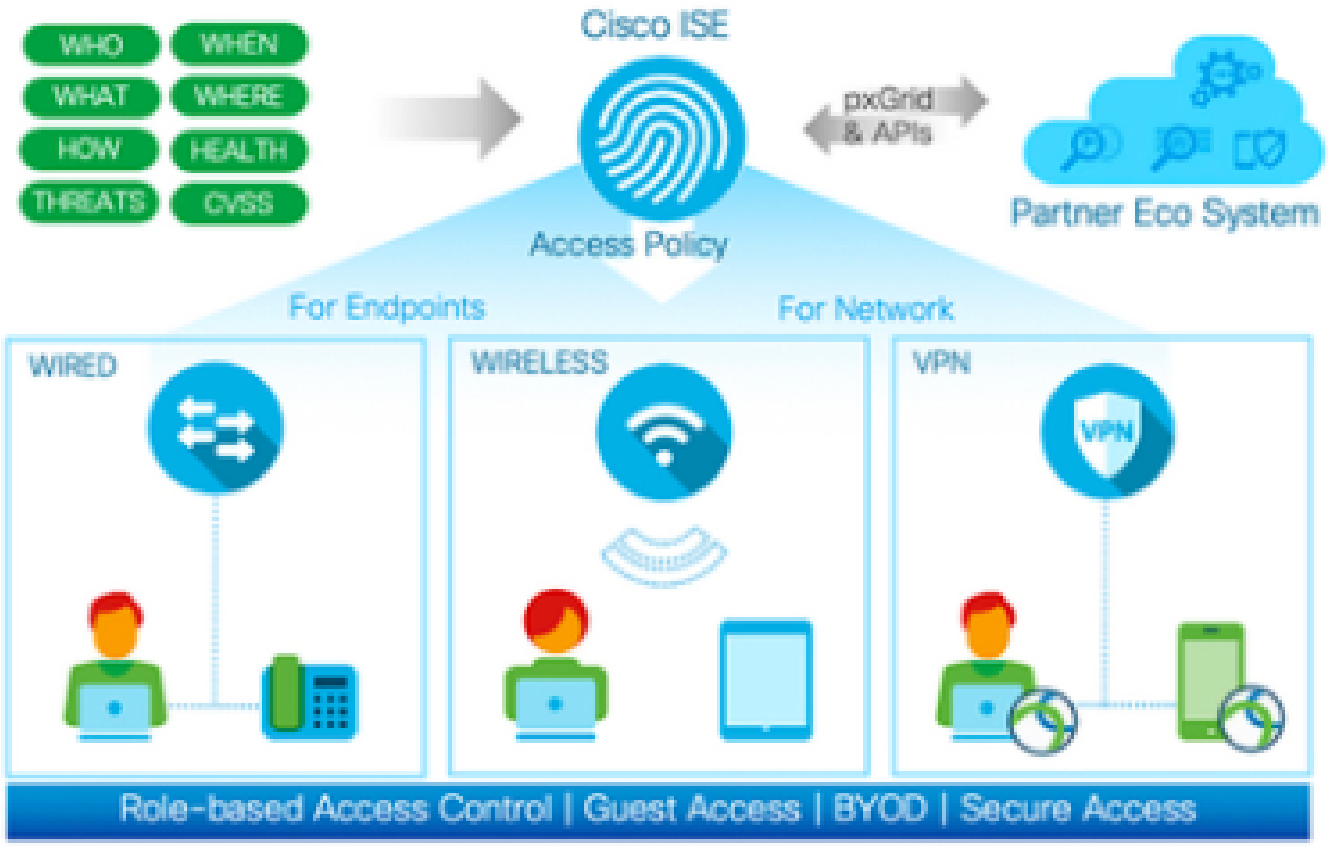
Résolution/vérification

- Après avoir configuré le « flood access-tunnel » dans l'interface interne du C9300, les clients reçoivent des adresses DHCP.



Remarque : assurez-vous d'activer flood access-tunnel sous lisp, si le périphérique final est configuré pour recevoir une offre de diffusion.

## Scénario 4 - Problème d'adaptateur LAN




cisco ISE

Description du problème :

- Les ordinateurs des utilisateurs reçoivent l'adresse IP APIPA et la connectivité des utilisateurs est affectée.

Symptômes

1. La table d'adresses Mac affiche les entrées avec « 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 session Show Authentication affiche de nombreuses entrées, pouvant dépasser 2000, voire 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
```

Étapes de dépannage

- La capture de paquets affiche de nombreux paquets entrants provenant du périphérique final avec différentes adresses MAC source.
- La limite de session Auth est de 2000 et une fois la limite franchie, des problèmes inattendus surviennent sur le réseau
- 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

Isolement

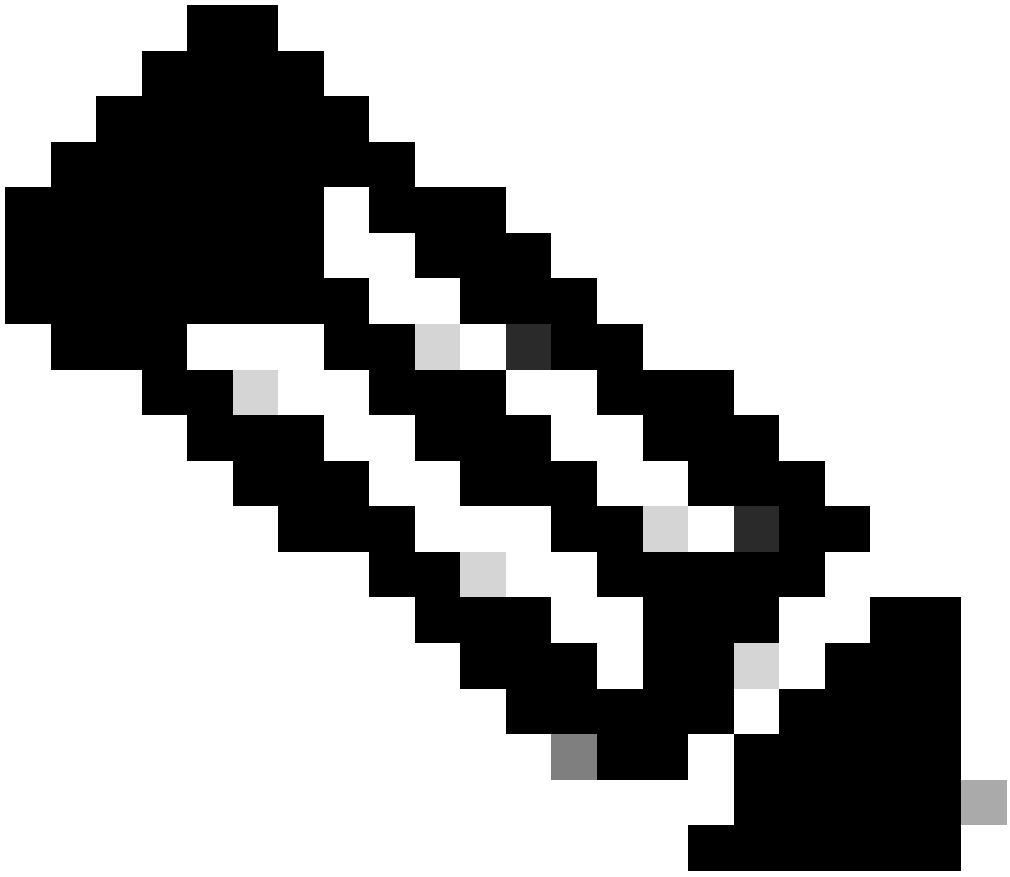
- Ceci indique un problème d'adaptateur de l'utilisateur final.Ceci envoie des paquets mal formés que le commutateur comprend comme des adresses MAC source aléatoires.

Plan d'action

- Configurez « authentication host-mode multi-domain » qui autorise seulement 2 adresses MAC.
- Identifier et isoler le périphérique coupable.

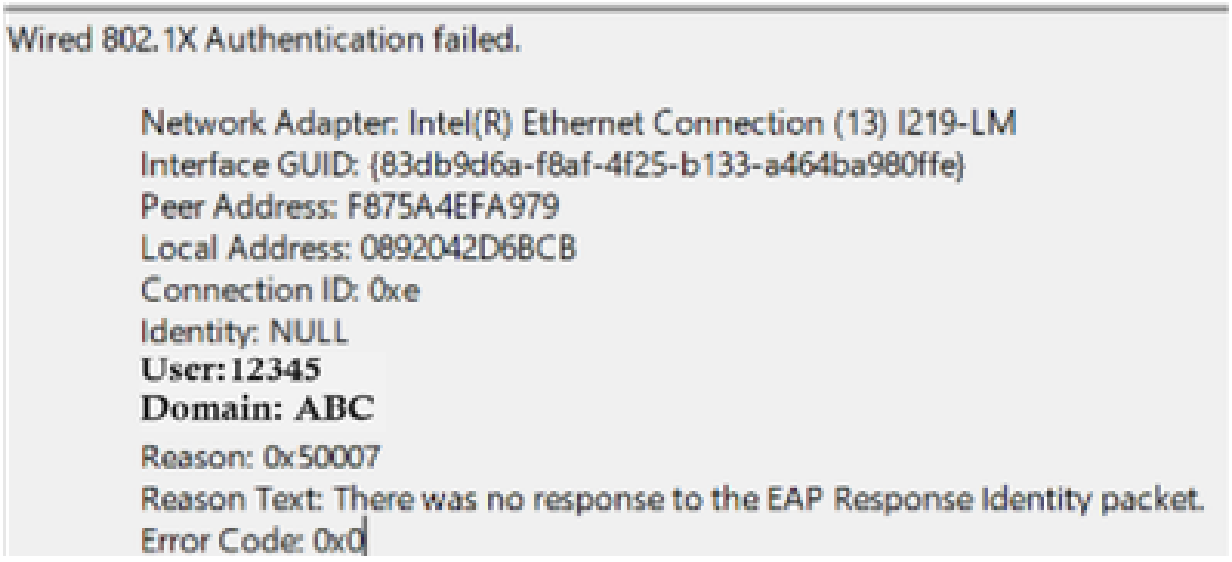
Résolution/vérification

- Après la configuration de cette solution de contournement, aucun problème ne sera observé.



- Remarque : assurez-vous d'activer la sécurité des ports ou la session d'authentification Dot1x en mode hôte multidomaine.

## Scénario 5 - Non-concordance MTU



ISE représente cette erreur sur le serveur.

Description du problème :

- Les ordinateurs des utilisateurs reçoivent l'adresse IP APIPA et la connectivité des utilisateurs est affectée.

Symptômes utilisateur

1. Le client final envoie une réponse EAP avec une longueur de paquet supérieure (exemple : 3736) à la longueur de paquet réelle attendue 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
```

Dépannage effectué

- MTU défini sur une taille inférieure sur le commutateur en tant qu'entrée système. (Exemple : 1 998 octets)
- Interface de sortie configurée avec une taille supérieure. (Exemple : 9 198 octets)

Isolement

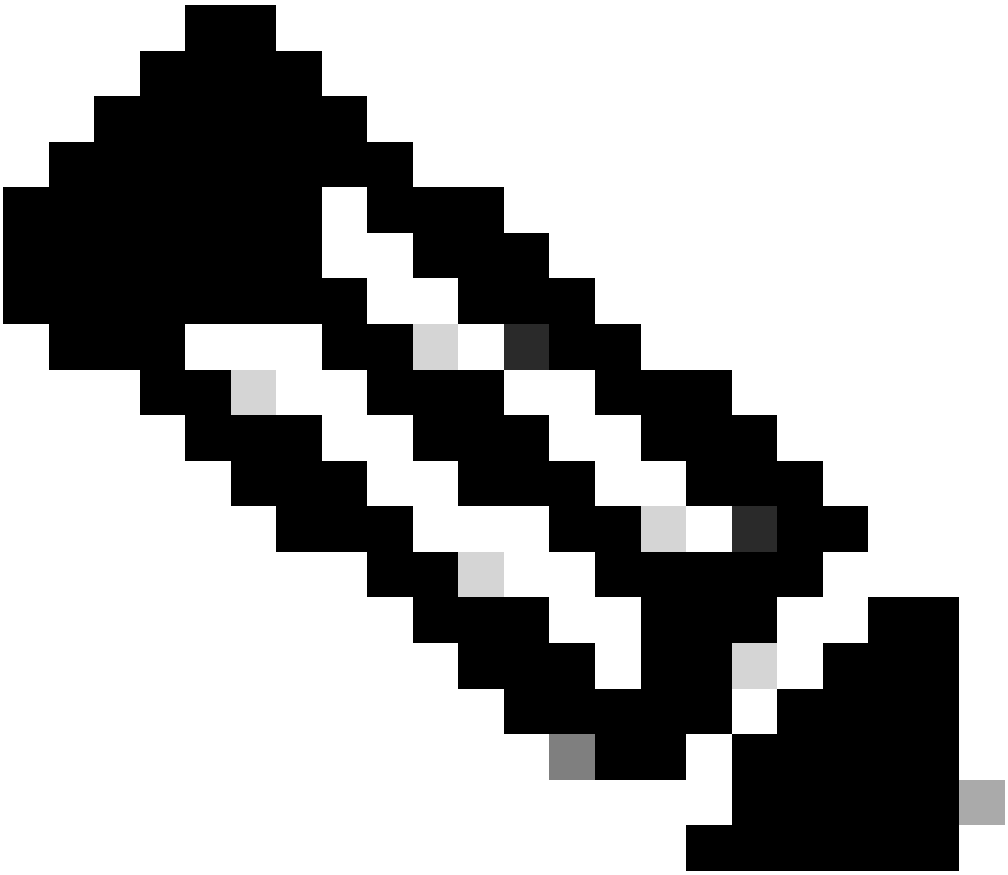
- Une non-concordance dans le MTU sur l'ensemble du chemin entraîne le problème.

Plan d'action

- Remplacez le MTU du système par 1500 et rechargez le commutateur

Résolution/vérification

- Une fois ces paramètres configurés, l'authentification réussit.



- Remarque : assurez-vous d'activer le même MTU sur tout le chemin du flux de paquets.

## Scénario 6 - Protection IPDT

Description du problème :

- Les ordinateurs des utilisateurs reçoivent l'adresse IP APIPA et la connectivité des utilisateurs est affectée.

Symptômes utilisateur

- Lorsque des machines virtuelles sont en haute disponibilité, si cette stratégie est appliquée dans l'interface :

stratégie de suivi des périphériques IPDT_POLICY

aucun protocole udp

activation du suivi

- Après un basculement, la réponse ARP est abandonnée par le commutateur d'accès.

Dépannage effectué

1. Les réponses ARP aux sondes seraient abandonnées par le commutateur.
2. Le commutateur est configuré avec IPDT Guard.
3. IPDT : protection lors de l'abandon de la sonde ARP et du périphérique final recevant APIPA.

Isolement

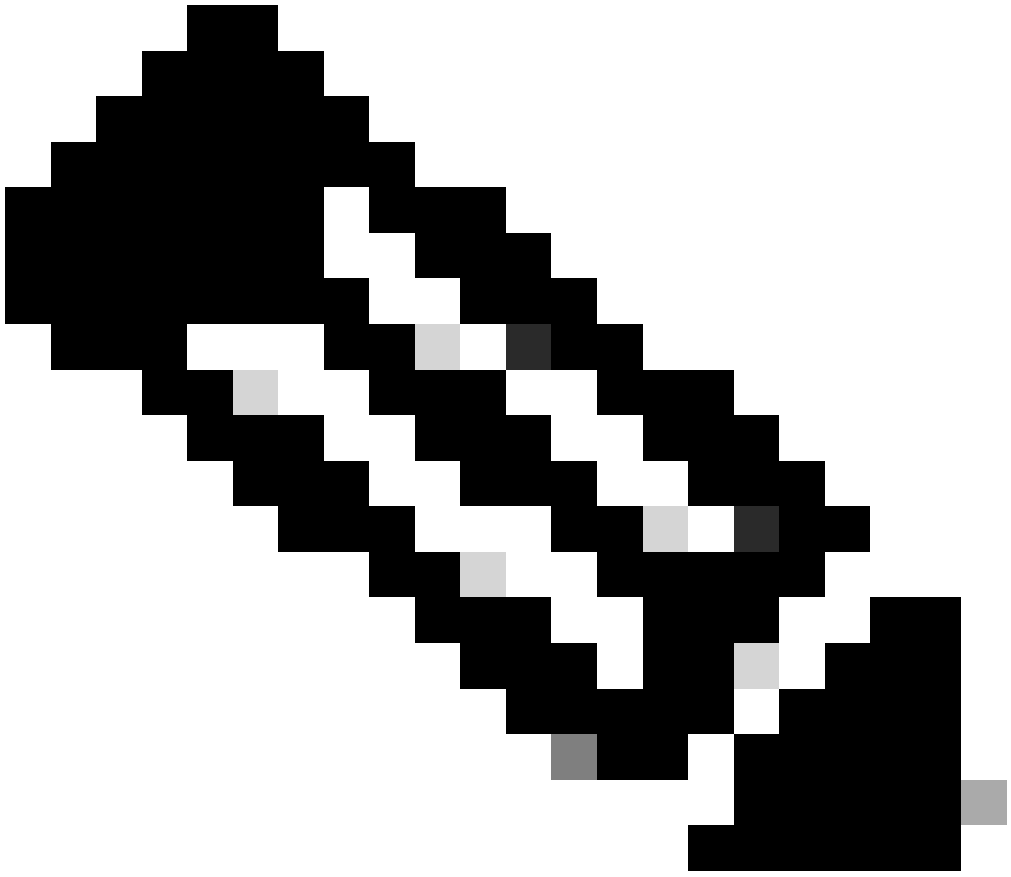
- Les paquets de sonde ARP atteignent IPDT et sont abandonnés en raison de la fonctionnalité Guard.
- La stratégie IPDT configurée avec la configuration « security-level guard » abandonne les paquets ARP, ce qui rend inaccessibles un petit nombre de périphériques finaux, voire tous

Plan d'action

- Remplacez le paramètre Guard par Glean.
  Configurez « security-level glean » dans la stratégie IPDT

Résolution/vérification

- Après avoir configuré les paramètres Glean, les sondes ARP sont traitées par le processus ARP et le problème est résolu.



- Remarque : il s'agit d'un défaut bien connu et il serait corrigé dans la version 17.15.1 et ultérieure.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.