Risoluzione dei problemi relativi all'errore di indirizzo APIPA nella rete

Sommario

Introduzione

Questo documento descrive i problemi relativi agli indirizzi APIPA e fornisce le relative soluzioni.

Componenti usati

- Switch Catalyst 9000.
- ASA Firewall come 5516
- server DHCP di qualsiasi tipo
- Catalyst 9300 in installazione SDA
- Software: N/D

Motivi

Gli utenti finali assegnano l'APIPA durante questi scenari,

- Server DHCP non disponibile.
- L'offerta DHCP viene scartata prima dell'hop corrente.
- Il probe ARP ottiene una risposta che rappresenta l'IP duplicato.

Scenari e risoluzione dei problemi

Scenario 1 - Configurazione proxy firewall

ASA 5516

Descrizione del problema:

- I computer utente ricevono l'indirizzo IP APIPA e la connettività dell'utente è compromessa.

Sintomi del problema

1. Gli utenti di una VLAN specifica riscontrano problemi intermittenti quando ricevono un indirizzo IP APIPA e perdono la connettività alla rete.
2. I firewall dispongono di più voci ARP per un singolo indirizzo MAC dell'utente finale, ad esempio:

<#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
```

Procedura di risoluzione dei problemi

1. I debug sul firewall puntano al firewall che invia la risposta all'sonda ARP degli utenti finali.

<#root>

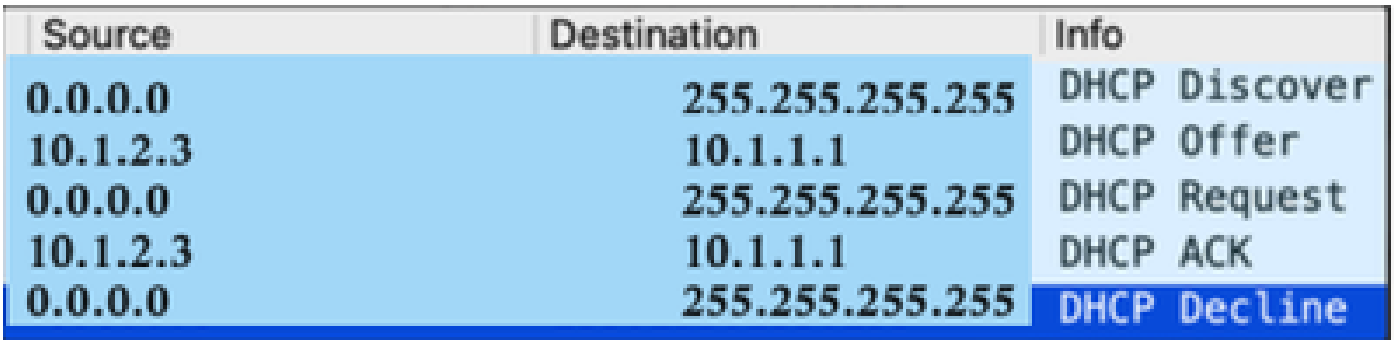
```
DHCPD/RA: creating ARP entry (10.1.1.12, abcd.abcd.abcd).


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

In questo modo il dispositivo terminale considera l'indirizzo duplicato.

2. Acquisizioni sul dispositivo terminale o sul firewall

Acquisisce e mostra il dispositivo terminale che invia i pacchetti DHCP Rifiuta una volta completato il processo DORA.



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

Isolare

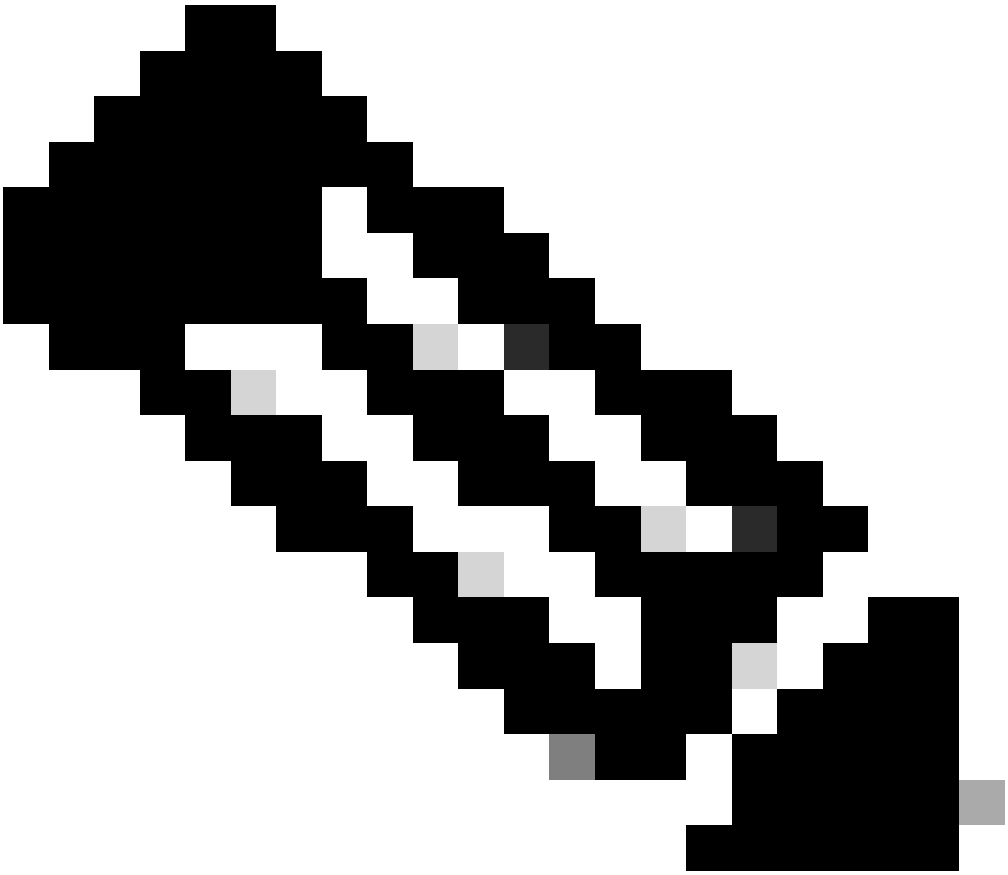
- L'interfaccia interna del firewall risponde alla sonda ARP come proxy una volta completato il processo DORA. In questo modo il PC rifiuta l'invio di DHCP.

Piano d'azione

- Disabilitare l'arp proxy sull'interfaccia interna del firewall utilizzando il comando "sysopt noproxyarp inside"

Risoluzione/verifica

- I dispositivi terminali ricevono l'indirizzo IP dopo aver disattivato il proxy-arp.



- Nota: accertarsi che nessun dispositivo agisca come proxy o invii una risposta per le sonde ARP dell'utente finale.

.

Scenario 2 - Ambito server DHCP

DHCP Server

Descrizione del problema:

- I computer utente ricevono l'indirizzo IP APIPA e la connettività dell'utente è compromessa.

Sintomi

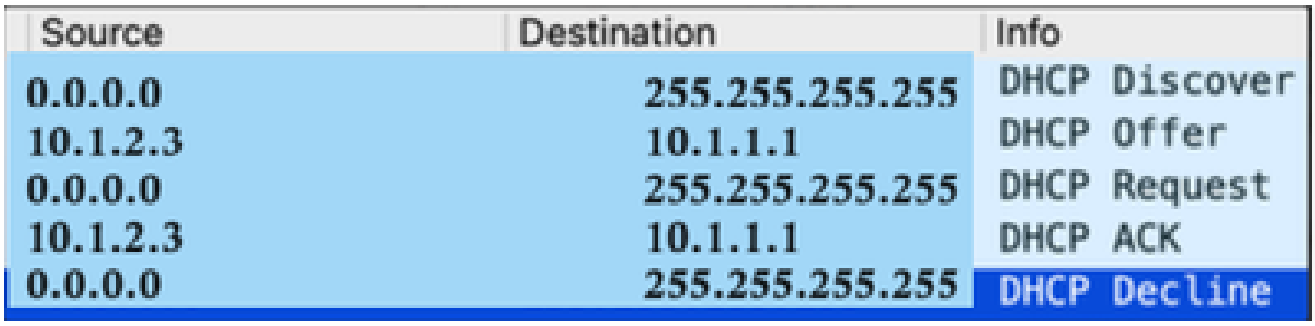
1. Gli utenti su una vlan specifica ottengono solo l'indirizzo IP APIPA e perdono la connessione alla rete.

Risoluzione dei problemi eseguita

- Rifiuto DHCP inviato agli utenti finali ed è stato configurato con indirizzo APIPA

Isolare

- Il server DHCP assegna un indirizzo IP dall'ambito A e lo stesso indirizzo IP a un altro laptop perché l'ambito B ha lo stesso intervallo. Questo causa il rifiuto di DHCP:

- 

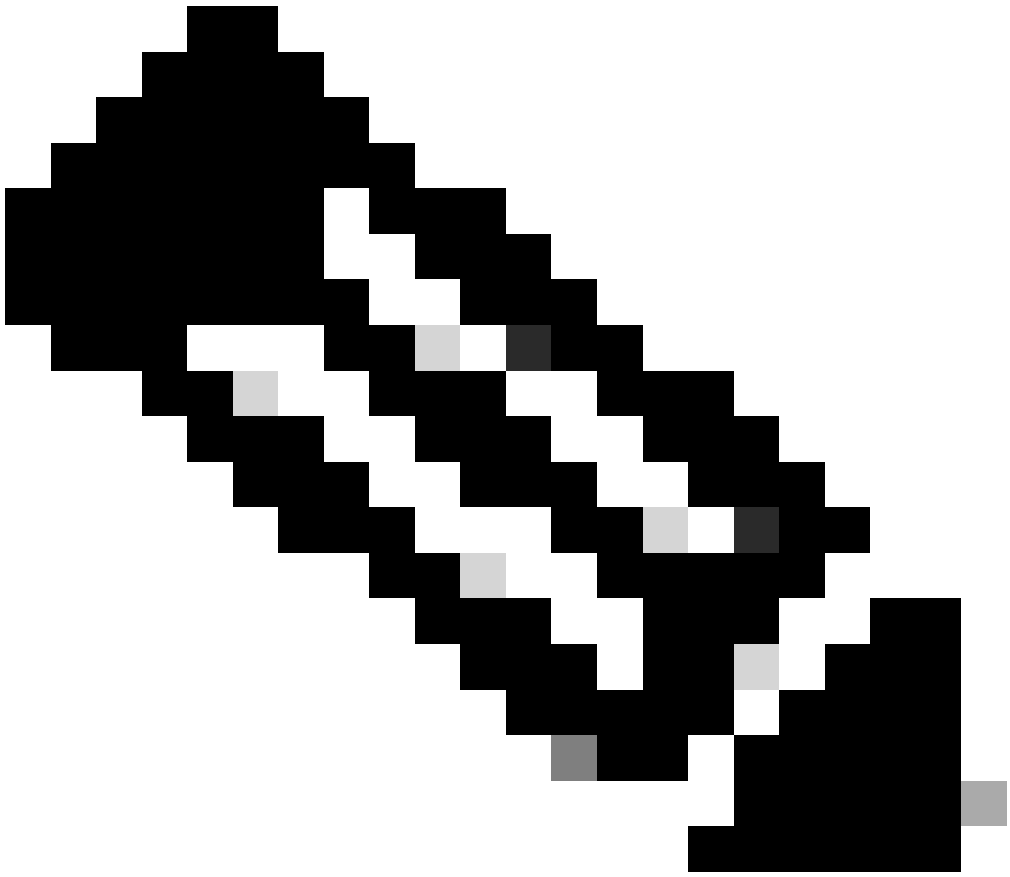
Source	Destination	Info
0.0.0.0	255.255.255.255	DHCP Discover
10.1.2.3	10.1.1.1	DHCP Offer
0.0.0.0	255.255.255.255	DHCP Request
10.1.2.3	10.1.1.1	DHCP ACK
0.0.0.0	255.255.255.255	DHCP Decline

Piano d'azione

- Assegna intervallo di ambito DHCP univoco

Risoluzione/verifica

- I dispositivi finali ricevono l'indirizzo IP dopo la modifica dell'ambito.



- Nota: verificare che nel server DHCP non siano configurati ambiti duplicati.

Scenario 3 - configurazione SDA C9300

Cat9300 in SDA

Descrizione del problema:

- I computer utente ricevono l'indirizzo IP APIPA e la connettività dell'utente è compromessa.

Sintomi utente

1. Alcuni utenti di una VLAN specifica non sono in grado di ottenere gli indirizzi DHCP tramite il punto di accesso wireless.
2. Il firewall dispone di più voci arp per un unico indirizzo MAC dell'utente finale

<#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
```

Risoluzione dei problemi eseguita

- Offerta DHCP scartata dal commutatore
- FTD popola ARP in base all'OFFERTA DHCP restituita dal server DHCP.

<#root>

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

Isolare

- Se la VLAN solo L2 è configurata per l'installazione wireless SDA, il pacchetto dell'offerta con flag di trasmissione non raggiunge l'access point. Poiché il tunnel di accesso non consente i pacchetti broadcast per impostazione predefinita.

Piano d'azione

- Consentire la "capacità di inondazione" all'interno dell'ambiente LISP.

<#root>

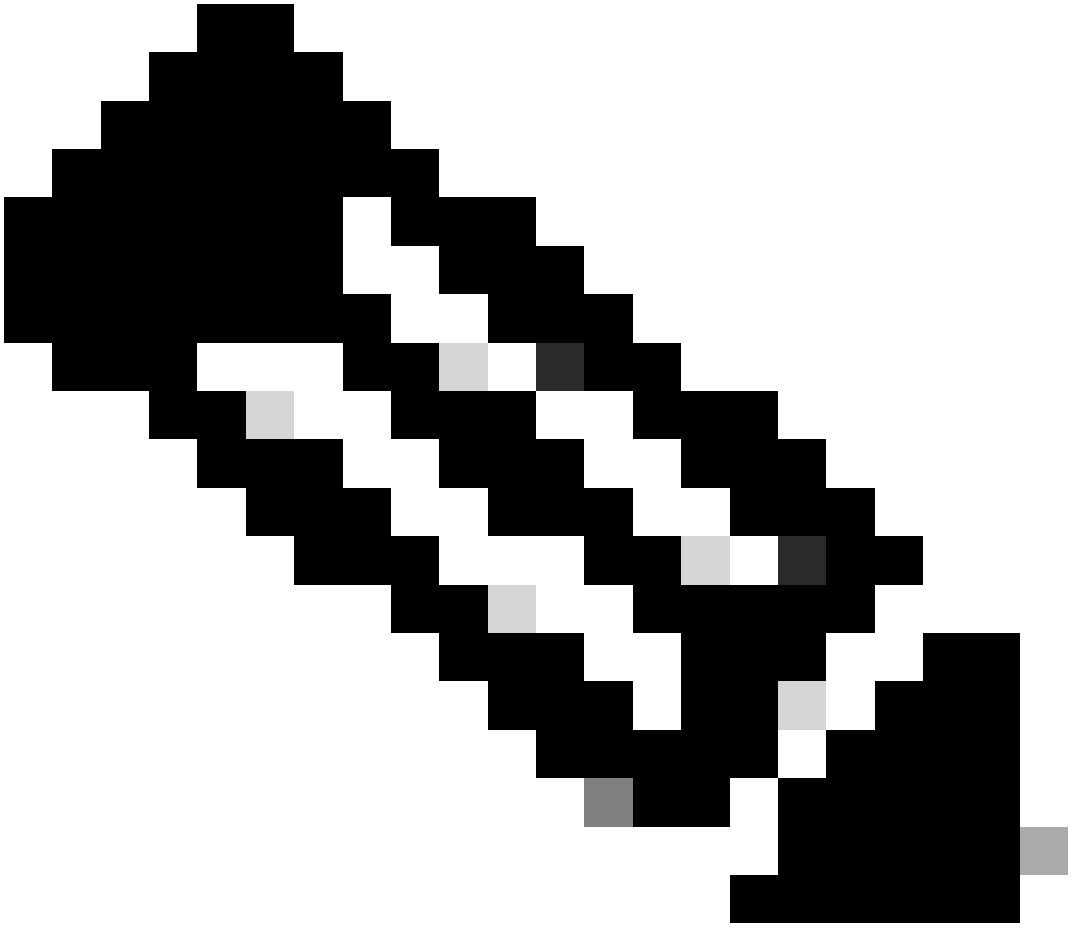
```
router lisp


instance-id 8456


flood access-tunnel
```

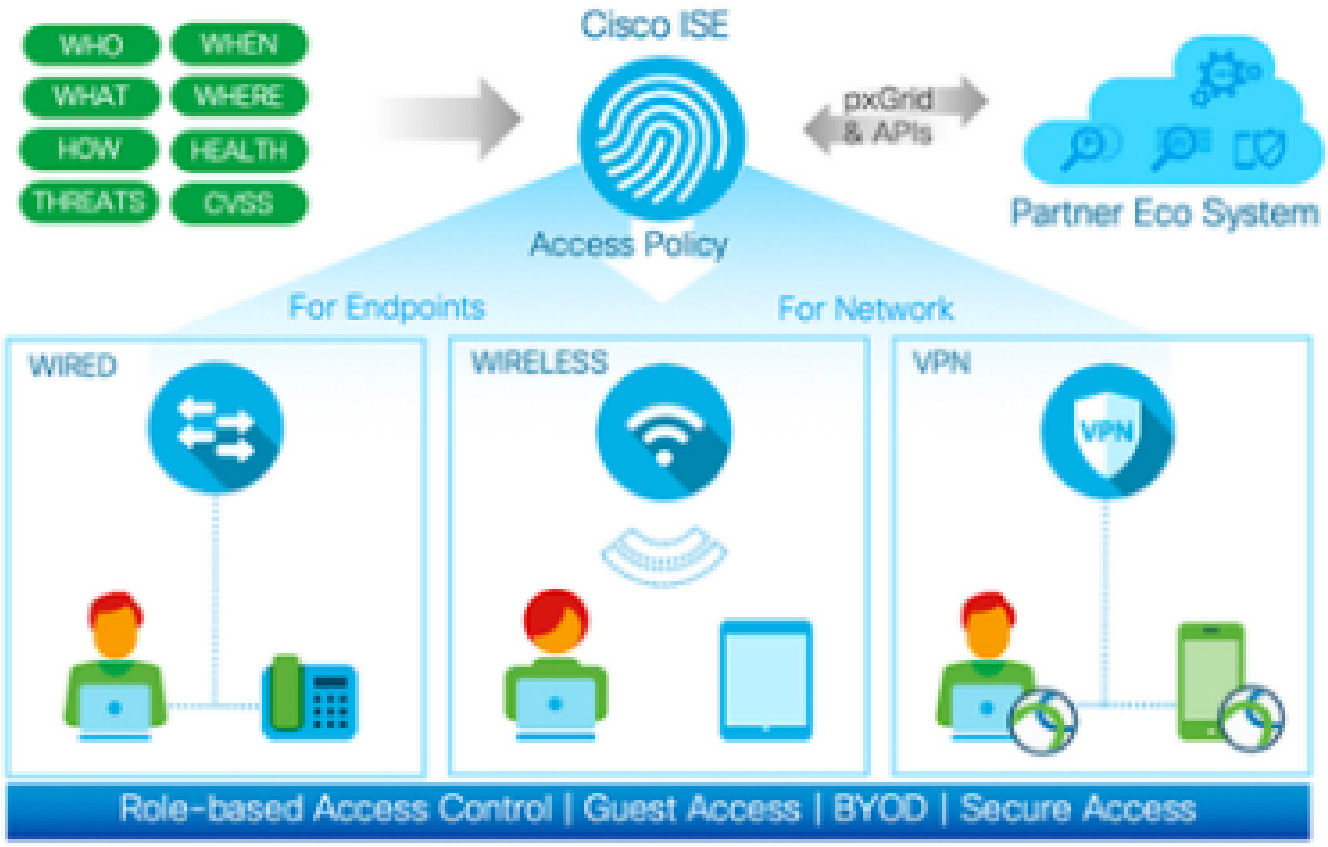
Risoluzione/verifica

- Dopo aver configurato `flood access-tunnel` nel C9300 connesso all'interfaccia interna, i client ricevono gli indirizzi DHCP.



Nota: abilitare il tunnel di accesso flood in lisp se il dispositivo terminale è configurato per ricevere l'offerta di trasmissione.

Scenario 4 - Problema con l'adattatore LAN



cisco ISE

Descrizione del problema:

- I computer utente ricevono l'indirizzo IP APIPA e la connettività dell'utente è compromessa.

Sintomi

1. La tabella degli indirizzi Mac mostra le voci con "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 sessione Mostra autenticazione visualizza molte voci, probabilmente superiori a 2000 o anche a 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
```

Procedura di risoluzione dei problemi

- L'acquisizione dei pacchetti visualizza molti pacchetti in arrivo dal dispositivo terminale con indirizzi MAC di origine diversi.
- Il limite di sessioni di autenticazione è 2000 e, una volta superato il limite, si verificano problemi imprevisti nella rete
- 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

Isolare

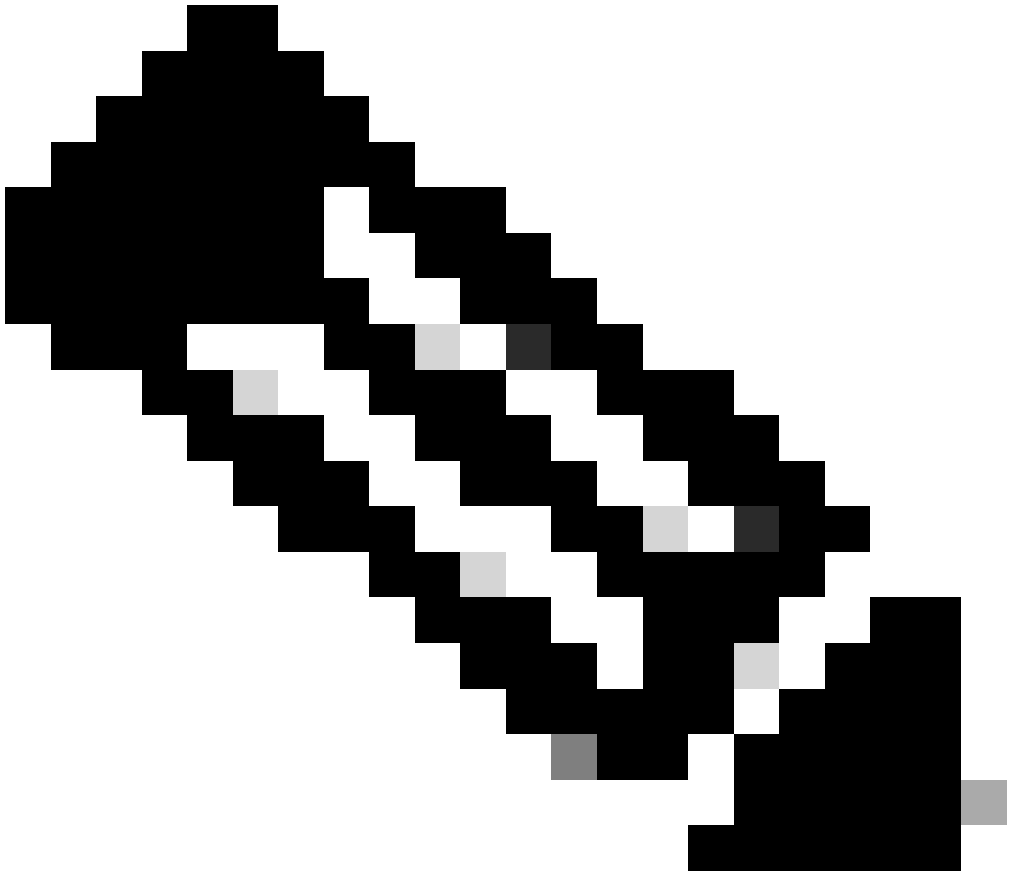
- Questa è un'indicazione di un problema dell'adattatore dell'utente finale. Lo switch invia pacchetti in formato non corretto che lo switch riconosce come indirizzi mac di origine casuali.

Piano d'azione

- Configurare "authentication host-mode multi-domain" che consente solo 2 indirizzi mac.
- Identificare e isolare il dispositivo responsabile.

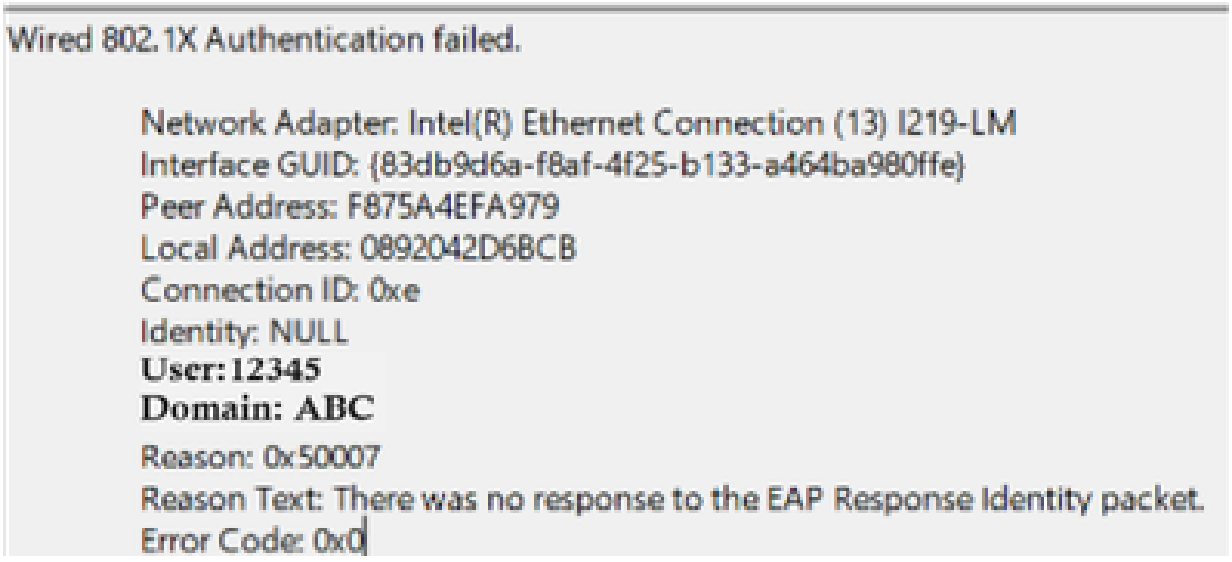
Risoluzione/verifica

- Dopo aver configurato questa soluzione, non si osserverà alcun problema.



- Nota: abilitare la sicurezza della porta o la modalità host della sessione di autenticazione Dot1x a più domini.

Scenario 5 - MTU non corrispondente



ISE rappresenta questo errore sul server.

Descrizione del problema:

- I computer utente ricevono l'indirizzo IP APIPA e la connettività dell'utente è compromessa.

Sintomi utente

1. Il client finale invia una risposta EAP con una lunghezza del pacchetto superiore a (ad esempio, 3736) la lunghezza prevista effettiva del pacchetto, pari a 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
```

Risoluzione dei problemi eseguita

- L'MTU è impostata su un valore inferiore sullo switch come voce a livello di sistema. (Esempio: 1998 byte)
- Interfaccia in uscita configurata con dimensioni maggiori. (Esempio: 9198byte)

Isolare

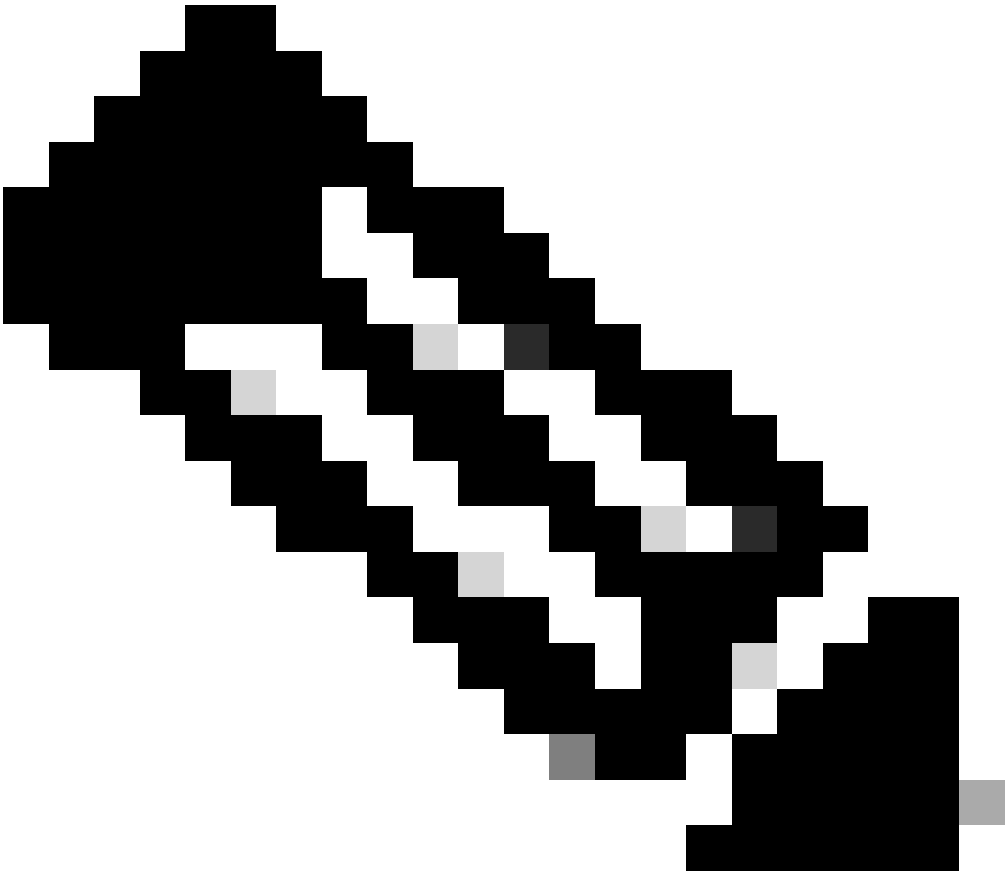
- Il problema è causato da una mancata corrispondenza dell'MTU nel percorso.

Piano d'azione

- Modificare l'MTU del sistema a 1500 e ricaricare lo switch

Risoluzione/verifica

- Dopo aver configurato queste impostazioni, l'autenticazione ha esito positivo.



- Nota: accertarsi di abilitare la stessa MTU per tutto il percorso del flusso di pacchetto.

Scenario 6 - Protezione IPDT

Descrizione del problema:

- I computer utente ricevono l'indirizzo IP APIPA e la connettività dell'utente è compromessa.

Sintomi utente

- Se si dispone di VM in HA, nell'interfaccia viene applicato questo criterio:

criterio di rilevamento dispositivi IPDT_POLICY

nessun protocollo udp

attivazione tracciamento

- Dopo un failover, la risposta ARP viene eliminata dallo switch di accesso.

Risoluzione dei problemi eseguita

1. Le risposte ARP alle sonde verrebbero scartate da uno switch.
2. Lo switch è configurato con IPDT Guard.
3. IPDT - Protezione nella caduta della sonda ARP e dispositivo terminale nell'acquisizione di APIPA.

Isolare

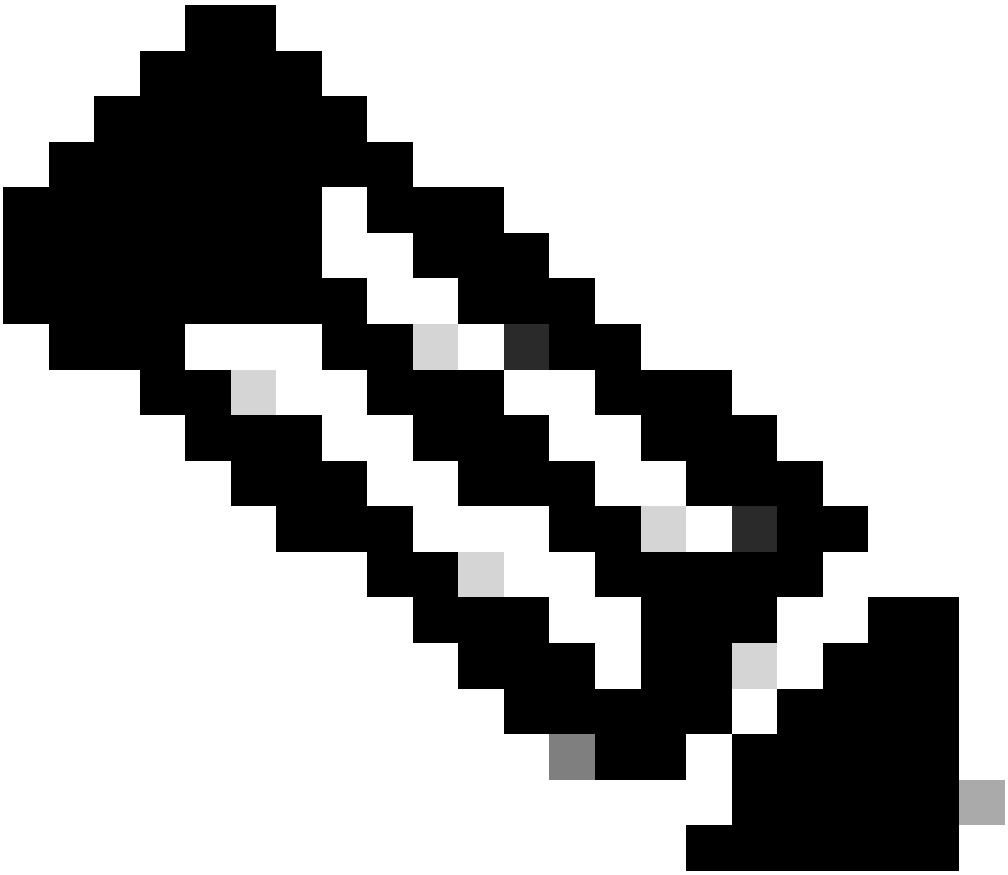
- I pacchetti di sonda ARP che raggiungono IPDT vengono scartati a causa della funzione Guard.
- Il criterio IPDT configurato con la configurazione 'security-level guard' rifiuta i pacchetti ARP rendendo irraggiungibili pochi o tutti i dispositivi terminali

Piano d'azione

- Modificate l'impostazione da Guardia (Guard) a Guancia (Glean).
  Configurare 'glean a livello di protezione' nel criterio IPDT

Risoluzione/verifica

- Dopo aver configurato le impostazioni di glean, le sonde ARP vengono elaborate dal processo ARP & il problema viene risolto.



- Nota: si tratta di un difetto noto che verrebbe risolto nella versione 17.15.1 e successive.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).