Risoluzione dei problemi di connettività del client DHCP su un Cisco 9800 WLC

Sommario

Introduzione

In questo documento vengono descritti vari problemi relativi al protocollo DHCP (Dynamic Host Configuration Protocol) incontrati dai client wireless quando sono connessi a un Cisco 9800 Wireless LAN Controller (WLC) e viene spiegato come risolverli.

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base di Cisco WLC 9800
- Conoscenze base di flusso DHCP

- Conoscenze base dei punti di accesso in modalità di connessione locale e flessibile

Informazioni sul flusso del traffico DHCP con client wireless

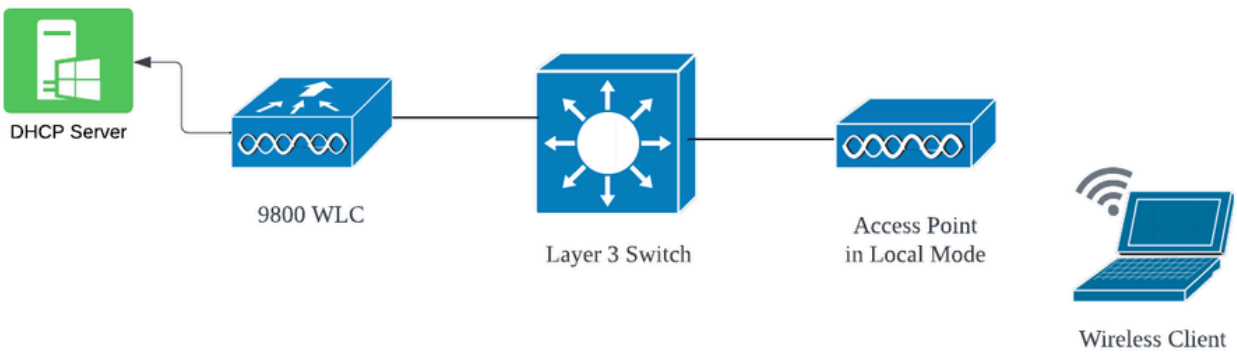
Quando il client wireless si connette, esegue il normale scambio DHCP inviando un frame di rilevamento DHCP broadcast per trovare un server DHCP al punto di accesso associato. A seconda della modalità di funzionamento dell'access point, la richiesta verrà inoltrata al WLC tramite il tunnel CAPWAP o passata direttamente all'hop successivo. Se un server DHCP è disponibile all'interno del dominio locale di layer 2, risponderà, facilitando una connessione riuscita. In assenza di un server DHCP subnet locale, il router (configurato con la SVI del client) deve essere configurato in modo da instradare il rilevamento DHCP al server appropriato. A tale scopo, in genere viene configurato un indirizzo helper IP sul router, che indica di inoltrare il traffico UDP specifico del broadcast (ad esempio le richieste DHCP) a un indirizzo IP predeterminato.

Il comportamento del traffico DHCP del client dipende interamente dalla modalità di funzionamento del punto di accesso. Esaminiamo ciascuno di questi scenari separatamente:

Scenario 1. Il punto di accesso funziona in modalità locale

Quando un access point è configurato in modalità locale, il traffico DHCP del client viene commutato centralmente, ossia le richieste DHCP dei client vengono inviate tramite un tunnel CAPWAP dal router AP al WLC, dove vengono quindi elaborate e inoltrate di conseguenza. In questo caso, è possibile scegliere tra due opzioni: utilizzare un server DHCP interno o scegliere un server DHCP esterno.

Topologia (punto di accesso in modalità locale)



Topologia di rete: punto di accesso in modalità locale

Studio del caso 1. Quando WLC è configurato come server DHCP interno

Il controller è in grado di offrire un server DHCP interno tramite le funzionalità integrate del software Cisco IOS XE. Tuttavia, si consiglia di utilizzare un server DHCP esterno. Prima di configurare il WLC come server DHCP interno, è necessario soddisfare alcuni prerequisiti, elencati di seguito:

- Configurare un'interfaccia virtuale commutata (SVI) per la VLAN client e assegnare ad essa l'indirizzo IP del server DHCP.
- L'indirizzo IP del server DHCP interno deve essere impostato sull'interfaccia del server, che può essere un'interfaccia di loopback, una SVI o un'interfaccia fisica di layer 3.
- Si consiglia di configurare l'interfaccia di loopback perché, a differenza delle interfacce fisiche che si connettono a segmenti di rete effettivi, l'interfaccia di loopback non è legata all'hardware e non corrisponde a una porta fisica sul dispositivo. Lo scopo principale di un'interfaccia di loopback è fornire un'interfaccia stabile e sempre attiva che non sia soggetta a guasti hardware o disconnessioni fisiche.

Configurazione in esecuzione: di seguito è riportato un esempio di configurazione interna del server DHCP in cui i client hanno ricevuto correttamente gli indirizzi IP. Di seguito sono riportati i registri operativi e i dettagli di installazione associati.

Configurare il WLC come server DHCP per la VLAN 10, con un ambito DHCP compreso tra 10.106.10.11/24 e 10.106.10.50/24.

```
WLC#show run | sec dhcp
ip dhcp excluded-address 10.106.10.0 10.106.10.10
ip dhcp excluded-address 10.106.10.51 10.106.10.255
ip dhcp pool vlan_10_Pool
network 10.106.10.0 255.255.255.0
lease 0 8
```

Interfaccia loopback configurata sul WLC:

```
WLC#show run interface loopback 0
interface Loopback0
ip address 10.10.10.25 255.255.255.0
end
```

VLAN client configurata come SVI [Interfaccia L3] con indirizzo helper come interfaccia di loopback sul WLC:

<#root>

```
WLC#show run int vlan10
ip address 10.106.10.10 255.255.255.0
ip helper-address 10.10.10.25 [helper address can be loopback interface, Wireless management interface
end
```

In alternativa, è possibile impostare l'indirizzo IP del server DHCP all'interno del profilo della policy, anziché configurare un indirizzo di supporto nella SVI. Tuttavia, si consiglia in genere di configurare questa configurazione per singola VLAN in modo da ottimizzare le procedure:

```
configure terminal
wireless profile policy $Policy_Profile_name
ipv4 dhcp required
ipv4 dhcp server $WMI_IP
```

Tracce radioattive sul WLC:

```
2024/03/29 13:28:06.502389611 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/29 13:28:06.502515811 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:06.502614149 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/29 13:28:06.502674118 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.505719129 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/29 13:28:08.505787349 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:08.505834315 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.543149257 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/29 13:28:08.543254480 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:08.543334850 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/29 13:28:08.543407760 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.543910482 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/29 13:28:08.543968250 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/29 13:28:08.544135443 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/29 13:28:08.544314185 {wncd_x_R0-0}{1}: [client-iplearn] [23608]: (note): MAC: Client_MAC Clien
```

Embedded Packet Capture sul WLC:

```
1401 18:58:06.501972 0.0.0.0          255.255.255.255    DHCP    348 DHCP Discover - Transaction ID 0x7030bf99
1402 18:58:06.501972 10.106.10.10     10.10.10.25        DHCP    344 DHCP Discover - Transaction ID 0x7030bf99
1403 18:58:06.501972 10.106.10.10     10.10.10.25        DHCP    344 DHCP Discover - Transaction ID 0x7030bf99
1429 18:58:08.504963 10.106.10.10     10.106.10.10       DHCP    342 DHCP Offer    - Transaction ID 0x7030bf99
1430 18:58:08.504963 10.106.10.10     10.106.10.10       DHCP    342 DHCP Offer    - Transaction ID 0x7030bf99
1431 18:58:08.504963 10.106.10.10     255.255.255.255    DHCP    346 DHCP Offer    - Transaction ID 0x7030bf99
1432 18:58:08.504963 10.106.10.10     255.255.255.255    DHCP    416 DHCP Offer    - Transaction ID 0x7030bf99
1433 18:58:08.542971 0.0.0.0          255.255.255.255    DHCP    452 DHCP Request  - Transaction ID 0x7030bf99
1434 18:58:08.542971 0.0.0.0          255.255.255.255    DHCP    374 DHCP Request  - Transaction ID 0x7030bf99
1435 18:58:08.542971 10.106.10.10     10.10.10.25        DHCP    370 DHCP Request  - Transaction ID 0x7030bf99
1436 18:58:08.542971 10.106.10.10     10.10.10.25        DHCP    370 DHCP Request  - Transaction ID 0x7030bf99
1437 18:58:08.542971 10.106.10.10     10.106.10.10       DHCP    342 DHCP ACK      - Transaction ID 0x7030bf99
1438 18:58:08.542971 10.106.10.10     10.106.10.10       DHCP    342 DHCP ACK      - Transaction ID 0x7030bf99
1439 18:58:08.543962 10.106.10.10     255.255.255.255    DHCP    346 DHCP ACK      - Transaction ID 0x7030bf99
1440 18:58:08.543962 10.106.10.10     255.255.255.255    DHCP    416 DHCP ACK      - Transaction ID 0x7030bf99
```

Embedded Packet Capture su WLC

Debug del client AP:

```
Mar 29 13:28:05 kernel: [*03/29/2024 13:28:05.7183] [1711718885:718317] [AP_NAME] [Client_MAC] <apr0v2>
Mar 29 13:28:05 kernel: [*03/29/2024 13:28:05.7184] [1711718885:718428] [[AP_NAME] [Client_MAC] <wired0
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7223] [1711718887:722360] [[AP_NAME] [Client_MAC] <wired0
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7224] chatter: dhcp_reply_nonat: 1711718887.722379604: 10
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7225] [1711718887:722524] [AP_NAME] [Client_MAC] <apr0v2>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7591] [1711718887:759139] [AP_NAME] [Client_MAC] <apr0v2>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7592] [1711718887:759248] [AP_NAME] [Client_MAC] <wired0>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7606] [1711718887:760687] [AP_NAME] [Client_MAC] <wired0>
Mar 29 13:28:07 kernel: [*03/29/2024 13:28:07.7607] [1711718887:760780] [AP_NAME] [Client_MAC] <apr0v2>
```

Acquisizione pacchetti lato client:

```
122 07:11:56.202853 0.0.0.0          255.255.255.255   DHCP   344 DHCP Discover - Transaction ID 0x595044d4
129 07:11:58.217331 10.106.10.10     255.255.255.255   DHCP   342 DHCP Offer    - Transaction ID 0x595044d4
130 07:11:58.219406 0.0.0.0          255.255.255.255   DHCP   370 DHCP Request  - Transaction ID 0x595044d4
131 07:11:58.227525 10.106.10.10     255.255.255.255   DHCP   342 DHCP ACK      - Transaction ID 0x595044d4
```

Client End Packet Capture

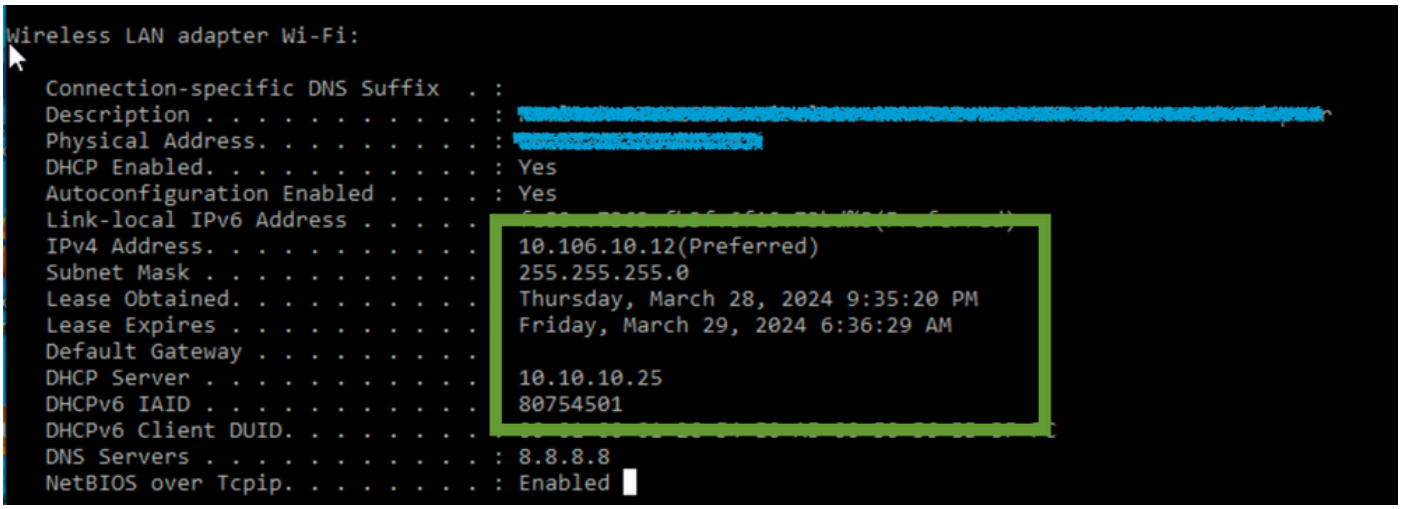
Nei log operativi forniti, è possibile vedere che il WLC riceve il messaggio DHCP Discover dal client wireless e la VLAN del client lo sta inoltrando all'indirizzo dell'helper (nell'esempio riportato è l'interfaccia di loopback interna). A seguito di questa operazione, il server interno invia un'offerta DHCP e, di conseguenza, il client invia una richiesta DHCP, che viene quindi riconosciuta dal server con un ACK DHCP.

Verifica dell'indirizzo IP del client wireless:

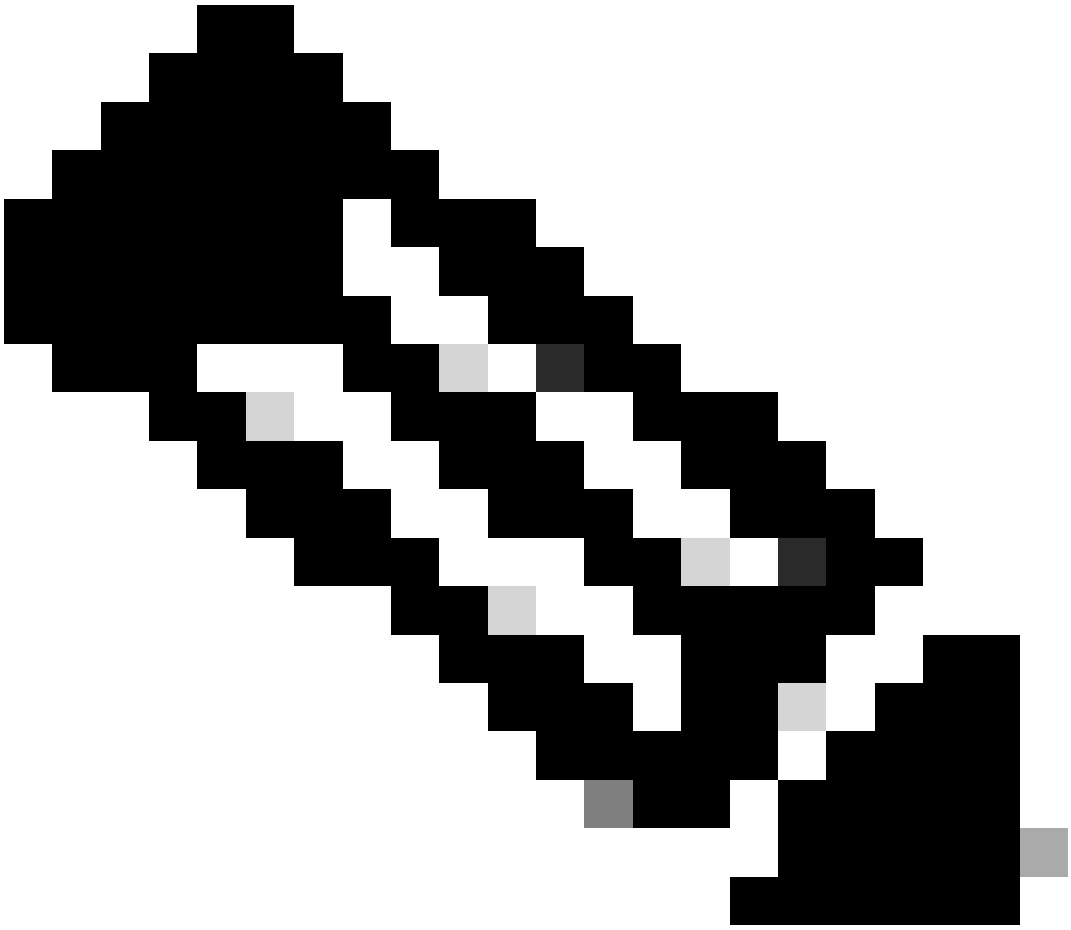
Sul WLC:

```
WLC#show ip dhcp binding
Bindings from all pools not associated with VRF:
IP address        Client-ID/Hardware address      Lease expiration                 Type         State
10.106.10.12     aaaa.aaaa.aaaa                    Mar 29 2024 10:58 PM      Automatic     Active     L
```

Sul client wireless:



Verifica IP sull'estremità client



Nota:
1. VRF non è supportato nei server DHCP interni.
2. DHCPv6 non è supportato nei server DHCP interni.

---

3. Su C9800, la SVI consente di configurare più indirizzi dell'helper, ma vengono utilizzati solo i primi due.
4. Questa funzionalità è stata testata e pertanto è supportata su tutte le piattaforme per un massimo del 20% della scala client massima della confezione. Ad esempio, per un 9800-80 che supporta 64.000 client, il numero massimo di binding DHCP supportati è circa 14.000.

Studio del caso 2. Se si utilizza un server DHCP esterno

Per server DHCP esterno si intende un server DHCP non integrato nello stesso WLC, ma configurato su un dispositivo di rete diverso [firewall, router] o su un'entità distinta all'interno dell'infrastruttura di rete. Questo server è dedicato alla gestione della distribuzione dinamica degli indirizzi IP e di altri parametri di configurazione di rete ai client della rete.

Quando si usa un server DHCP esterno, la funzione del WLC è solo di ricevere e inoltrare il traffico. Il modo in cui il traffico DHCP viene instradato dal WLC, sia esso broadcast o unicast, varia a seconda delle preferenze. Consideriamo ciascuno di questi metodi separatamente.

Traffico DHCP trasmesso nel dominio di livello 2

In questa configurazione, un altro dispositivo di rete, ad esempio un firewall, un uplink o un core switch, funge da agente di inoltro. Quando un client invia una richiesta di rilevamento DHCP, l'unico compito del WLC è inoltrare la trasmissione tramite l'interfaccia di layer 2. Per un corretto funzionamento, è necessario verificare che l'interfaccia di layer 2 della VLAN client sia configurata correttamente e autorizzata tramite la porta dati del WLC e il dispositivo uplink.

Configurazione desiderata sull'estremità WLC per la VLAN client 20 per questa istanza:

VLAN di layer 2 configurata sul WLC:

```
WLC#show run vlan 20
vlan 20
name Client_vlan
end
```

Porta dati configurata sul WLC per consentire il traffico della VLAN client:

```
WLC#show run int tw0/0/0
interface TwoGigabitEthernet0/0/0
switchport trunk allowed vlan 10,20,58
switchport mode trunk
negotiation auto
end
```

Radioactive Traces su 9800 WLC:

```
2024/03/30 10:40:43.114800606 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.114863170 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.121515725 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.121583319 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.132967882 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: IPv6 DHCP from intf
2024/03/30 10:40:43.132999148 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: IPv6 DHCP from intf
2024/03/30 10:40:43.146521529 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/30 10:40:43.146605773 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.146685159 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.149359205 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.149419477 {wncd_x_R0-0}{1}: [client-orch-sm] [23608]: (ERR): MAC: DHCP_Server_MAC V
2024/03/30 10:40:43.149534985 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.149685174 {wncd_x_R0-0}{1}: [client-iplearn] [23608]: (note): MAC: Client_MAC Clien
```

Embedded Packet Capture acquisita su 9800 WLC:

```
    187 16:10:43.113992 0.0.0.0           255.255.255.255      DHCP     424 DHCP Discover - Transaction ID 0xa1a4f5eb
    188 16:10:43.113992 0.0.0.0           255.255.255.255      DHCP     346 DHCP Discover - Transaction ID 0xa1a4f5eb
    189 16:10:43.113992 0.0.0.0           255.255.255.255      DHCP     346 DHCP Discover - Transaction ID 0xa1a4f5eb
    190 16:10:43.113992 0.0.0.0           255.255.255.255      DHCP     346 DHCP Discover - Transaction ID 0xa1a4f5eb
    192 16:10:43.120980 10.106.20.10      255.255.255.255      DHCP     346 DHCP Offer    - Transaction ID 0xa1a4f5eb
    193 16:10:43.120980 10.106.20.10      255.255.255.255      DHCP     346 DHCP Offer    - Transaction ID 0xa1a4f5eb
    194 16:10:43.120980 10.106.20.10      255.255.255.255      DHCP     346 DHCP Offer    - Transaction ID 0xa1a4f5eb
    195 16:10:43.120980 10.106.20.10      255.255.255.255      DHCP     416 DHCP Offer    - Transaction ID 0xa1a4f5eb
    201 16:10:43.145988 0.0.0.0           255.255.255.255      DHCP     452 DHCP Request  - Transaction ID 0xa1a4f5eb
    202 16:10:43.145988 0.0.0.0           255.255.255.255      DHCP     374 DHCP Request  - Transaction ID 0xa1a4f5eb
    203 16:10:43.145988 0.0.0.0           255.255.255.255      DHCP     374 DHCP Request  - Transaction ID 0xa1a4f5eb
    204 16:10:43.145988 0.0.0.0           255.255.255.255      DHCP     374 DHCP Request  - Transaction ID 0xa1a4f5eb
    205 16:10:43.148979 10.106.20.10      255.255.255.255      DHCP     346 DHCP ACK      - Transaction ID 0xa1a4f5eb
    206 16:10:43.148979 10.106.20.10      255.255.255.255      DHCP     346 DHCP ACK      - Transaction ID 0xa1a4f5eb
    207 16:10:43.148979 10.106.20.10      255.255.255.255      DHCP     346 DHCP ACK      - Transaction ID 0xa1a4f5eb
    208 16:10:43.148979 10.106.20.10      255.255.255.255      DHCP     416 DHCP ACK      - Transaction ID 0xa1a4f5eb
```

Embedded Packet Capture su WLC

Debug del client AP:

```
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3650] [1711796737:183177] [AP_NAME] [Client_MAC] <apr0v2>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3651] [1711796737:184281] [[AP_NAME] [Client_MAC] <wired0
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3465] [1711796737:185404 [[AP_NAME] [Client_MAC] <wired0>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3465] chatter: dhcp_reply_nonat: 1711796737.459745189: 10
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3670] [1711796737:195085] [AP_NAME] [Client_MAC] <apr0v2>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3683] [1711796737:368344] [AP_Name] [Client_Mac] <apr0v1>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3684] [1711796737:368439] [AP_Name] [Client_Mac] <wired0>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3931] [1711796737:393131] [AP_Name] [Client_Mac] <apr0v1>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.3932] [1711796737:393250] [AP_Name] [Client_Mac] <wired0>
Mar 30 11:05:37 kernel: [*03/30/2024 11:05:37.4597] [1711796737:459726] [AP_Name] [Client_Mac] <wired0>
```

Acquisizione sul lato client:

```
  3 03:17:46.193239 0.0.0.0          255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x56883262
 31 03:17:50.649855 0.0.0.0          255.255.255.255    DHCP    342 DHCP Discover - Transaction ID 0x56883262
 34 03:17:53.259282 10.106.20.10     255.255.255.255    DHCP    342 DHCP Offer    - Transaction ID 0x56883262
 35 03:17:53.259282 10.106.20.10     255.255.255.255    DHCP    342 DHCP Offer    - Transaction ID 0x56883262
 36 03:17:53.262280 0.0.0.0          255.255.255.255    DHCP    370 DHCP Request  - Transaction ID 0x56883262
 37 03:17:53.273130 10.106.20.10     255.255.255.255    DHCP    342 DHCP ACK      - Transaction ID 0x56883262
```

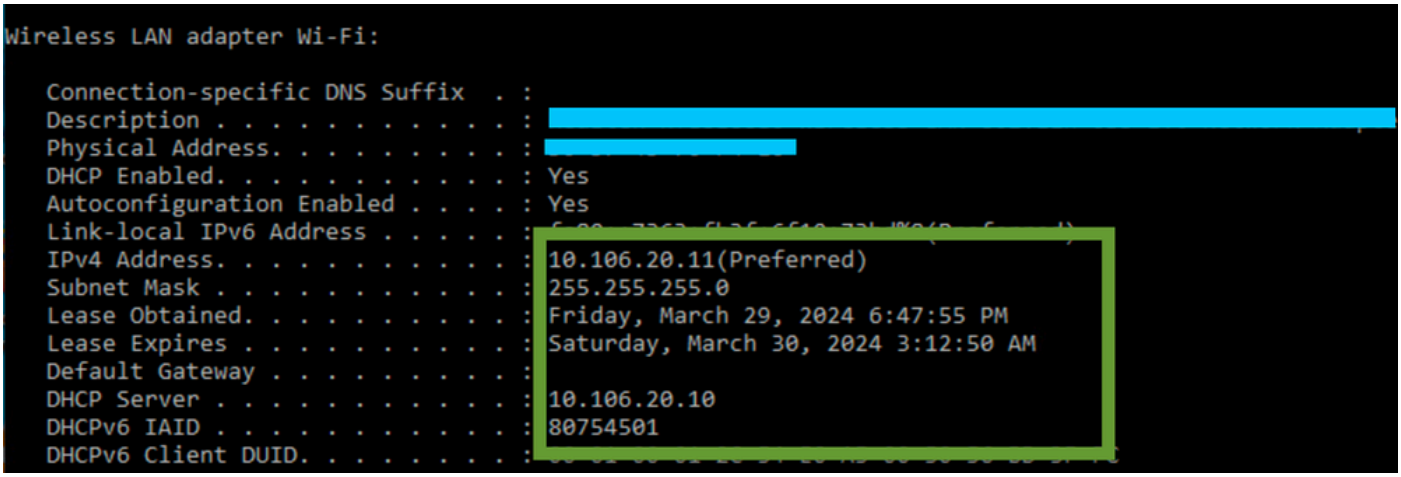
Client End Packet Capture

Nei log operativi forniti, si nota che il WLC sta intercettando la trasmissione Discover del protocollo DHCP dal client wireless e quindi la sta trasmettendo all'hop successivo tramite l'interfaccia L2. Non appena il WLC riceve l'offerta DHCP dal server, inoltra questo messaggio al client seguito da richiesta DHCP e ACK.

Verifica dell'indirizzo IP del client wireless:

È possibile controllare il lease IP sul server DHCP e lo stato corrispondente.

Sul client wireless:



Verifica IP sull'estremità client

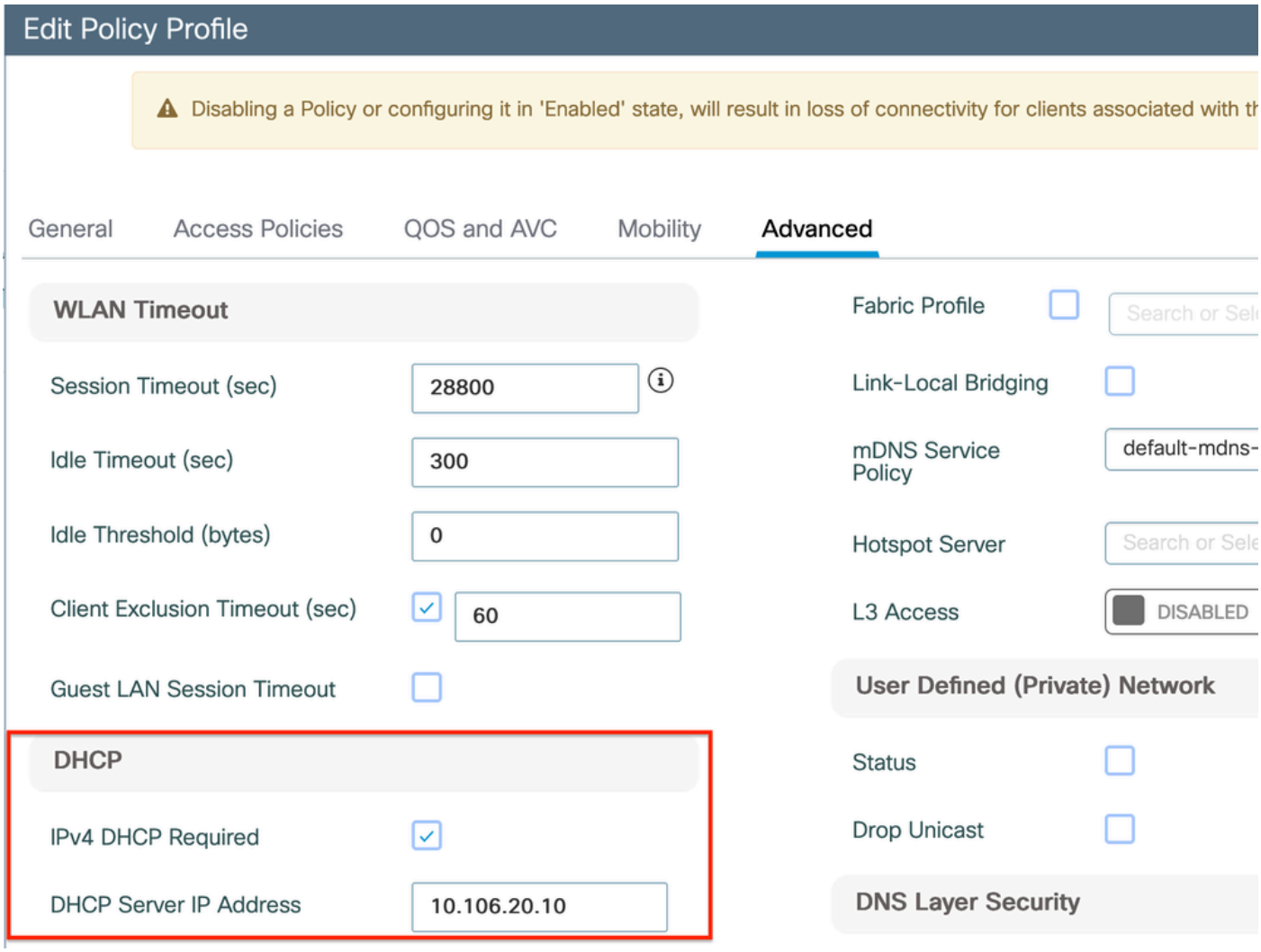
9800 WLC funziona come agente di inoltro

In questa configurazione, il WLC inoltra direttamente i pacchetti DHCP ricevuti dai client wireless al server DHCP in modalità unicast. Per abilitare questa funzionalità, verificare che la VLAN SVI per il client sia configurata sul WLC.

Ci sono 2 modi per configurare l'IP del server DHCP in 9800 WLC:

1. Configurare l'indirizzo IP del server DHCP nel profilo dei criteri in Impostazioni avanzate.

Tramite GUI: Passare a Configuration > Tags & Profile > Policy > Policy_name > Advanced. Sotto la sezione DHCP è possibile configurare l'indirizzo IP del server DHCP come mostrato:



Impostazione del profilo dei criteri sul WLC

Via CLI:

```
configure terminal
wireless profile policy $Policy_Profile_name
ipv4 dhcp required
ipv4 dhcp server $DHCP_Server_IP
```

2. Nella configurazione SVI, è necessario specificare l'indirizzo dell'helper. Configurando più server DHCP nella configurazione dell'indirizzo dell'helper è possibile fornire ridondanza. Anche se è possibile impostare l'indirizzo del server DHCP per ciascuna WLAN all'interno del profilo della policy, l'approccio consigliato è configurarlo per singola interfaccia. A tale scopo, è possibile assegnare un indirizzo dell'helper alla SVI corrispondente.

Quando si utilizza la funzione di inoltro, l'origine del traffico DHCP è l'indirizzo IP dell'interfaccia virtuale commutata (SVI) del client. Il traffico viene quindi indirizzato attraverso l'interfaccia corrispondente alla destinazione (indirizzo IP del server DHCP), come determinato dalla tabella di routing.

Di seguito è riportato un esempio della configurazione di lavoro su 9800 che funge da agente di inoltro:

Interfaccia di layer 3 configurata per VLAN client su WLC con indirizzo dell'helper:

```
WLC#show run int vlan 20
interface vlan 20
ip address 10.106.20.1 255.255.255.0
ip helper-address 10.106.20.10
end
```

Porta dati configurata sul WLC per consentire il traffico della VLAN client:

```
WLC#show run int tw0/0/0
interface TwoGigabitEthernet0/0/0
switchport trunk allowed vlan 10,20,58
switchport mode trunk
negotiation auto
end
```

Tracce RA dal WLC:

```
2024/03/30 13:46:38.549504590 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:38.549611716 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/30 13:46:38.549666984 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.597696305 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.597778465 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.597829829 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.598444184 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.598506350 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.598544420 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.621660873 {wncd_x_R0-0}{1}: [auth-mgr-feat_dsensor] [23608]: (info): [Client_MAC:ca
2024/03/30 13:46:41.621771405 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.621851320 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.621908730 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.625257607 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 relay src_ip:
2024/03/30 13:46:41.625329089 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 13:46:41.625490562 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 13:46:41.625655045 {wncd_x_R0-0}{1}: [client-iplearn] [23608]: (note): MAC: Client_MAC Client
```

Embedded Packet Capture su WLC:

No.	Time	Source	Destination	Protocol	Lengtr	Info
462	19:16:34.544969	0.0.0.0	255.255.255.255	DHCP	424	DHCP Discover - Transaction ID 0x137ea7ac
463	19:16:34.545961	10.106.20.1	10.106.20.10	DHCP	346	DHCP Discover - Transaction ID 0x137ea7ac
594	19:16:38.548967	0.0.0.0	255.255.255.255	DHCP	424	DHCP Discover - Transaction ID 0x137ea7ac
595	19:16:38.548967	10.106.20.1	10.106.20.10	DHCP	346	DHCP Discover - Transaction ID 0x137ea7ac
647	19:16:41.596953	10.106.20.10	10.106.20.1	DHCP	346	DHCP Offer - Transaction ID 0x137ea7ac
648	19:16:41.596953	10.106.20.1	255.255.255.255	DHCP	416	DHCP Offer - Transaction ID 0x137ea7ac
649	19:16:41.597961	10.106.20.10	10.106.20.1	DHCP	346	DHCP Offer - Transaction ID 0x137ea7ac
650	19:16:41.597961	10.106.20.1	255.255.255.255	DHCP	416	DHCP Offer - Transaction ID 0x137ea7ac
653	19:16:41.620954	0.0.0.0	255.255.255.255	DHCP	452	DHCP Request - Transaction ID 0x137ea7ac
654	19:16:41.620954	10.106.20.1	10.106.20.10	DHCP	374	DHCP Request - Transaction ID 0x137ea7ac
655	19:16:41.624967	10.106.20.10	10.106.20.1	DHCP	346	DHCP ACK - Transaction ID 0x137ea7ac
656	19:16:41.624967	10.106.20.1	255.255.255.255	DHCP	416	DHCP ACK - Transaction ID 0x137ea7ac

Embedded Packet Capture su WLC

In entrambe le versioni Radioactive Traces (RA) e Embedded Packet Capture (EPC) sul WLC, il WLC, in qualità di agente di inoltro, invia direttamente i pacchetti DHCP dal client al server DHCP.

Debug del client AP:

```
Mar 30 13:46:37 kernel: [*03/30/2024 13:46:37.7476] [1711806397:747677] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:37 kernel: [*03/30/2024 13:46:37.7481] [1711806397:748177] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7973] chatter: dhcp_reply_nonat: 1711806400.797214204: 10
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7973] [1711806400:797362] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7978] [1711806400:797870] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.7979] [1711806400:797903] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8204] [1711806400:820455] [AP_Name] [Client_MAC] <apr0v1>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8205] [1711806400:820550] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8248] [1711806400:824829] [AP_Name] [Client_MAC] <wired0>
Mar 30 13:46:40 kernel: [*03/30/2024 13:46:40.8249] [1711806400:824911] [AP_Name] [Client_MAC] <apr0v1>
```

Acquisizione sul lato client:

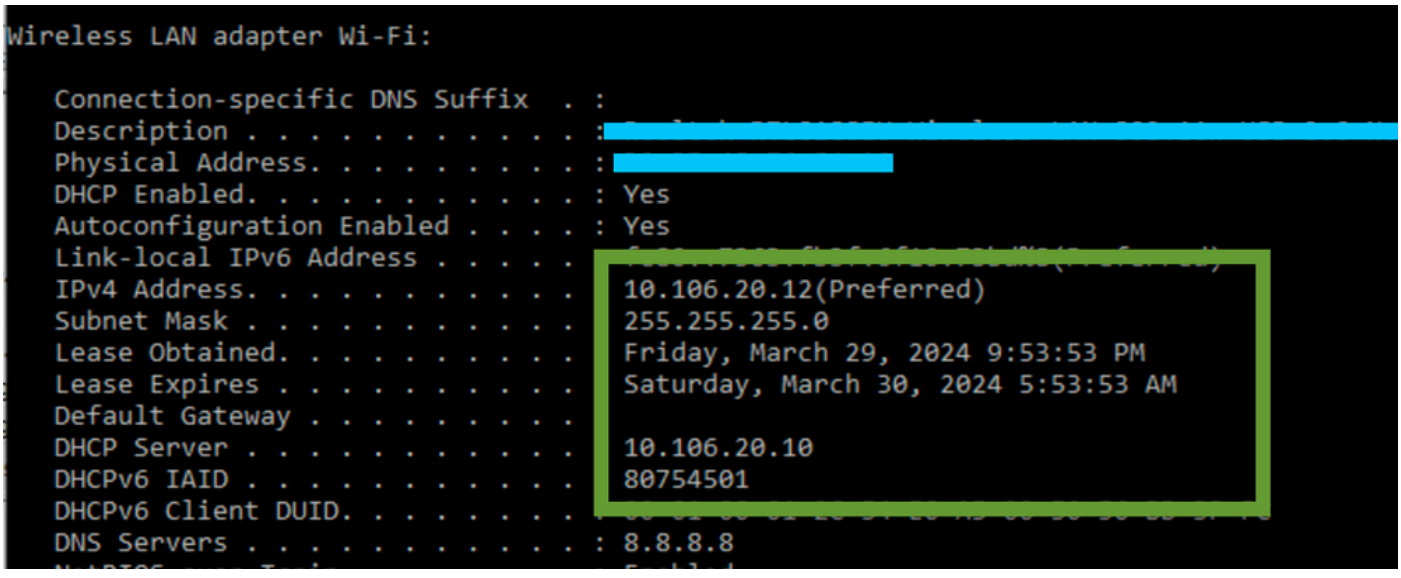
No.	Time	Source	Destination	Protocol	Length	Info
1	10:23:46.630692	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
50	10:23:50.627940	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
59	10:23:53.694541	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x137ea7ac
60	10:23:53.696530	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0x137ea7ac
61	10:23:53.698634	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x137ea7ac
62	10:23:53.737816	10.106.20.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x137ea7ac

Client End Packet Capture

Verifica dell'indirizzo IP del client wireless:

È possibile controllare il lease IP sul server DHCP e lo stato corrispondente.

Sul client wireless:



Verifica IP sull'estremità client

Opzione DHCP 80 con opzione secondaria 5/150 in 9800 WLC

In alcuni scenari, si potrebbe preferire definire esplicitamente l'interfaccia di origine per il traffico DHCP piuttosto che dipendere dalla tabella di routing, per evitare potenziali complicazioni alla rete. Ciò è particolarmente importante quando il dispositivo di rete successivo sul percorso, come uno switch di layer 3 o un firewall, utilizza i controlli Reverse Path Forwarding (RPF). Ad esempio, una situazione in cui l'interfaccia di gestione wireless è impostata sulla VLAN 50, mentre la SVI del client è sulla VLAN 20 e viene utilizzata come inoltro DHCP per il traffico del client. Il percorso predefinito è diretto al gateway della VLAN/subnet di gestione wireless.

A partire dalla versione 17.03.03 sul WLC 9800, è possibile scegliere l'interfaccia di origine per il traffico DHCP come VLAN client o un'altra VLAN, ad esempio WMI (Wireless Management Interface), che garantisce la connettività al server DHCP.

Di seguito viene riportato un elemento della configurazione:

```
!
interface vlan 50
 description Wireless Management
 ip address 10.100.16.10 255.255.255.0
!
interface vlan 20
 description Wireless_Client_vlan
 ip address 192.168.4.2 255.255.255.0
 ip helper-address 10.100.17.14
!
ip route 0.0.0.0 0.0.0.0 10.100.16.1
```

In questo scenario, il traffico verso il server DHCP 10.100.17.14 verrà originato dalla VLAN 50 (10.100.16.10), in quanto l'interfaccia di uscita del pacchetto viene selezionata in base a una ricerca nella tabella di routing IP e in genere uscirebbe dalla VLAN Wireless Management Interface (WMI) a causa della route predefinita configurata.
Tuttavia, se uno switch uplink implementa i controlli di inoltro di percorso inverso (RPF), potrebbe ignorare un pacchetto in arrivo dalla VLAN 50 ma con un indirizzo IP di origine appartenente a una subnet diversa [VLAN 20].

Per evitare questo problema, impostare un'interfaccia di origine precisa per i pacchetti DHCP con il comando IP DHCP relay source-interface. In questo caso specifico, si desidera che i pacchetti DHCP provengano dall'interfaccia WMI sulla VLAN 50:

```
interface vlan 20
 description Wireless_Client_vlan=
 ip address 192.168.4.2 255.255.255.0
 ip helper-address 10.100.17.14
 ip dhcp relay source-interface vlan 50
```

Quando si usa ip dhcp relay source-interface questo comando, sia l'interfaccia di origine dei pacchetti DHCP che il comando GIADDR vengono impostati sull'interfaccia specificata nel comando relay DHCP (VLAN50, in questo caso). Questo è un problema, in quanto non è la VLAN client a cui si desidera assegnare gli indirizzi DHCP.

In che modo il server DHCP sa come assegnare l'indirizzo IP dal pool di client corretto?

La risposta è che quando si usa ip dhcp relay source-interface il comando, C9800 aggiunge automaticamente le informazioni sulla subnet del client in una sottoopzione proprietaria 150 dell'opzione 82 chiamata selezione del collegamento, come mostrato nell'immagine:

```
Relay agent IP address: 10.100.16.10
Client MAC address: [redacted]
Client hardware address padding: 00000000000000000000
Server host name not given
Boot file name not given
Magic cookie: DHCP
> Option: (53) DHCP Message Type (Discover)
> Option: (55) Parameter Request List
> Option: (57) Maximum DHCP Message Size
> Option: (61) Client identifier
> Option: (51) IP Address Lease Time
v Option: (82) Agent Information Option
    Length: 6
  v Option 82 Suboption: (150) Link selection (Cisco proprietary) (192.168.4.2)
      Length: 4
      Link selection (Cisco proprietary): 192.168.4.2
```

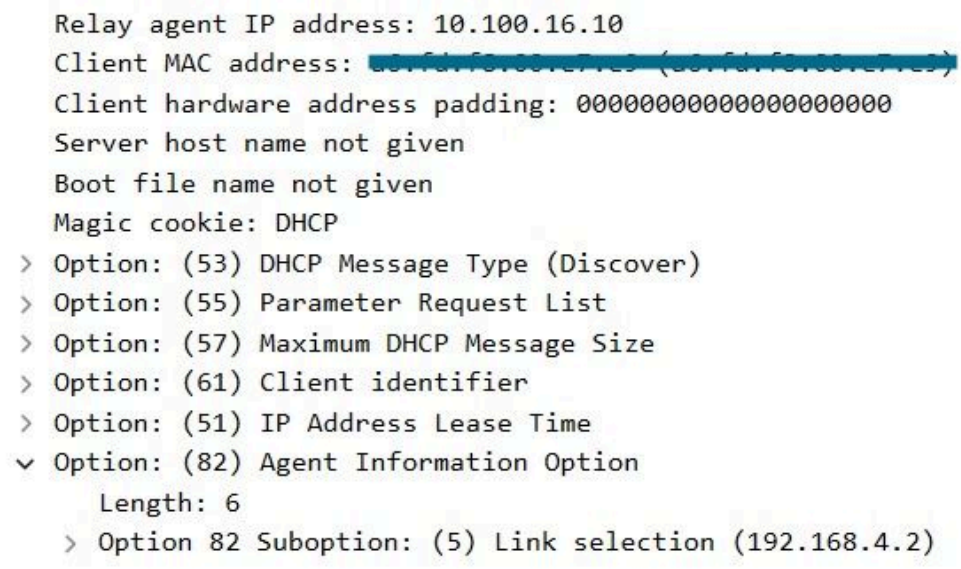
Option 182 suboption 150 su WLC Packet Capture

Per impostazione predefinita, viene aggiunta la sottoopzione 150 (proprietà cisco). Accertarsi che il server DHCP utilizzato sia in grado di interpretare e agire in base a queste informazioni. Si consiglia di modificare la configurazione del C9800 in modo da utilizzare l'opzione standard 82 e l'opzione secondaria 5 per inviare le informazioni di selezione del collegamento. A tale scopo, è possibile configurare il comando globale seguente:

<#root>

```
C9800(config)#ip dhcp compatibility suboption link-selection standard
```

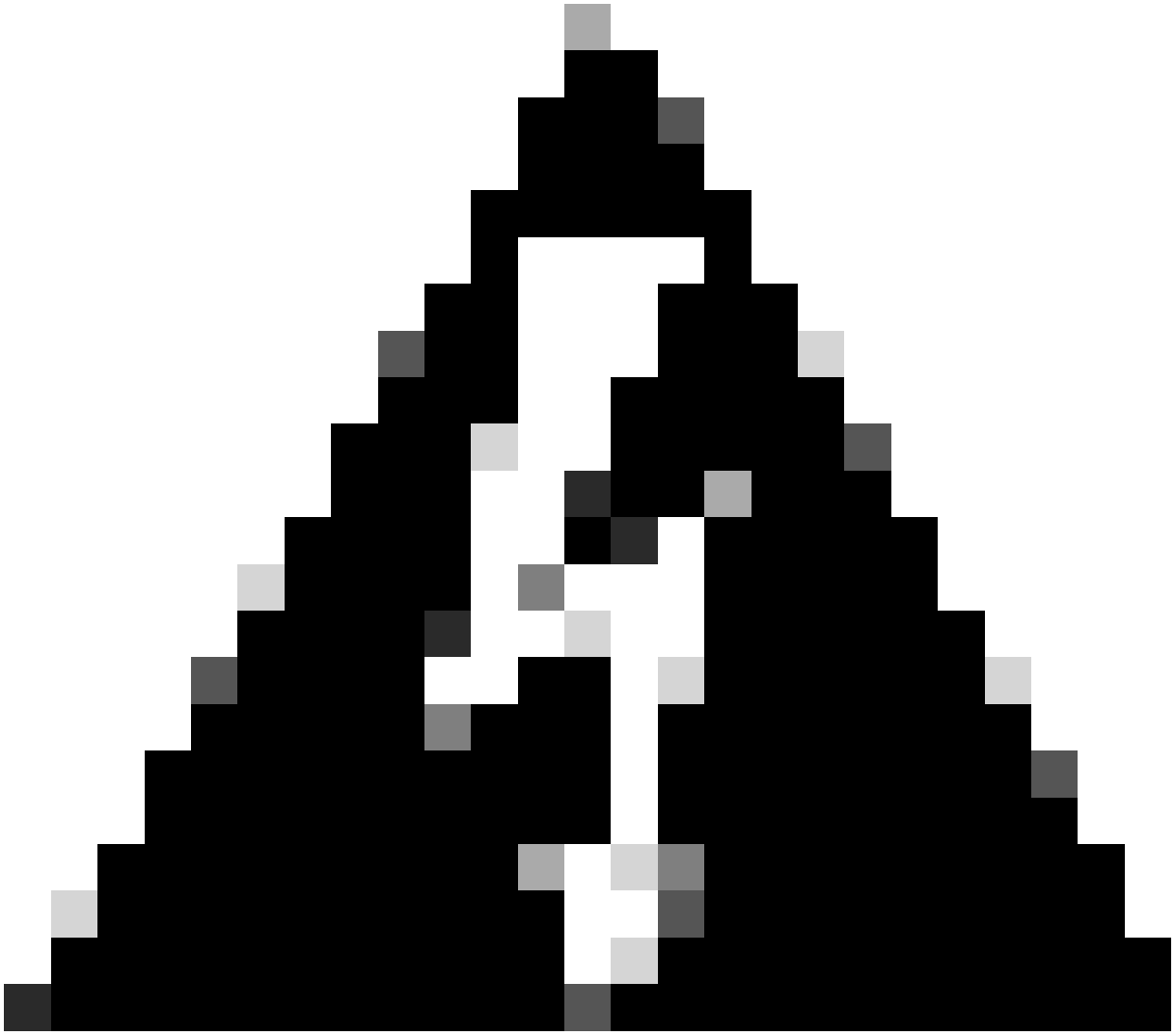
Una volta applicato il comando specificato, il sistema sostituirà l'opzione secondaria 150 con l'opzione secondaria 5 nei pacchetti DHCP. La sottoopzione 5 è riconosciuta più diffusamente dai dispositivi di rete, pertanto è possibile che i pacchetti vengano scartati con minore probabilità. L'applicazione di questa modifica è evidente anche nell'acquisizione fornita:



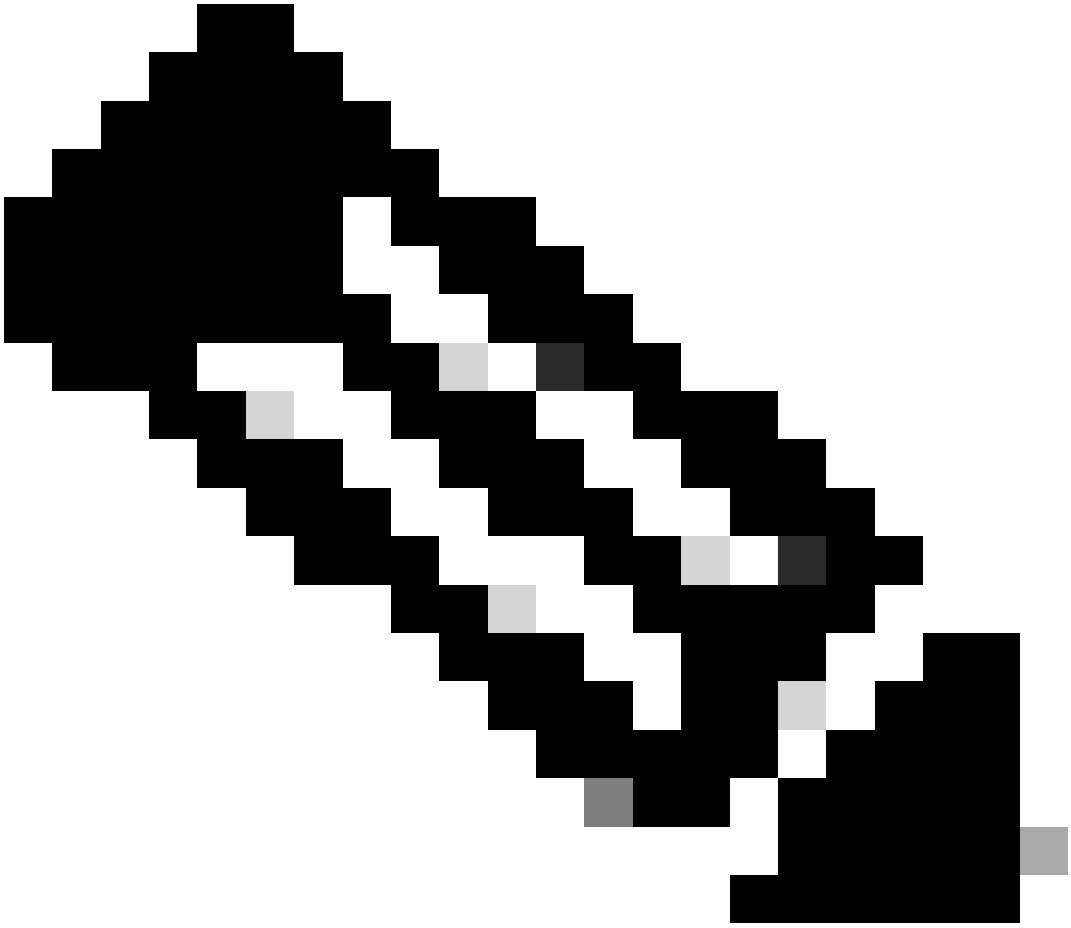
Opzione 182, opzione secondaria 5, sull'acquisizione del pacchetto WLC

Con l'implementazione dell'opzione secondaria 5, il traffico DHCP deve essere riconosciuto da altri dispositivi di rete. Tuttavia, è possibile che vengano ancora visualizzati messaggi NAK (negative acknowledgement), in particolare quando il server DHCP Windows è in uso. Ciò si può verificare perché il server DHCP non autorizza l'indirizzo IP di origine, probabilmente perché non dispone di una configurazione corrispondente per tale indirizzo IP di origine.

Quali operazioni è necessario eseguire sul server DHCP? Per il server DHCP Windows, è necessario creare un ambito fittizio per autorizzare l'indirizzo IP dell'agente di inoltro.



Avviso: tutti gli indirizzi IP degli agenti di inoltro (GIADDR) devono far parte di un intervallo di indirizzi IP di ambito DHCP attivo. Tutti i GIADDR al di fuori degli intervalli di indirizzi IP dell'ambito DHCP vengono considerati un relay non autorizzato e il server DHCP Windows non riconosce le richieste del client DHCP da tali agenti di inoltro. È possibile creare un ambito speciale per autorizzare gli agenti di inoltro. Creare un ambito con il comando GIADDR (o più indirizzi se i GIADDR sono indirizzi IP sequenziali), escludere gli indirizzi GIADDR dalla distribuzione, quindi attivare l'ambito. In questo modo verranno autorizzati gli agenti di inoltro, ma non verrà consentita l'assegnazione degli indirizzi GIADDR.

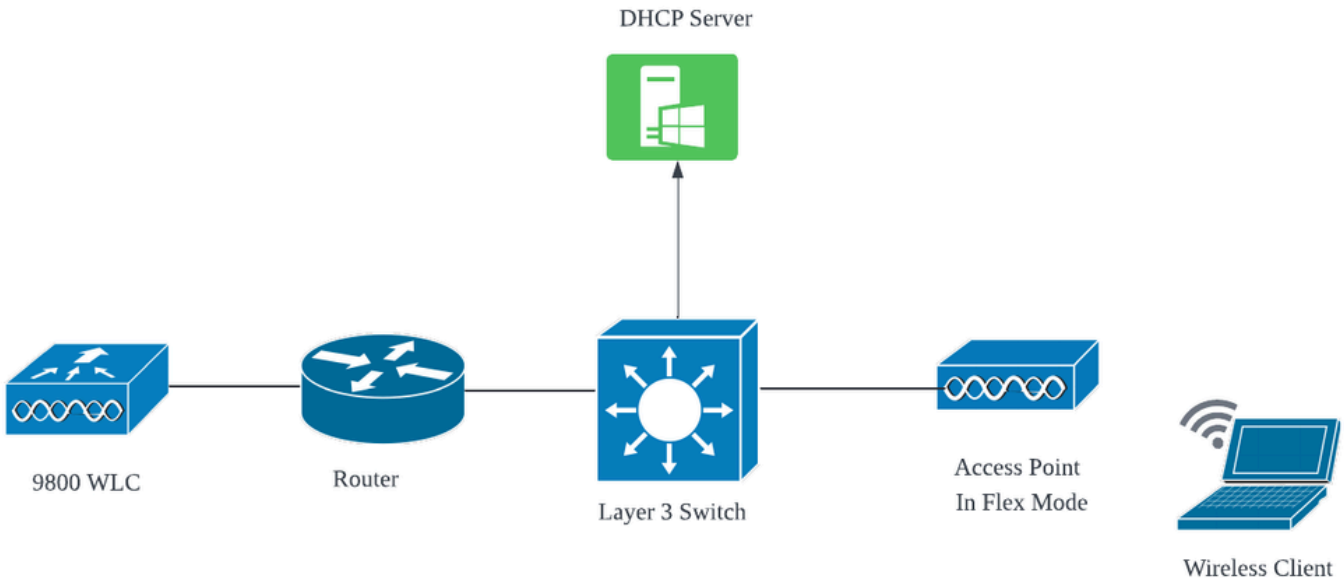


Nota: in una configurazione con ancoraggio esterno, il traffico DHCP viene elaborato centralmente con la modalità AP impostata su Locale. Inizialmente, le richieste DHCP vengono inviate al WLC esterno, che le inoltra quindi al WLC di ancoraggio tramite un tunnel per la mobilità. È il WLC di ancoraggio che gestisce il traffico in base alle sue impostazioni configurate. Pertanto, tutte le configurazioni correlate a DHCP devono essere implementate sul WLC di ancoraggio.

Scenario 2. L'access point funziona in modalità Flex

I punti di accesso FlexConnect sono progettati per filiali e uffici remoti, consentendo loro di operare in modalità standalone quando perdono la connettività al controller WLC (Wireless LAN Controller) centrale. I punti di accesso FlexConnect possono commutare localmente il traffico tra un client e la rete senza dover eseguire il backhaul del traffico verso il WLC. Ciò riduce la latenza e mantiene la larghezza di banda della WAN. Nell'access point in modalità flex il traffico DHCP può essere commutato a livello centrale o locale.

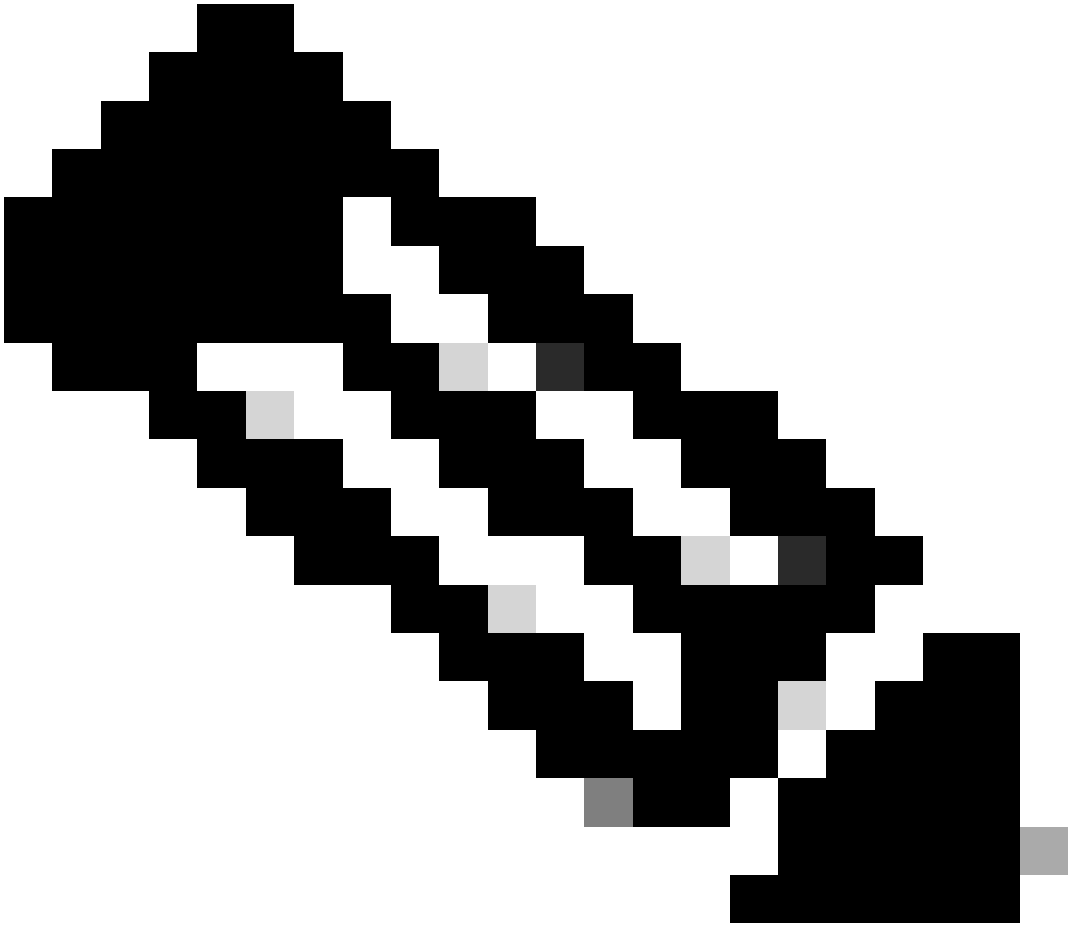
Topologia (Flex Mode AP)



Topologia di rete: punto di accesso in modalità Flex

AP modalità FlexConnect con DHCP centrale

Indipendentemente dalla modalità AP, la configurazione, il flusso operativo e le procedure di risoluzione dei problemi rimangono coerenti quando si utilizza un server DHCP centrale. Tuttavia, per i punti di accesso in modalità FlexConnect, in genere si consiglia di utilizzare un server DHCP locale a meno che non si disponga di una SVI client impostata sul sito locale.



Nota: se sul sito remoto non è disponibile una subnet client, è possibile utilizzare FlexConnect NAT-PAT. FlexConnect NAT/PAT esegue NAT (Network Address Translation) per il traffico proveniente dai client connessi all'access point, associandolo all'indirizzo IP di gestione dell'access point. Ad esempio, se i punti di accesso sono in funzione in modalità FlexConnect in sedi distaccate remote e i client connessi devono comunicare con un server DHCP che si trova nella sede centrale in cui risiedono i controller, è possibile attivare FlexConnect NAT/PAT insieme all'impostazione DHCP centrale nel profilo della policy.

AP modalità FlexConnect con DHCP locale

Quando un access point FlexConnect è configurato per utilizzare il protocollo DHCP locale, i dispositivi client associati all'access point ricevono la configurazione dell'indirizzo IP da un server DHCP disponibile nella stessa rete locale. Il server DHCP locale può essere un router, un server DHCP dedicato o qualsiasi altro dispositivo di rete che fornisce servizi DHCP nella subnet locale. Con il protocollo DHCP locale, il traffico DHCP viene commutato all'interno della rete locale, ossia il punto di accesso inoltra le richieste DHCP dei client direttamente all'hop adiacente, ad esempio il commutatore di accesso. Le richieste vengono quindi gestite in base alla configurazione della rete.

Prerequisito:

1. Consultare la guida di FlexConnect per verificare che la configurazione sia in linea con le istruzioni e le best practice descritte nella guida.

2. La VLAN client deve essere elencata nel profilo flessibile.
3. L'access point deve essere configurato in modalità trunk, con la VLAN di gestione dell'access point designata come VLAN nativa, e le VLAN per il traffico dei client devono essere autorizzate sul trunk.

Di seguito è riportato un esempio di configurazione della porta dello switch connesso al punto di accesso con la VLAN di gestione a 58 e la VLAN del client a 20:

```
Switch#show run int gig1/0/2
!
interface GigabitEthernet1/0/2
switchport trunk allowed vlan 20,58
switchport trunk encapsulation dot1q
switchport trunk native vlan 58
switchport mode trunk
end
!
```

Configurazione di lavoro: per la condivisione dei registri operativi con il server DHCP locale quando il punto di accesso è configurato per la modalità flex:

Debug del client AP:

```
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6056] [1712144373:605628] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6057] chatter: dhcp_req_local_sw_nonat: 1712144373.6056478
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6058] [1712144373:605830] [AP_Name] [client_mac] <wired0>
Apr 3 11:39:33 kernel: [*04/03/2024 11:39:33.6058] chatter: dhcp_reply_nonat: 1712144373.605647862: 0.0
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.7462] [1712144376:746192] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9149] chatter: dhcp_from_inet: 1712144376.914892705: 10.10
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9150] chatter: dhcp_reply_nonat: 1712144376.914892705: 10.
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9151] [1712144376:915159] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9161] [1712144376:916101] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9373] [1712144376:937350] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9645] [1712144376:964530] [AP_Name] [client_mac] <apr0v1>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9646] chatter: dhcp_req_local_sw_nonat: 1712144376.9645492
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9647] [1712144376:964749] [AP_Name] [client_mac] <wired0>
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9736] CLSM[client_mac]: client moved from IPLEARN_PENDING
Apr 3 11:39:36 kernel: [*04/03/2024 11:39:36.9736] [1712144376:973687] [AP_Name] [client_mac] <apr0v1>
```

Acquisizione uplink AP:

1399	18:37:…	0.0.0.0	255.255.255.255	DHCP	420	DHCP Discover - Transaction ID 0xb530583d
1400	18:37:…	0.0.0.0	255.255.255.255	DHCP	420	DHCP Discover - Transaction ID 0xb530583d
1499	18:37:…	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0xb530583d
1500	18:37:…	0.0.0.0	255.255.255.255	DHCP	420	DHCP Discover - Transaction ID 0xb530583d
1545	18:38:…	10.106.20.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xb530583d
1546	18:38:…	10.106.20.10	255.255.255.255	DHCP	420	DHCP Offer - Transaction ID 0xb530583d
1547	18:38:…	10.106.20.10	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0xb530583d
1548	18:38:…	10.106.20.10	255.255.255.255	DHCP	420	DHCP Offer - Transaction ID 0xb530583d
1553	18:38:…	0.0.0.0	255.255.255.255	DHCP	370	DHCP Request - Transaction ID 0xb530583d
1555	18:38:…	0.0.0.0	255.255.255.255	DHCP	448	DHCP Request - Transaction ID 0xb530583d
1556	18:38:…	10.106.20.10	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0xb530583d
1558	18:38:…	10.106.20.10	255.255.255.255	DHCP	420	DHCP ACK - Transaction ID 0xb530583d

Acquisizione uplink AP

Acquisizione sul lato client:

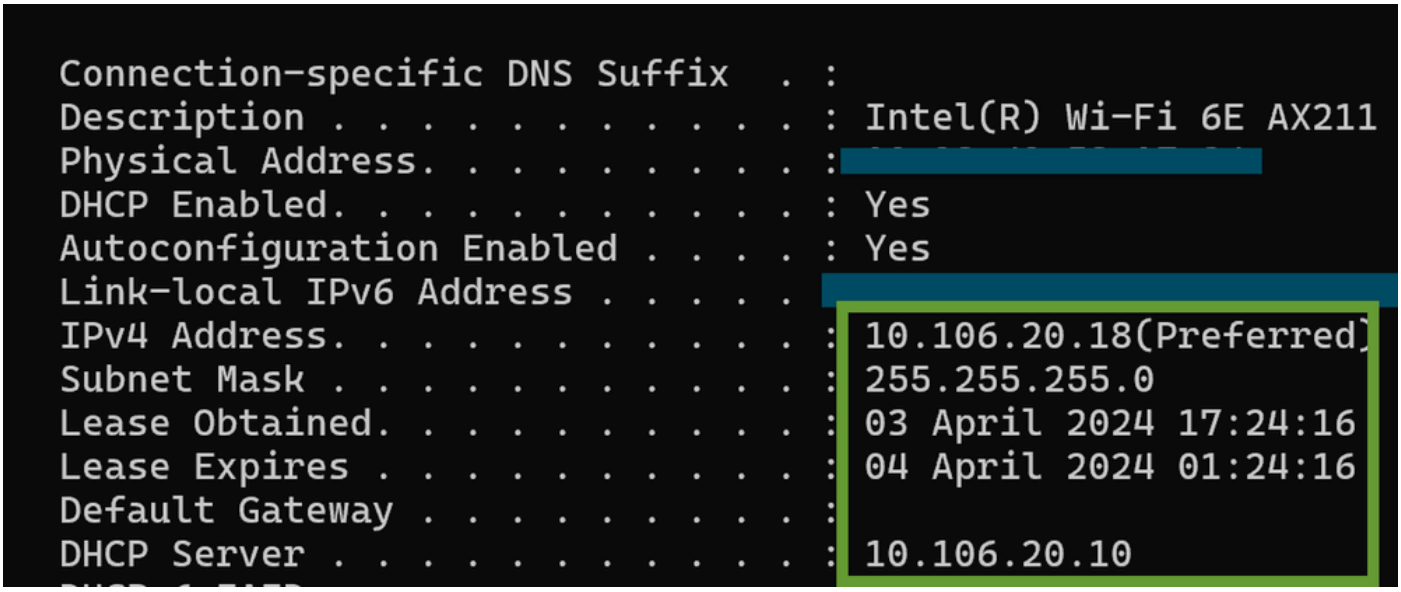
```
16540 111.905836    0.0.0.0           255.255.255.255      DHCP      343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10      10.106.20.18         DHCP      342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0           255.255.255.255      DHCP      385 DHCP Request  - Transaction ID 0x628c01b4
16543 112.304391    10.106.20.10      10.106.20.18         DHCP      342 DHCP ACK      - Transaction ID 0x628c01b4
```

Client End Packet Capture

Verifica dell'indirizzo IP del client wireless:

È possibile controllare il lease IP sul server DHCP e lo stato corrispondente.

Sul client wireless:



Verifica IP sull'estremità client

Risoluzione dei problemi relativi a DHCP

La risoluzione dei problemi DHCP implica l'identificazione e la risoluzione dei problemi che impediscono ai client di ottenere un indirizzo IP da un server DHCP quando sono connessi alla rete wireless. Di seguito sono riportati alcuni passaggi comuni e alcune considerazioni relative alla risoluzione dei problemi DHCP:

1. Verifica della configurazione client

- Verificare che il client sia configurato per ottenere automaticamente un indirizzo IP.
- Verificare che la scheda di rete sia abilitata e funzioni correttamente.

2. Controllare lo stato del server DHCP

- Verificare che il server DHCP sia operativo e raggiungibile dal segmento di rete del client.
- Verificare l'indirizzo IP, la subnet mask e le impostazioni predefinite del gateway del server DHCP.

3. Verifica configurazione ambito

- Esaminare l'ambito DHCP per verificare che disponga di un intervallo di indirizzi IP sufficiente per i client.
- Verificare la durata del lease e le opzioni dell'ambito, ad esempio server DNS e gateway predefinito
- In alcuni ambienti, ad esempio Active Directory, verificare che il server DHCP sia autorizzato a fornire servizi DHCP all'interno della rete.

4. Esaminare la configurazione del WLC 9800

- Sono stati rilevati molti problemi dovuti a una configurazione errata, ad esempio un'interfaccia di loopback mancante, una SVI del client o l'assenza di un indirizzo dell'helper configurato. Prima di raccogliere i log, si consiglia di verificare che la configurazione sia stata implementata correttamente.
- Quando si utilizza un server DHCP interno: per quanto riguarda l'esaurimento dell'ambito DHCP, è importante assicurarsi, in particolare quando si configura DHCP tramite la CLI, che il timer di lease sia configurato in base alle proprie esigenze. Per impostazione predefinita, il timer di lease è impostato su infinite su 9800 WLC.
- Verificare che il traffico VLAN del client sia autorizzato sulla porta uplink WLC quando si utilizza un server DHCP centrale. Al contrario, quando si usa un server DHCP locale, verificare che la VLAN pertinente sia consentita sulla porta di uplink del punto di accesso.

5. Impostazioni firewall e protezione

- Verificare che i firewall o il software di sicurezza non blocchino il traffico DHCP (porta 67 per il server DHCP e porta 68 per il client DHCP).

Raccolta log

Log da WLC

1. Abilitare l'indicatore orario del prompt di esecuzione dei termini per disporre di un riferimento temporale per tutti i comandi.

2. Utilizzare show tech-support wireless !! per rivedere la configurazione

2. È possibile controllare il numero di client, la distribuzione dello stato del client e i client esclusi.
show wireless summary !! Numero totale di punti di accesso e client
show wireless exclusionlist !! Nel caso in cui un client venga considerato escluso
show wireless exclusionlist client mac-address MAC@ !! per ottenere ulteriori dettagli su client concreti esclusi e verificare se il motivo è elencato come furto IP per qualsiasi client.

3. Controllare l'assegnazione degli indirizzi IP dei client, cercare indirizzi non corretti o informazioni impreviste sull'indirizzo statico, VLAN contrassegnate come danneggiate perché il server DHCP non risponde o pacchetti ignorati in SISF che gestisce DHCP/ARP.

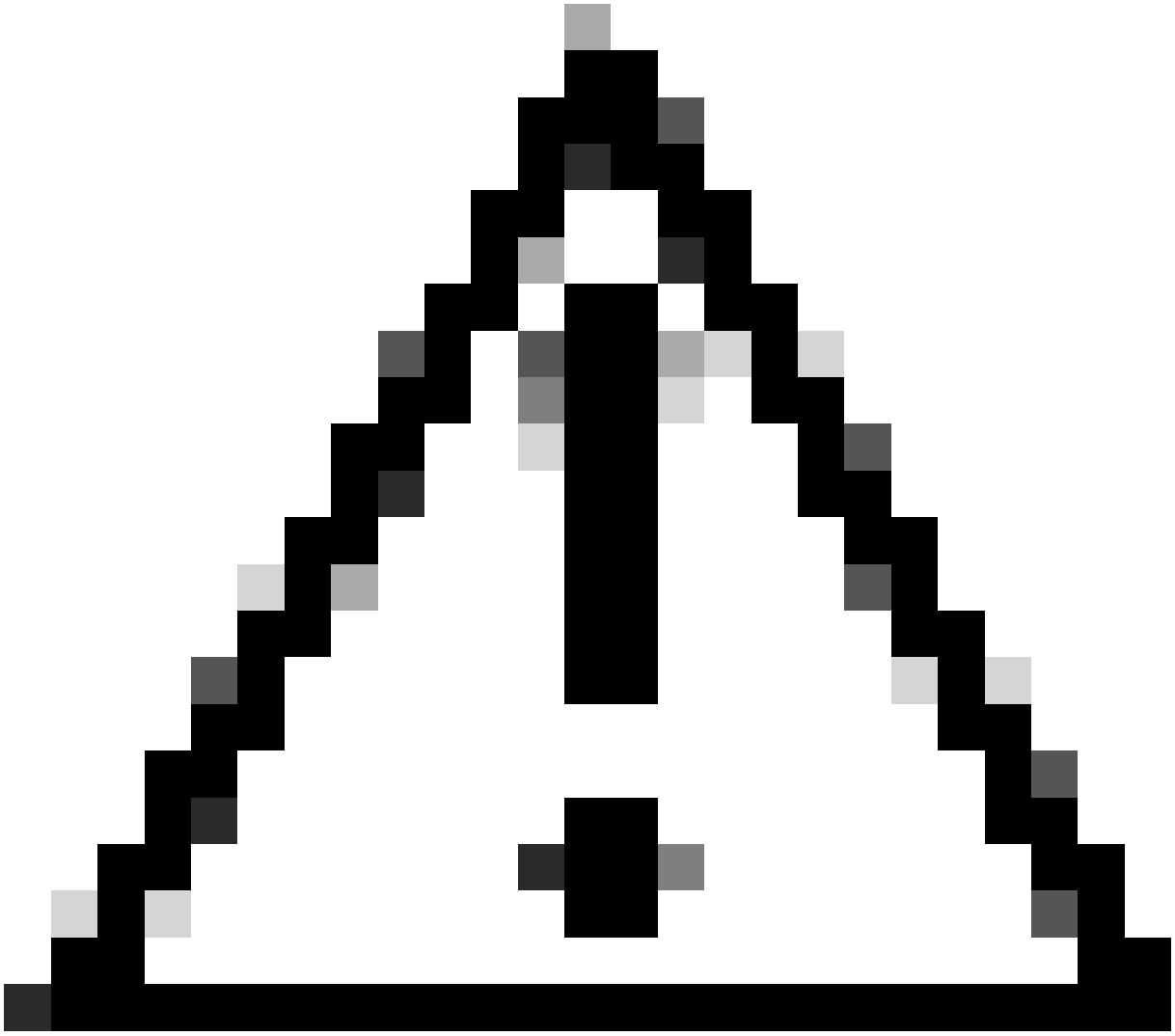
show wireless device-tracking database ip !! Controllare tramite IP e verificare come si è verificato l'apprendimento degli indirizzi:
show wireless device-tracking database mac !! Controllare da Mac e vedere quale client IP è assegnato.
show wireless vlan details !! Verificare che la VLAN non sia contrassegnata come dirty a causa di errori DHCP in caso di gruppo VLAN in uso.
show wireless device-tracking feature drop !!Cadute nel SISF

4. Uscite specifiche dal WLC per MAC@ client concreto show wireless device-tracking feature drop

Abilitare la traccia radioattiva per l'indirizzo MAC del client quando il client tenta di connettersi alla rete wireless.

Via CLI:

debug wireless {mac | ip} {aaaa.bbbb.cccc | x.x.x.x } {monitor-time} {N seconds} !! Setting time allows us to enable traces for up to 24 days
!!Reproduce [Clients should stuck in IP learn]
no debug wireless mac <Client_MAC>
!!WLC generates a debug trace file with Client_info, command to check for debug trace file generated.
dir bootflash: | i debug



Attenzione: il debug condizionale abilita la registrazione a livello di debug che a sua volta aumenta il volume dei log generati. Se si lascia attiva questa opzione, si riduce il tempo di visualizzazione dei log. Si consiglia pertanto di disattivare sempre il debug al termine della sessione di risoluzione dei problemi.

Per disabilitare tutte le operazioni di debug, eseguire i seguenti comandi:

```
# clear platform condition all
# undebug all
```

Tramite GUI:

Passaggio 1. Passa a Troubleshooting > Radioactive Trace .
Passaggio 2. Fare clic su Add e immettere l'indirizzo Mac del client per il quale si desidera risolvere il problema. È possibile aggiungere diversi indirizzi Mac da tracciare.

Passaggio 3. Quando si è pronti per avviare la traccia radioattiva, fare clic su Avvia. Una volta avviato, il log di debug viene scritto su disco in relazione a qualsiasi elaborazione del control plane correlata agli indirizzi MAC tracciati.

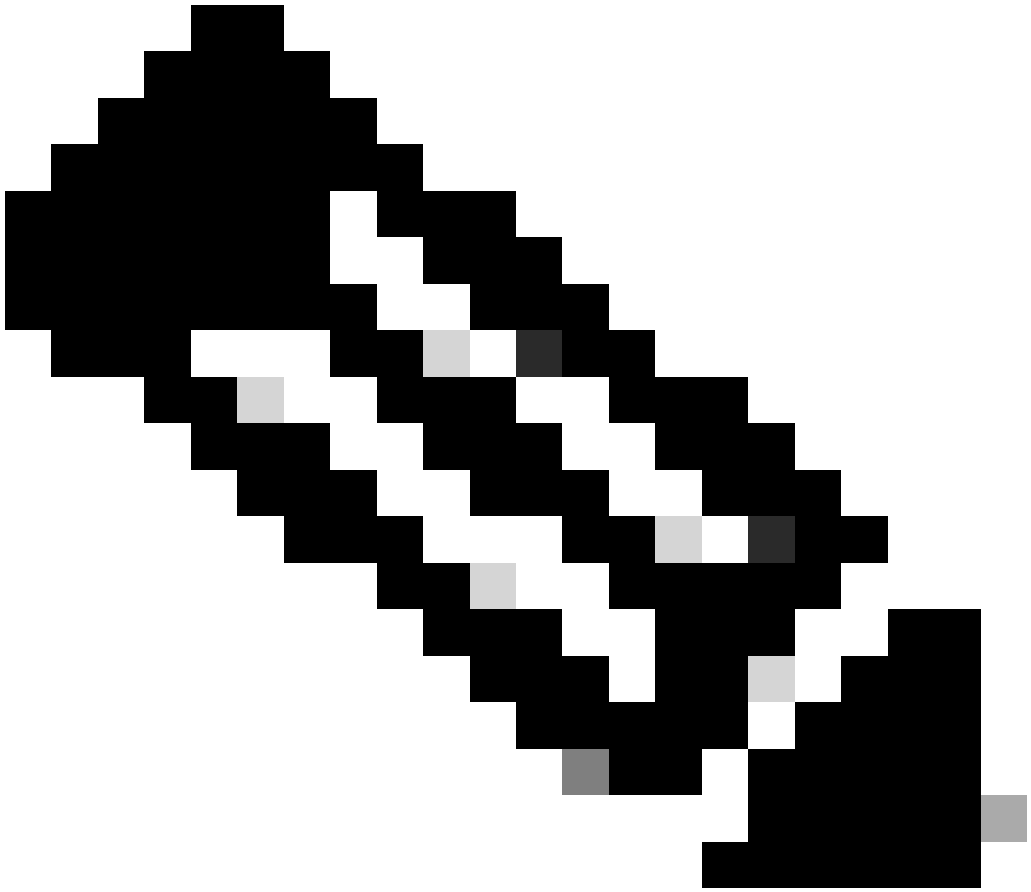
Passaggio 4. Quando si riproduce il problema che si desidera risolvere, fare clic su Stop .

Passaggio 5. Per ogni indirizzo mac sottoposto a debug, è possibile generare un file di log che fascicola tutti i log relativi a tale indirizzo mac facendo clic su Generate .

Passaggio 6. Scegliere il periodo di tempo che deve trascorrere prima che il file di registro fascicolato venga completato e fare clic su Applica al dispositivo.

Passaggio 7. È ora possibile scaricare il file facendo clic sull'icona accanto al nome del file. Questo file è presente nell'unità flash di avvio del controller e può anche essere copiato dalla CLI.

!!Embedded Acquisizioni filtrate per indirizzo MAC del client in entrambe le direzioni. Filtro MAC interno del client disponibile dopo la versione 17.1.



Nota: EPC su 9800 sarà utile quando DHCP centrale è abilitato su 9800 WLC.

Via CLI:

monitor capture MYCAP clear
monitor capture MYCAP interface Po1 both
monitor capture MYCAP buffer size 100
monitor capture MYCAP match any
monitor capture MYCAP inner mac CLIENT_MAC@
monitor capture MYCAP start
!!Reproduce
monitor capture MYCAP stop
monitor capture MYCAP export flash:|tftp:|http:.../filename.pcap

Tramite GUI:
Passaggio 1. Passare a Troubleshooting > Packet Capture > +Add .

Passaggio 2. Definire il nome dell'acquisizione del pacchetto. È consentito un massimo di 8 caratteri.

Passaggio 3. Definire gli eventuali filtri.

Passaggio 4. Selezionare la casella Monitora traffico di controllo se si desidera visualizzare il traffico puntato alla CPU del sistema e inserito nuovamente nel piano dati.

Passaggio 5. Definire le dimensioni del buffer. È consentito un massimo di 100 MB.

Passaggio 6. Definire il limite, in base alla durata, per un intervallo da 1 a 1000000 secondi, o in base al numero di pacchetti, per un intervallo da 1 a 100000 pacchetti, in base alle esigenze.

Passaggio 7. Scegliere l'interfaccia dall'elenco di interfacce nella colonna sinistra e selezionare la freccia per spostarla nella colonna destra.

Passaggio 8. Salva e applica al dispositivo.

Passaggio 9. Per avviare la cattura, selezionare Avvia.

Passaggio 10. È possibile lasciare in esecuzione l'acquisizione fino al limite definito. Per interrompere manualmente la cattura, selezionare Interrompi.

Passaggio 11. Una volta arrestato, il pulsante Esporta diventa disponibile e consente di scaricare il file di acquisizione (.pcap) sul desktop locale tramite server HTTP o TFTP o server FTP o disco rigido o flash del sistema locale.

Registri dal lato AP

```
show tech !! Collect show tech to have all config details and client stats for the AP.
term mon
!!Basic
debug client MAC@
```

Registri dal server DHCP

Quando si usa un server DHCP esterno, è necessario raccogliere i registri di debug e le acquisizioni dei pacchetti sul lato server per verificare il flusso del traffico DHCP.

Altri log

Se si osserva che i messaggi discover di DHCP sono visibili sul WLC 9800 in una configurazione DHCP centrale, o nei log di debug dell'access point in una configurazione DHCP locale, è necessario procedere a raccogliere i dati di acquisizione dall'uplink per confermare che i pacchetti non stanno scendendo nella porta Ethernet. A seconda delle funzionalità dello switch, è possibile eseguire un'acquisizione di pacchetti incorporata o un'acquisizione SPAN (Switched Port Analyzer) sullo switch uplink. Si consiglia di tracciare il flusso del traffico DHCP passo per passo per determinare il punto in cui la comunicazione viene interrotta, sia dal client DHCP al server DHCP che in direzione inversa.

Problemi noti

Numero 1. Il client sta tentando di ottenere un indirizzo IP da una VLAN precedentemente conservata. Possono verificarsi situazioni in cui un client wireless passa da un SSID a un altro associato a VLAN client diverse. In questi casi, il client può persistere nella richiesta di un indirizzo IP dalla VLAN a cui era precedentemente connesso. Poiché l'IP non rientra nell'ambito DHCP della VLAN corrente, il server DHCP invia un messaggio NAK (riconoscimento negativo) e il client non sarà in grado di acquisire un indirizzo IP.

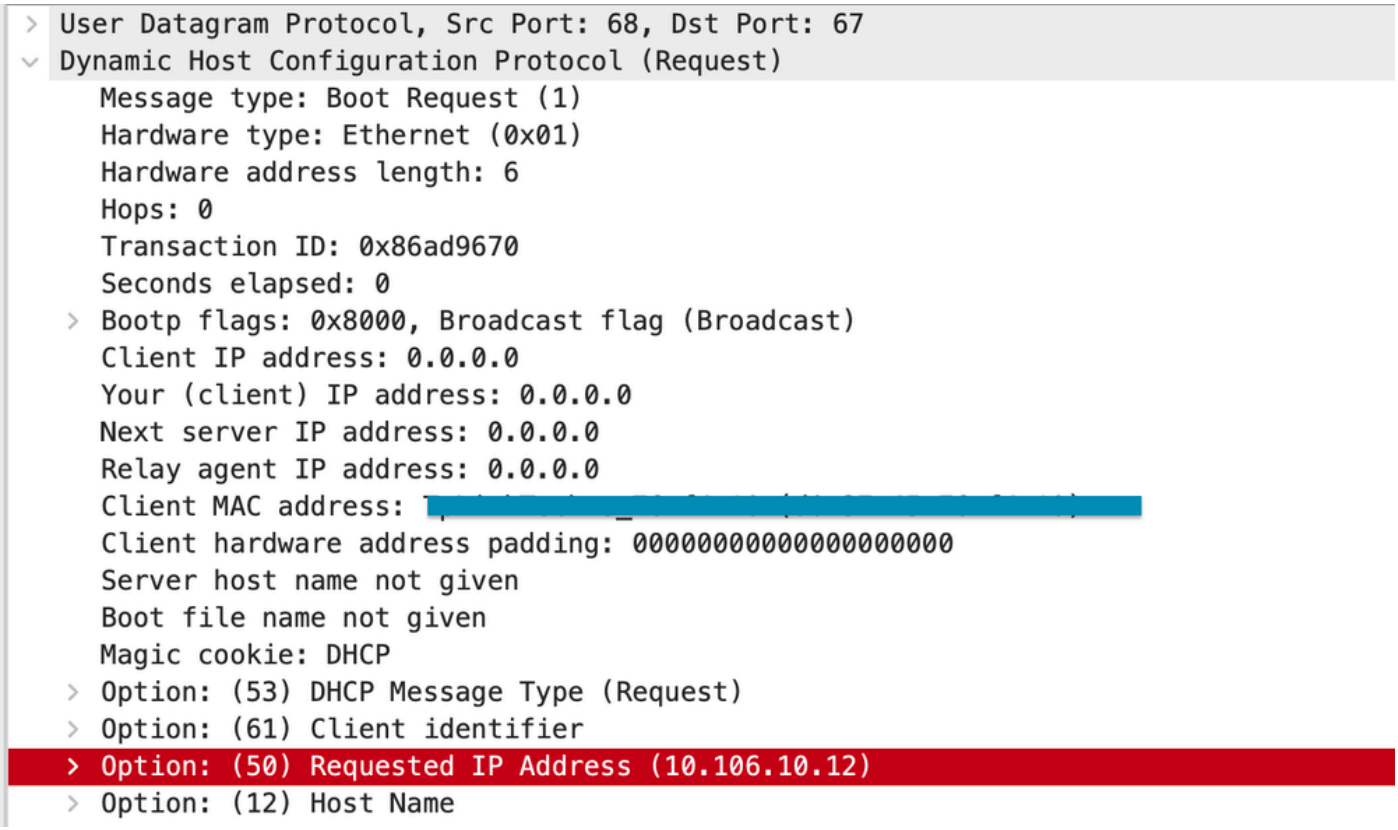
Nei log di traccia radioattivi, è evidente che il client continua a cercare un IP dalla VLAN a cui era precedentemente connesso, ossia la VLAN 10, nonostante il fatto che la VLAN client per l'SSID corrente sia la VLAN 20.

```
2024/03/30 10:40:43.050956833 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.051051895 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
2024/03/30 10:40:43.058538643 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): RX: DHCPv4 from interfac
2024/03/30 10:40:43.058658561 {wncd_x_R0-0}{1}: [sisf-packet] [23608]: (info): TX: DHCPv4 from interfac
```

Embedded Packet Capture su WLC:

```
166 16:10:…  0.0.0.0          255.255.255.255      DHCP      368 DHCP Request  - Transaction ID 0x86ad9670
167 16:10:…  0.0.0.0          255.255.255.255      DHCP      368 DHCP Request  - Transaction ID 0x86ad9670
168 16:10:…  10.106.20.10     255.255.255.255      DHCP      346 DHCP NAK      - Transaction ID 0x86ad9670
169 16:10:…  10.106.20.10     255.255.255.255      DHCP      346 DHCP NAK      - Transaction ID 0x86ad9670
```

Embedded Packet Capture su WLC



Opzione DHCP 50 sull'acquisizione del pacchetto WLC

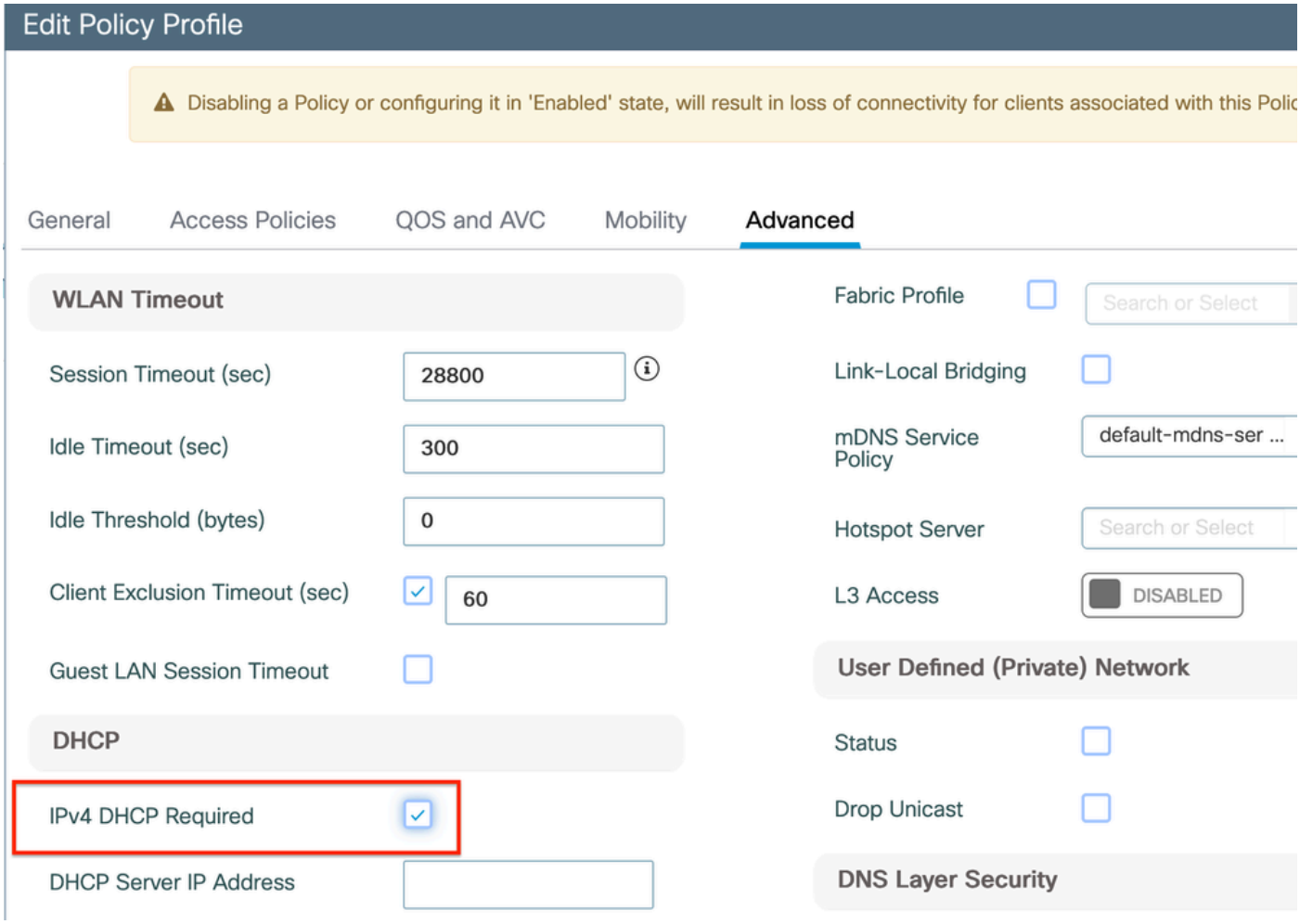
Risoluzione: per assicurarsi che un client completi il processo DHCP, è possibile abilitare l'opzione IPv4 DHCP obbligatorio nella configurazione dei criteri. Questa impostazione deve essere abilitata, soprattutto quando il client passa da un SSID all'altro, per consentire al server DHCP di inviare un NAK al client se richiede un indirizzo IP da una VLAN associata al SSID precedente. In caso contrario, il client potrebbe continuare a utilizzare o richiedere l'indirizzo IP che aveva in precedenza, causando interruzioni nelle comunicazioni. Tenere presente, tuttavia, che l'attivazione di questa funzionalità avrà effetto sui client wireless configurati con un indirizzo IP statico.

Procedere come segue per abilitare l'opzione desiderata:

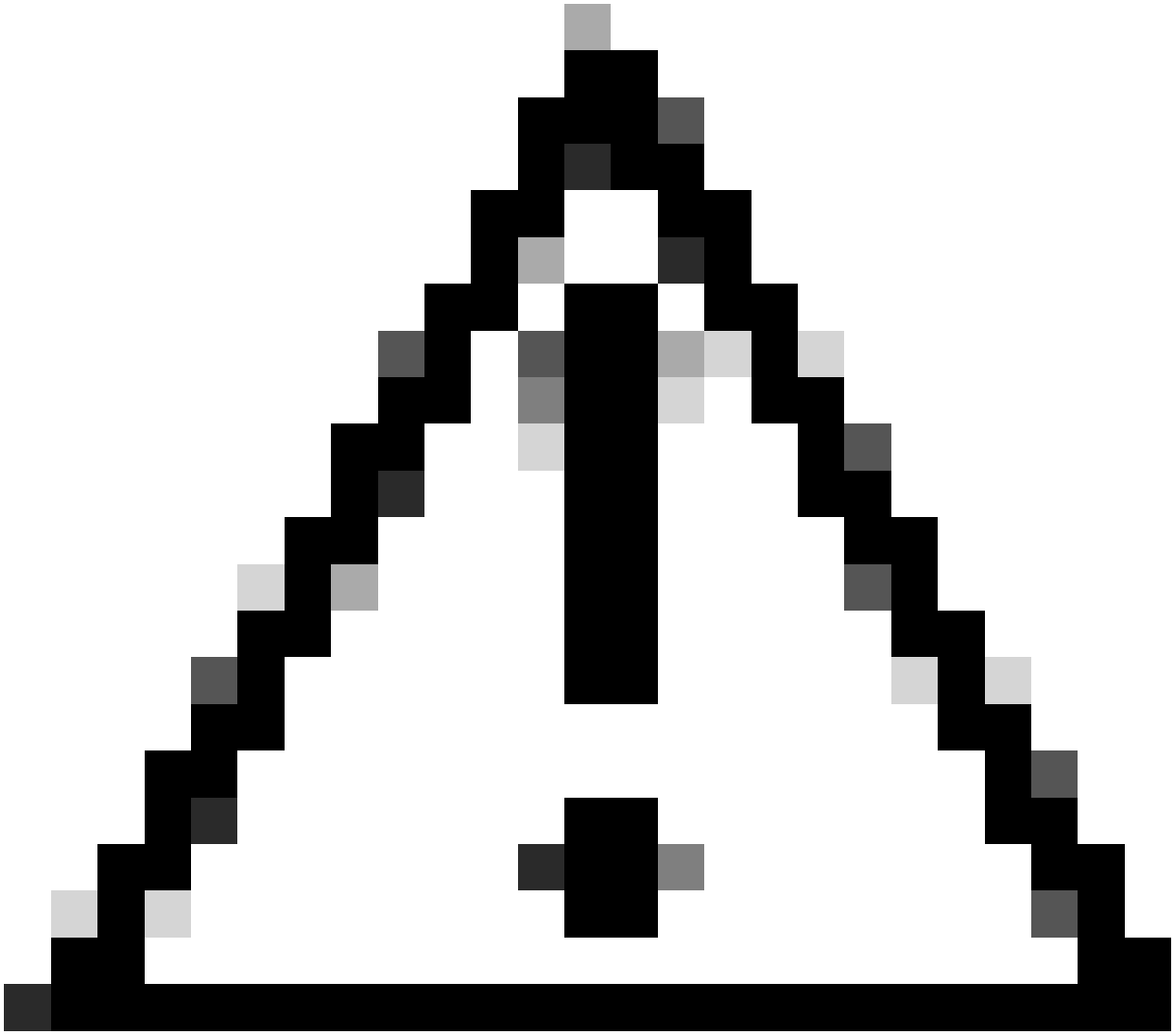
Via CLI:

```
configure terminal
wireless profile policy $Policy_Profile_name
ipv4 dhcp required
```

Tramite GUI: selezionare Configuration > Tags & Profile > Policy > Policy_name > Advanced. Under the DHCP section enable ipv4 DHCP required (Nella sezione DHCP è necessario abilitare il protocollo DHCP ipv4).



Impostazione del profilo dei criteri sul WLC



Attenzione: per una configurazione con ancoraggio esterno, è importante allineare le impostazioni DHCP su entrambi i WLC. Se il protocollo DHCP IPV4 richiesto è abilitato, deve essere abilitato sia sul WLC esterno che su quello di ancoraggio. Una discrepanza nella configurazione relativa a DHCP nel profilo dei criteri tra i due potrebbe causare problemi ai client per quanto riguarda i ruoli di mobilità.

Problema 2: il client viene eliminato o escluso a causa di un problema di furto IP. Il termine furto IP, nel contesto della rete, si riferisce a una situazione in cui più client wireless stanno tentando di utilizzare lo stesso indirizzo IP. Ciò può essere dovuto a diversi motivi elencati di seguito:

1. Assegnazione IP statico non autorizzata: quando un utente imposta un indirizzo IP statico sul proprio dispositivo che coincide con un indirizzo IP già assegnato o assegnato sulla rete, può verificarsi un conflitto IP. Questo si verifica quando due dispositivi tentano di funzionare con un indirizzo IP identico e ciò può interrompere le connessioni di rete di uno dei dispositivi interessati o di entrambi. Per evitare tali problemi, è essenziale verificare che ogni client della rete sia configurato con un indirizzo IP univoco.

2. Server DHCP non autorizzato: la presenza di un server DHCP non autorizzato o non autorizzato nella rete può causare l'allocazione di indirizzi IP in conflitto con il piano di indirizzamento IP stabilito nella rete. Tali conflitti possono causare collisioni di indirizzi IP per diversi

dispositivi o ottenere impostazioni di rete non corrette. Per risolvere questo problema, è necessario identificare ed eliminare il server DHCP non autorizzato dalla rete in modo da evitare ulteriori conflitti IP nella stessa subnet.

3. Voce non aggiornata del client in 9800 WLC: a volte, il controller può mantenere voci obsolete/non aggiornate di un indirizzo IP che un client sta tentando di acquisire. In questi casi, diventa necessario rimuovere manualmente queste voci obsolete dal 9800 WLC. Ecco come procedere:

- Eseguire la traccia radioattiva per l'indirizzo MAC presente nell'elenco di esclusione e filtrarla con il mac legittimo nella traccia radioattiva.

- Sarà possibile visualizzare i log degli errori: %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON: MAC client: Affected_Client_MAC con IP: 10.37.57.24 è stato aggiunto all'elenco di esclusione, Legit MAC client: Legit_Client_MAC, IP: 10.37.57.24, motivo: furto di indirizzi IP

- Eseguire quindi i seguenti comandi:
show wireless device-tracking database mac | sec $Legit_Client_MAC
show wireless device-tracking database ip | sec $Legit_Client_MAC

(Se ci sono voci non aggiornate, è possibile vedere più di un IP per un indirizzo Mac legittimo del client: uno è l'IP originale mentre l'altro è quello obsoleto/non aggiornato).

Risoluzione: eliminare manualmente le voci obsolete da 9800 WLC utilizzando clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. Nella distribuzione flessibile con il server DHCP locale che utilizza la stessa subnet: nelle configurazioni FlexConnect, è comune per varie postazioni remote utilizzare un server DHCP locale che assegna indirizzi IP da una subnet identica. Questo scenario può portare a client wireless in siti diversi che ricevono lo stesso indirizzo IP. I controller in questo framework di rete sono programmati per rilevare quando più connessioni client utilizzano un indirizzo IP identico, interpretando questo come potenziale furto IP. Di conseguenza, questi client vengono generalmente inseriti in un elenco bloccato per evitare conflitti di indirizzi IP.

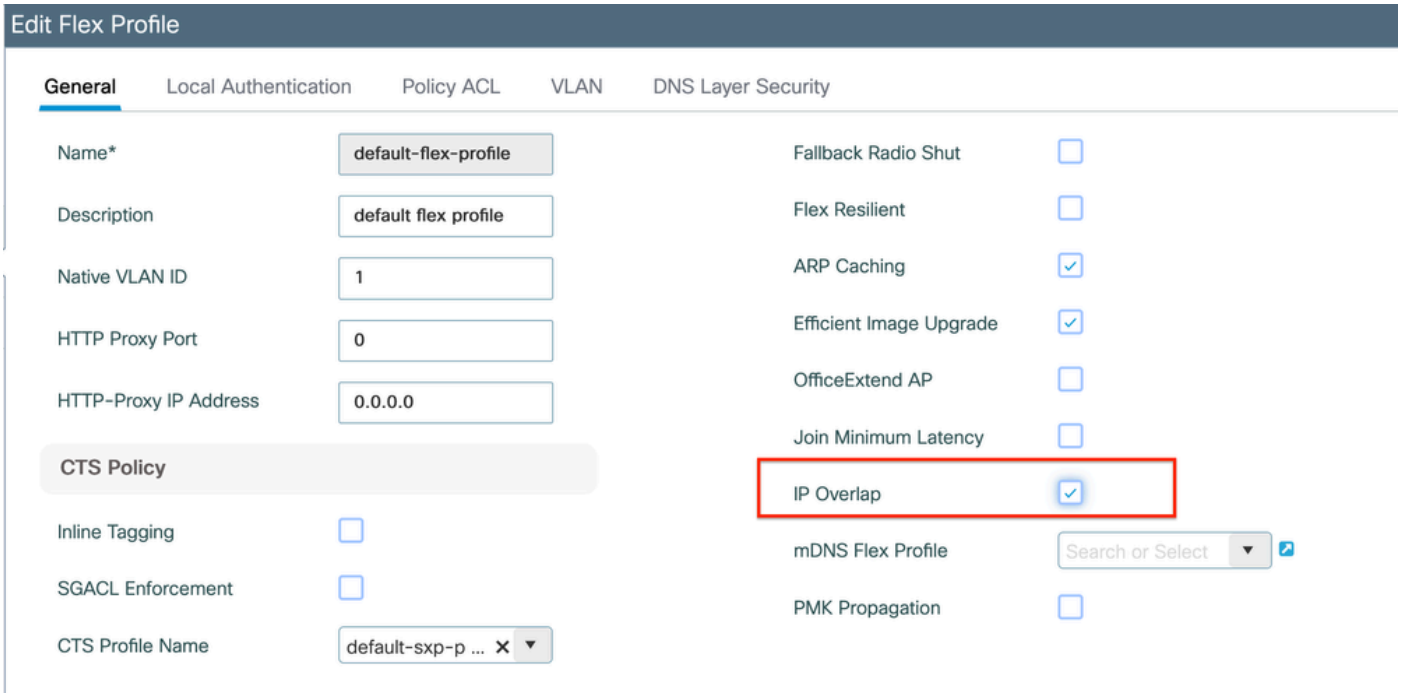
Risoluzione: abilitare la funzione di sovrapposizione IP nel profilo FlexConnect. La funzionalità 'Sovrapposizione dell'indirizzo IP del client nell'installazione Flex' consente di utilizzare gli stessi indirizzi IP in più siti FlexConnect, mantenendo tutte le funzionalità supportate nelle installazioni FlexConnect.

Per impostazione predefinita, questa funzione è disattivata. Per abilitarlo, eseguire la procedura seguente:

Via CLI:

```
configure terminal
 wireless profile flex $Flex_Profile_name
 ip overlap
```

Tramite GUI: selezionare Configuration > Tags & Profiles > Flex. Fare clic su Existing Flex Profile/Add to new Flex profile (Aggiungi a nuovo profilo Flex) e in General tab enable IP Overlap (Generale).



Impostazione Flex Profile su WLC

Numero 3. I client wireless non ricevono un indirizzo IP dalla VLAN desiderata. Questo problema si verifica spesso quando si utilizza la VLAN 1 o quando la VLAN assegnata ai client è la stessa utilizzata per la gestione dei punti di accesso in un'implementazione FlexConnect. La causa principale di questo problema è in genere un'assegnazione non corretta delle VLAN. Di seguito sono riportati alcuni scenari da prendere in considerazione per configurare gli ID VLAN sugli switch serie 9800:

1. Quando si usa un server AAA con la funzione di sostituzione AAA attivata, è fondamentale verificare che l'ID VLAN appropriato venga inviato dal server AAA. Se si fornisce invece un nome VLAN, verificare che corrisponda al nome VLAN configurato sul WLC 9800.

2. Quando la VLAN 1 è configurata per il traffico client wireless, il comportamento può variare in base alla modalità del punto di accesso (AP):

Per un access point in modalità locale/commutazione centrale:

- Se si specifica VLAN-name = valore predefinito, il client viene assegnato alla VLAN 1
- Utilizzando VLAN-ID 1, il client viene assegnato alla VLAN di gestione wireless

Per un access point in modalità Flex/Switching locale:

- Se si specifica VLAN-name = valore predefinito, il client viene assegnato alla VLAN 1
- Utilizzando VLAN-ID 1, un client viene assegnato alla VLAN nativa FlexConnect

Di seguito sono riportati alcuni esempi di scenari sperimentati in laboratorio con i relativi risultati:

1. Per impostazione predefinita, se l'utente non configura alcuna VLAN nel profilo della policy, il WLC assegna la VLAN-ID 1 in modo che i client utilizzino la VLAN di gestione wireless in modalità locale e la VLAN nativa dell'access point per FlexConnect.

2. Se la VLAN nativa con il profilo flessibile è configurata con un ID VLAN nativo diverso da quello configurato sullo switch, si verifica il problema, il client riceve l'IP dalla VLAN di gestione (VLAN nativa) anche se il profilo della policy è configurato con il nome della VLAN "predefinita".

3. Se la VLAN nativa con il profilo flessibile è configurata con l'ID VLAN uguale alla VLAN nativa configurata sullo switch, solo il client sarà in grado di ottenere un indirizzo IP dalla VLAN 1 con l'impostazione predefinita configurata nel profilo della policy.

4. Se è stato selezionato un nome VLAN anziché un ID VLAN, verificare che il nome della VLAN nel profilo Flex sia lo stesso.

Informazioni correlate

- Server DHCP interno su 9800
- Server DHCP esterno in uso
- Opzione DHCP 82 Sottoopzione 5 nel server DHCP Windows
- NAT-PAT in Flex AP
- La VLAN 1 viene utilizzata per il client wireless
- Supporto tecnico Cisco e download

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).