Problemen met DHCP-clientconnectiviteit op een Cisco 9800 WLC

Inhoud

- Inleiding
- Voorwaarden
- De stroom van DHCP-verkeer met draadloze clients begrijpen
- Scenario 1. Het access point (AP) werkt in de lokale modus
  - Topologie (Local Mode AP)
  - Casestudy 1. Wanneer WLC is geconfigureerd als interne DHCP-server
  - Casestudy 2. Wanneer een externe DHCP-server wordt gebruikt
    - DHCP Traffic Broadcast over Layer 2-domein
    - 9800 WLC fungeert als Relay Agent
    - DHCP-optie 80 met suboptie 5/150 in 9800 WLC
- Scenario 2. Het access point (AP) werkt in Flex Mode
  - Topologie (Flex Mode AP)
  - FlexConnect-modus access point met centrale DHCP
  - FlexConnect-modus access point met lokale DHCP
- Probleemoplossing van DHCP-probleem
  - Logbestanden verzamelen
    - Logs van WLC
    - Logbestanden vanaf de AP-kant
    - Logbestanden vanaf DHCP-server
    - Andere logbestanden
  - Bekende problemen
- Gerelateerde informatie

Inleiding

Dit document beschrijft verschillende DHCP-gerelateerde problemen (Dynamic Host Configuration Protocol) die worden aangetroffen door draadloze clients bij verbinding met een Cisco 9800 draadloze LAN-controller (WLC) en hoe deze kunnen worden opgelost.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van Cisco WLC 9800
- Basiskennis van DHCP Flow

- Basiskennis van lokale en flex access mode AP

De stroom van DHCP-verkeer met draadloze clients begrijpen

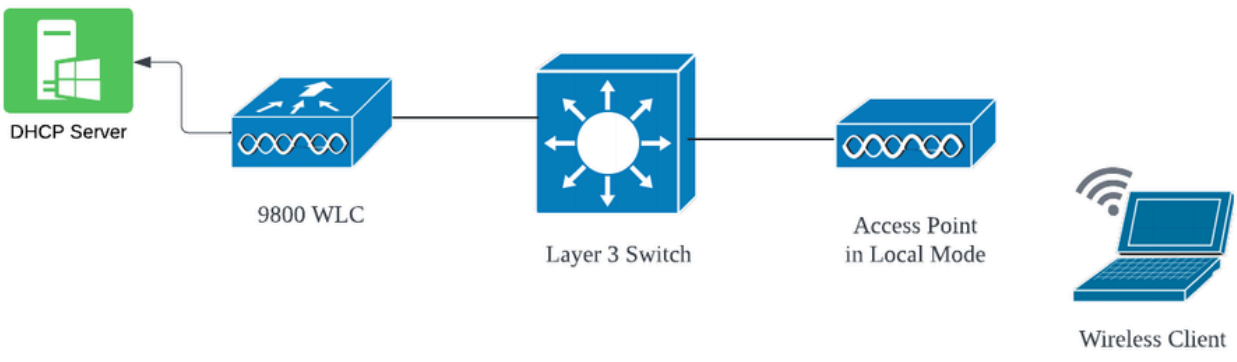
Wanneer de draadloze client verbinding maakt, wordt de gebruikelijke DHCP-uitwisseling uitgevoerd door een DHCP-detectieframe voor uitzending te verzenden om een DHCP-server te vinden op de gekoppelde AP. Afhankelijk van de werkwijze van de AP, zal het ofwel het verzoek doorsturen naar de WLC via de CAPWAP-tunnel of het direct doorgeven aan de volgende hop. Als een DHCP-server beschikbaar is binnen het lokale Layer 2-domein, zal deze reageren, waardoor een succesvolle verbinding mogelijk wordt. Bij afwezigheid van een lokale DHCP-server moet de router (geconfigureerd met de SVI van de client) zijn ingesteld om de DHCP-detectie naar de juiste server te leiden. Dit wordt doorgaans gedaan door een IP Helper Address op de router te configureren, die het instrueert om specifieke broadcast-UDP-verkeer (zoals DHCP-verzoeken) door te sturen naar een vooraf bepaald IP-adres.

Het gedrag van client-DHCP-verkeer is volledig afhankelijk van de modus waarin uw access point (AP) werkt. Laten we elk van deze scenario's afzonderlijk onderzoeken:

Scenario 1. Het access point (AP) werkt in de lokale modus

Wanneer een AP is ingesteld in Local Mode, wordt client-DHCP-verkeer centraal geschakeld, wat betekent dat de DHCP-verzoeken van clients worden verzonden via een CAPWAP-tunnel van de AP naar de WLC, waar ze vervolgens worden verwerkt en doorgestuurd. In dit geval hebt u twee keuzes: u kunt een interne DHCP-server gebruiken of kiezen voor een externe DHCP-server.

Topologie (Local Mode AP)



Netwerktopologie: lokale modus AP

Casestudy 1. Wanneer WLC is geconfigureerd als interne DHCP-server

De controller kan een interne DHCP-server aanbieden via de geïntegreerde functies van de Cisco IOS XE-software. Het gebruik van een externe DHCP-server wordt echter als de beste praktijk beschouwd. Alvorens WLC als Interne DHCP-server op te zetten, moet aan verschillende voorwaarden worden voldaan, die als volgt zijn:

- Zorg ervoor dat u een Switched Virtual Interface (SVI) voor de client-VLAN configureert en het IP-adres van de DHCP-server eraan toewijst.
- Het IP-adres van de interne DHCP-server moet worden ingesteld op de server-facing interface, die een loopback interface, een SVI of een Layer 3 fysieke interface kan zijn.
- De interface van Loopback wordt geadviseerd om te vormen omdat, in tegenstelling tot fysieke interfaces die met daadwerkelijke netwerksegmenten verbinden, de loopbackinterface niet aan hardware wordt gebonden en niet aan een fysieke haven op het apparaat beantwoordt. Het primaire doel van een loopback interface is om een stabiele, altijd-up interface te bieden die niet onderhevig is aan hardwarestoringen of fysieke afsluitingen.

Werkende Opstelling: Hier is een voorbeeld van een interne DHCP serverconfiguratie waar de cliënten met succes IP adressen ontvingen. Hier zijn de operationele logbestanden en de bijbehorende installatiedetails.

Stel de WLC in als de DHCP-server voor VLAN 10, met een DHCP-bereik van 10.106.10.11/24 tot 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
```

Geconfigureerde Loopback-interface op WLC:

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

Client VLAN geconfigureerd als SVI [L3 Interface] met helperadres als loopback-interface op 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
```

U kunt ook het IP-adres van de DHCP-server instellen binnen het beleidsprofiel in plaats van een helperadres te configureren onder het SVI-algoritme. Over het algemeen wordt echter aangeraden om dit per VLAN te configureren voor de best practices:

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

Radioactieve sporen op 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
```

Ingesloten pakketvastlegging op 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
```

Ingesloten pakketvastlegging op WLC

Debugs bij AP-client:

```
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>
```

Packet Capture voor clientzijde:

```
   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
```

Opname van client-eindpakket

In de verstrekte operationele logboeken, kunt u zien dat de WLC het DHCP Discover bericht van de draadloze client ontvangt, en het VLAN van de client het aan het helperadres (dat in het verstrekte voorbeeld de interne loopback interface is) aflost. Na dit, geeft de interne server een aanbieding van DHCP uit, en later, verzendt de cliënt een DHCP- Verzoek, dat dan door de server met een DHCP ACK wordt erkend.

Verificatie van draadloze client-IP:

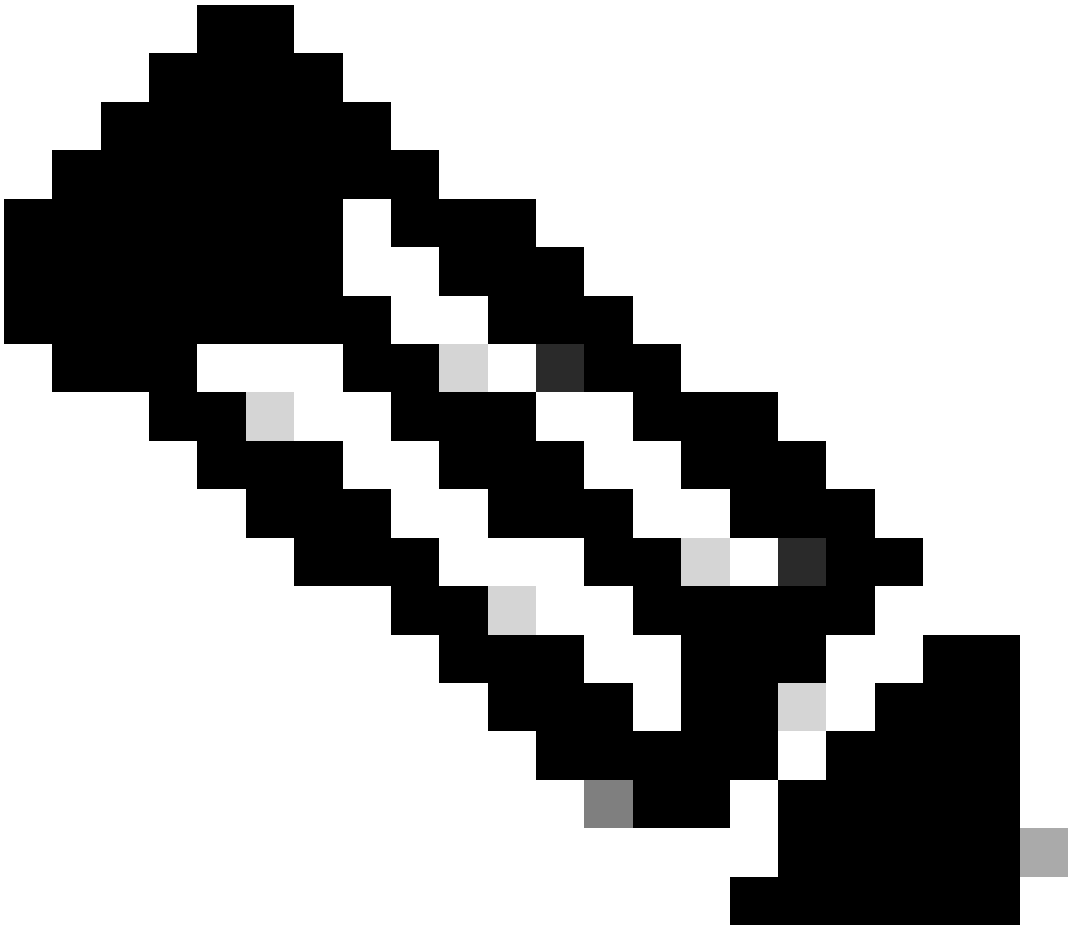
Bij WLC:

```
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
```

Op draadloze client:

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : [redacted]
   Physical Address. . . . . . . . . : [redacted]
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : [redacted]
   IPv4 Address. . . . . . . . . . . : 10.106.10.12(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Thursday, March 28, 2024 9:35:20 PM
   Lease Expires . . . . . . . . . . : Friday, March 29, 2024 6:36:29 AM
   Default Gateway . . . . . . . . . :
   DHCP Server . . . . . . . . . . . : 10.10.10.25
   DHCPv6 IAID . . . . . . . . . . . : 80754501
   DHCPv6 Client DUID. . . . . . . . : [redacted]
   DNS Servers . . . . . . . . . . . : 8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

IP-verificatie op eindpunt client



Opmerking:
1. VRF wordt niet ondersteund in de interne DHCP-servers.
2. DHCPv6 wordt niet ondersteund in de interne DHCP-servers.

---

3. Op C9800 kan SVI meerdere helperadressen configureren, maar alleen de eerste 2 worden gebruikt.
4. Dit is getest en wordt dus ondersteund op alle platforms voor maximaal 20% van de maximale clientschaal van de doos. Voor een 9800-80 die 64.000 clients ondersteunt, is de maximale ondersteunde DHCP-binding ongeveer 14.000.

Casestudy 2. Wanneer een externe DHCP-server wordt gebruikt

Een externe DHCP-server verwijst naar een DHCP-server die niet in WLC zelf is geïntegreerd, maar op een ander netwerkapparaat [Firewall, Routers] of een afzonderlijke entiteit binnen de netwerkinfrastructuur is geconfigureerd. Deze server is gewijd aan het beheer van de dynamische distributie van IP-adressen en andere netwerkconfiguratieparameters naar clients in het netwerk.

Wanneer het gebruiken van een externe DHCP server, is de functie van WLC alleen om verkeer te ontvangen en af te lossen. Hoe het verkeer van DHCP van WLC wordt gerouteerd, of het uitzending of unicast is, zal afhankelijk van uw voorkeur variëren. Laten we elk van deze methodes apart bekijken.

DHCP-traffic broadcast over Layer 2-domein

Bij deze installatie fungeert een ander netwerkapparaat, zoals een firewall, uplink of core switch, als relay agent. Wanneer een client een DHCP-detectieverzoek uitzendt, is de enige taak van WLC om deze uitzending via Layer 2 te doorsturen. Om dit correct te laten werken, moet u ervoor zorgen dat Layer 2 interface van de client-VLAN correct is geconfigureerd en toegestaan via de WLC-datapoort en het uplink-apparaat.

Gewenste configuratie op het WLC-einde voor client VLAN 20 voor deze instantie:

Configureerde Layer 2 VLAN op WLC:

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

Configureerde datapoort op WLC om het verkeer van client-VLAN toe te staan:

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

Radioactieve sporen op de 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
```

Ingesloten pakketvastlegging genomen op 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
```

Ingesloten pakketvastlegging op WLC

Debugs bij AP-client:

```
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>
```

Opname aan clientzijde:

```
  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
```

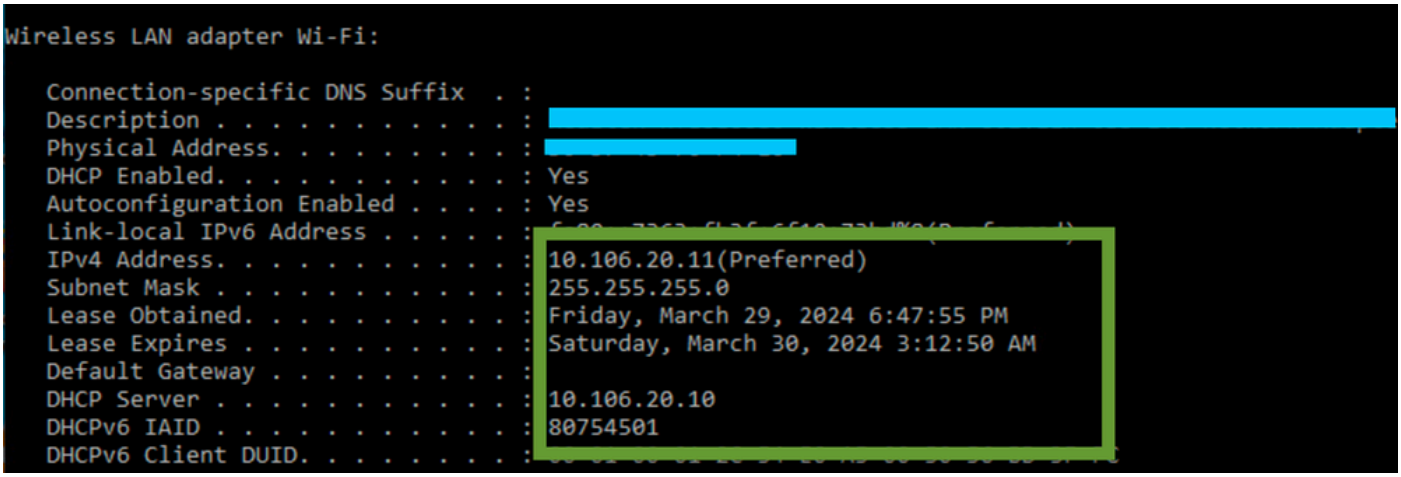
Opname van client-eindpakket

In de aangeboden operationele logboeken, merkt u in de logboeken op dat de WLC de DHCP Discover-uitzending van de draadloze client onderschept en vervolgens uitzendt naar de volgende hop via zijn L2-interface. Zodra de WLC de DHCP-aanbieding van de server ontvangt, stuurt het dit bericht door naar de client gevolgd door DHCP-verzoek en ACK.

Verificatie van draadloze client-IP:

U kunt de IP-lease controleren op de DHCP-server en de bijbehorende status.

Op draadloze client:



IP-verificatie op client-end

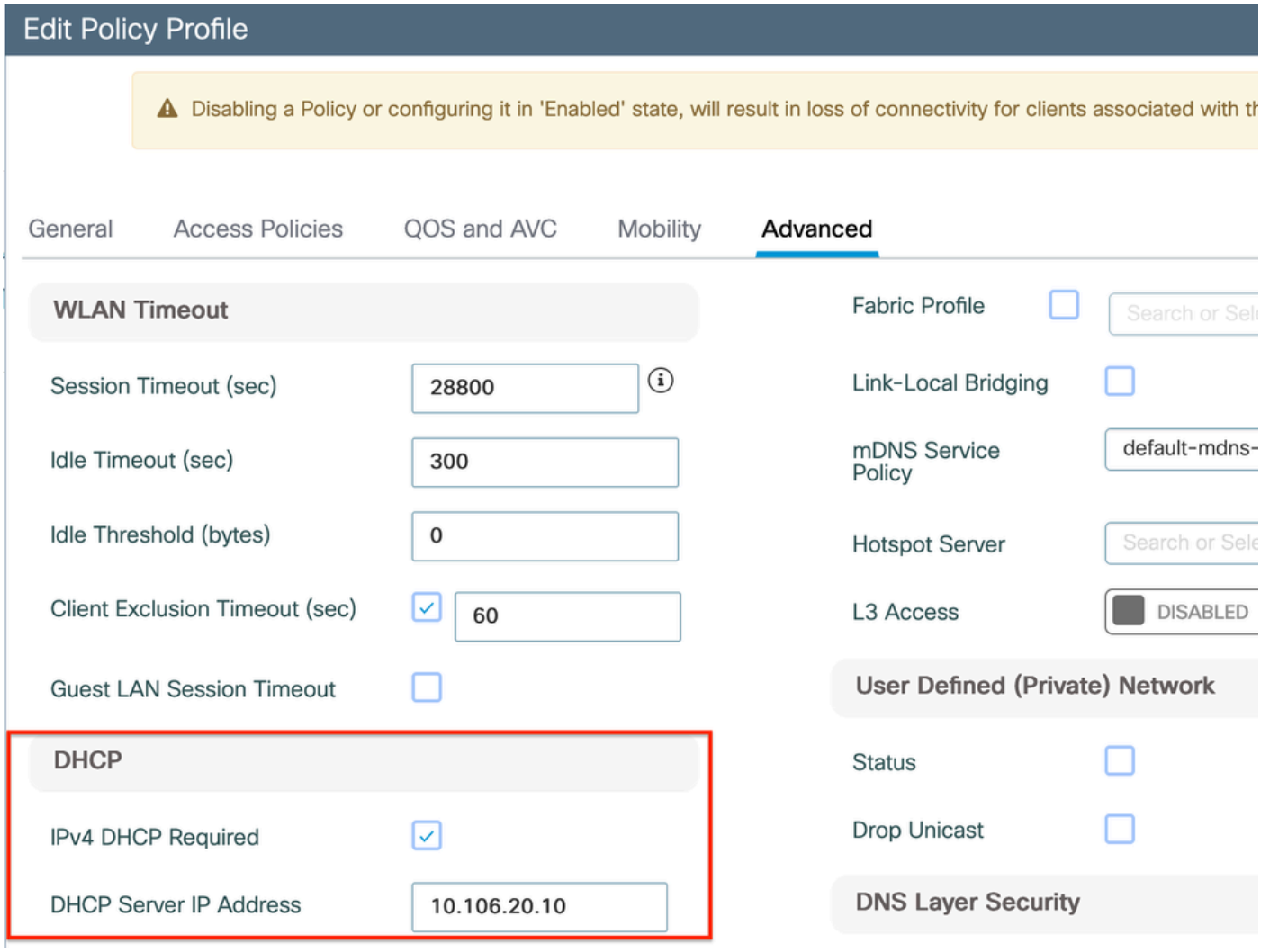
9800 WLC fungeert als Relay Agent

In deze configuratie, door:sturen WLC direct de pakketten van DHCP het van draadloze cliënten aan de server van DHCP door unicast ontvangt. Om dit in te schakelen, dient u ervoor te zorgen dat VLAN SVI voor de client is geconfigureerd op de WLC.

Er zijn 2 manieren om de DHCP-server IP in 9800 WLC te configureren:

1. Configureer DHCP-server IP onder beleidsprofiel onder geavanceerde instelling.

Via GUI: Navigeer naar Configuration > Tags & Profile > Policy > Policy_name > Advanced. Onder de DHCP-sectie kunt u de DHCP-server IP configureren zoals aangegeven in de afbeelding:



Policy Profile Setting op WLC

Via CLI:

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

2. Binnen de SVI-configuratie moet u het helperadres opgeven. Het is mogelijk om meerdere DHCP-servers in te stellen in de configuratie van het Help-adres om redundantie te bieden. Terwijl het instellen van het DHCP-serveradres voor elk WLAN binnen het beleidsprofiel mogelijk is, is de aanbevolen benadering om het per interface te configureren. Dit kan worden bereikt door een helperadres toe te wijzen aan het corresponderende SVI.

Wanneer u de relay-functie gebruikt, wordt de bron van het DHCP-verkeer het IP-adres van de Switched Virtual Interface (SVI) van de client. Dit verkeer wordt vervolgens gerouteerd door de interface die overeenkomt met de bestemming (het IP-adres van de DHCP-server) zoals bepaald door de routeringstabel.

Hier is een voorbeeld van de werkconfiguratie van de 9800 die dient als relais-agent:

geconfigureerd Layer 3 Interface voor client-VLAN op WLC met helperadres:

```
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
```

Configureerde datapoort op WLC om het verkeer van client-VLAN toe te staan:

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

RA sporen van 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
```

Ingesloten pakketvastlegging op 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

Ingesloten pakketvastlegging op WLC

In zowel de Radioactive Traces (RA) als de Embedded Packet Capture (EPC) op de WLC, zult u merken dat de WLC, handelend als relay agent, de DHCP-pakketten rechtstreeks van de client naar de DHCP-server unicast.

Debugs bij AP-client:

```
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>
```

Opname aan clientzijde:

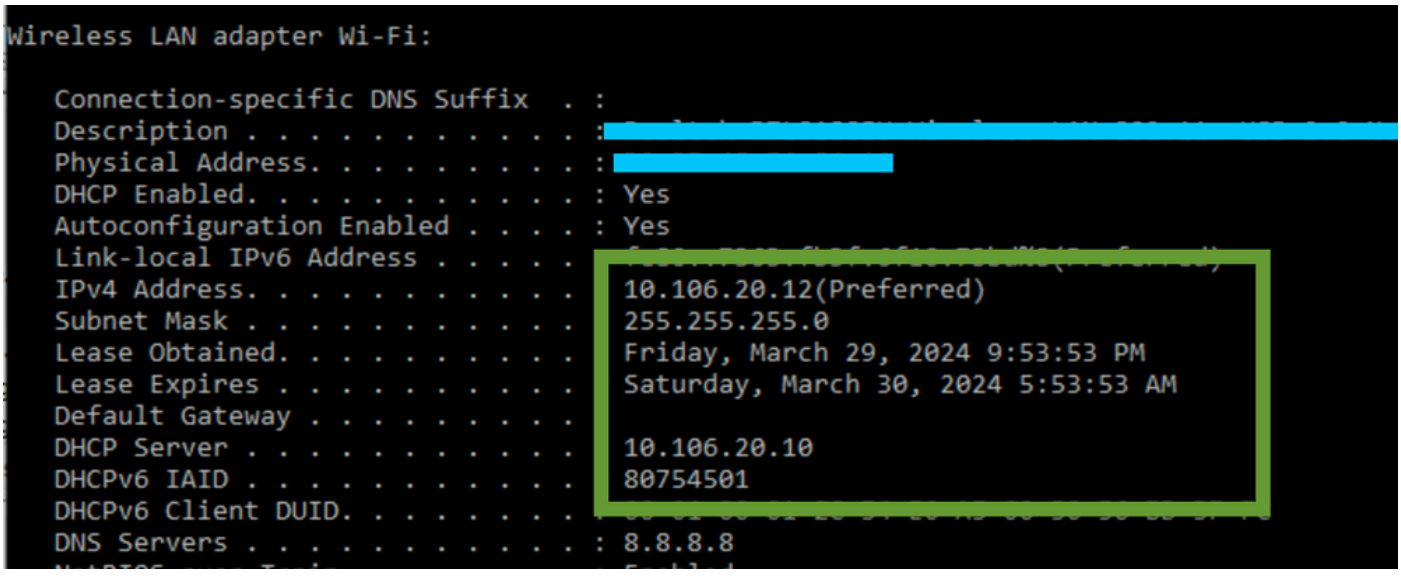
No.	Time	Source	Destination	Protocol	Length	Info
1	10:23:46.630692	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
50	10:23:50.627940	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
59	10:23:53.694541	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer - 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

Opname van client-eindpakket

Verificatie van draadloze client-IP:

U kunt de IP-lease controleren op de DHCP-server en de bijbehorende status.

Op draadloze client:



IP-verificatie op client-end

DHCP-optie 80 met suboptie 5/150 in 9800 WLC

In bepaalde scenario's, kunt u er de voorkeur aan geven de broninterface voor DHCP-verkeer expliciet te definiëren in plaats van afhankelijk van de routeringstabel, om potentiële netwerkcomplicaties te voorkomen. Dit is met name van belang wanneer het volgende netwerkapparaat langs het pad, zoals een Layer 3-switch of firewall, gebruik maakt van controles van Reverse Path Forwarding (RPF). Neem bijvoorbeeld een situatie waar de draadloze beheerinterface is ingesteld op VLAN 50, terwijl de client SVI op VLAN 20 staat en wordt gebruikt als DHCP-relay voor clientverkeer. De standaardroute is gericht op de gateway van het draadloze beheer VLAN/subnet.

Beginnend met versie 17.03.03 op 9800 WLC, is het mogelijk om de broninterface voor het verkeer van DHCP te kiezen om of de cliënt VLAN of een ander VLAN, zoals de Draadloze Interface van het Beheer (WMI) te zijn, die connectiviteit aan de server van DHCP waarborgt.

Hier zou een stukje van de configuratie zijn:

```
!
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 dit scenario wordt het verkeer naar de DHCP-server 10.100.17.14 gesourcet van VLAN 50 (10.100.16.10), omdat de uitgangsinterface van het pakket is geselecteerd op basis van een raadpleging in de IP-routeringstabel. Meestal zal het verkeer via Wireless Management Interface (WMI) VLAN worden afgesloten vanwege de standaardroute die is geconfigureerd.
Als een uplink-switch echter RPF-controles (Reverse Path Forwarding) implementeert, kan het een pakket dat van VLAN 50 komt, afwijzen, maar met een IP-bronadres dat tot een ander subnetnetwerk [VLAN 20] behoort.

Om dit te voorkomen, moet u een nauwkeurige broninterface voor de DHCP-pakketten instellen met de opdracht IP DHCP Relay Source-Interface. In dit specifieke geval, zou u de pakketten DHCP uit de interface WMI op VLAN 50 willen voortkomen:

```
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
```

Wanneer u opdracht gebruiktip dhcp relay source-interface, worden zowel de broninterface van de DHCP-pakketten als het GIADR ingesteld op de interface die in de DHCP Relay-opdracht (VLAN50, in dit geval) is gespecificeerd. Dit is een probleem, aangezien dit niet de client-VLAN is waar u DHCP-adressen wilt toewijzen.

Hoe weet de DHCP-server hoe het IP aan de juiste client-pool kan worden toegewezen?

Het antwoord hierop is dat wanneer ip dhcp relay source-interface de opdracht wordt gebruikt, C9800 automatisch de clientsubnetinformatie toevoegt in een bedrijfseigen suboptie 150 van optie 82, de zogenaamde linkselectie, zoals u kunt zien bij de opname:

```
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
```

Optie 182 suboptie 150 bij WLC-pakketvastlegging

Standaard wordt suboptie 150 (bedrijfseigen Cisco) toegevoegd. Zorg ervoor dat de gebruikte DHCP-server deze informatie kan interpreteren en erop kan reageren. Aanbevolen wordt om de C9800-configuratie te wijzigen en de standaardoptie 82, suboptie 5 te gebruiken om de informatie over de linkselectie te verzenden. U kunt dit doen door de volgende globale opdracht te configureren:

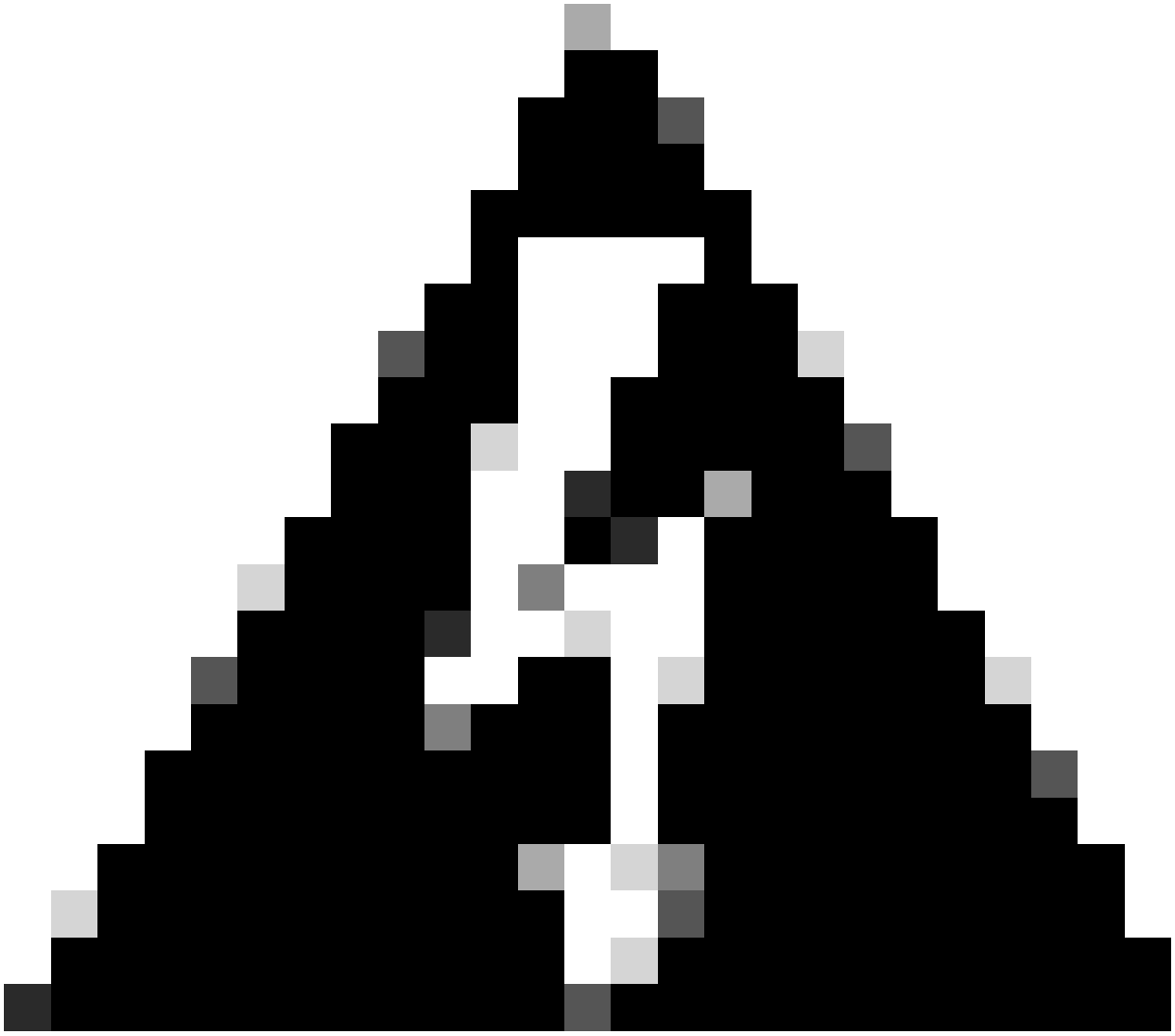
```
<#root>

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

Zodra de gespecificeerde opdracht is toegepast, vervangt het systeem suboptie 150 met suboptie 5 in de DHCP-pakketten. Suboptie 5 wordt meer algemeen erkend door netwerkapparaten, waardoor wordt verzekerd dat de pakketten minder waarschijnlijk zullen worden gelaten vallen. De toepassing van deze wijziging is ook duidelijk in de opgenomen gegevens:

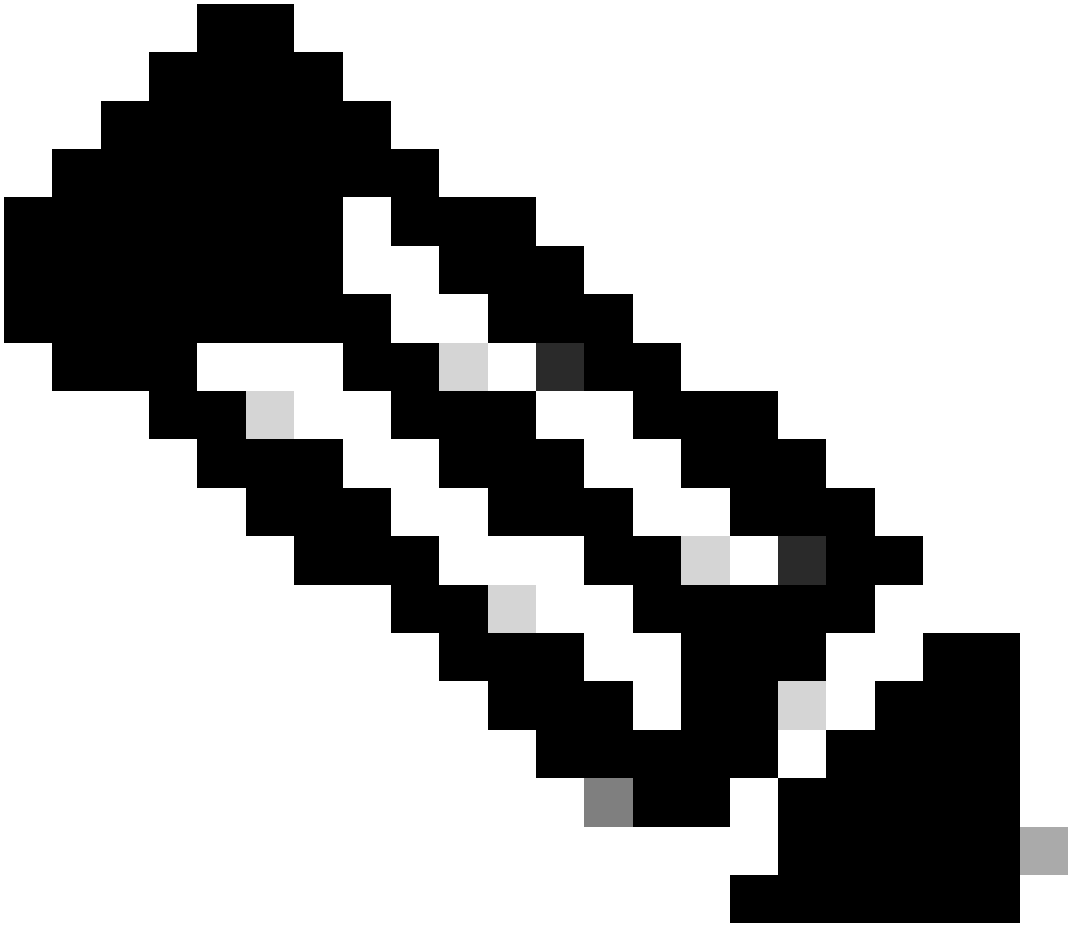
Optie 182 suboptie 5 bij WLC-pakketvastlegging

Met de implementatie van suboptie 5, moet uw DHCP-verkeer worden erkend door andere netwerkapparaten. U kunt echter nog steeds NAK-berichten (negatieve bevestiging) tegenkomen, met name wanneer de Windows DHCP-server in gebruik is. Dit kan te wijten zijn aan de DHCP-server die het IP-adres van de bron niet autoriseert, mogelijk omdat er geen overeenkomstige configuratie is voor die IP van de bron.

Wat moet u doen op de DHCP-server? Voor de Windows DHCP-server moet u een dummy scope maken om het IP-adres van de relay-agent te autoriseren.



Waarschuwing: alle IP-adressen van relay-agents (GIADR) moeten deel uitmaken van een actief IP-adresbereik met DHCP-bereik. Alle GIADR's buiten het DHCP-bereik van IP-adressen worden beschouwd als een schurkenrelay en Windows DHCP Server zal geen DHCP-clientverzoeken van die relayagents bevestigen. Er kan een speciale scope worden gecreëerd voor de autorisatie van relay agents. Maak een scope met de GIADR (of meerdere als de GIADR's opeenvolgende IP-adressen zijn), sluit het GIADR-adres(sen) uit van distributie en activeer vervolgens de scope. Dit machtigt de relay agents en voorkomt dat de GIADR-adressen worden toegewezen.

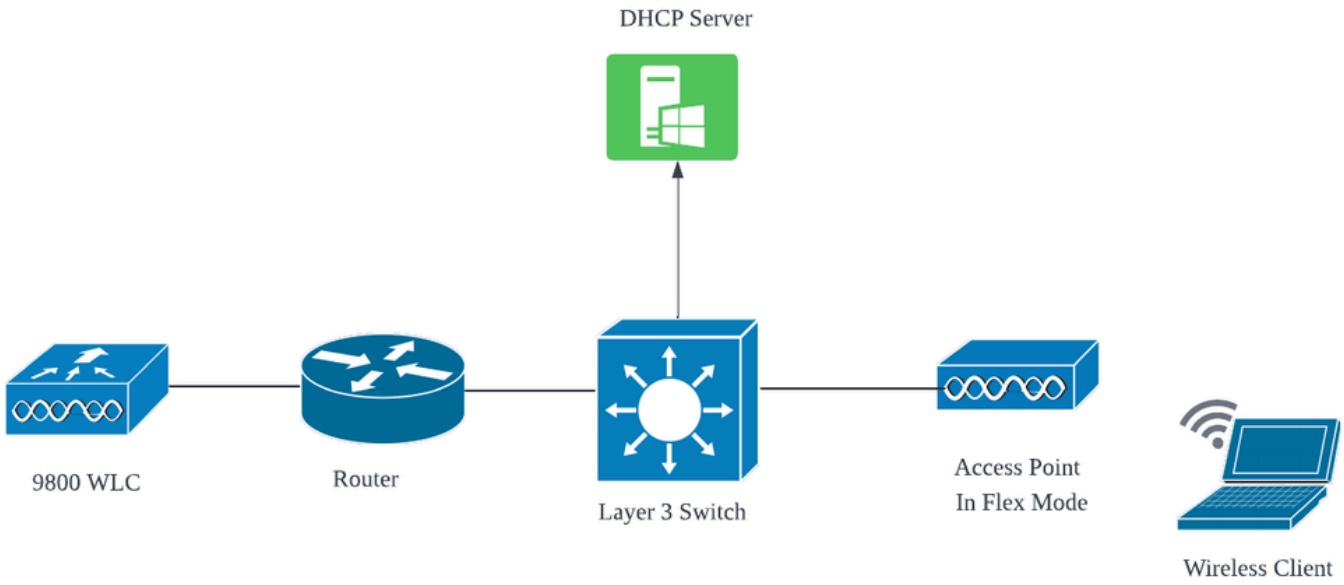


Opmerking: in een installatie van een buitenlands anker wordt DHCP-verkeer centraal verwerkt met de AP-modus ingesteld als Lokaal. Aanvankelijk worden de DHCP-verzoeken naar de buitenlandse WLC gestuurd, die ze vervolgens via een mobiliteitstunnel doorstuurt naar de anker WLC. Het is het anker WLC dat het verkeer volgens zijn geconfigureerde instellingen verwerkt. Daarom moeten alle configuraties met betrekking tot DHCP worden geïmplementeerd op het anker WLC.

Scenario 2. Het access point (AP) werkt in Flex Mode

FlexConnect AP's zijn ontworpen voor filialen en externe vestigingen, waardoor ze in een standalone modus kunnen werken wanneer ze de verbinding met de centrale draadloze LAN-controller (WLC) verliezen. FlexConnect AP's kunnen lokaal switches tussen een client en het netwerk zonder dat het verkeer naar de WLC moet worden teruggesleept. Dit vermindert de latentie en behoudt de WAN-bandbreedte. Op flex-modus kan het DHCP-verkeer centraal of lokaal worden geschakeld.

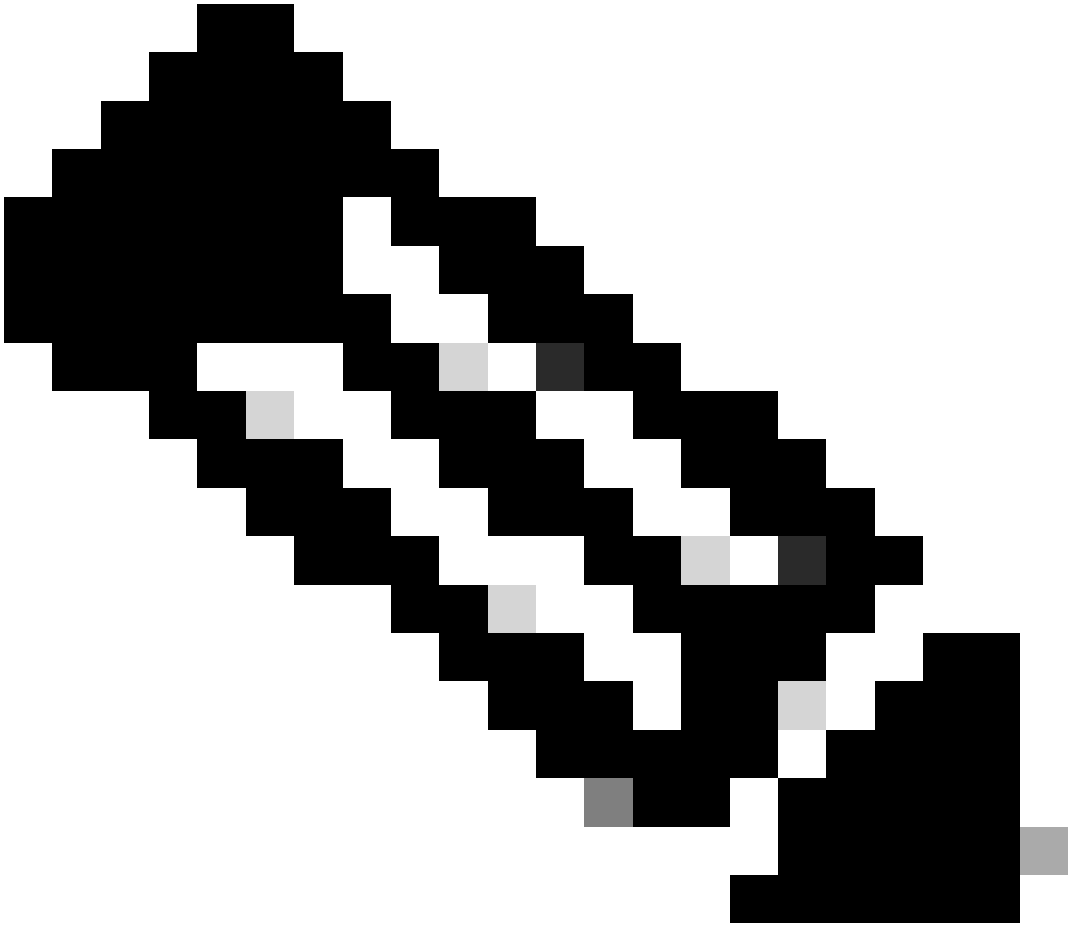
Topologie (Flex Mode AP)



Netwerktopologie: Flex Mode AP

FlexConnect-modus access point met centrale DHCP

Ongeacht de AP-modus, blijven de configuratie, de operationele stroom en de stappen voor probleemoplossing consistent bij gebruik van een centrale DHCP-server. Voor AP's in FlexConnect-modus is het echter over het algemeen aangeraden om een lokale DHCP-server te gebruiken tenzij u op de lokale site een client-SVI hebt ingesteld.



Opmerking: als er geen clientsubnetverbinding beschikbaar is op de externe site, kunt u profiteren van FlexConnect NAT-PAT. FlexConnect NAT/PAT voert netwerkadresomzetting (NAT) uit voor het verkeer dat afkomstig is van clients die zijn aangesloten op het toegangspunt, en brengt dit in kaart met het IP-adres voor beheertaken van het toegangspunt. Als u bijvoorbeeld AP's hebt die in FlexConnect-modus werken bij externe vestigingen en de verbonden clients moeten communiceren met een DHCP-server op het hoofdkantoor waar de controllers zich bevinden, kunt u FlexConnect NAT/PAT activeren in combinatie met de centrale DHCP-instelling in het beleidsprofiel.

FlexConnect-modus access point met lokale DHCP

Wanneer een FlexConnect AP is geconfigureerd om lokale DHCP te gebruiken, ontvangen clientapparaten die aan het AP zijn gekoppeld hun IP-adresconfiguratie van een DHCP-server die beschikbaar is binnen hetzelfde lokale netwerk. Deze lokale DHCP-server zou een router, een speciale DHCP-server of een ander netwerkapparaat kunnen zijn dat DHCP-services biedt binnen het lokale subnet. Met lokale DHCP wordt het DHCP-verkeer binnen het lokale netwerk geschakeld, wat betekent dat het AP DHCP-verzoek van clients rechtstreeks naar de aangrenzende hop doorgeeft, zoals de access switch. Van daaruit worden de verzoeken behandeld volgens de configuratie van uw netwerk.

Voorwaarde:

1. Raadpleeg de FlexConnect-handleiding om ervoor te zorgen dat uw configuratie aansluit bij de instructies en best practices die in de handleiding worden beschreven.

2. De client VLAN moet onder flex-profiel worden vermeld.
3. AP moet op trunkwijze worden ingesteld, met het AP beheer VLAN aangewezen als inheems VLAN, en VLANs voor cliëntverkeer zouden op de trunk moeten worden toegelaten.

Hier is een voorbeeld van configuratie van met AP verbonden switchport met beheer VLAN als 58 en client-VLAN als 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
!
```

Werkinstelling: Voor referentie die de operationele logbestanden deelt met de lokale DHCP-server wanneer AP is geconfigureerd voor flex-modus:

Debugs bij AP-client:

```
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>
```

Opname van AP-uplink:

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

Opname van AP-uplink

Opname aan clientzijde:

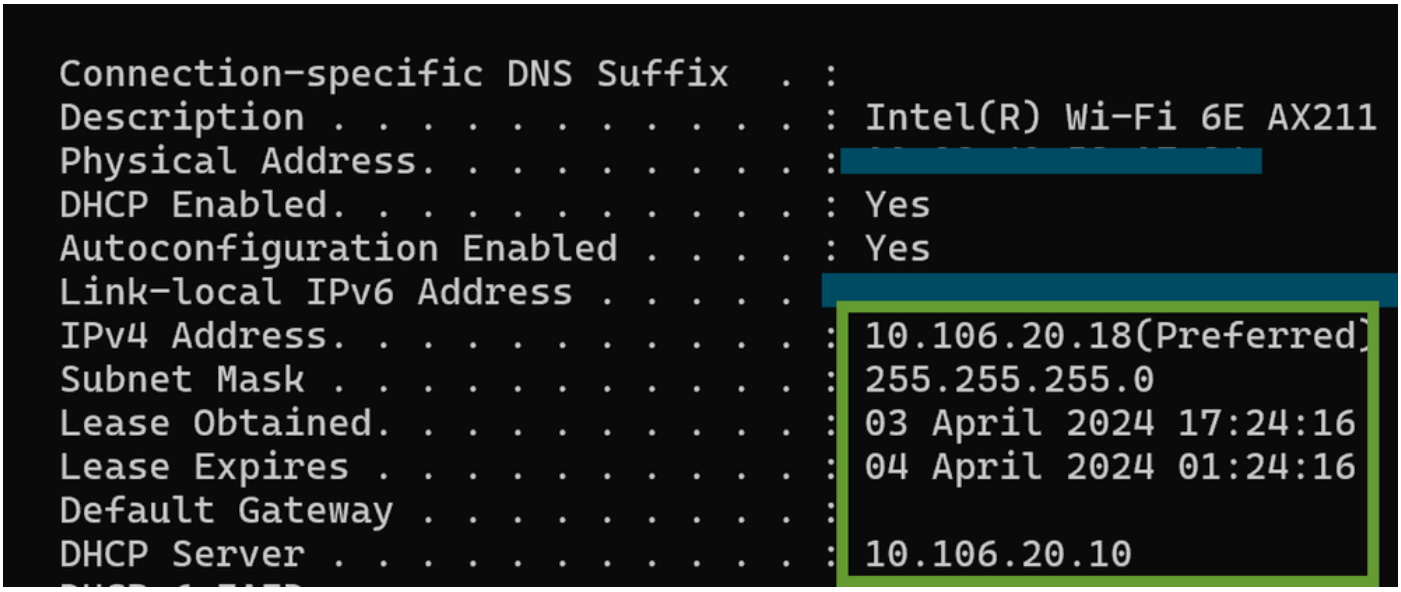
```
16540 111.905836    0.0.0.0           255.255.255.255     DHCP      343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10      10.106.20.18        DHCP      342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0           255.255.255.255     DHCP      385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

Opname van client-eindpakket

Verificatie van draadloze client-IP:

U kunt de IP-lease controleren op de DHCP-server en de bijbehorende status.

Op draadloze client:



IP-verificatie op eindpunt van client

Probleemoplossing van DHCP-probleem

Problemen met DHCP oplossen houdt in dat problemen worden geïdentificeerd en opgelost die voorkomen dat clients een IP-adres kunnen verkrijgen van een DHCP-server wanneer ze verbonden zijn met het draadloze netwerk. Hier zijn enkele veelvoorkomende stappen en overwegingen bij het oplossen van DHCP-problemen:

1. Controleer de clientconfiguratie

- Zorg ervoor dat de client is geconfigureerd om automatisch een IP-adres te verkrijgen.
- Controleer of de netwerkadapter ingeschakeld is en goed werkt.

2. Controleer DHCP-serverstatus

- Bevestig dat de DHCP-server operationeel en bereikbaar is via het netwerksegment van de client.
- Controleer het IP-adres, het subnetmasker en de standaardinstellingen van de gateway.

3. Configuratie van bereik bekijken

- Inspecteer het DHCP-bereik om er zeker van te zijn dat er een voldoende aantal IP-adressen voor de clients beschikbaar is.
- Controleer de leaseduur en opties van de scope, zoals DNS-servers en standaardgateway
- Zorg er in bepaalde omgevingen (zoals Active Directory) voor dat de DHCP-server geautoriseerd is om DHCP-services binnen het netwerk te leveren.

4. Controleer de configuratie op 9800 WLC

- Veel problemen zijn gezien als gevolg van verkeerde configuratie, zoals een ontbrekende loopback interface, client SVI of de afwezigheid van een geconfigureerd helper-adres. Vóór logboekinzameling, wordt het aanbevolen om te verifiëren dat de configuratie correct is geïmplementeerd.
- Bij gebruik van een interne DHCP-server: Met betrekking tot de uitputting van de DHCP-scope is het belangrijk om er, in het bijzonder bij het configureren van DHCP via de CLI, voor te zorgen dat de lease-timer is geconfigureerd volgens uw vereisten. Standaard is de leasetimer ingesteld op infinite op 9800 WLC.
- Controleer dat client-VLAN-verkeer is toegestaan op de WLC-uplinkpoort wanneer u een centrale DHCP-server gebruikt. Wanneer u een lokale DHCP-server gebruikt, dient u er daarentegen voor te zorgen dat het relevante VLAN is toegestaan op de AP-uplinkpoort.

5. Firewall- en beveiligingsinstellingen

- Zorg ervoor dat firewalls of beveiligingssoftware DHCP-verkeer niet blokkeren (poort 67 voor DHCP-server en poort 68 voor DHCP-client).

Logbestanden verzamelen

Logs van WLC

1. Laat term exec prompt timestamp toe om tijdverwijzing voor alle bevelen te hebben.

2. Gebruik show tech-support wireless !! om de configuratie te bekijken

2. U kunt het aantal klanten, de distributie van de cliëntstaat, en uitgesloten cliënten controleren.
show wireless summary !! Totaal aantal AP's en clients
show wireless exclusionlist !! Indien een cliënt als uitgesloten wordt beschouwd
show wireless exclusionlist client mac-address MAC@ !! om meer informatie te krijgen over concrete client uitgesloten en te controleren of de reden wordt vermeld als IP-diefstal voor een client.

3. Controleer IP-adrestoewijzing voor clients, zoek naar onjuiste adressen of onverwacht statisch adresleren, VLAN's die als dirty zijn gemarkeerd omdat er geen respons is van DHCP-server, of pakketdalingen in SISF die DHCP/ARP verwerkt.

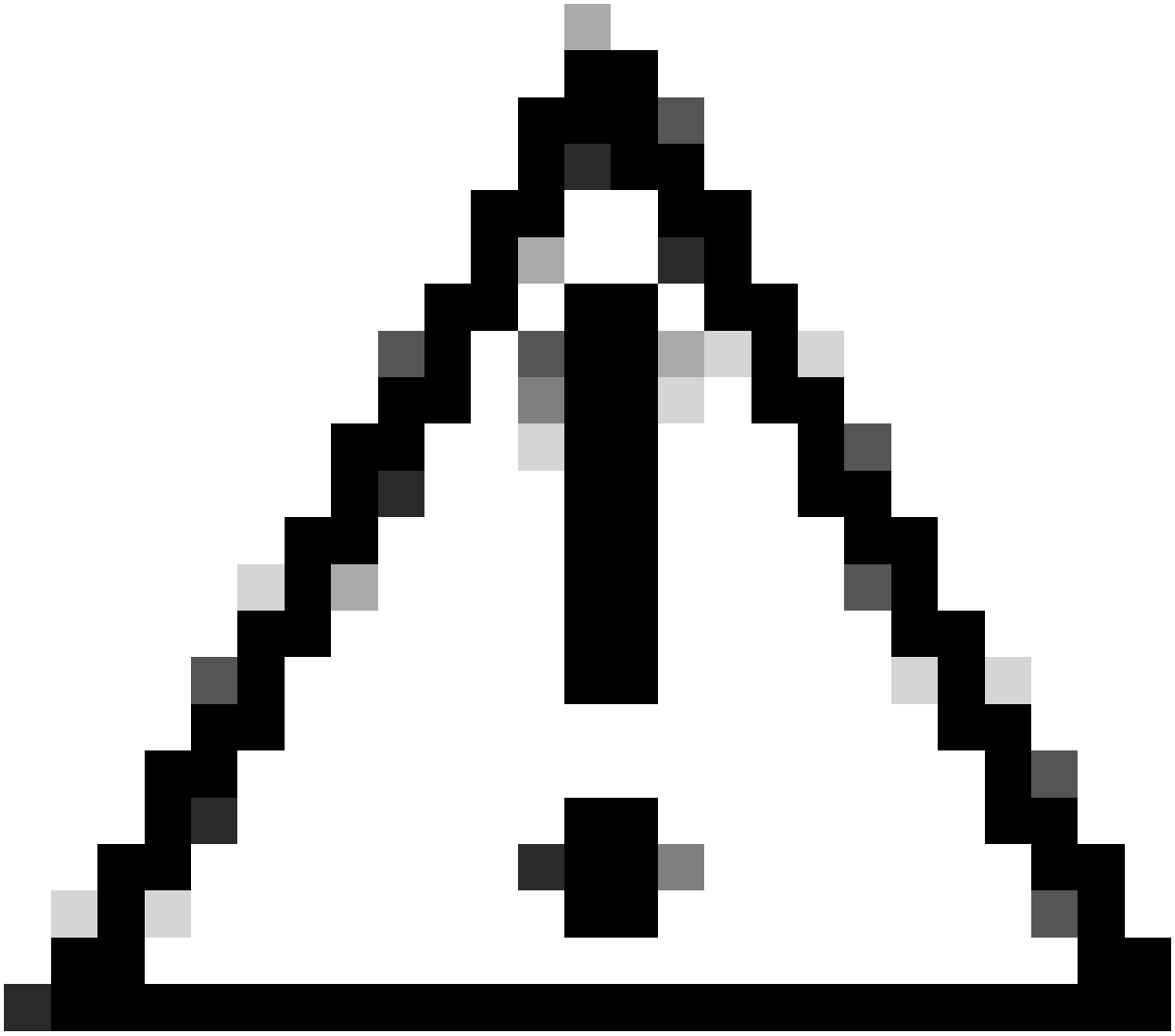
show wireless device-tracking database ip !! Controleer IP en bekijk hoe het leren van adressen heeft plaatsgevonden:
show wireless device-tracking database mac !! Controleer op Mac en bekijk welke IP-client is toegewezen.
show wireless vlan details !! Controleer of VLAN niet is gemarkeerd als vuil vanwege DHCP-fouten bij gebruik van een VLAN-groep.
show wireless device-tracking feature drop !!Drops in SISF

4. Specifieke uitgangen van WLC voor concrete client MAC@ show wireless device-tracking feature drop

Schakel radioactief traceren in voor client-MAC-adres wanneer de client probeert een draadloos netwerk te verbinden.

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



Waarschuwing: het voorwaardelijke debuggen maakt debug-level logging mogelijk, waardoor het volume van de gegenereerde logs toeneemt. Als u dit programma laat draaien, vermindert u hoe ver u terug in de tijd kunt kijken naar logbestanden van. Daarom wordt aangeraden om debugging altijd uit te schakelen aan het eind van de probleemoplossing sessie.

Om alle debugging uit te schakelen voert u deze opdrachten uit:

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

Via GUI:

Stap 1. Naar navigeren Troubleshooting > Radioactive Trace .
Stap 2. Klik Add en voer een client-Mac-adres in dat u wilt oplossen. U kunt meerdere Mac-adressen aan de track toevoegen.

Stap 3. Wanneer u klaar bent om de radioactieve tracering te starten, klikt u op Start. Zodra begonnen, debug het registreren wordt geschreven aan schijf over om het even welke verwerking van het controlevliegtuig met betrekking tot de gevolgde adressen van MAC.

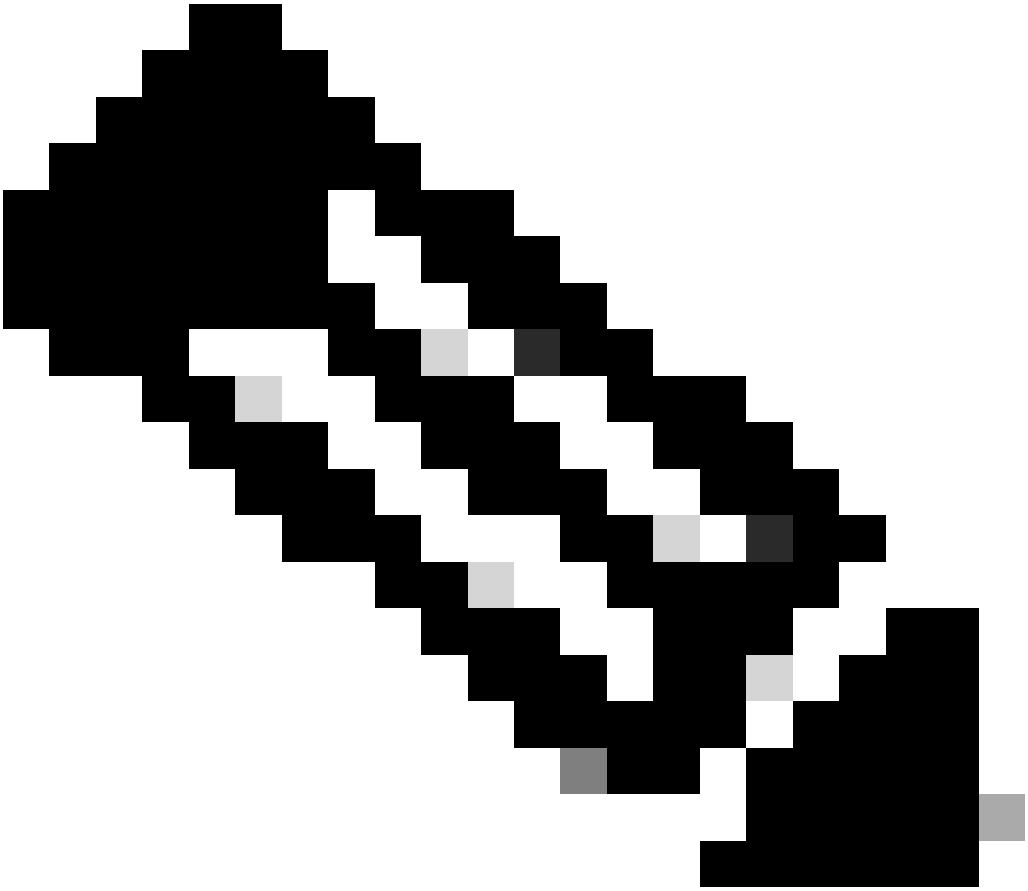
Stap 4. Wanneer u het probleem dat u wilt oplossen reproduceert, klikt u op Stop .

Stap 5. Voor elk gedebuggd mac-adres kunt u een logbestand genereren door te klikken op alle logbestanden die betrekking hebben op dat mac-adres Generate .

Stap 6. Kies hoe lang u wilt dat uw gecollationeerde logbestand gaat en klik op Toepassen op apparaat.

Stap 7. U kunt het bestand nu downloaden door op het kleine pictogram naast de bestandsnaam te klikken. Dit bestand is aanwezig in de boot flash drive van de controller en kan ook uit het vak worden gekopieerd via CLI.

!!Ingesloten Captures gefilterd op client-MAC-adres in beide richtingen, client inwendige MAC-filter beschikbaar na 17.1.



Opmerking: EPC op 9800 is handig als centrale DHCP is ingeschakeld op 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

Via GUI:
Stap 1. Navigeer naar Troubleshooting > Packet Capture > +Add .

Stap 2. Bepaal de naam van de pakketopname. U mag maximaal 8 tekens gebruiken.

Stap 3. Definieer eventuele filters.

Stap 4. Schakel het vakje Monitor Control Traffic in als u wilt zien dat verkeer wordt gestraft naar de systeem CPU en opnieuw wordt ingespoten in het dataplatform.

Stap 5. Definieer de buffergrootte. Een maximum van 100 MB is toegestaan.

Stap 6. Definieer de limiet, hetzij door de duur die een bereik van 1 - 1000000 seconden toestaat, hetzij door het aantal pakketten dat een bereik van 1 - 100000 pakketten toestaat, zoals gewenst.

Stap 7. Kies de interface uit de lijst met interfaces in de linkerkolom en selecteer de pijl om deze naar de rechterkolom te verplaatsen.

Stap 8. Opslaan en toepassen op apparaat.

Stap 9. Om de opname te starten, selecteert u Start.

Stap 10. U kunt de opname tot de gedefinieerde limiet laten lopen. Selecteer Stop om de opname handmatig te stoppen.

Stap 11. Zodra gestopt, wordt een Export knop beschikbaar om te klikken met de optie om het opnamebestand (.pcap) op de lokale desktop te downloaden via HTTP of TFTP server of FTP server of lokale systeem harde schijf of flash.

Logbestanden vanaf de AP-kant

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

Logbestanden vanaf DHCP-server

Wanneer u een externe DHCP-server gebruikt, is het nodig om debug-logbestanden te verzamelen en pakketopnamen te maken aan de serverkant om de stroom van DHCP-verkeer te verifiëren.

Andere logbestanden

Als u opmerkt dat de DHCP-detectieberichten zichtbaar zijn op de 9800 WLC in een Central DHCP-instelling, of dat binnen AP debug-logbestanden in een lokale DHCP-instelling worden geopend, moet u doorgaan om opnamegegevens van de uplink te verzamelen om te bevestigen dat de pakketten niet vallen in de Ethernet-poort.Afhankelijk van de mogelijkheden van de switch, hebt u de mogelijkheid om een ingesloten pakketopname of een SPAN-opname (Switched Port Analyzer) uit te voeren op de uplink-switch. Het is aan te raden om de DHCP-verkeersstroom stap voor stap te overtrekken om het punt te bepalen waarop de communicatie wordt onderbroken, zowel van de DHCP-client naar de DHCP-server als in de omgekeerde richting.

Bekende problemen

Probleem 1. De client probeert een IP-adres te verkrijgen van een VLAN dat eerder is behouden. Er kunnen zich situaties voordoen waarin een switch tussen twee SSID's gekoppeld aan verschillende client-VLAN's kan optreden. In dergelijke gevallen kan de client doorgaan met het aanvragen van een IP-adres van het VLAN waarmee het eerder verbonden was. Omdat dit IP niet binnen de DHCP-scope van het huidige VLAN valt, geeft de DHCP-server een NAK (negatieve bevestiging) uit, waardoor de client geen IP-adres kan verkrijgen.

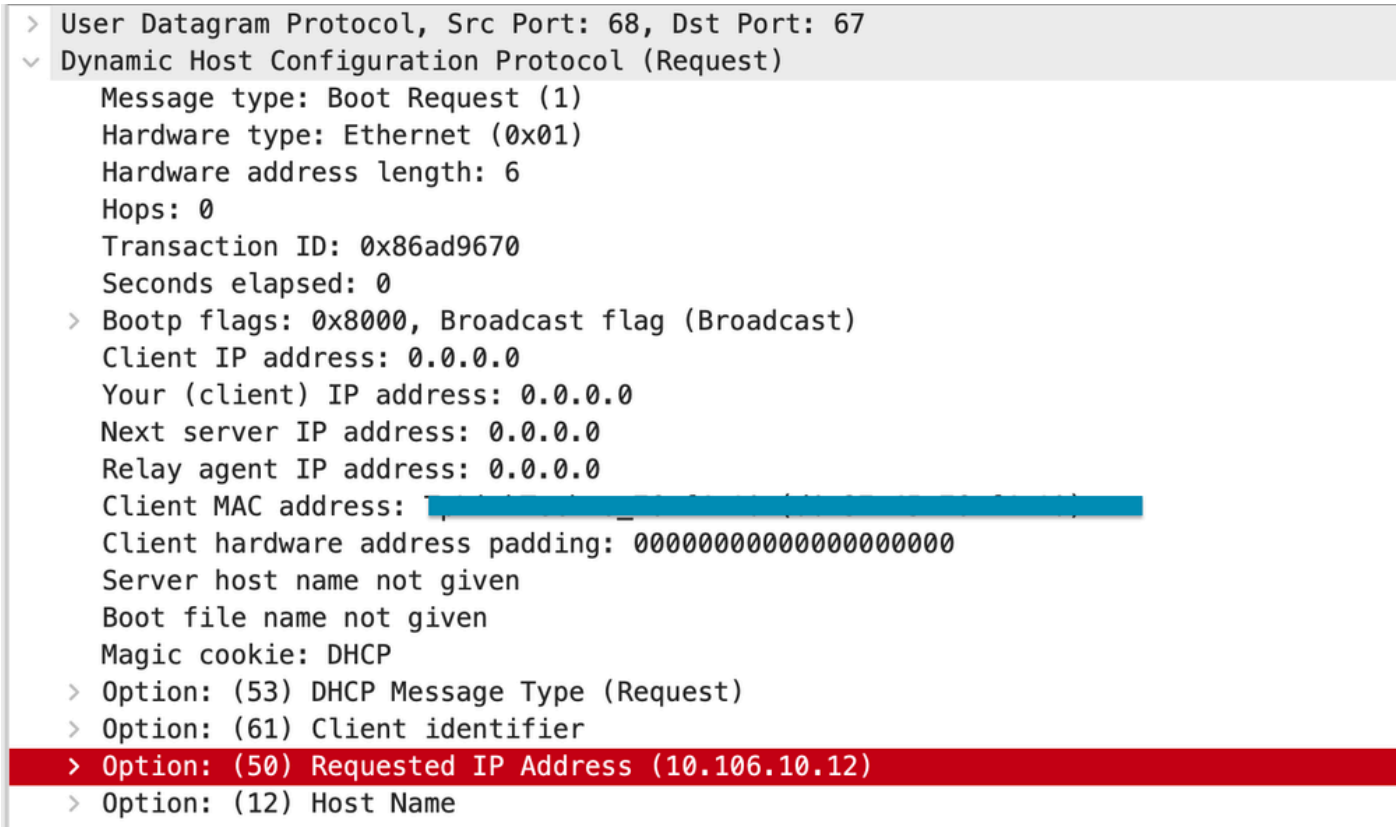
In de Radioactieve overtrek logboeken, is het duidelijk dat de client blijft zoeken naar een IP van het VLAN waarmee het voorheen verbonden was, namelijk VLAN 10, ondanks het feit dat de client VLAN voor de huidige SSID VLAN 20 is.

```
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
```

Ingesloten pakketvastlegging op 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
```

Ingesloten pakketvastlegging op WLC



DHCP-optie 50 bij WLC-pakketvastlegging

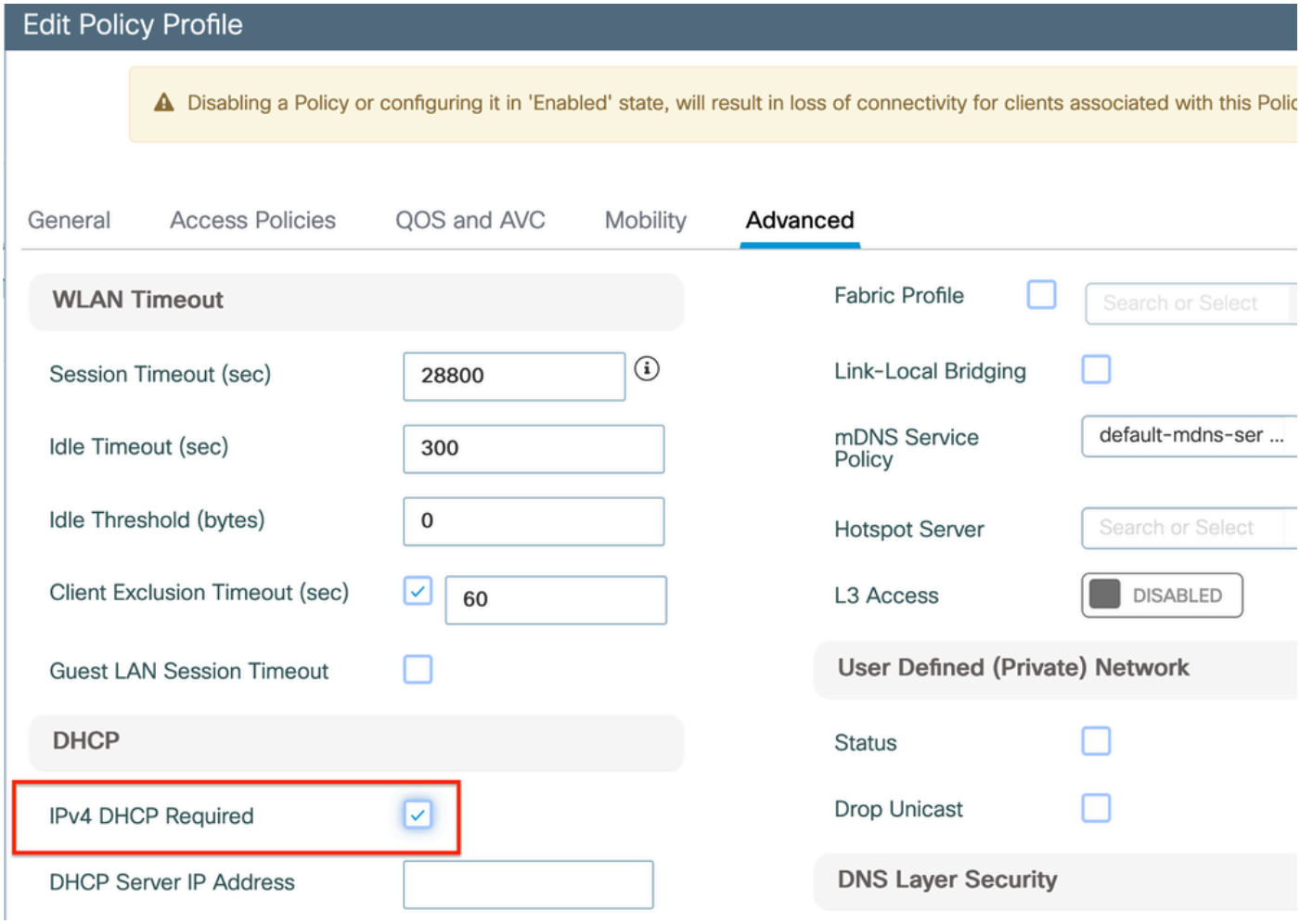
Resolutie: Om ervoor te zorgen dat een client het volledige DHCP-proces voltooit, kunt u de optie IPv4 DHCP Required in de beleidsconfiguratie inschakelen. Deze instelling moet worden ingeschakeld, met name wanneer de client overschakelt tussen SSID's, om de DHCP-server toe te staan een NAK naar de client te verzenden als deze een IP-adres aanvraagt bij een VLAN dat aan de vorige SSID is gekoppeld. Anders kan de client het IP-adres blijven gebruiken of opvragen dat hij eerder had, wat tot verstoorde communicatie kan leiden. Houd er echter rekening mee dat het inschakelen van deze optie gevolgen zal hebben voor draadloze clients die zijn geconfigureerd met een statisch IP-adres.

Hier is het proces om de gewenste optie in te schakelen:

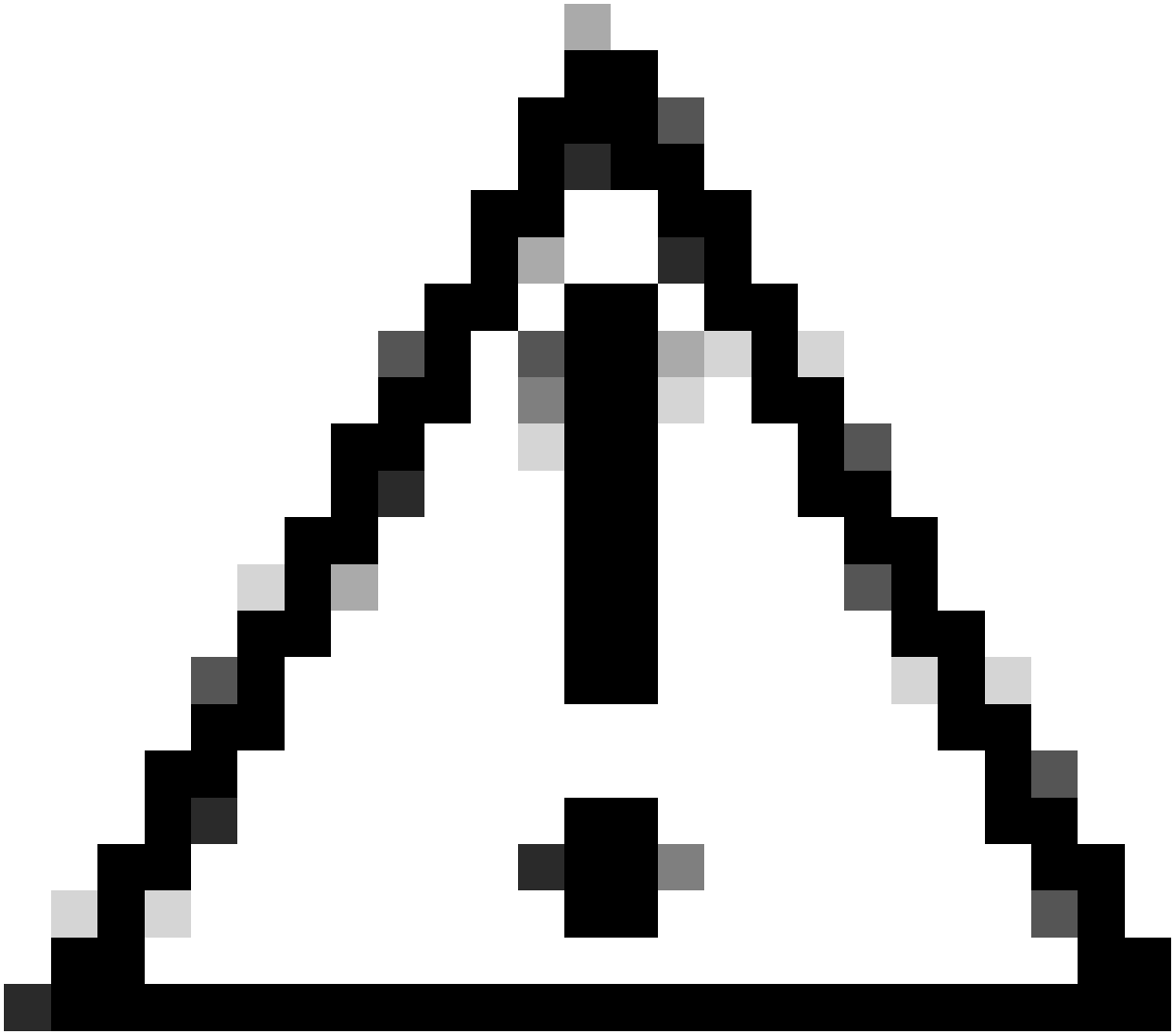
Via CLI:

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

Via GUI: Navigeer naar Configuration > Tags & Profile > Policy > Policy_name > Advanced. Onder DHCP-sectie ipv4 DHCP inschakelen vereist.



Policy Profile Setting op WLC



Voorzichtig: voor een buitenlands ankeropstelling, is het belangrijk om de instellingen van DHCP over beide WLCs te richten. Als IPV4 DHCP ingeschakeld is, moet het ingeschakeld zijn op zowel de vreemde als de ankerWLC's. Een discrepantie in de DHCP-gerelateerde configuratie onder het beleidsprofiel tussen de twee kan ervoor zorgen dat clients problemen met hun mobiliteitsrollen ervaren.

Probleem 2: client wordt verwijderd of uitgesloten vanwege IP-diefstal. IP-diefstal, in de context van netwerken, verwijst naar een situatie waarin meerdere draadloze clients proberen hetzelfde IP-adres te gebruiken. Dit kan te wijten zijn aan vele redenen die hieronder worden opgesomd:

1. Statische IP-toewijzing door onbevoegden: wanneer een gebruiker een statisch IP-adres op zijn apparaat instelt dat samenvalt met een reeds toegewezen of geoormerkt IP-adres op het netwerk, kan dit leiden tot een IP-conflict. Dit gebeurt wanneer twee apparaten proberen te werken met een identiek IP-adres, wat de netwerkverbindingen voor een van beide of beide apparaten kan verstoren. Om dergelijke problemen te voorkomen, is het van essentieel belang dat elke client in het netwerk is geconfigureerd met een uniek IP-adres.

2. Rogue DHCP Server: De aanwezigheid van een niet-geautoriseerde of schurkenDHCP-server op het netwerk kan leiden tot IP-

adrestoewijzing die botst met het ingestelde IP-adresseringsschema van het netwerk. Zulke conflicten kunnen ertoe leiden dat verschillende apparaten IP-adresbotsingen ondervinden of onjuiste netwerkinstellingen verkrijgen. Om dit probleem aan te pakken, moeten inspanningen worden geleverd om de bedrieglijke DHCP-server te identificeren en te elimineren uit het netwerk om verdere IP-conflicten binnen hetzelfde subnetnummer te voorkomen.

3. Stale Entry of client in 9800 WLC: Soms kan de controller verouderde/verouderde gegevens van een IP-adres dat een klant probeert te verkrijgen, behouden. In deze gevallen wordt het noodzakelijk om deze verouderde ingangen handmatig te verwijderen uit de 9800 WLC. Zo moet u het doen:

- Draai het radioactieve spoor voor het adres mac dat in de uitsluitingslijst is en filtreer het met wetit mac in het radioactieve spoor.

- U kunt de foutenlogboeken zien: %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REDEN: Client MAC: Affected_Client_MAC met IP: 10.37.57.24 is toegevoegd aan de uitsluitingslijst, legit client MAC: Legit_Client_MAC, IP: 10.37.57.24, reden: IP-adresdiefstal

- Voer vervolgens deze opdrachten uit:
show wireless device-tracking database mac | sec $Legit_Client_MAC
show wireless device-tracking database ip | sec $Legit_Client_MAC

(Als er enige verouderde items zijn, kunt u meer dan één IP zien voor een legaal client-Mac-adres: de ene is het oorspronkelijke IP, terwijl de andere verouderd/verouderd is].

Resolutie: Verwijder de oude vermeldingen handmatig van 9800 WLC met behulp van clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. In flex-implementatie met lokale DHCP-server met dezelfde subnetverbinding: in FlexConnect-configuraties is het voor verschillende externe locaties gebruikelijk om een lokale DHCP-server te gebruiken die IP-adressen toewijst aan een identiek subnetnummer. Dit scenario kan ertoe leiden dat draadloze clients op verschillende locaties hetzelfde IP-adres ontvangen. Controllers binnen dit netwerkkader zijn geprogrammeerd om te detecteren wanneer meerdere clientverbindingen een identiek IP-adres gebruiken, en dit te interpreteren als potentiële IP-diefstal. Hierdoor worden deze clients meestal op een geblokkeerde lijst geplaatst om conflicten met IP-adressen te voorkomen.

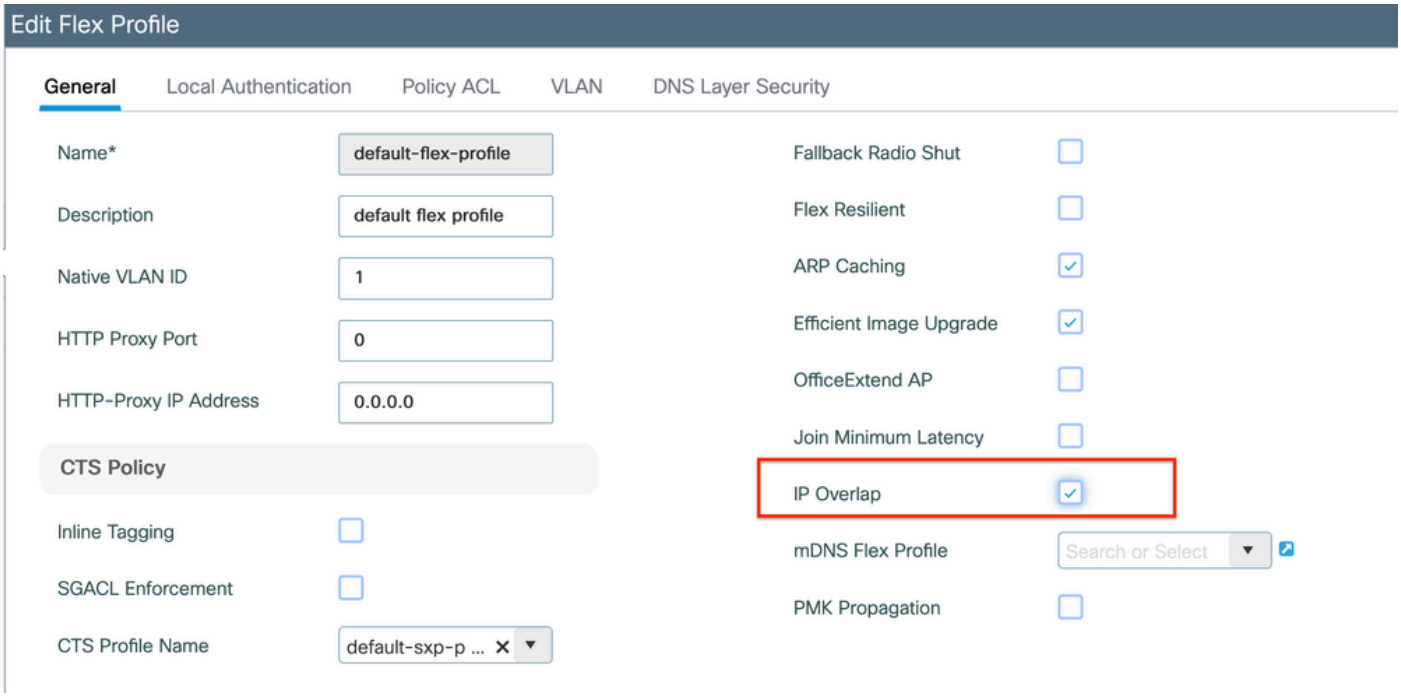
Resolutie: Schakel de overlappende IP-functie in binnen uw FlexConnect-profiel. De 'Overlapping Client IP Address in Flex Implementation'-functionaliteit maakt het gebruik van dezelfde IP-adressen op meerdere FlexConnect-sites mogelijk, terwijl alle functies en mogelijkheden die in FlexConnect-implementaties worden ondersteund, behouden blijven.

Deze optie is standaard uitgeschakeld. U kunt het op deze procedure inschakelen:

Via CLI:

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

Via GUI: Selecteer Configuration > Tags & Profiles > Flex. Klik op bestaand Flex-profiel/Toevoegen aan nieuw Flex-profiel en schakel onder het tabblad Algemeen IP-overlap in.



Flex Profile Setting op WLC

Probleem 3. Draadloze clients kunnen geen IP-adres van het beoogde VLAN ontvangen. Dit probleem treedt vaak op wanneer VLAN 1 wordt gebruikt of wanneer het VLAN dat aan clients is toegewezen, hetzelfde is als het VLAN dat wordt gebruikt voor AP-beheer in een FlexConnect-implementatie. De hoofdoorzaak van deze kwestie is doorgaans onjuiste VLAN-toewijzingen. Hier vindt u een aantal scenario's die u in overweging moet nemen bij het configureren van VLAN-ID's in de 9800-serie:

1. Wanneer u een AAA-server gebruikt terwijl de AAA-override-functie is geactiveerd, is het van cruciaal belang dat de juiste VLAN-id wordt verzonden vanaf de AAA-server. Als in plaats daarvan een VLAN-naam wordt opgegeven, bevestig dat deze overeenkomt met de VLAN-naam die op de 9800 WLC is geconfigureerd.

2. Wanneer VLAN 1 is geconfigureerd voor draadloos clientverkeer, kan het gedrag variëren, afhankelijk van de modus van het toegangspunt (AP):

Voor een AP in de lokale modus/Centraal schakelen:

- VLAN-naam opgeven = standaard, de client wordt toegewezen aan VLAN 1
- Met VLAN-ID 1 wordt een client toegewezen aan draadloos beheer VLAN

Voor een AP in Flex modus/Local Switching:

- VLAN-naam opgeven = standaard, de client wordt toegewezen aan VLAN 1
- Gebruikend VLAN-ID 1, wordt een client toegewezen aan FlexConnect native VLAN

Hier zijn een paar voorbeelden van scenario's die in het laboratorium zijn geëxperimenteerd, samen met hun resultaten:

1. Standaard, als de gebruiker niets onder het beleidsprofiel vormt, wijst de WLC VLAN-ID 1 toe zodat clients het draadloze beheer VLAN in de lokale modus en het AP native VLAN voor FlexConnect zullen gebruiken.

2. Als het Native VLAN onder flex-profiel is geconfigureerd met een native VLAN-id die verschilt van de id die op de switch is geconfigureerd, ziet u het probleem, de client krijgt IP van beheer VLAN (native VLAN), zelfs als het beleidsprofiel is geconfigureerd met de naam "standaard" VLAN.

3. Als Native VLAN onder flex-profiel met VLAN-ID hetzelfde is geconfigureerd als het native VLAN dat op de switch is geconfigureerd, kan alleen de client een IP van VLAN 1 krijgen met een standaardconfiguratie onder beleidsprofiel.

4. Als u een VLAN-naam hebt geselecteerd in plaats van een VLAN-id, controleert u of de VLAN-naam in het Flex Profile dezelfde is.

Gerelateerde informatie

- Interne DHCP-server op 9800
- Externe DHCP-server in gebruik
- DHCP-optie 82 Sub Option 5 in Windows DHCP-server
- NAT-PAT in Flex AP
- VLAN 1 wordt gebruikt voor draadloze client
- Cisco Technical Support en downloads

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.