Fehlerbehebung bei Verbindungsproblemen von DHCP-Clients auf einem Cisco 9800 WLC

Inhalt

Einleitung

In diesem Dokument werden verschiedene Probleme im Zusammenhang mit dem Dynamic Host Configuration Protocol (DHCP) beschrieben, auf die Wireless-Clients stoßen, wenn sie mit einem Cisco 9800 Wireless LAN Controller (WLC) verbunden sind. Außerdem wird beschrieben, wie diese Probleme behoben werden.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Grundkenntnisse des Cisco WLC 9800

- Grundkenntnisse von DHCP Flow
- Grundkenntnisse des AP im lokalen und Flex Connect-Modus

Verständnis des DHCP-Datenverkehrs mit Wireless-Clients

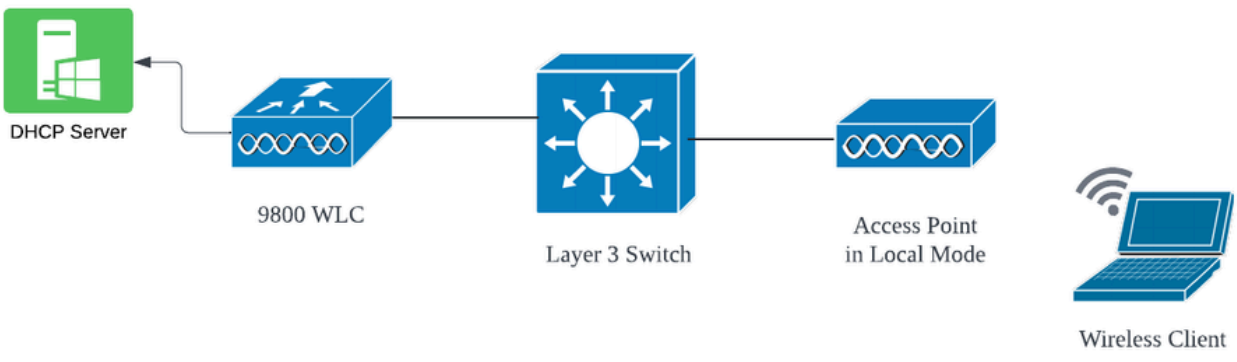
Wenn der Wireless-Client eine Verbindung herstellt, führt er den üblichen DHCP-Austausch durch, indem er einen Broadcast-DHCP-Erkennungsframe sendet, um einen DHCP-Server für den zugehörigen WAP zu finden. Je nach Betriebsart des AP leitet er die Anforderung entweder über den CAPWAP-Tunnel an den WLC weiter oder leitet sie direkt an den nächsten Hop weiter. Wenn ein DHCP-Server innerhalb der lokalen Layer-2-Domäne verfügbar ist, reagiert er und ermöglicht eine erfolgreiche Verbindung. Wenn kein lokaler Subnetz-DHCP-Server vorhanden ist, muss der Router (der mit der SVI des Clients konfiguriert ist) so konfiguriert werden, dass die DHCP-Erkennung an den entsprechenden Server weitergeleitet wird. Hierzu wird auf dem Router in der Regel eine IP-Hilfsadresse konfiguriert, die den Router anweist, bestimmten Broadcast-UDP-Datenverkehr (z. B. DHCP-Anfragen) an eine vorbestimmte IP-Adresse weiterzuleiten.

Das Verhalten des DHCP-Datenverkehrs der Clients hängt vollständig vom Modus ab, in dem der Access Point (AP) betrieben wird. Betrachten wir jedes dieser Szenarien einzeln:

Szenario 1. Der Access Point (AP) arbeitet im lokalen Modus.

Wenn ein WAP im lokalen Modus eingerichtet wird, wird der DHCP-Datenverkehr des Clients zentral weitergeleitet, d. h. die DHCP-Anfragen der Clients werden über einen CAPWAP-Tunnel vom WAP an den WLC gesendet, wo sie dann entsprechend verarbeitet und weitergeleitet werden. In diesem Fall haben Sie zwei Möglichkeiten: Sie können entweder einen internen DHCP-Server verwenden oder einen externen DHCP-Server wählen.

Topologie (AP im lokalen Modus)



Anwenderbericht 1. Wenn der WLC als interner DHCP-Server konfiguriert ist

Der Controller kann dank der integrierten Funktionen der Cisco IOS XE Software einen internen DHCP-Server bereitstellen. Es wird jedoch als Best Practice erachtet, einen externen DHCP-Server zu verwenden. Bevor der WLC als interner DHCP-Server eingerichtet werden kann, müssen mehrere Voraussetzungen erfüllt sein:

- Konfigurieren Sie eine Switched Virtual Interface (SVI) für das Client-VLAN, und weisen Sie ihm die IP-Adresse des DHCP-Servers zu.
- Die IP-Adresse des internen DHCP-Servers sollte an der zum Server gerichteten Schnittstelle festgelegt werden, bei der es sich um eine Loopback-Schnittstelle, eine SVI oder eine physische Layer-3-Schnittstelle handeln kann.
- Die Konfiguration einer Loopback-Schnittstelle wird empfohlen, da diese im Gegensatz zu physischen Schnittstellen, die eine Verbindung zu den tatsächlichen Netzwerksegmenten herstellen, nicht an die Hardware gebunden ist und keinem physischen Port des Geräts entspricht. Der Hauptzweck einer Loopback-Schnittstelle besteht in der Bereitstellung einer stabilen, stets verfügbaren Schnittstelle, die keinen Hardwarefehlern oder physischen Verbindungsunterbrechungen unterliegt.

Working Setup (Funktionierende Einrichtung): Dies ist ein Beispiel für eine interne DHCP-Serverkonfiguration, bei der Clients erfolgreich IP-Adressen erhalten haben. Im Folgenden sind die Betriebsprotokolle und die zugehörigen Einrichtungsdetails aufgeführt.

Richten Sie den WLC als DHCP-Server für VLAN 10 ein, mit einem DHCP-Bereich von 10.106.10.11/24 bis 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
```

Konfigurierte Loopback-Schnittstelle auf WLC:

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

Client-VLAN konfiguriert als SVI [L3-Schnittstelle] mit Hilfsadresse als Loopback-Schnittstelle auf dem 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
```

Alternativ können Sie die IP-Adresse des DHCP-Servers im Richtlinienprofil festlegen, anstatt eine Hilfsadresse unter der SVI zu konfigurieren. Im Allgemeinen wird jedoch empfohlen, die Konfiguration für jedes VLAN durchzuführen, um Best Practices zu erhalten:

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

Radioaktive Spuren auf 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
```

Integrierte Paketerfassung auf 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
```

Integrierte Paketerfassung auf WLC

AP-Client-Debugging:

```
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>
```

Clientseitige Paketerfassung:

```
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-Paketerfassung

In den bereitgestellten Betriebsprotokollen können Sie sehen, dass der WLC die DHCP Discover-Nachricht vom Wireless-Client empfängt und vom VLAN des Clients an die Helper-Adresse weitergeleitet wird (im vorliegenden Beispiel ist dies die interne Loopback-Schnittstelle). Daraufhin gibt der interne Server ein DHCP Offer aus, woraufhin der Client eine DHCP Request sendet, die dann vom Server mit einem DHCP ACK quittiert wird.

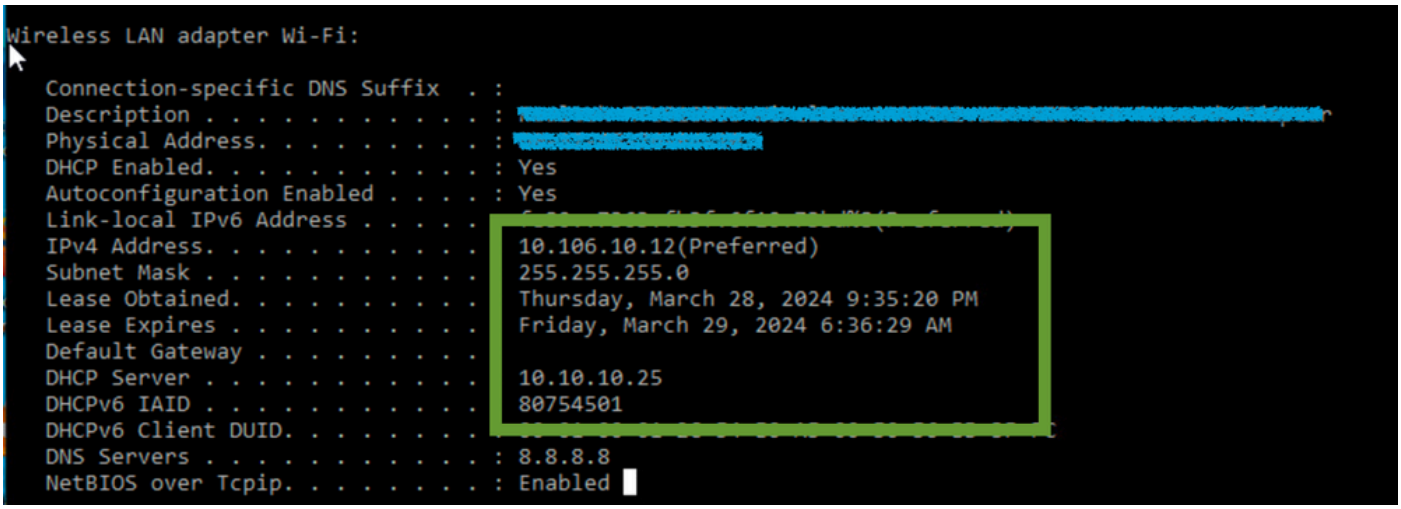
Verifizierung der Wireless Client IP:

Auf WLC:

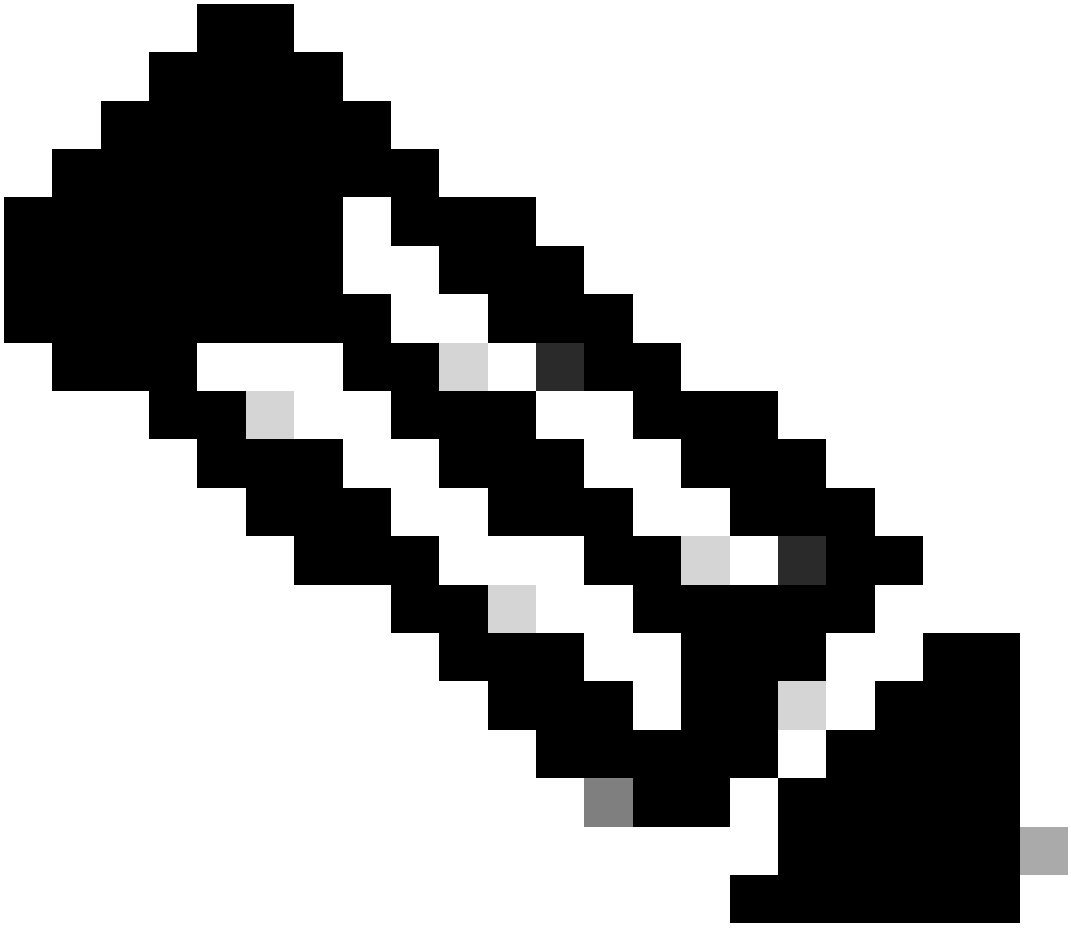
```
WLC#show ip dhcp binding
```

```
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
```

Auf Wireless-Client:



IP-Verifizierung am Client-Ende



Anmerkung:
1. VRF wird von den internen DHCP-Servern nicht unterstützt.
2. DHCPv6 wird von den internen DHCP-Servern nicht unterstützt.
3. Auf C9800 ermöglicht SVI die Konfiguration mehrerer Helferadressen, es werden jedoch nur die ersten beiden verwendet.
4. Dies wurde getestet und wird daher plattformübergreifend für maximal 20 % der maximalen Client-Skalierung der Box unterstützt. Bei einem Router der Serie 9800-80, der 64.000 Clients unterstützt, beträgt die maximale Anzahl der unterstützten DHCP-Bindungen etwa 14.000.

Anwenderbericht 2. Bei Verwendung eines externen DHCP-Servers

Ein externer DHCP-Server ist ein DHCP-Server, der nicht in den WLC selbst integriert ist, sondern auf einem anderen Netzwerkgerät [Firewall, Router] oder einer separaten Einheit innerhalb der Netzwerkinfrastruktur konfiguriert ist. Dieser Server ist speziell für die dynamische Verteilung von IP-Adressen und anderen Netzwerkkonfigurationsparametern an Clients im Netzwerk ausgelegt.

Bei Verwendung eines externen DHCP-Servers dient der WLC lediglich dazu, Datenverkehr zu empfangen und weiterzuleiten. Wie der DHCP-Datenverkehr vom WLC geroutet wird (Broadcast oder Unicast), hängt von Ihren Präferenzen ab. Betrachten wir jede dieser Methoden getrennt.

DHCP-Datenverkehr wird über die Layer-2-Domäne übertragen

In dieser Konfiguration agiert ein anderes Netzwerkgerät, z. B. eine Firewall, ein Uplink oder ein Core-Switch, als Relay-Agent. Wenn ein Client eine DHCP-Erkennungsanforderung sendet, ist die einzige Aufgabe des WLC, diese Nachricht über die Layer-2-Schnittstelle weiterzuleiten. Damit dies ordnungsgemäß funktioniert, müssen Sie sicherstellen, dass die Layer-2-Schnittstelle des Client-VLAN richtig konfiguriert ist und über den Datenport des WLC und das Uplink-Gerät zugelassen wird.

Gewünschte Konfiguration am WLC-Ende für das Client-VLAN 20 für diese Instanz:

Konfiguriertes Layer-2-VLAN auf dem WLC:

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

Konfigurierter Daten-Port auf dem WLC für den Datenverkehr des Client-VLAN:

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

Radioaktive Spuren auf 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 Client
```

Integrierte Paketerfassung auf 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
```

Integrierte Paketerfassung auf WLC

AP-Client-Debugging:

```
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>
```

Client-seitige Erfassung:

```
  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
```

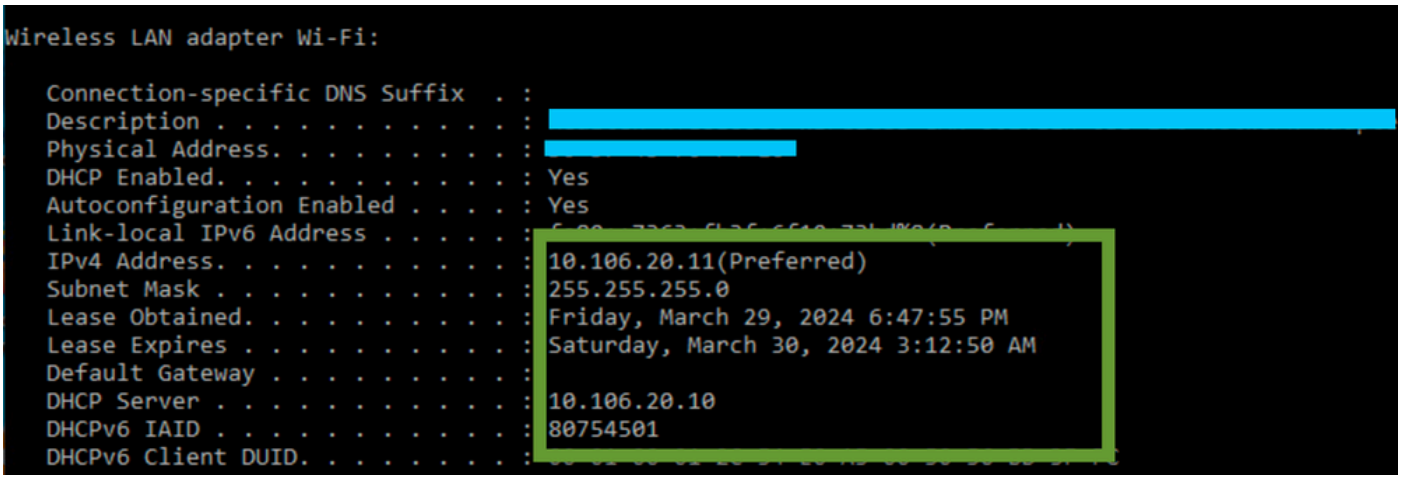
Client-End-Paketerfassung

In den bereitgestellten Betriebsprotokollen ist zu erkennen, dass der WLC den DHCP Discover-Broadcast vom Wireless-Client abfängt und dann über seine L2-Schnittstelle an den nächsten Hop weitersendet. Sobald der WLC das DHCP-Angebot vom Server erhält, leitet er diese Nachricht an den Client weiter, gefolgt von einer DHCP-Anfrage und ACK.

Verifizierung der Wireless Client IP:

Sie können die IP-Lease auf dem DHCP-Server und den entsprechenden Status überprüfen.

Auf Wireless-Client:



IP-Verifizierung auf Client-Ende

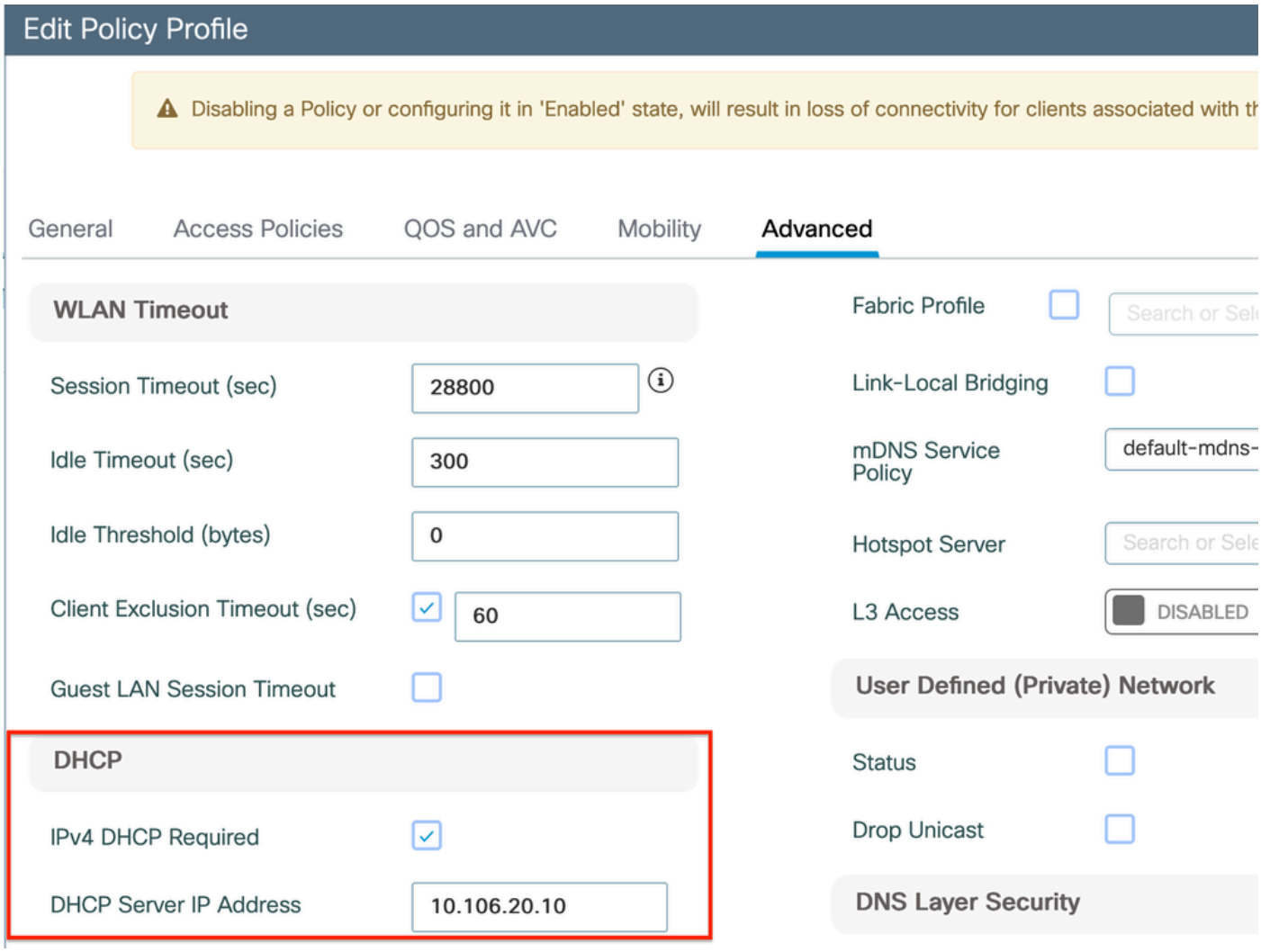
9800 WLC dient als Relay Agent

In dieser Konfiguration leitet der WLC die von Wireless-Clients empfangenen DHCP-Pakete per Unicast direkt an den DHCP-Server weiter. Um dies zu aktivieren, stellen Sie sicher, dass die VLAN-SVI für den Client auf dem WLC konfiguriert ist.

Es gibt zwei Möglichkeiten, die DHCP-Server-IP in 9800 WLC zu konfigurieren:

1. Konfigurieren Sie die IP-Adresse des DHCP-Servers unter "policy profile" (Richtlinienprofil) unter "advanced setting" (Erweiterte Einstellung).

Über GUI: Navigieren Sie zu Configuration > Tags & Profile > Policy > Policy_name > Advanced. Im DHCP-Abschnitt können Sie die IP-Adresse des DHCP-Servers wie folgt konfigurieren:



Richtlinienprofileinstellung auf WLC

Über CLI:

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

2. Innerhalb der SVI-Konfiguration müssen Sie die Adresse des Helfers angeben. Es ist möglich, mehrere DHCP-Server in der Konfiguration der Hilfsadresse einzurichten, um Redundanz zu gewährleisten. Zwar ist die Festlegung der DHCP-Serveradresse für jedes WLAN innerhalb des Richtlinienprofils möglich, es wird jedoch empfohlen, die Adresse auf Schnittstellenbasis zu konfigurieren. Hierzu kann der entsprechenden SVI eine Hilfsadresse zugewiesen werden.

Bei Verwendung der Relay-Funktion ist die Quelle des DHCP-Datenverkehrs die IP-Adresse der Switched Virtual Interface (SVI) des Clients. Dieser Datenverkehr wird dann über die Schnittstelle weitergeleitet, die dem Ziel (der IP-Adresse des DHCP-Servers) entspricht, wie in der Routing-Tabelle festgelegt.

Hier ist ein Beispiel für die funktionierende Konfiguration des 9800, der als Relay-Agent fungiert:

Konfigurierte Layer-3-Schnittstelle für Client-VLAN auf WLC mit Helferadresse:

```
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
```

Konfigurierter Daten-Port auf dem WLC für den Datenverkehr des Client-VLAN:

```
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-Ablaufverfolgungen vom 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
```

Integrierte Paketerfassung auf 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

Integrierte Paketerfassung auf WLC

Sowohl bei den radioaktiven Traces (RA) als auch bei der Embedded Packet Capture (EPC) auf dem WLC stellen Sie fest, dass der WLC als Relay-Agent die DHCP-Pakete direkt vom Client an den DHCP-Server per Unicast sendet.

AP-Client-Debugging:

```
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>
```

Client-seitige Erfassung:

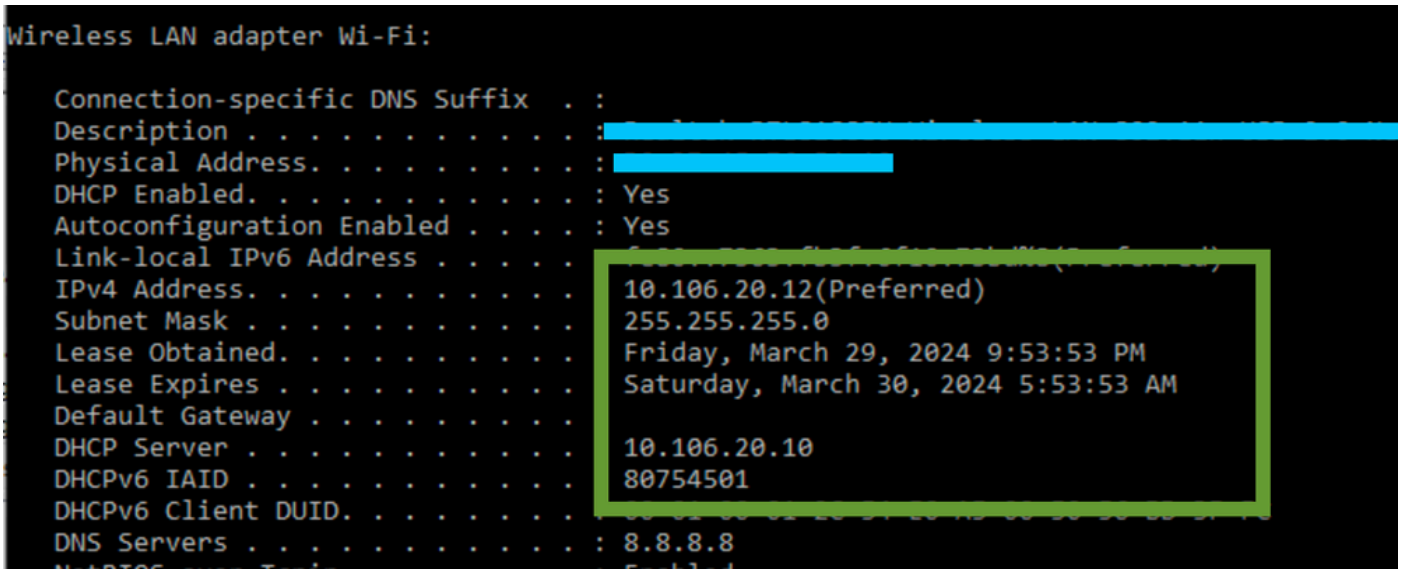
No.	Time	Source	Destination	Protocol	Length	Info
1	10:23:46.630692	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
50	10:23:50.627940	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x137ea7ac
59	10:23:53.694541	10.106.20.1	255.255.255.255	DHCP	342	DHCP Offer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

Verifizierung der Wireless Client IP:

Sie können die IP-Lease auf dem DHCP-Server und den entsprechenden Status überprüfen.

Auf Wireless-Client:



IP-Verifizierung auf Client-Ende

DHCP-Option 80 mit Suboption 5/150 in 9800 WLC

In bestimmten Szenarien ziehen Sie es möglicherweise vor, die Quellschnittstelle für den DHCP-Datenverkehr explizit zu definieren, anstatt von der Routing-Tabelle abhängig zu sein, um potenzielle Netzwerkkomplikationen zu vermeiden. Dies ist besonders dann von Bedeutung, wenn das nächste Netzwerkgerät entlang des Pfads, z. B. ein Layer-3-Switch oder eine Firewall, Reverse Path Forwarding (RPF)-Prüfungen verwendet. Nehmen wir als Beispiel eine Situation, in der die Wireless-Management-Schnittstelle auf VLAN 50 festgelegt ist, während sich die Client-SVI auf VLAN 20 befindet und als DHCP-Relay für Client-Datenverkehr verwendet wird. Die Standardroute wird zum Gateway des Wireless-

Management-VLANs/Subnetzes geleitet.

Ab Version 17.03.03 des 9800 WLC kann als Quellschnittstelle für DHCP-Datenverkehr entweder das Client-VLAN oder ein anderes VLAN, z. B. die Wireless Management Interface (WMI), gewählt werden, die die Verbindung zum DHCP-Server gewährleistet.

Dies ist ein Ausschnitt aus der Konfiguration:

```
!
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 diesem Szenario stammt der Datenverkehr zum DHCP-Server 10.100.17.14 von VLAN 50 (10.100.16.10), da die Ausgangsschnittstelle des Pakets auf der Grundlage einer Suche in der IP-Routing-Tabelle ausgewählt wird. Normalerweise wird das Paket aufgrund der konfigurierten Standardroute über das WMI-VLAN verlassen.
Wenn jedoch ein Uplink-Switch Reverse Path Forwarding (RPF)-Prüfungen implementiert, kann er ein Paket verwerfen, das von VLAN 50 eingeht, aber eine IP-Quelladresse hat, die zu einem anderen Subnetz gehört [VLAN 20].

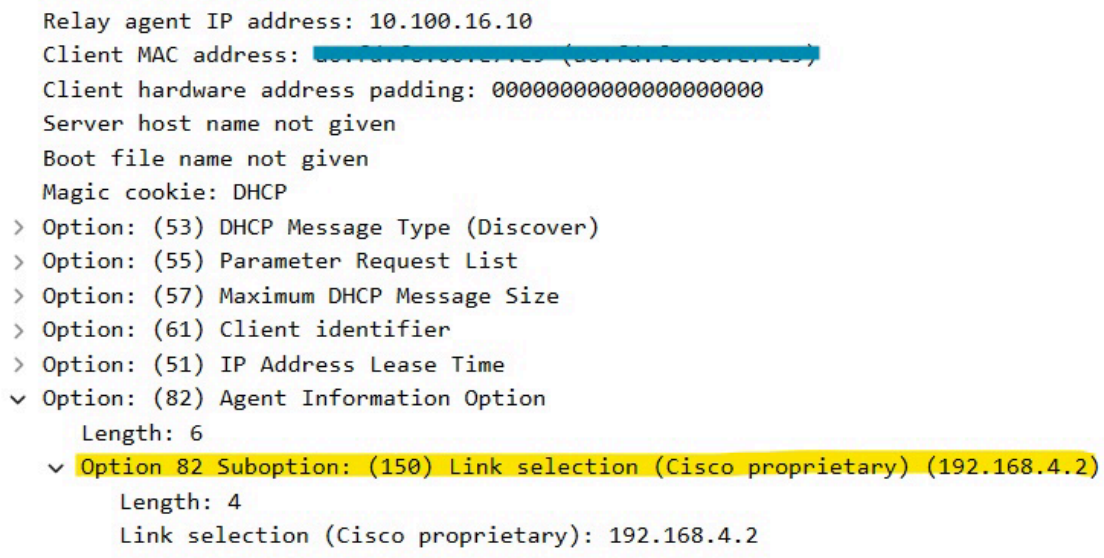
Um dies zu verhindern, sollten Sie mit dem Befehl IP DHCP relay source-interface eine präzise Quellschnittstelle für die DHCP-Pakete festlegen. In diesem speziellen Fall sollten die DHCP-Pakete von der WMI-Schnittstelle in VLAN 50 stammen:

```
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
```

Bei Verwendung ip dhcp relay source-interface des Befehls "command" wird sowohl die Quellschnittstelle der DHCP-Pakete als auch der GIADDR auf die im DHCP-Relay-Befehl angegebene Schnittstelle gesetzt (in diesem Fall VLAN50). Dies ist problematisch, da es sich nicht um das Client-VLAN handelt, dem Sie DHCP-Adressen zuweisen möchten.

Woher weiß der DHCP-Server, wie er die IP aus dem richtigen Client-Pool zuweist?

Wenn der Befehl verwendet wird, fügt C9800 ip dhcp relay source-interface die Client-Subnetz-Informationen automatisch in eine proprietäre Suboption 150 von Option 82 ein, die als Verbindungsauswahl bezeichnet wird, wie Sie in der Aufzeichnung sehen können:



Option 182, Unteroption 150 auf WLC Packet Capture

Standardmäßig wird die Suboption 150 (proprietär von Cisco) hinzugefügt. Stellen Sie sicher, dass der verwendete DHCP-Server diese Informationen interpretieren und darauf reagieren kann. Es wird empfohlen, die C9800-Konfiguration zu ändern und die Standardoption 82, Unteroption 5 zum Senden der Verbindungsauswahlinformationen zu verwenden. Hierzu können Sie den folgenden globalen Befehl konfigurieren:

<#root>

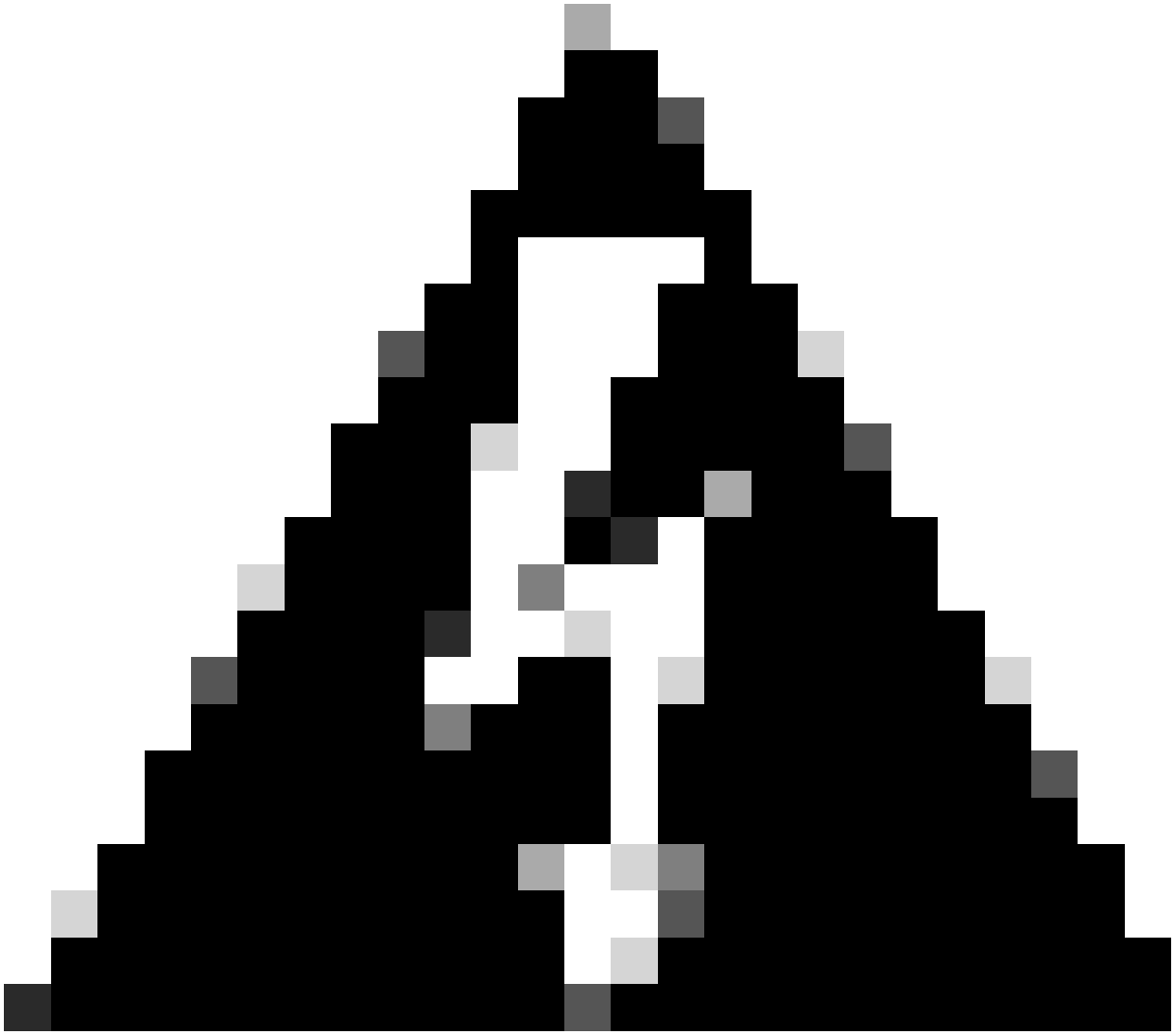
```
C9800(config)#ip dhcp compatibility suboption link-selection standard
```

Sobald der angegebene Befehl angewendet wurde, ersetzt das System die Suboption 150 in den DHCP-Paketen durch die Suboption 5. Suboption 5 wird von Netzwerkgeräten eher erkannt, wodurch die Wahrscheinlichkeit sinkt, dass Pakete verworfen werden. Die Anwendung dieser Änderung zeigt sich auch in der vorgesehenen Erfassung:

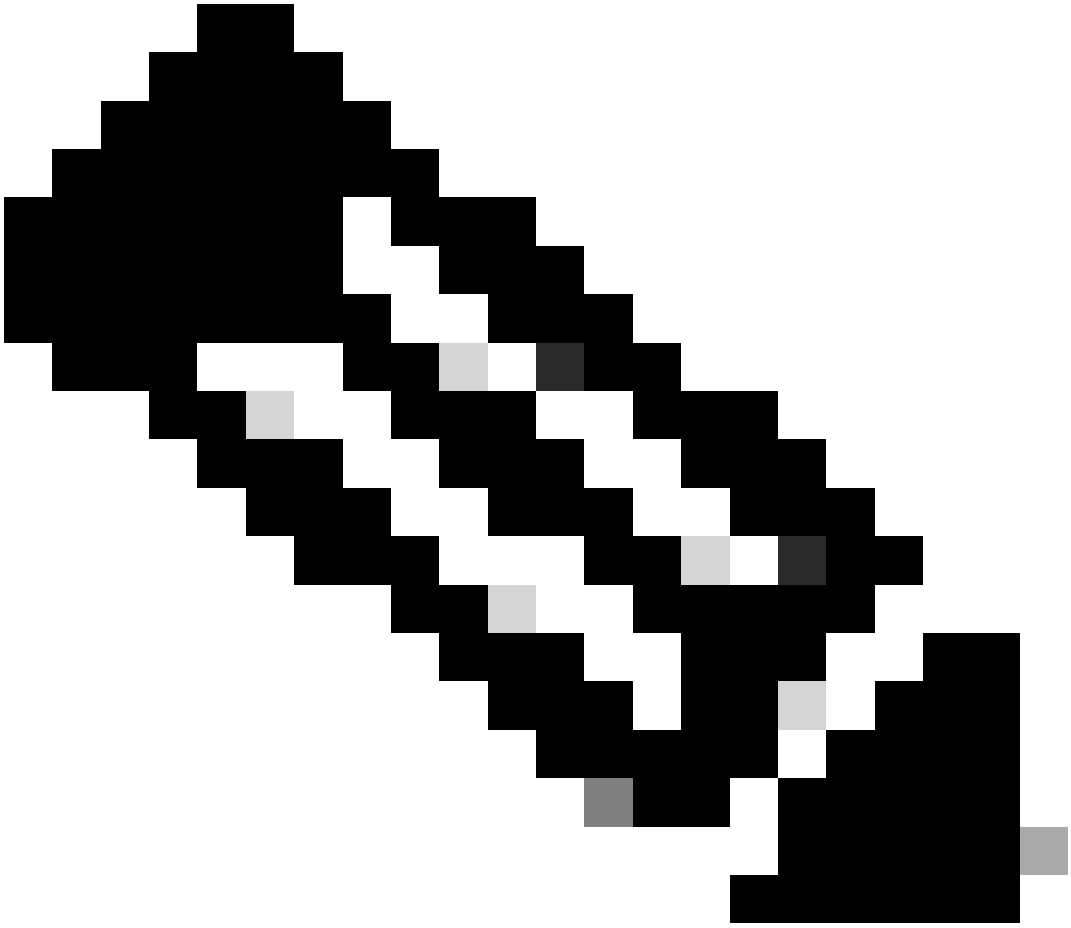
Option 182, Unteroption 5 bei WLC-Paketerfassung

Mit der Implementierung von Suboption 5 sollte Ihr DHCP-Verkehr von anderen Netzwerkgeräten quittiert werden. Es können jedoch weiterhin NAK-Meldungen (negative Bestätigungsmeldungen) auftreten, insbesondere wenn der Windows-DHCP-Server verwendet wird. Dies kann daran liegen, dass der DHCP-Server die Quell-IP-Adresse nicht autorisiert, möglicherweise weil er keine entsprechende Konfiguration für diese Quell-IP besitzt.

Was müssen Sie auf dem DHCP-Server tun? Für den Windows DHCP-Server müssen Sie einen Dummy-Bereich erstellen, um die IP-Adresse des Relay-Agenten zu autorisieren.



Warnung: Alle GIADDR-Adressen (Relay Agent IP-Adressen) müssen Teil eines aktiven IP-Adressbereichs des DHCP-Bereichs sein. Alle GIADDRs außerhalb der IP-Adressbereiche des DHCP-Bereichs gelten als unautorisiertes Relay, und der Windows-DHCP-Server bestätigt DHCP-Client-Anfragen dieser Relay-Agenten nicht. Für die Autorisierung von Relay-Agenten kann ein spezieller Bereich erstellt werden. Erstellen Sie einen Bereich mit dem GIADDR (oder mehrere, wenn die GIADDRs sequenzielle IP-Adressen sind), schließen Sie die GIADDR-Adresse(n) aus der Verteilung aus, und aktivieren Sie dann den Bereich. Auf diese Weise werden die Relay-Agenten autorisiert, und die Zuweisung der GIADDR-Adressen wird verhindert.

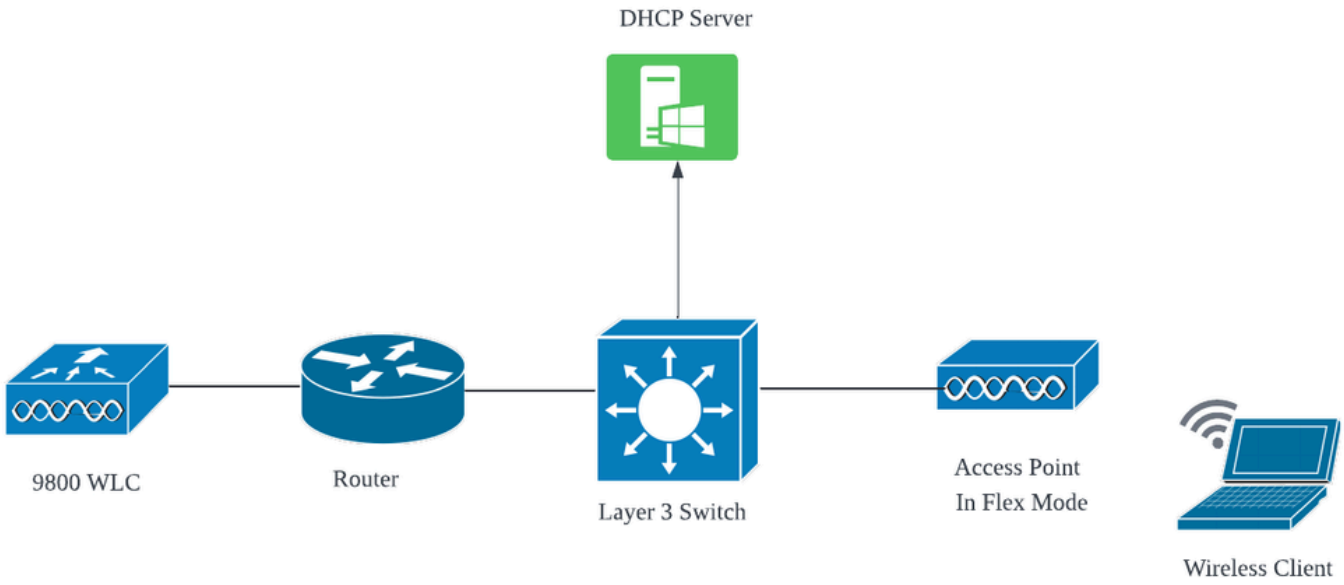


Hinweis: In einer Foreign-Anker-Konfiguration wird der DHCP-Datenverkehr zentral verarbeitet, wobei der AP-Modus auf Lokal festgelegt ist. Die DHCP-Anfragen werden zunächst an den fremden WLC gesendet, der sie dann über einen Mobility-Tunnel an den Anker-WLC weiterleitet. Der Anker-WLC verarbeitet den Datenverkehr gemäß den konfigurierten Einstellungen. Aus diesem Grund sollten alle DHCP-bezogenen Konfigurationen auf dem Anker-WLC implementiert werden.

Szenario 2. Der Access Point (AP) arbeitet im Flex-Modus.

FlexConnect APs sind für Zweigstellen und Außenstellen konzipiert und ermöglichen den Betrieb im Standalone-Modus, wenn die Verbindung zum zentralen Wireless LAN Controller (WLC) unterbrochen wird. FlexConnect-APs können den Datenverkehr lokal zwischen einem Client und dem Netzwerk umschalten, ohne einen Backhaul des Datenverkehrs zum WLC durchzuführen. Dies reduziert die Latenz und spart WAN-Bandbreite. Im Flex Mode AP kann der DHCP-Verkehr entweder zentral oder lokal vermittelt werden.

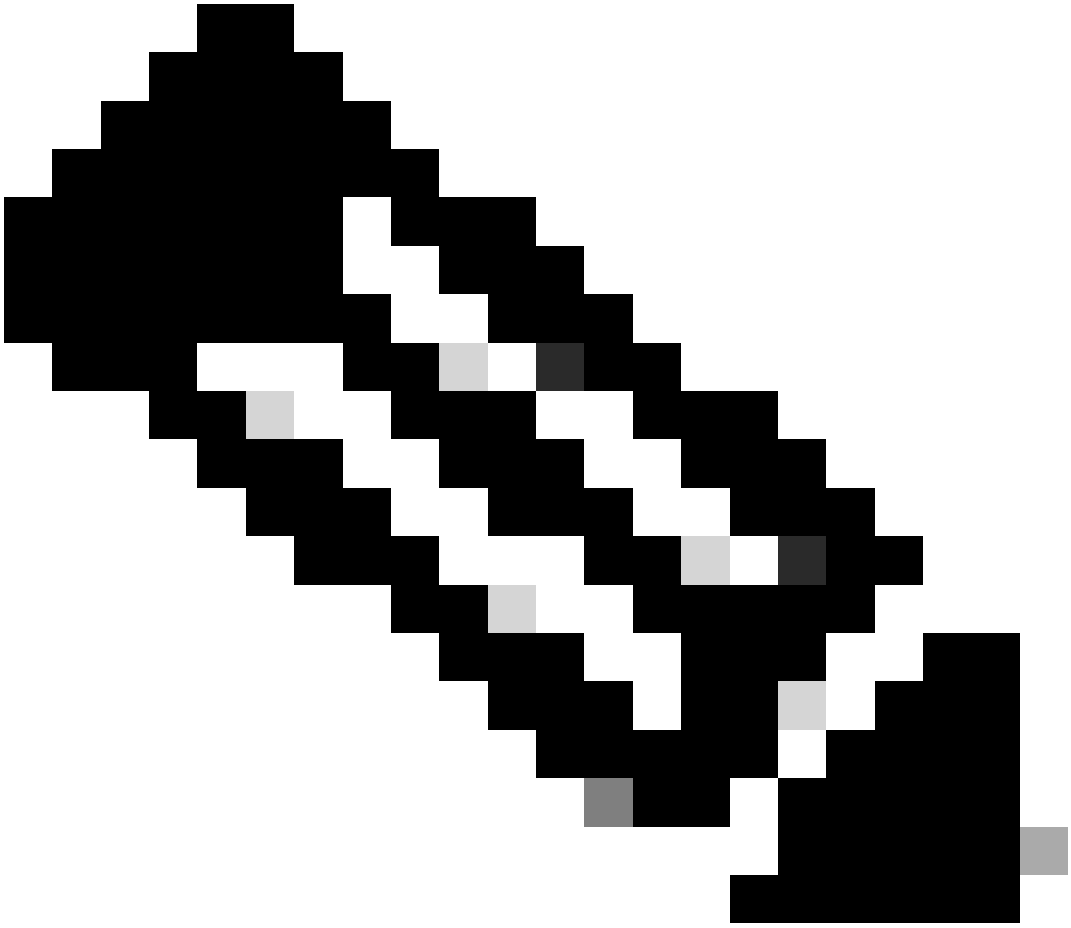
Topologie (Flex Mode AP)



Netzwerktopologie: AP im Flex-Modus

FlexConnect-Modus-AP mit zentralem DHCP

Unabhängig vom AP-Modus bleiben Konfiguration, Betriebsablauf und Schritte zur Fehlerbehebung bei Verwendung eines zentralen DHCP-Servers konsistent. Für APs im FlexConnect-Modus wird jedoch generell empfohlen, einen lokalen DHCP-Server zu verwenden, es sei denn, am lokalen Standort ist eine Client-SVI eingerichtet.



Hinweis: Wenn am Remote-Standort kein Client-Subnetz verfügbar ist, können Sie FlexConnect NAT-PAT nutzen. FlexConnect NAT/PAT führt die Network Address Translation (NAT) für den Datenverkehr durch, der von Clients stammt, die mit dem AP verbunden sind, und ordnet ihn der Management-IP-Adresse des AP zu. Wenn beispielsweise APs in Remote-Zweigstellen im FlexConnect-Modus arbeiten und die verbundenen Clients mit einem DHCP-Server in der Zentrale kommunizieren müssen, in der sich die Controller befinden, können Sie FlexConnect NAT/PAT in Verbindung mit der zentralen DHCP-Einstellung im Richtlinienprofil aktivieren.

FlexConnect-Modus-AP mit lokalem DHCP

Wenn ein FlexConnect-WAP für die Verwendung von lokalem DHCP konfiguriert ist, erhalten Client-Geräte, die dem WAP zugeordnet sind, ihre IP-Adresskonfiguration von einem DHCP-Server, der im selben lokalen Netzwerk verfügbar ist. Bei diesem lokalen DHCP-Server kann es sich um einen Router, einen dedizierten DHCP-Server oder ein anderes Netzwerkgerät handeln, das DHCP-Services innerhalb des lokalen Subnetzes bereitstellt. Bei lokalem DHCP wird der DHCP-Datenverkehr innerhalb des lokalen Netzwerks weitergeleitet, d. h. der WAP leitet DHCP-Anfragen von Clients direkt an den benachbarten Hop weiter, z. B. an den Access Switch. Von dort aus werden die Anfragen entsprechend der Konfiguration Ihres Netzwerks bearbeitet.

Voraussetzung:

1. Lesen Sie den FlexConnect-Leitfaden, um sicherzustellen, dass Ihre Konfiguration mit den Anweisungen und Best Practices im Leitfaden übereinstimmt.

2. Das Client-VLAN muss unter "flex profile" aufgeführt sein.
3. Der WAP muss im Trunk-Modus eingerichtet werden, wobei das WAP-Verwaltungs-VLAN als natives VLAN festgelegt ist und die VLANs für den Client-Datenverkehr auf dem Trunk zugelassen werden sollten.

Das nachfolgende Beispiel zeigt eine Switch-Port-Konfiguration mit AP-Verbindung und einem Management-VLAN als 58 und einem 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
!
```

Working Setup (Funktionseinrichtung): Zur Referenzfreigabe der Betriebsprotokolle mit dem lokalen DHCP-Server, wenn der Access Point für den Flex-Modus konfiguriert ist:

AP-Client-Debugging:

```
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: 10.1
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>
```

AP-Uplink-Erfassung:

```
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
```

AP-Uplink-Erfassung

Client-seitige Erfassung:

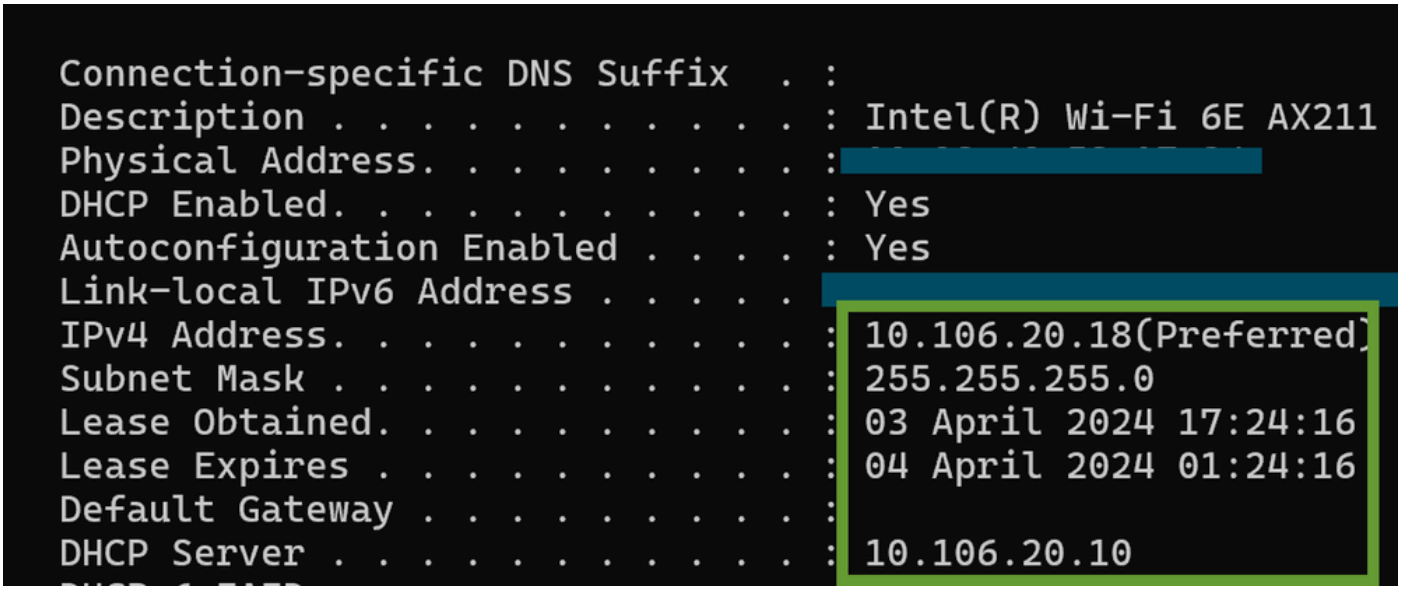
```
16540 111.905836    0.0.0.0          255.255.255.255   DHCP    343 DHCP Discover - Transaction ID 0x628c01b4
16541 111.931651    10.106.20.10     10.106.20.18      DHCP    342 DHCP Offer    - Transaction ID 0x628c01b4
16542 111.936185    0.0.0.0          255.255.255.255   DHCP    385 DHCP Request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

Client-End-Paketerfassung

Verifizierung der Wireless Client IP:

Sie können die IP-Lease auf dem DHCP-Server und den entsprechenden Status überprüfen.

Auf Wireless-Client:



IP-Verifizierung auf Client-Ende

Fehlerbehebung bei DHCP-Problemen

Zur Behebung von DHCP-Problemen müssen Probleme identifiziert und behoben werden, die verhindern, dass Clients eine IP-Adresse von einem DHCP-Server erhalten, wenn sie mit dem Wireless-Netzwerk verbunden sind. Im Folgenden finden Sie einige allgemeine Schritte und Überlegungen zur Fehlerbehebung bei DHCP-Problemen:

1. Client-Konfiguration überprüfen

- Stellen Sie sicher, dass der Client so konfiguriert ist, dass er automatisch eine IP-Adresse bezieht.
- Bestätigen Sie, dass der Netzwerkadapter aktiviert ist und ordnungsgemäß funktioniert.

2. DHCP-Serverstatus überprüfen

- Vergewissern Sie sich, dass der DHCP-Server betriebsbereit und vom Netzwerksegment des Clients aus erreichbar ist.
- Überprüfen Sie die IP-Adresse, die Subnetzmaske und die Standardgateway-Einstellungen des DHCP-Servers.

3. Überprüfen der Bereichskonfiguration

- Überprüfen Sie den DHCP-Bereich, um sicherzustellen, dass er über einen ausreichenden IP-Adressbereich für Clients verfügt.
- Überprüfung der Leasedauer und der Optionen des Bereichs, z. B. DNS-Server und Standard-Gateway
- Stellen Sie in einigen Umgebungen (z. B. Active Directory) sicher, dass der DHCP-Server autorisiert ist, DHCP-Dienste im Netzwerk bereitzustellen.

4. Überprüfen der Konfiguration des 9800 WLC

- Viele Probleme sind aufgrund von Fehlkonfigurationen aufgetreten, z. B. fehlende Loopback-Schnittstelle, Client-SVI oder das Fehlen einer konfigurierten Helper-Adresse. Vor der Protokollsammlung sollte überprüft werden, ob die Konfiguration korrekt implementiert wurde.
- Bei Verwendung eines internen DHCP-Servers: Hinsichtlich der Erschöpfung des DHCP-Bereichs ist es wichtig, insbesondere bei der Konfiguration von DHCP über die CLI sicherzustellen, dass der Lease-Timer gemäß Ihren Anforderungen konfiguriert wird. Standardmäßig ist der Lease-Timer auf "infinite" (Unendlich) für den 9800 WLC eingestellt.
- Überprüfen Sie, ob der Client-VLAN-Datenverkehr am WLC-Uplink-Port bei Verwendung eines zentralen DHCP-Servers zulässig ist. Stellen Sie bei Verwendung eines lokalen DHCP-Servers dagegen sicher, dass das relevante VLAN auf dem Uplink-Port des Access

Points zugelassen ist.

5. Firewall- und Sicherheitseinstellungen

- Stellen Sie sicher, dass keine Firewalls oder Sicherheitssoftware den DHCP-Datenverkehr blockieren (Port 67 für den DHCP-Server und Port 68 für den DHCP-Client).

Protokollsammlung

Protokolle von WLC

1. Aktivieren Sie term exec prompt timestamp, um eine Zeitreferenz für alle Befehle zu erhalten.

2. Verwenden Sie show tech-support wireless !! , um die Konfiguration zu überprüfen.

2. Sie können die Anzahl der Clients, die Verteilung des Clientstatus und die ausgeschlossenen Clients überprüfen.
show wireless summary !! Gesamtzahl der APs und Clients
show wireless exclusionlist !! Falls ein Client als ausgeschlossen angesehen wird
show wireless exclusionlist client mac-address MAC@ !! um mehr Details über konkrete Client ausgeschlossen und überprüfen, ob der Grund als IP-Diebstahl für jeden Client aufgeführt.

3. Überprüfen Sie die IP-Adresszuweisung für Clients, suchen Sie nach falschen Adressen oder unerwartetem Lernen statischer Adressen, als fehlerhaft markierte VLANs, weil der DHCP-Server nicht reagiert, oder verwerfen Pakete in SISF, die DHCP/ARP verarbeiten.

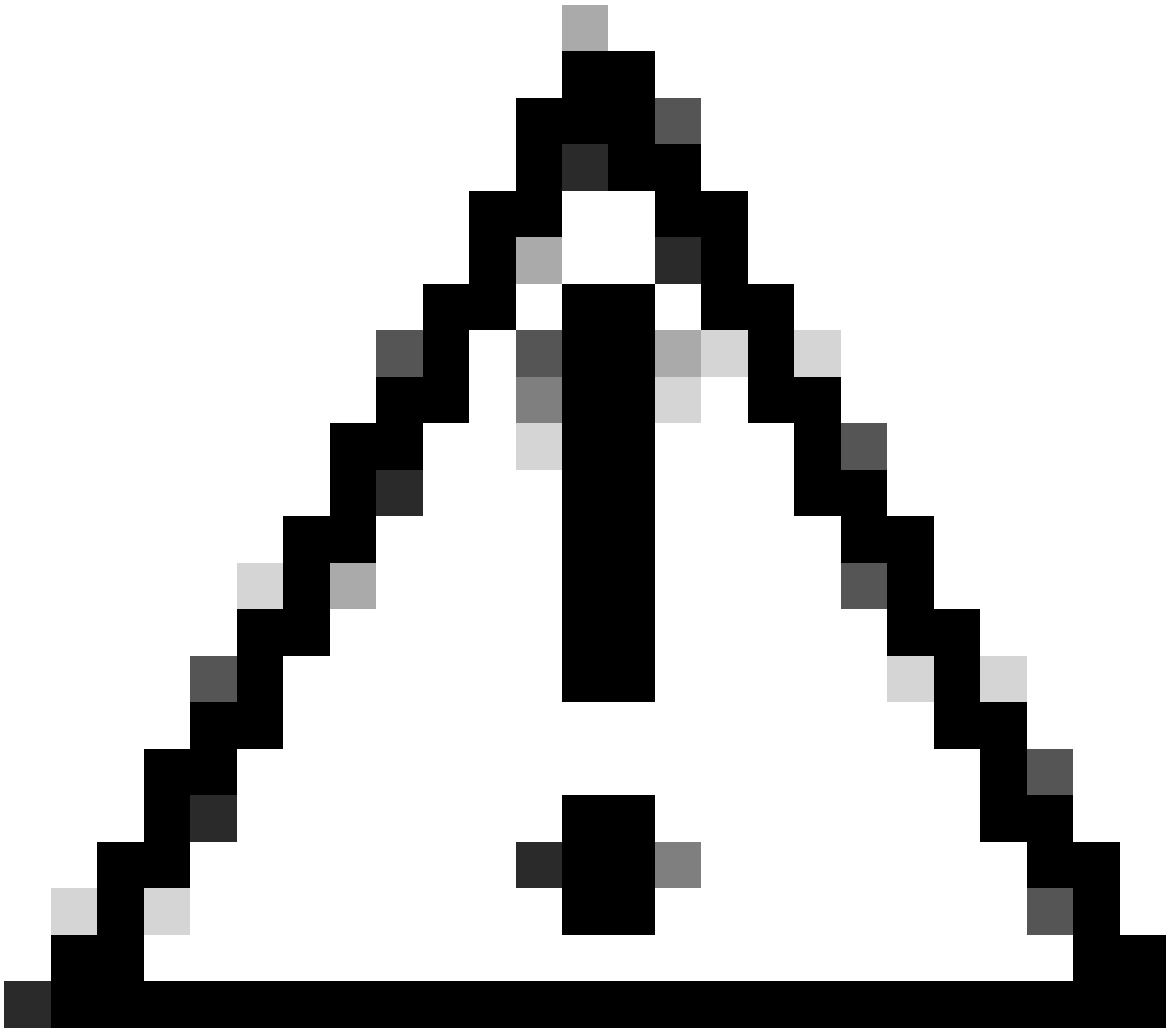
show wireless device-tracking database ip !! Nach IP überprüfen und feststellen, wie der Adressenerwerb erfolgt ist:
show wireless device-tracking database mac !! Überprüfen Sie auf dem Mac, welchem IP-Client er zugewiesen ist.
show wireless vlan details !! Stellen Sie sicher, dass das VLAN aufgrund von DHCP-Fehlern bei Verwendung der VLAN-Gruppe nicht als fehlerhaft gekennzeichnet ist.
show wireless device-tracking feature drop !!Einbrüche bei SISF

4. Spezifische Ausgänge von WLC für Betonclient MAC@ show wireless device-tracking feature drop

Aktivieren Sie die radioaktive Spur für die MAC-Adresse des Clients, wenn der Client versucht, eine Verbindung mit dem Wireless-Netzwerk herzustellen.

Über 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



Achtung: Das bedingte Debuggen ermöglicht die Protokollierung auf Debugebene, wodurch sich wiederum die Anzahl der generierten Protokolle erhöht. Wenn Sie diese Option nicht ausführen, wird der Zeitaufwand für das Anzeigen von Protokollen reduziert. Daher wird empfohlen, das Debuggen immer am Ende der Fehlerbehebungssitzung zu deaktivieren.

Führen Sie die folgenden Befehle aus, um das Debuggen vollständig zu deaktivieren:

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

Über GUI:

Schritt 1: Navigieren Sie zu Troubleshooting > Radioactive Trace .
Schritt 2: Klicken Sie aufAdd, und geben Sie eine Client-MAC-Adresse ein, mit der Sie das Problem beheben möchten. Sie können mehrere

Mac-Adressen zum Verfolgen hinzufügen.

Schritt 3: Wenn Sie bereit sind, die radioaktive Verfolgung zu starten, klicken Sie auf Start. Nach dem Start wird die Debug-Protokollierung für jede Verarbeitung auf der Steuerungsebene in Bezug auf die verfolgten MAC-Adressen auf die Festplatte geschrieben.

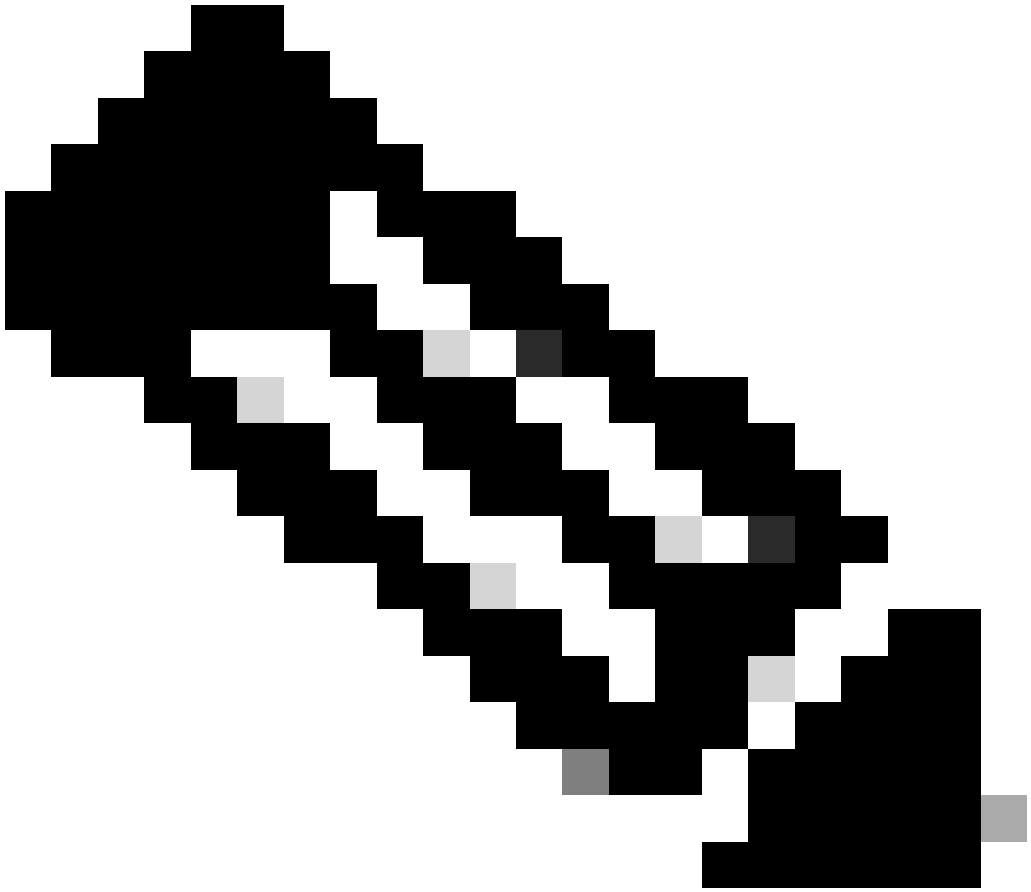
Schritt 4: Wenn Sie das Problem reproduzieren, das Sie beheben möchten, klicken Sie auf Stop .

Schritt 5: Für jede debuggte MAC-Adresse können Sie eine Protokolldatei erstellen, in der alle Protokolle zu dieser MAC-Adresse aufgelistet sind. Klicken Sie dazu auf Generate .

Schritt 6: Wählen Sie aus, wie lange die sortierte Protokolldatei zurückgehen soll, und klicken Sie auf Auf Gerät anwenden.

Schritt 7. Sie können die Datei jetzt herunterladen, indem Sie auf das kleine Symbol neben dem Dateinamen klicken. Diese Datei befindet sich im Boot-Flash-Laufwerk des Controllers und kann auch über die CLI kopiert werden.

!! Embedded Captures gefiltert nach Client-MAC-Adresse in beide Richtungen, interner Client-MAC-Filter verfügbar nach 17.1.



Hinweis: EPC auf 9800 ist nützlich, wenn zentrales DHCP auf 9800 WLC aktiviert ist.

Über 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

Über GUI:
Schritt 1: Navigieren Sie zu Troubleshooting > Packet Capture > +Add .

Schritt 2: Definieren Sie den Namen der Paketerfassung. Es sind maximal 8 Zeichen zulässig.

Schritt 3: Definieren Sie ggf. Filter.

Schritt 4: Aktivieren Sie das Kontrollkästchen Control Traffic überwachen, wenn der Datenverkehr zur System-CPU geleitet und zurück in die Datenebene eingespeist werden soll.

Schritt 5: Puffergröße definieren. Es sind maximal 100 MB zulässig.

Schritt 6: Definieren Sie einen Grenzwert, entweder nach Dauer, die einen Bereich von 1 bis 1000000 Sekunden zulässt, oder nach Anzahl der Pakete, die einen Bereich von 1 bis 100000 Paketen erlaubt, wie gewünscht.

Schritt 7. Wählen Sie die Schnittstelle aus der Liste der Schnittstellen in der linken Spalte aus, und klicken Sie auf den Pfeil, um sie in die rechte Spalte zu verschieben.

Schritt 8: Speichern und auf Gerät anwenden.

Schritt 9. Wählen Sie Start aus, um die Erfassung zu starten.

Schritt 10. Sie können die Erfassung bis zum definierten Limit laufen lassen. Um die Erfassung manuell zu beenden, wählen Sie Stopp.

Schritt 11. Nach dem Beenden wird eine Schaltfläche "Exportieren" verfügbar, auf die Sie klicken können. Sie bietet die Option zum Herunterladen der Erfassungsdatei (.pcap) auf dem lokalen Desktop über einen HTTP- oder TFTP-Server oder einen FTP-Server oder eine lokale Festplatte oder einen Flash-Speicher des Systems.

Protokolle vom Access Point

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

Protokolle vom DHCP-Server

Bei Verwendung eines externen DHCP-Servers müssen serverseitig Debug-Protokolle und Paketerfassungen gesammelt werden, um den DHCP-Datenverkehr zu überprüfen.

Andere Protokolle

Wenn Sie feststellen, dass die DHCP-Erkennungsmeldungen auf dem 9800 WLC in einer zentralen DHCP-Konfiguration oder in AP-Debug-Protokollen in einer lokalen DHCP-Konfiguration sichtbar sind, sollten Sie mit dem Sammeln von Erfassungsdaten vom Uplink fortfahren, um zu bestätigen, dass die Pakete nicht im Ethernet-Port verworfen werden.Je nach den Funktionen des Switches können Sie eine integrierte Paketerfassung oder eine SPAN-Erfassung (Switched Port Analyzer) am Uplink durchführen Plink-Schalter. Es empfiehlt sich, den DHCP-Datenverkehrsfluss Schritt für Schritt zu verfolgen, um den Punkt zu ermitteln, an dem die Kommunikation unterbrochen wird, und zwar sowohl vom DHCP-Client zum DHCP-Server als auch in umgekehrter Richtung.

Bekannte Probleme

Ausgabe 1. Der Client versucht, eine IP-Adresse von einem zuvor beibehaltenen VLAN abzurufen. Situationen können auftreten, in denen ein Wireless-Client zwischen zwei SSIDs wechselt, die verschiedenen Client-VLANs zugeordnet sind. In solchen Fällen kann der Client darauf bestehen, eine IP-Adresse von dem VLAN anzufordern, mit dem er zuvor verbunden war. Da sich diese IP nicht im DHCP-Bereich des aktuellen VLAN befindet, gibt der DHCP-Server eine NAK (negative Bestätigung) aus, sodass der Client keine IP-Adresse abrufen kann.

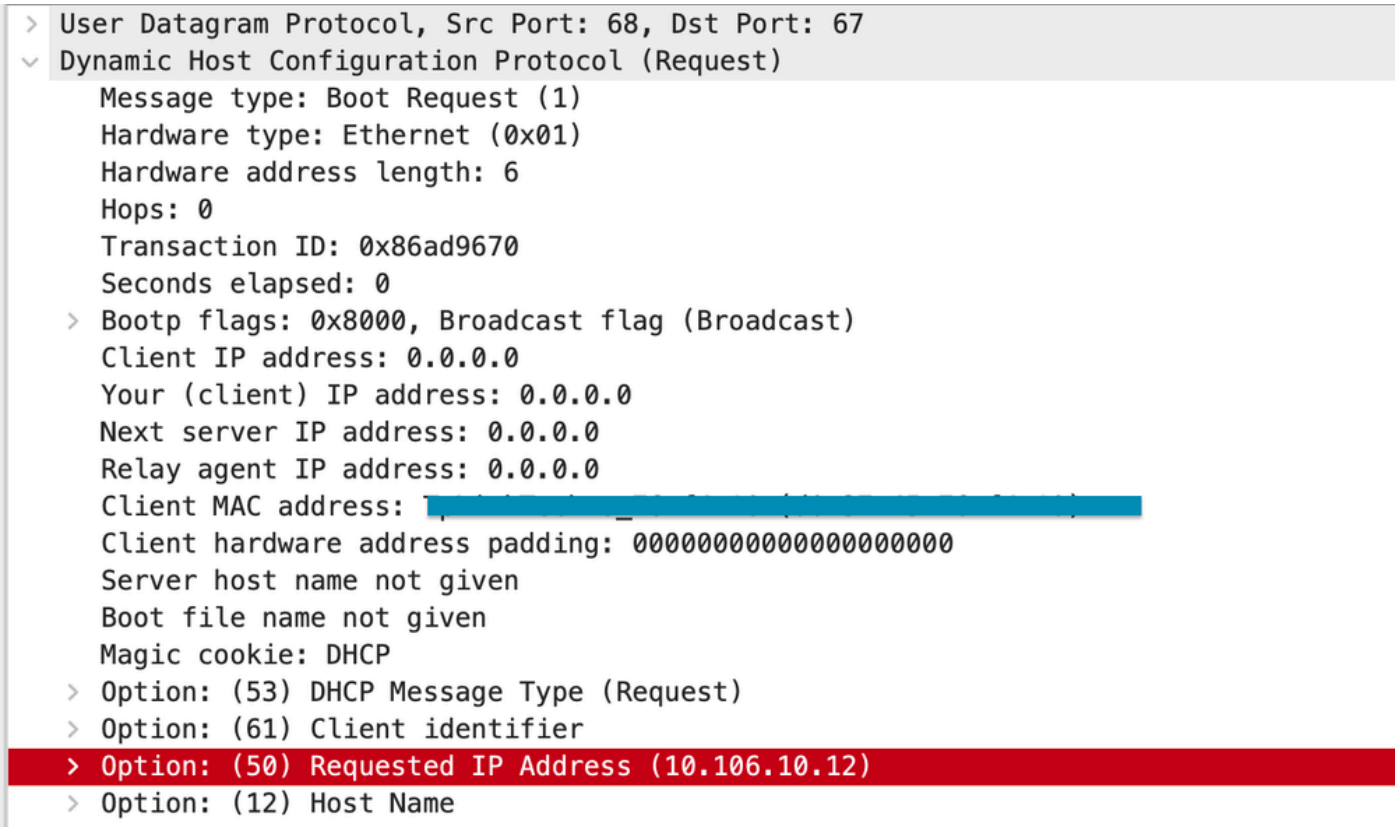
In den radioaktiven Trace-Protokollen ist ersichtlich, dass der Client weiterhin eine IP aus dem VLAN sucht, mit dem er zuvor verbunden war, nämlich VLAN 10, obwohl das Client-VLAN für die aktuelle SSID VLAN 20 ist.

```
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
```

Integrierte Paketerfassung auf 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
```

Integrierte Paketerfassung auf WLC



DHCP-Option 50 bei WLC-Paketerfassung

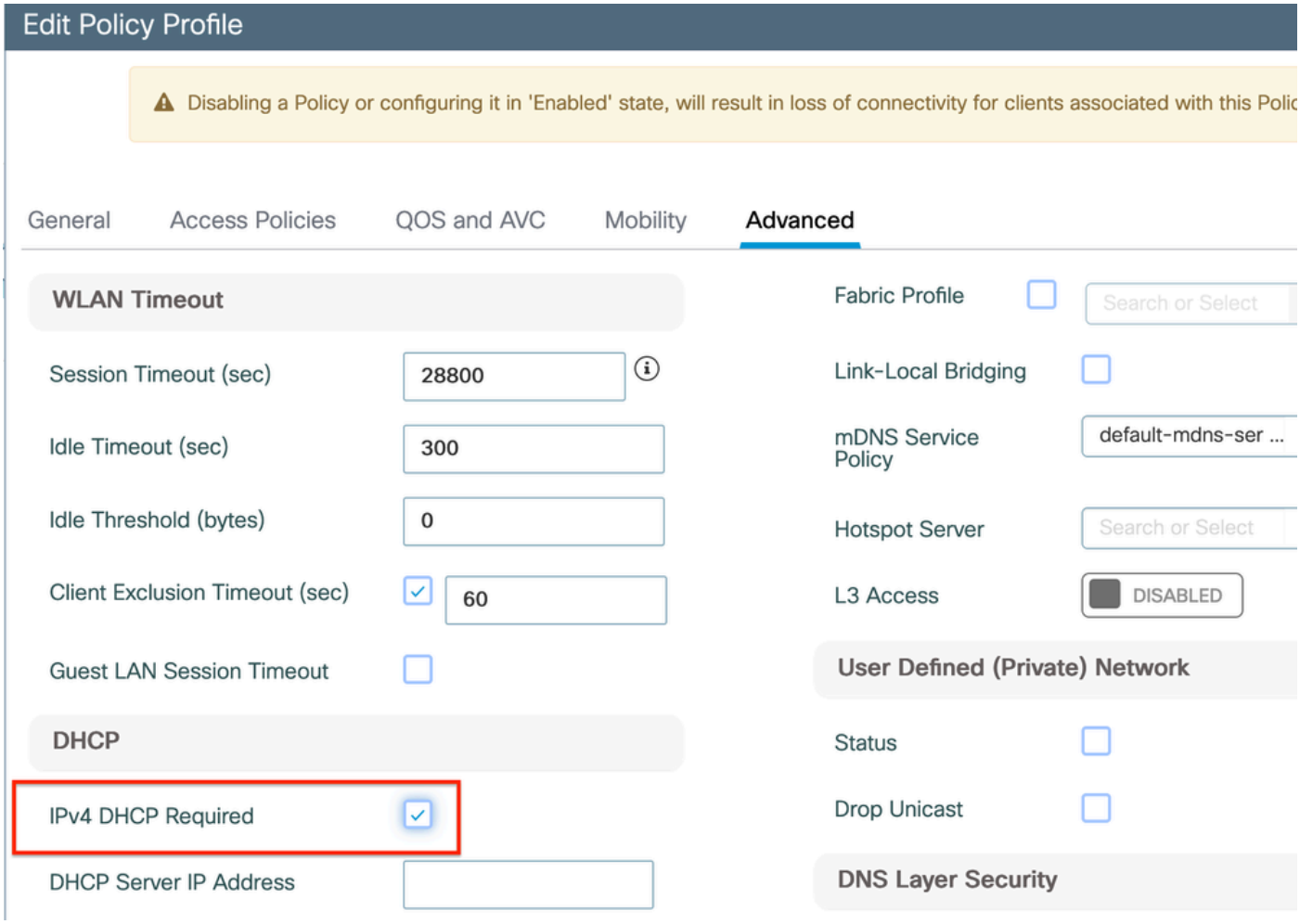
Auflösung: Um sicherzustellen, dass ein Client den vollständigen DHCP-Prozess abschließt, können Sie die Option IPv4 DHCP Required in der Richtlinienkonfiguration aktivieren. Diese Einstellung sollte aktiviert werden, insbesondere wenn der Client zwischen SSIDs wechselt, damit der DHCP-Server ein NAK an den Client senden kann, wenn er eine IP-Adresse von einem mit der vorherigen SSID verknüpften VLAN anfordert. Andernfalls kann der Client die zuvor gespeicherte IP-Adresse weiter verwenden oder anfordern, was zu einer Unterbrechung der Kommunikation führt. Beachten Sie jedoch, dass sich die Aktivierung dieser Funktion auf Wireless-Clients auswirkt, für die eine statische IP-Adresse konfiguriert ist.

Gehen Sie folgendermaßen vor, um die gewünschte Option zu aktivieren:

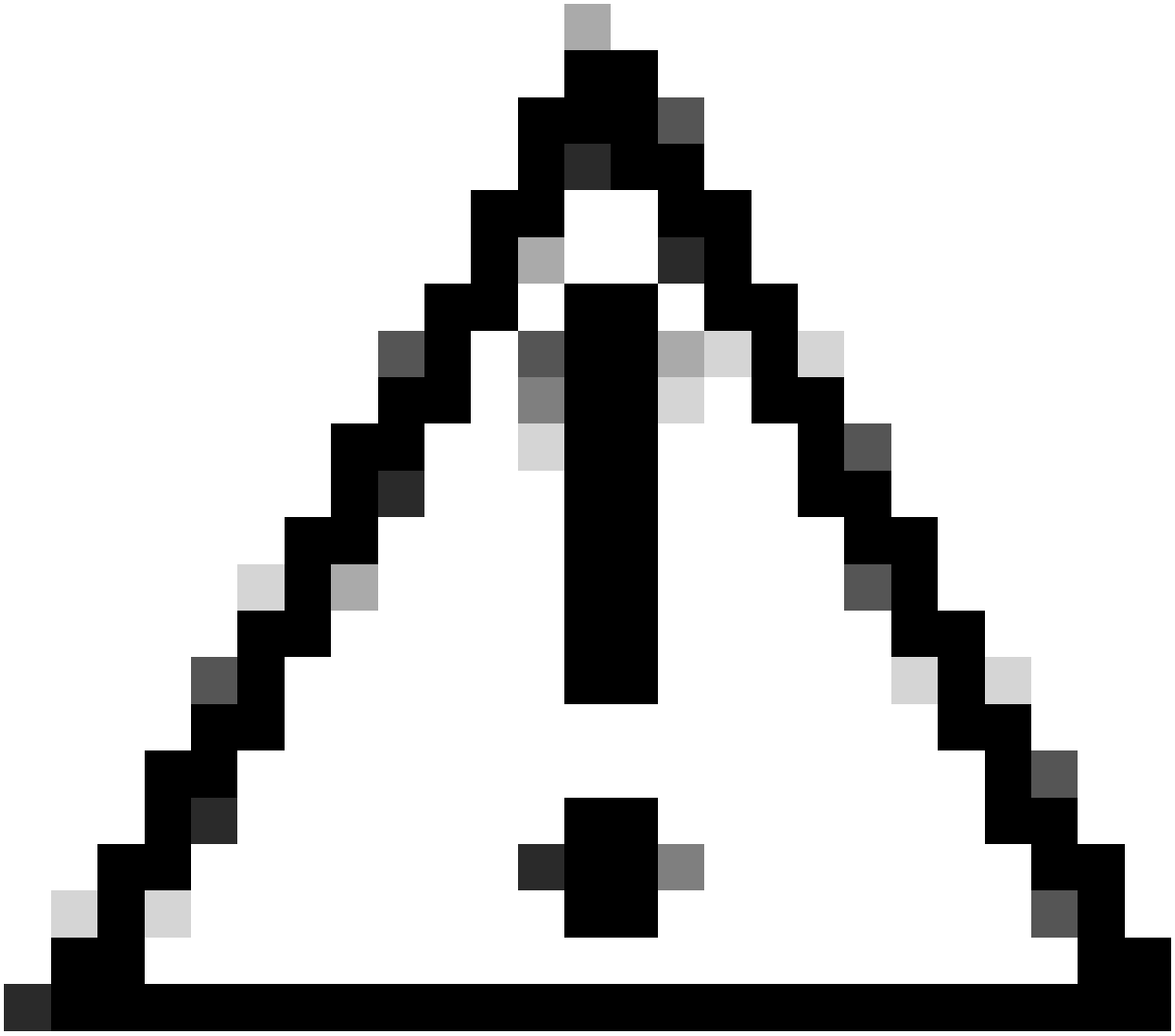
Über CLI:

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

Über GUI: Navigieren Sie zu Configuration > Tags & Profile > Policy > Policy_name > Advanced. Im Abschnitt DHCP aktivieren Sie ipv4 DHCP erforderlich.



Richtlinienprofileinstellung auf WLC



Achtung: Bei einer Konfiguration mit einem Foreign-Anker ist es wichtig, die DHCP-Einstellungen für beide WLCs auszurichten. Wenn IPV4-DHCP aktiviert sein muss, muss es sowohl auf den Fremd- als auch auf den Anker-WLCs aktiviert sein. Eine Diskrepanz in der DHCP-bezogenen Konfiguration unter dem Richtlinienprofil zwischen den beiden kann dazu führen, dass die Clients Probleme mit ihren Mobilitätsrollen haben.

Problem 2: Client wird aufgrund von IP-Diebstahl gelöscht oder ausgeschlossen. IP-Diebstahl bezieht sich im Netzwerkkontext auf eine Situation, in der mehr als ein Wireless-Client versucht, dieselbe IP-Adresse zu verwenden. Dies kann auf verschiedene Gründe zurückzuführen sein, die im Folgenden aufgeführt sind:

1. Nicht autorisierte statische IP-Zuweisung: Wenn ein Benutzer auf seinem Gerät eine statische IP-Adresse festlegt, die mit einer bereits zugewiesenen oder im Netzwerk vorgemerkten IP übereinstimmt, kann dies zu einem IP-Konflikt führen. Dies tritt auf, wenn zwei Geräte versuchen, mit einer identischen IP-Adresse zu arbeiten, wodurch die Netzwerkverbindungen für eines oder beide Geräte unterbrochen werden können. Um solche Probleme zu vermeiden, muss sichergestellt werden, dass jeder Client im Netzwerk mit einer eindeutigen IP-Adresse konfiguriert ist.

2. Nicht autorisierter DHCP-Server: Wenn ein nicht autorisierter oder nicht autorisierter DHCP-Server im Netzwerk vorhanden ist, kann dies zu einer IP-Adresszuweisung führen, die mit dem festgelegten IP-Adressierungsplan des Netzwerks kollidiert. Solche Konflikte können dazu führen, dass mehrere Geräte mit IP-Adressen kollidieren oder falsche Netzwerkeinstellungen erhalten. Um dieses Problem zu beheben, sollten Sie versuchen, den nicht autorisierten DHCP-Server zu identifizieren und vom Netzwerk zu entfernen, um weitere IP-Konflikte im gleichen Subnetz zu verhindern.

3. Veralteter Eintrag des Clients in 9800 WLC: Manchmal kann der Controller veraltete/veraltete Einträge einer IP-Adresse beibehalten, die ein Client abzurufen versucht. In diesen Fällen müssen diese veralteten Einträge manuell aus dem 9800 WLC entfernt werden. So geht's:

- Führen Sie die radioaktive Spur für die MAC-Adresse aus, die in der Ausschlussliste aufgeführt ist, und filtern Sie sie mit der legit mac in der radioaktiven Spur.

- Sie können die Fehlerprotokolle sehen: %CLIENT_ORCH_LOG-5-ADD_TO_BLACKLIST_REASON: Client MAC: Affected_Client_MAC mit IP: 10.37.57.24 wurde zur Ausschlussliste hinzugefügt, legit Client MAC: Legit_Client_MAC, IP: 10.37.27 57.24, Grund: Diebstahl von IP-Adressen

- Führen Sie dann die folgenden Befehle aus:
show wireless device-tracking database mac | sec $Legit_Client_MAC
show wireless device-tracking database ip | sec $Legit_Client_MAC

(Wenn es veraltete Einträge gibt, können Sie mehr als eine IP-Adresse für einen legit Client-Mac-Adresse sehen: eine ist die ursprüngliche IP-Adresse, während die andere die veraltete ist].

Auflösung: Löschen Sie die alten Einträge aus 9800 WLC manuell, indem Sie clear wireless device-tracking mac-address $Legit-Client_MAC ip-address 10.37.57.24

4. Bei der Flex-Bereitstellung mit einem lokalen DHCP-Server, der dasselbe Subnetz verwendet: In FlexConnect-Konfigurationen verwenden verschiedene Remote-Standorte in der Regel einen lokalen DHCP-Server, der IP-Adressen aus einem identischen Subnetz zuweist. Dieses Szenario kann dazu führen, dass Wireless-Clients an verschiedenen Standorten dieselbe IP-Adresse erhalten. Controller in diesem Netzwerk-Framework sind so programmiert, dass sie erkennen, wenn mehrere Client-Verbindungen eine identische IP-Adresse verwenden, was dies als möglichen IP-Diebstahl interpretiert. Daher werden diese Clients in der Regel in eine Sperrliste aufgenommen, um IP-Adresskonflikte zu vermeiden.

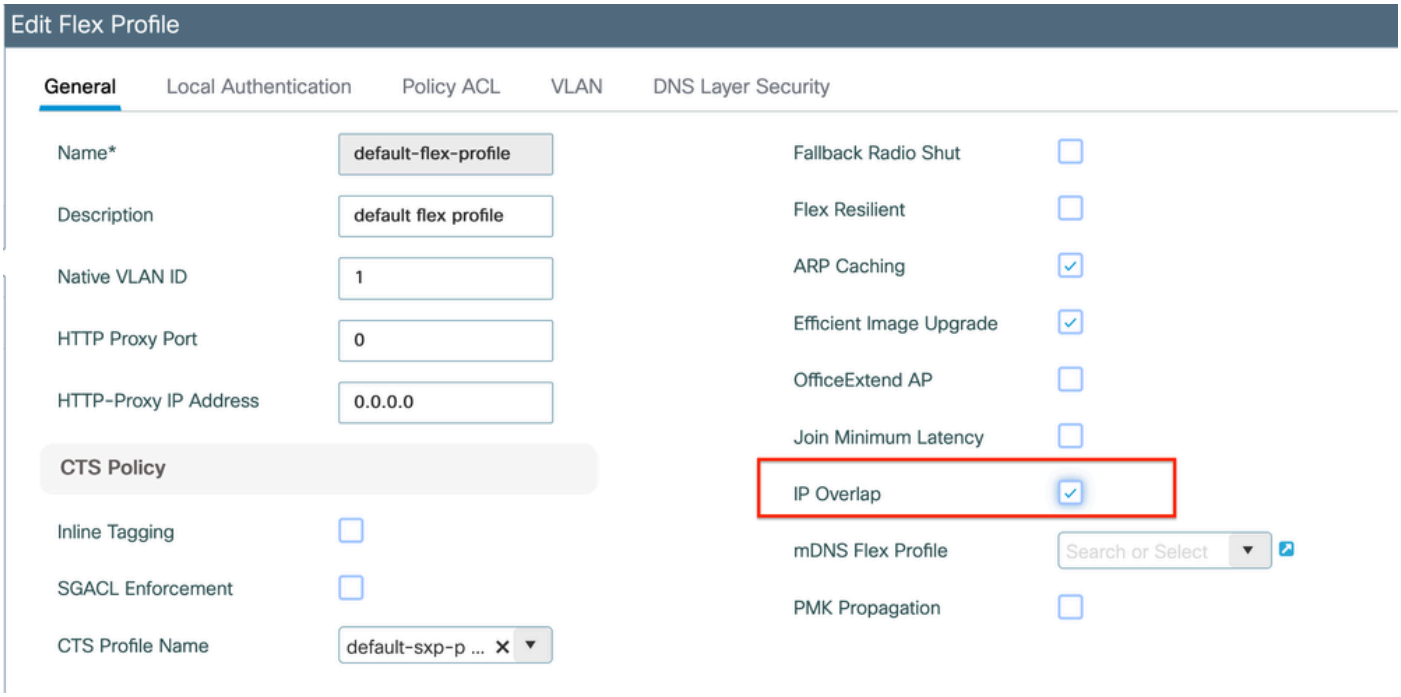
Auflösung: Aktivieren Sie die IP-Überlappungsfunktion in Ihrem FlexConnect-Profil. Die Funktion "Überlappende Client-IP-Adresse bei Flex Deployment" ermöglicht die Verwendung derselben IP-Adressen an mehreren FlexConnect-Standorten, wobei alle in FlexConnect-Bereitstellungen unterstützten Funktionen und Leistungsmerkmale beibehalten werden.

Diese Funktion ist standardmäßig deaktiviert. Sie können es folgendermaßen aktivieren:

Über CLI:

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

Über GUI: Wählen Sie Configuration > Tags & Profiles > Flex. Klicken Sie auf Bestehendes Flex-Profil/Zu neuem Flex-Profil hinzufügen, und aktivieren Sie auf der Registerkarte Allgemein die Option IP-Überlappung.



Flex Profile-Einstellung auf WLC

Ausgabe 3. Wireless-Clients können keine IP-Adresse vom beabsichtigten VLAN empfangen. Dieses Problem tritt häufig auf, wenn VLAN 1 verwendet wird oder wenn das den Clients zugewiesene VLAN mit dem VLAN identisch ist, das für die AP-Verwaltung in einer FlexConnect-Bereitstellung verwendet wird. Die Ursache dieses Problems liegt in der Regel in falschen VLAN-Zuweisungen. Es folgen einige Szenarien, die bei der Konfiguration von VLAN-IDs für die Serie 9800 berücksichtigt werden sollten:

1. Bei Verwendung eines AAA-Servers mit aktivierter Funktion zum Überschreiben von AAA muss unbedingt sichergestellt werden, dass vom AAA-Server die entsprechende VLAN-ID gesendet wird. Wenn Sie stattdessen einen VLAN-Namen angeben, stellen Sie sicher, dass dieser mit dem auf dem 9800 WLC konfigurierten VLAN-Namen übereinstimmt.

2. Wenn VLAN 1 für den Datenverkehr von Wireless-Clients konfiguriert ist, kann das Verhalten je nach Modus des Access Points (AP) variieren:

Für einen Access Point im lokalen Modus/zentralen Switching:

- Durch Festlegen von VLAN-Name = default wird der Client VLAN 1 zugewiesen.
- Mithilfe von VLAN-ID 1 wird ein Client dem drahtlosen Management-VLAN zugewiesen.

Für einen AP im Flex-Modus/mit lokalem Switching:

- Durch Festlegen von VLAN-Name = default wird der Client VLAN 1 zugewiesen.
- Mithilfe der VLAN-ID 1 wird ein Client dem nativen FlexConnect-VLAN zugewiesen.

Im Folgenden finden Sie einige weitere Beispiele von Szenarien, mit denen im Labor experimentiert wurde, sowie deren Ergebnisse:

1. Wenn der Benutzer im Richtlinienprofil keine Konfiguration vornimmt, weist der WLC standardmäßig die VLAN-ID 1 zu, sodass die Clients das Wireless-Management-VLAN im lokalen Modus und das native VLAN für den AP für FlexConnect verwenden.

2. Wenn das Native-VLAN unter Flex-Profil mit einer nativen VLAN-ID konfiguriert ist, die sich von der auf dem Switch konfigurierten unterscheidet, wird das Problem angezeigt, dass der Client die IP vom Management-VLAN (natives VLAN) erhält, selbst wenn das Richtlinienprofil mit dem "Standard"-VLAN-Namen konfiguriert ist.

3. Wenn das native VLAN unter Flex-Profile mit der VLAN-ID konfiguriert ist, die mit dem auf dem Switch konfigurierten nativen VLAN identisch ist, kann nur der Client eine IP von VLAN 1 mit der unter Richtlinienprofil konfigurierten Standardeinstellung abrufen.

4. Wenn Sie einen VLAN-Namen anstelle einer VLAN-ID ausgewählt haben, stellen Sie sicher, dass der VLAN-Name im Flex Profile-Objekt derselbe ist.

Zugehörige Informationen

- Interner DHCP-Server auf 9800
- Externer DHCP-Server im Einsatz
- DHCP-Option 82 Sub-Option 5 in Windows-DHCP-Server
- NAT-PAT in Flex AP
- VLAN 1 wird für den Wireless-Client verwendet
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.