# Konfigurationsbeispiel für FlexConnect OEAP mit Split Tunneling

## Einführung

Dieses Dokument zeigt, wie Sie einen Access Point in FlexConnect Office Extend-Modus konfigurieren und Split-Tunneling aktivieren, sodass Sie festlegen können, welcher Datenverkehr lokal im Heimbüro geswitcht werden soll und welcher Datenverkehr zentral im WLC geschaltet werden soll.

## Voraussetzungen

### Anforderungen

Bei der Konfiguration in diesem Dokument wird davon ausgegangen, dass der WLC bereits in einer DMZ mit aktivierter NAT konfiguriert ist und dass der Access Point vom Heimbüro aus dem WLC beitreten kann.

### Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Wireless LAN Controller mit AireOS 8.10.130.0-Software.
- Wave1-APs: 1700/2700/3700.
- Wave2-APs: 1800/2800/3800/4800 und der Catalyst Serie 9100.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt.

Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Übersicht

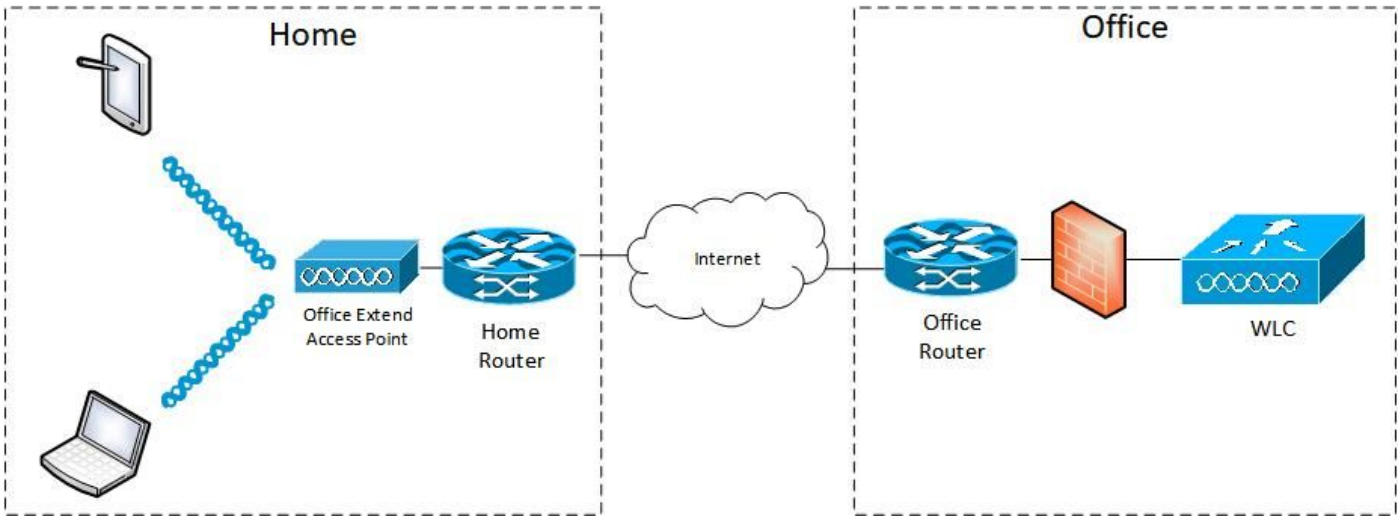
Ein Cisco OfficeExtend Access Point (Cisco OEAP) bietet eine sichere Kommunikation von einem Cisco WLC zu einem Cisco AP an einem Remote-Standort und erweitert nahtlos das Unternehmens-WLAN über das Internet auf den Wohnsitz eines Mitarbeiters. Das Anwendererlebnis im Heimbüro ist genauso wie im Büro. Die DTLS-Verschlüsselung (Datagram Transport Layer Security) zwischen Access Point und Controller stellt sicher, dass alle Kommunikationen ein Höchstmaß an Sicherheit bieten. Jeder Access Point in Innenräumen in FlexConnect kann als Office Extend AP fungieren.

### Wichtige Fakten

- Cisco OEAPs sind so konzipiert, dass sie hinter einem Router oder einem anderen Gateway-Gerät arbeiten, das Network Address Translation (NAT) verwendet. Mit NAT kann ein Gerät, z. B. ein Router, als Agent zwischen dem Internet (öffentlich) und einem privaten Netzwerk (privat) agieren, sodass eine ganze Gruppe von Computern durch eine einzige IP-Adresse dargestellt werden kann. Die Anzahl der Cisco OEAPs, die Sie hinter einem NAT-Gerät bereitstellen können, ist unbegrenzt.
- Alle unterstützten AP-Innenraummodelle mit integrierter Antenne können als OEAP konfiguriert werden, mit Ausnahme der Access Points der Serie AP-700I, AP-700W und AP802.
- Alle OfficeExtend-Access Points sollten derselben Access Point-Gruppe angehören, und diese Gruppe sollte nicht mehr als 15 WLANs enthalten. Ein Controller mit OfficeExtend-Access Points in einer Access Point-Gruppe veröffentlicht nur bis zu 15 WLANs für jeden angeschlossenen OfficeExtend-Access Point, da er ein WLAN für die persönliche SSID reserviert.

# Konfigurieren

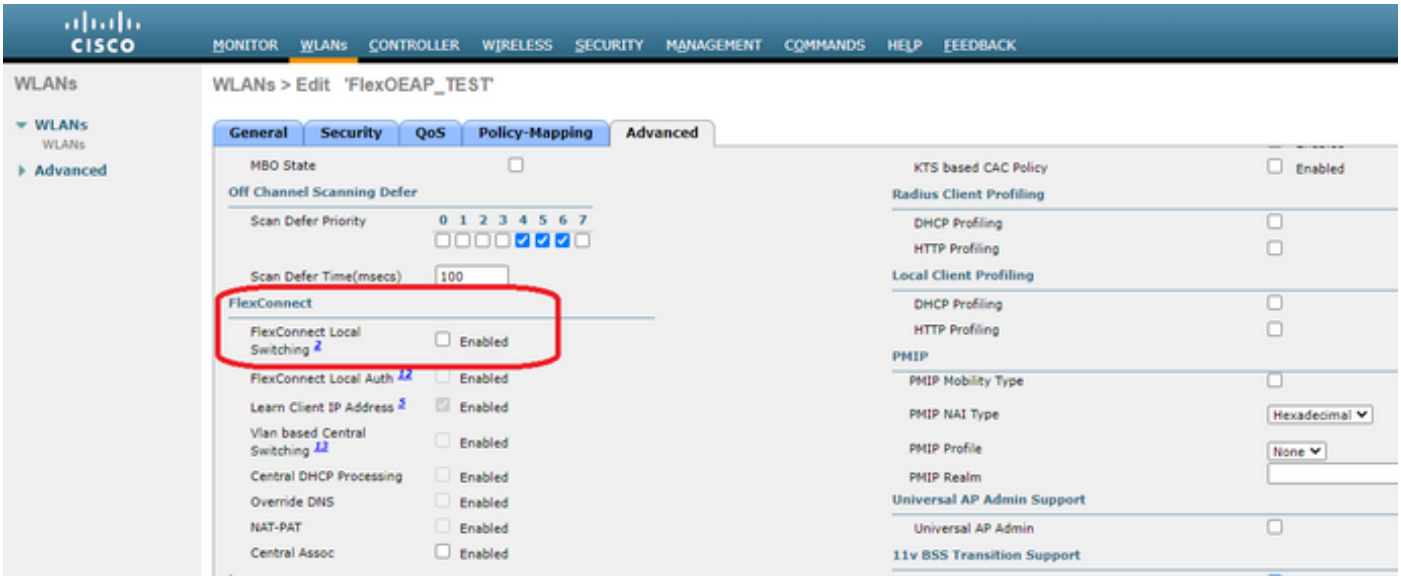
## Netzwerkdiagramm



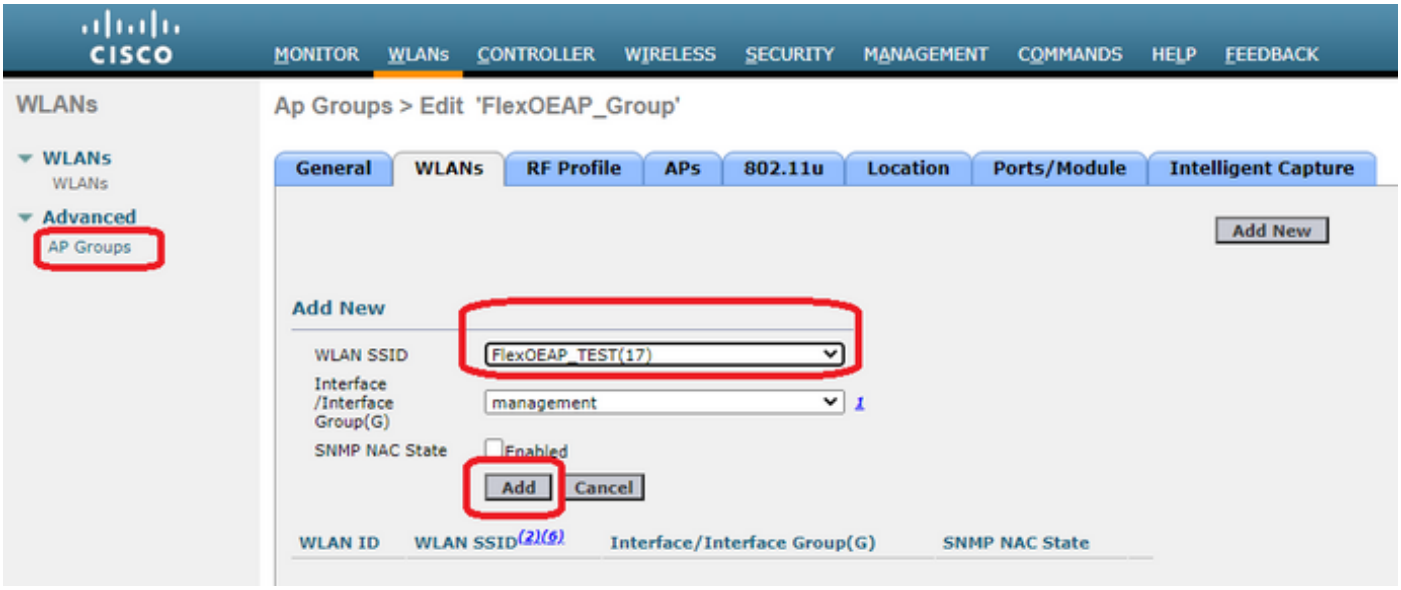

## Konfigurationen

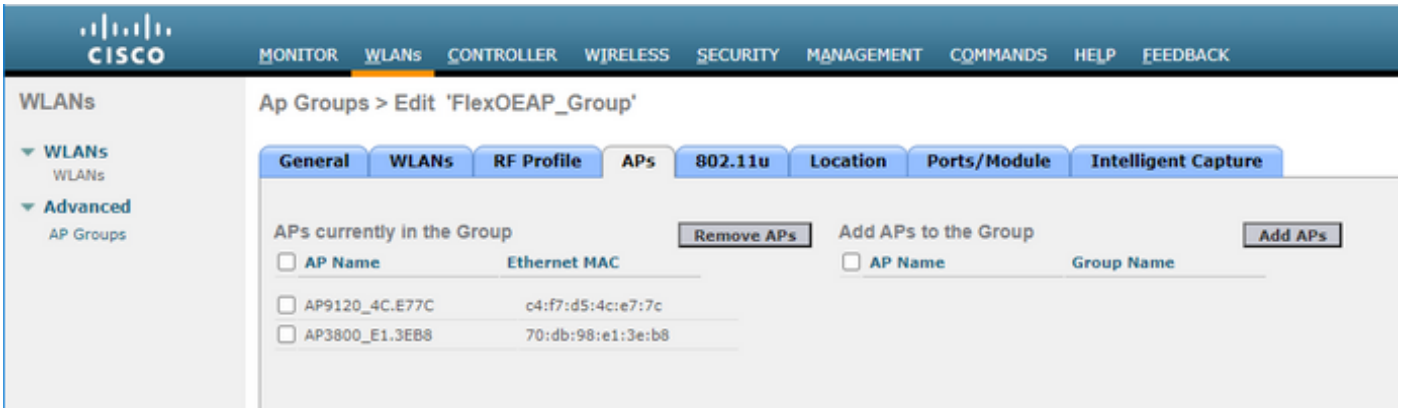
### WLAN-Konfiguration

Schritt 1: Sie müssen ein WLAN erstellen, das der AP-Gruppe zugewiesen wird. Für dieses WLAN muss die Option "FlexConnect Local Switching" nicht aktiviert sein.




Schritt 2: Erstellen Sie eine AP-Gruppe, **fügen Sie** das WLAN und den FlexConnect Office Extend AP hinzu.



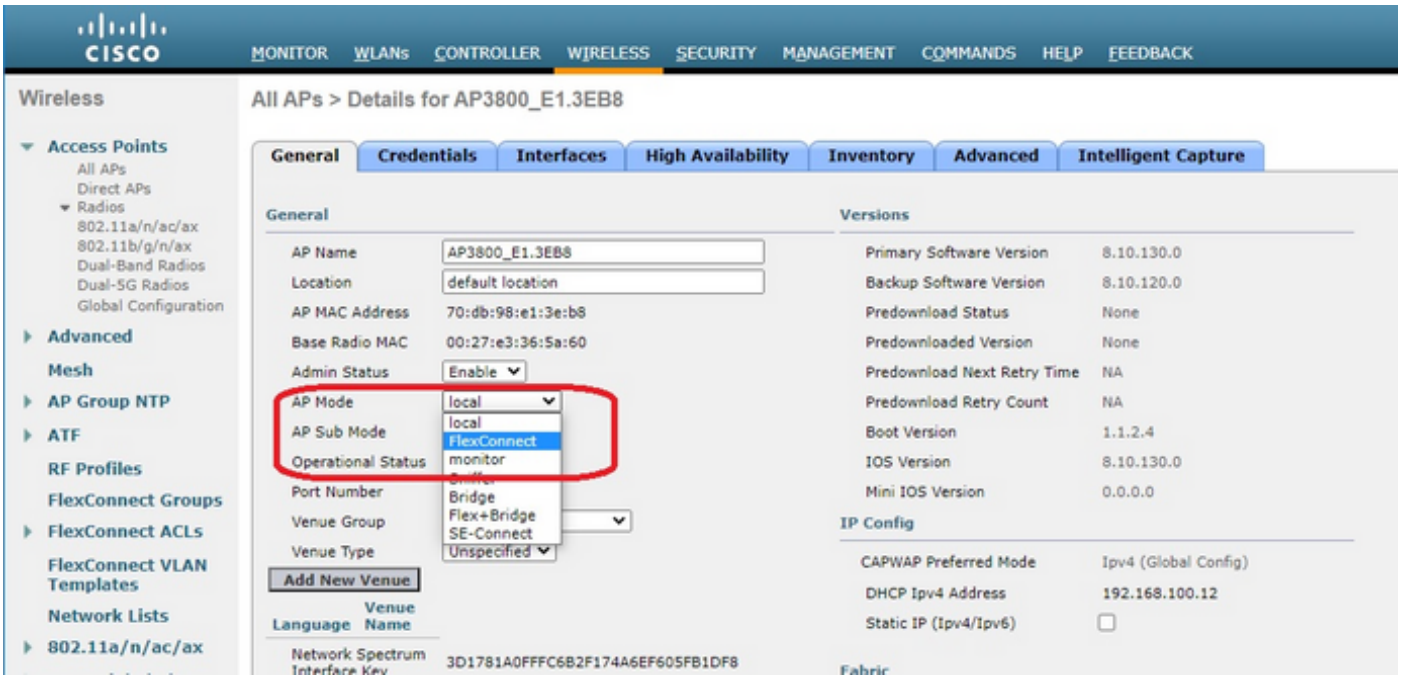




## AP-Konfiguration

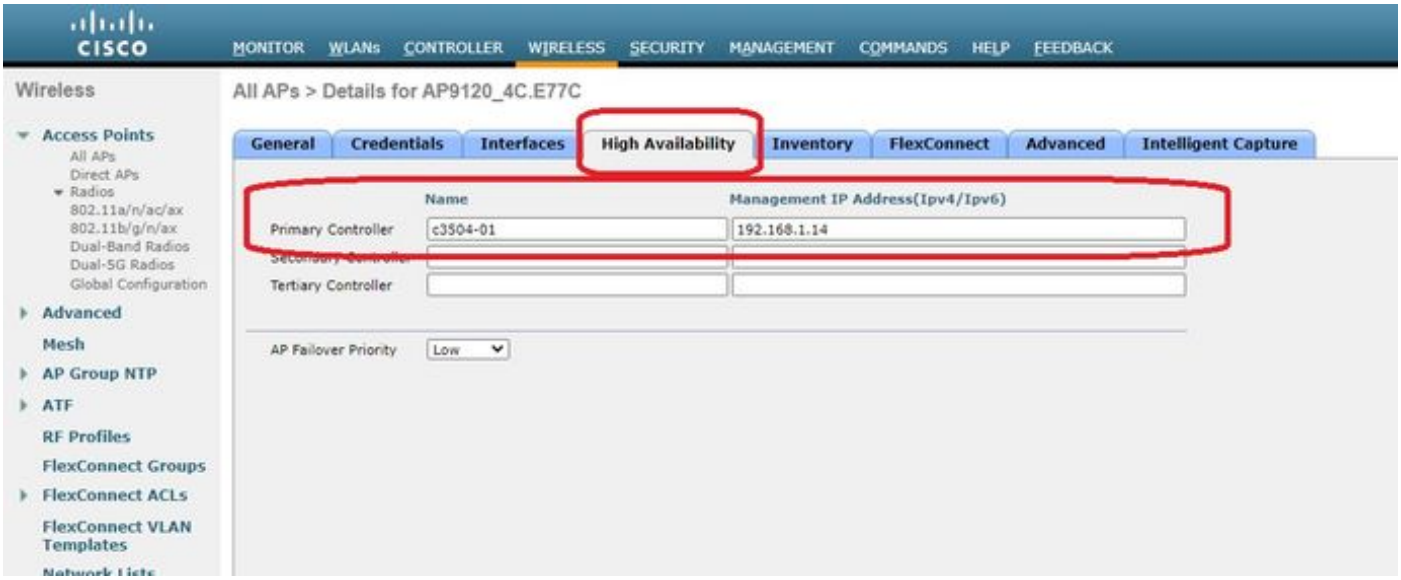
Nachdem der Access Point dem Controller im FlexConnect-Modus zugeordnet wurde, können Sie ihn als OfficeExtend Access Point konfigurieren.

Schritt 1: Wenn der Access Point dem WLC beitritt, ändern Sie den AP-Modus in **FlexConnect**,

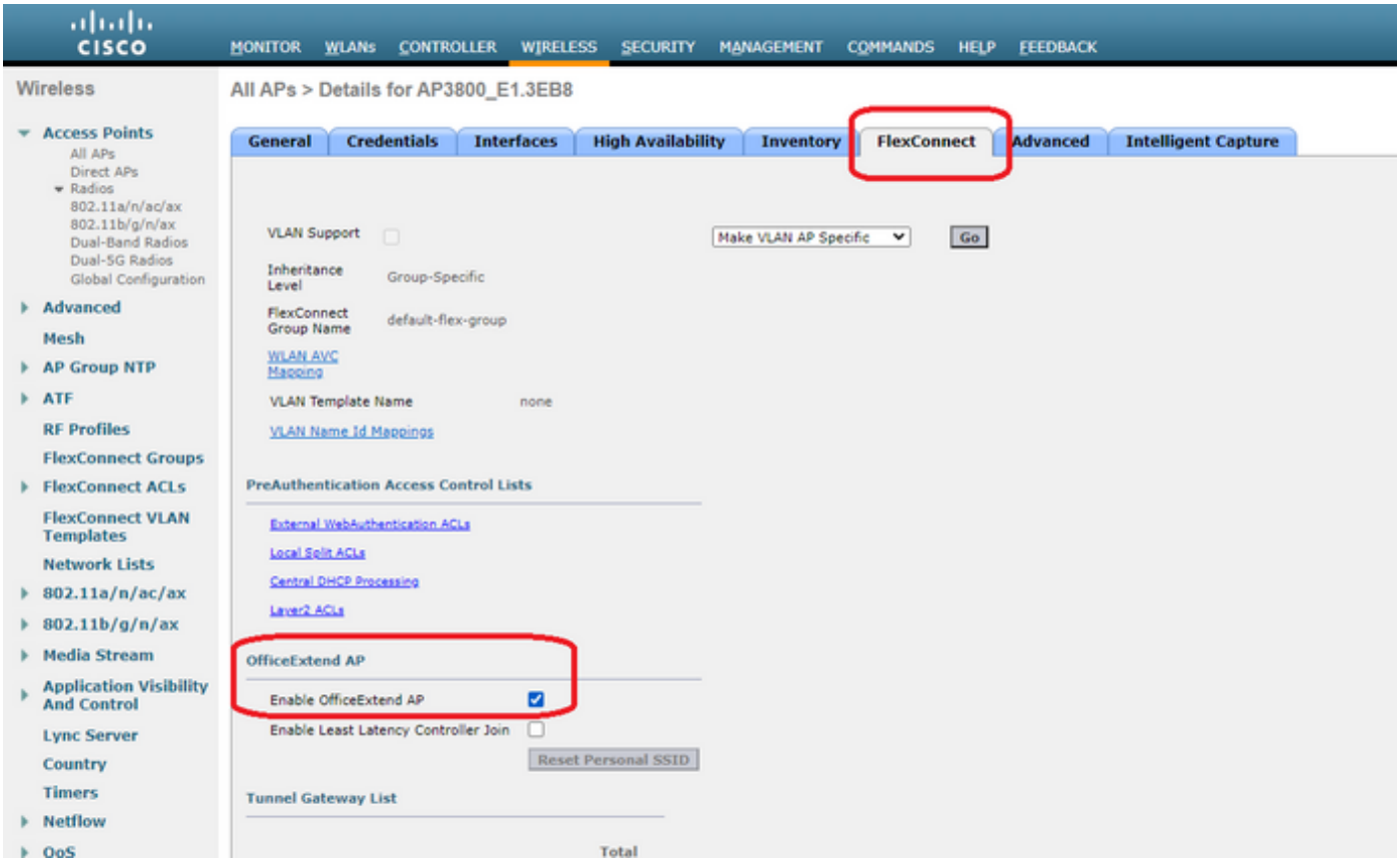
und klicken Sie auf **Apply**.



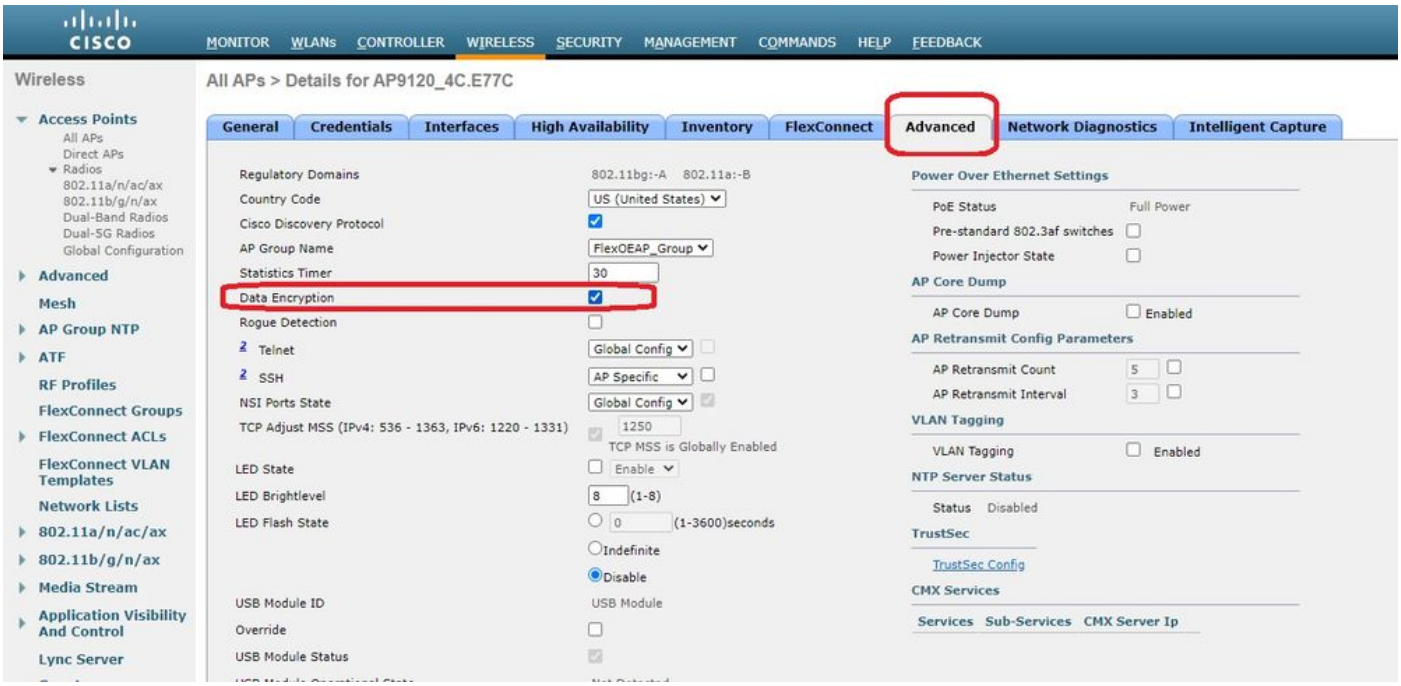

Schritt 2: Stellen Sie sicher, dass auf der Registerkarte "Hohe Verfügbarkeit" mindestens ein primärer WLC konfiguriert ist:




Schritt 3: Wechseln Sie zur Registerkarte FlexConnect, und aktivieren Sie das Kontrollkästchen **Enable OfficeExtend AP** Mode.




DTLS-**Datenverschlüsselung** wird automatisch aktiviert, wenn Sie den OfficeExtend-Modus für einen Access Point aktivieren. Sie können jedoch die DTLS-Datenverschlüsselung für einen bestimmten Access Point aktivieren oder deaktivieren, indem Sie **Datenverschlüsselung** das Kontrollkästchen auf Alle APs > Details für (Erweitert) Seite:




**Hinweis**: Der Telnet- und SSH-Zugriff wird automatisch deaktiviert, wenn Sie den OfficeExtend-Modus für einen Access Point aktivieren. Sie können den Telnet- oder SSH-Zugriff für einen bestimmten Access Point jedoch aktivieren oder deaktivieren, indem Sie das Kontrollkästchen **Telnet** oder **SSH** auf der Seite All APs > Details for (Advanced) aktivieren.

**Hinweis**: Die Link-Latenz wird automatisch aktiviert, wenn Sie den OfficeExtend-Modus für einen Access Point aktivieren. Sie können die Latenz der Verbindungen für einen bestimmten Access Point jedoch aktivieren oder deaktivieren, indem Sie auf der Seite Alle APs > Details für (Erweitert) das Kontrollkästchen **Link-**Latenz **aktivieren** aktivieren.

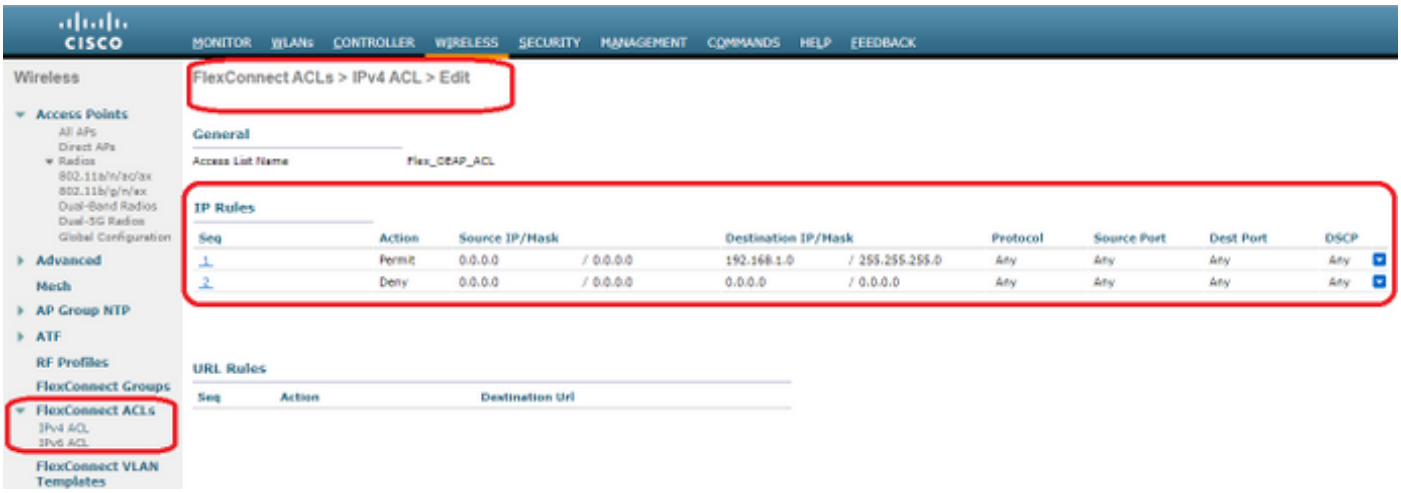
Schritt 3: Klicken Sie auf **Übernehmen**, und der Access Point wird neu geladen.

Schritt 4: Wenn der Access Point dem WLC wieder beitritt, befindet er sich im OEAP-Modus.

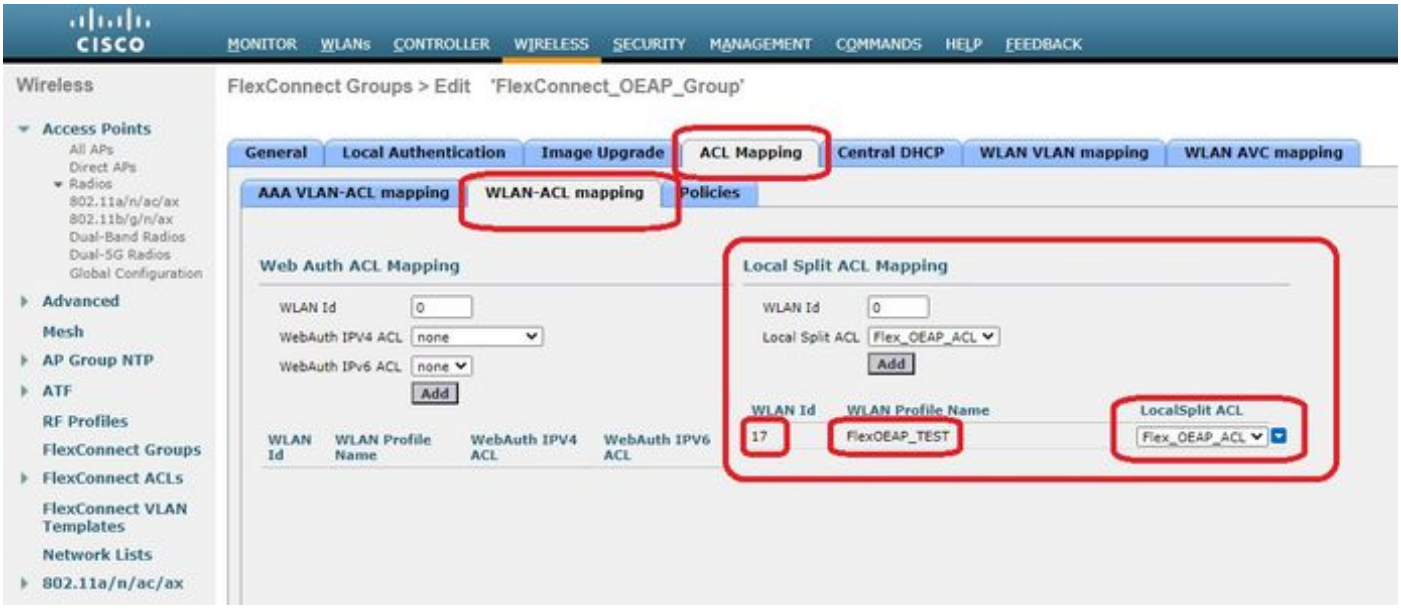
**Hinweis**: Es wird empfohlen, die unter AP-Richtlinien allgemein definierte Sicherheit für den Access Point-Beitritt zu konfigurieren, sodass nur autorisierte APs dem WLC beitreten können. Sie können auch die LSC AP-Bereitstellung verwenden.

Schritt 5: Erstellen Sie eine FlexConnect-ACL, um festzulegen, welcher Datenverkehr zentral (Verweigern) und lokal (Zulassen) geswitcht werden soll.

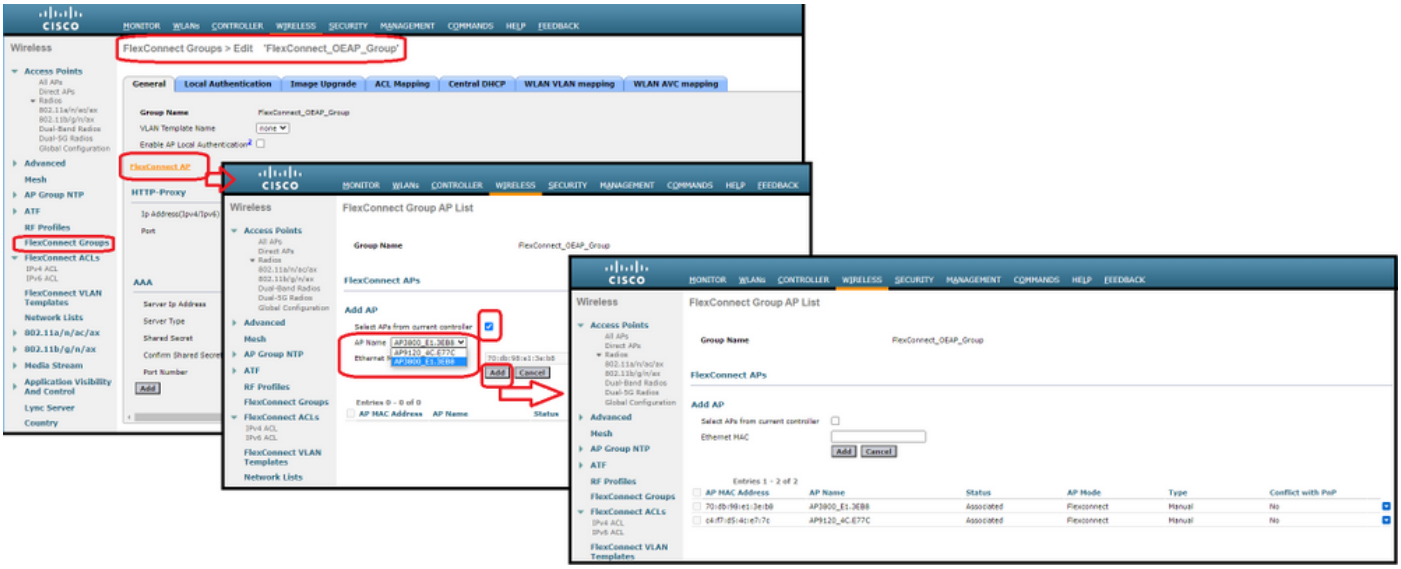
Hier haben wir das Ziel, den gesamten Datenverkehr lokal auf das Subnetz 192.168.1.0/24 umzustellen.




Schritt 6: Erstellen Sie eine FlexConnect-Gruppe, gehen Sie zu ACL Mapping und dann zu WLAN-ACL Mapping. Auf der rechten Seite sehen Sie "Local Split ACL Mapping" (Zuordnung der lokalen Zugriffskontrolllisten). Geben Sie hier die WLAN-ID und die FlexConnect-ACL ein, und klicken Sie auf **Hinzufügen.**




Schritt 7: **Fügen Sie** den Access Point der FlexConnect-Gruppe hinzu:



# Überprüfen

1. Überprüfen Sie den Status und die Definition der FlexConnect-ACLs:

```
c3504-01) >show flexconnect acl summary

ACL Name Status
-------------------------------- -------
Flex_OEAP_ACL Applied


(c3504-01) >show flexconnect acl detailed Flex_OEAP_ACL

Source Destination Source Port Dest Port
Index IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action
------ ------------------------------ ------------------------------ ---- ----------- --------
--- ----- -------
1 0.0.0.0/0.0.0.0 192.168.1.0/255.255.255.0 Any 0-65535 0-65535 Any Permit
2 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 Any 0-65535 0-65535 Any Deny
```

2. Überprüfen Sie, ob das lokale FlexConnect-Switching deaktiviert ist:

```
(c3504-01) >show wlan 17


WLAN Identifier.................................. 17
Profile Name..................................... FlexOEAP_TEST
Network Name (SSID).............................. FlexOEAP_TEST
Status........................................... Enabled
...
Interface........................................ management
...
FlexConnect Local Switching.................. Disabled
FlexConnect Central Association.............. Disabled
flexconnect Central Dhcp Flag................ Disabled
flexconnect nat-pat Flag..................... Disabled
flexconnect Dns Override Flag................ Disabled
flexconnect PPPoE pass-through............... Disabled
flexconnect local-switching IP-source-guar.... Disabled
FlexConnect Vlan based Central Switching ..... Disabled
FlexConnect Local Authentication............. Disabled
FlexConnect Learn IP Address................. Enabled
Flexconnect Post-Auth IPv4 ACL............... Unconfigured
Flexconnect Post-Auth IPv6 ACL............... Unconfigured
...
Split Tunnel Configuration
Split Tunnel.............................. Disabled
Call Snooping.................................... Disabled
Roamed Call Re-Anchor Policy..................... Disabled
...
```

Überprüfen der FlexConnect-Gruppenkonfiguration:

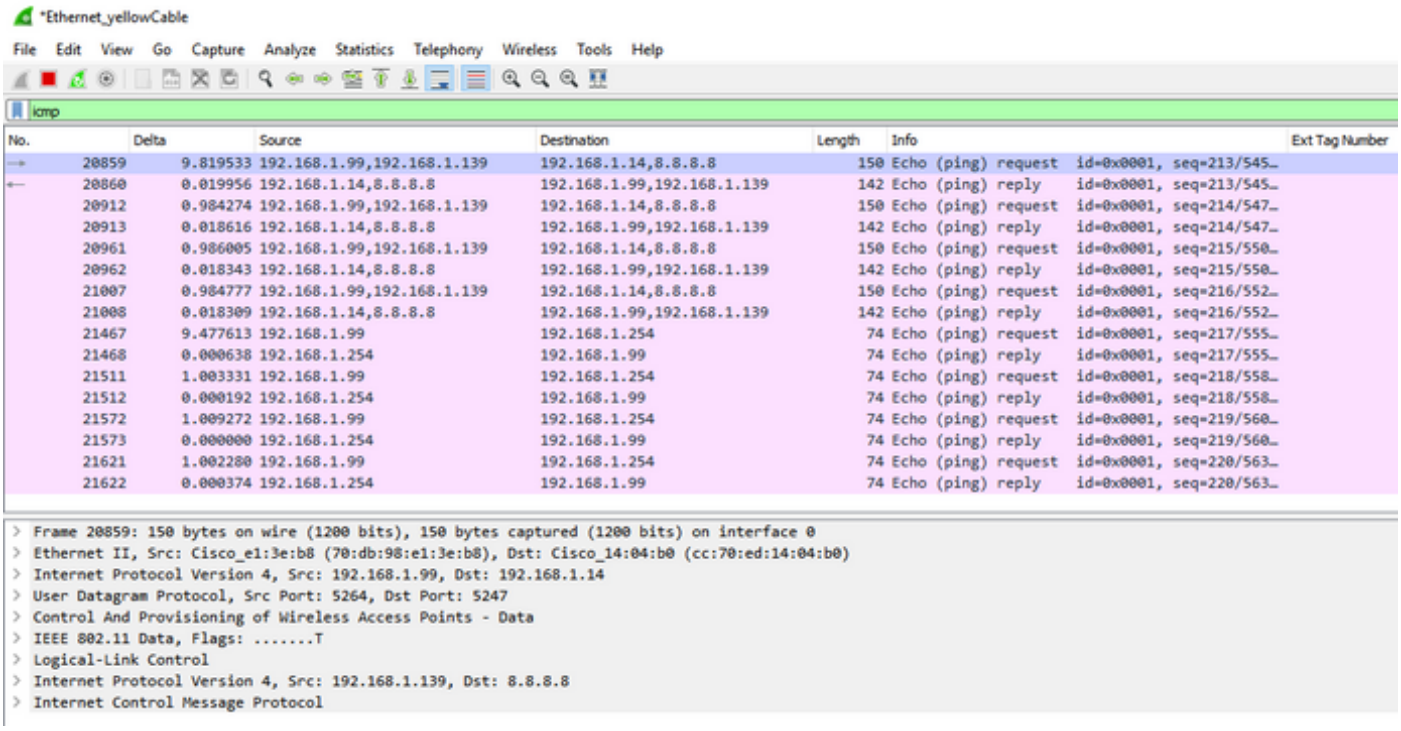
```
(c3504-01) >show flexconnect group summary

FlexConnect Group Summary: Count: 2
Group Name # Aps
-------------------- --------

FlexConnect_OEAP_Group 2
default-flex-group 0

(c3504-01) >show flexconnect group detail FlexConnect_OEAP_Group

Number of AP's in Group: 2

AP Ethernet MAC Name Status Mode Type Conflict with PnP
------------------- ------------------- -------------- -------------- ---------- ------------
------

70:db:98:e1:3e:b8 AP3800_E1.3EB8 Joined Flexconnect Manual No
c4:f7:d5:4c:e7:7c AP9120_4C.E77C Joined Flexconnect Manual No

Efficient AP Image Upgrade ..... Disabled

Efficient AP Image Join ........ Disabled

Auto ApType Conversion......... Disabled

Master-AP-Mac Master-AP-Name Model Manual
```

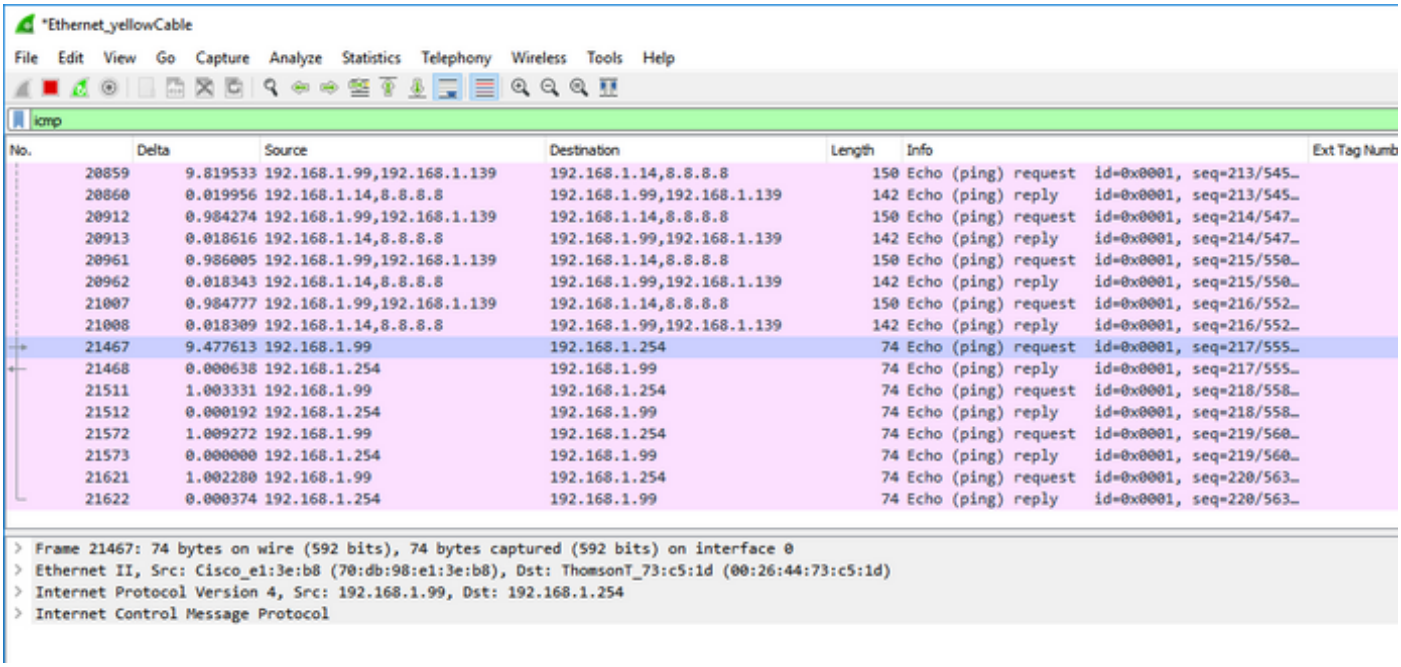
```
Group Radius Servers Settings:
Type Server Address Port
------------ --------------- -------
Primary Unconfigured Unconfigured
Secondary Unconfigured Unconfigured

Group Radius/Local Auth Parameters :
Radius Retransmit Count..... 3 (default)
Active Radius Timeout..... 5 (default)

Group Radius AP Settings:
AP RADIUS server..... Disabled
EAP-FAST Auth..... Disabled
LEAP Auth..... Disabled
EAP-TLS Auth..... Disabled
EAP-TLS CERT Download..... Disabled
PEAP Auth..... Disabled
Server Key Auto Generated... No
Server Key..... <hidden>
Authority ID..... 436973636f00000000000000000000000
Authority Info..... Cisco A_ID
PAC Timeout..... 0
HTTP-Proxy Ip Address.....
HTTP-Proxy Port..... 0
Multicast on Overridden interface config: Disabled
DHCP Broadcast Overridden interface config: Disabled
Number of User's in Group: 0
FlexConnect Vlan-name to Id Template name: none
Group-Specific FlexConnect Local-Split ACLs :

WLAN ID SSID ACL
-------- -------------------- -----
17 FlexOEAP_TEST Flex_OEAP_ACL
Group-Specific Vlan Config:
Vlan Mode..... Enabled
Native Vlan..... 100
Override AP Config..... Disabled
Group-Specific FlexConnect Wlan-Vlan Mapping:

WLAN ID Vlan ID
-------- --------------------

WLAN ID SSID Central-Dhcp Dns-Override Nat-Pat
```

Sie können überprüfen, ob der Datenverkehr am Access Point tatsächlich aufgeteilt wird, indem Sie den Datenverkehr an der AP-Schnittstelle erfassen.

> **Tipp**: Zur Fehlerbehebung können Sie die DTLS-Verschlüsselung deaktivieren, um den in Capwap eingekapselten Datenverkehr sehen zu können.

Das folgende Beispiel zeigt die Paketerfassung von Datenverkehr, der mit den ACL-Anweisungen "deny" (Ablehnen) zum WLC übereinstimmt, und Datenverkehr, der mit den ACL-Anweisungen "permit" (Zulassen) übereinstimmt und lokal am AP geschaltet wird:




> **Hinweis**: Der lokal geswitchte Datenverkehr wird vom Access Point als NAT eingestuft, da das Client-Subnetz im Normalfall zum Netzwerk des Büros gehört und die lokalen Geräte im Heimbüro nicht wissen, wie das Client-Subnetz erreicht werden kann. Der AP übersetzt den Client-Datenverkehr mithilfe der AP-IP-Adresse, die sich im Subnetz des lokalen Heimbüros befindet.

Sie können die NAT-Verarbeitung durch den Access Point überprüfen, eine Verbindung mit dem Access Point herstellen und "***show ip nat translations***" ausgeben. Beispiel:

```
AP3800_E1.3EB8#show ip nat translations

TCP NAT upstream translations:
(192.168.1.139, 1223, 192.168.1.2, 5000) => (192.168.1.99, 1223, 192.168.1.2, 5000) [*0
gw_h/nat/from_inet_tcp:0] i0 exp42949165
```

```
(192.168.1.139, 1095, 192.168.1.2, 5000) => (192.168.1.99, 1095, 192.168.1.2, 5000) [*0
gw_h/nat/from_inet_tcp:0] i0 exp85699
...

TCP NAT downstream translations:
(192.168.1.2, 5000, 192.168.1.99, 1223) => (192.168.1.2, 5000, 192.168.1.139, 1223)
[gw_h/nat/to_inet_tcp:0 *0] i0 exp42949165
(192.168.1.2, 5000, 192.168.1.99, 1207) => (192.168.1.2, 5000, 192.168.1.139, 1207)
[gw_h/nat/to_inet_tcp:0 *0] i0 exp85654
```

Wenn Split-Tunneling entfernt wird, wird der gesamte Datenverkehr zentral auf dem WLC abgewickelt. Hier sehen wir, wie der ICMP zum 192.168.1.2 in den Capwap-Tunnel gelangt: