# 使用分割隧道配置FlexConnect OEAP

## 目录



## 简介

本文档介绍如何将室内接入点(AP)配置为FlexConnect Office Extend AP(OEAP)模式，以及如何启用分割隧道，以便您可以定义哪些流量必须在家庭办公室本地交换，哪些流量必须在无线局域网控制器(WLC)集中交换。

作者：Tiago Antunes、Nicolas Darchis Cisco TAC工程师。

## 先决条件

### 要求

本文档中的配置假设WLC已在启用网络地址转换(NAT)的隔离区(DMZ)中配置，并且AP能够从家庭办公室加入WLC。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

- WLC，带AireOS 8.10(130.0)软件版本。
- Wave1 AP:1700/2700/3700 的多播地址发送一次邻居消息。
- 第2波AP:1800/2800/3800/4800和Catalyst 9100系列。

本文档中的信息都是基于特定实验室环境中的设备编写的。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 概述

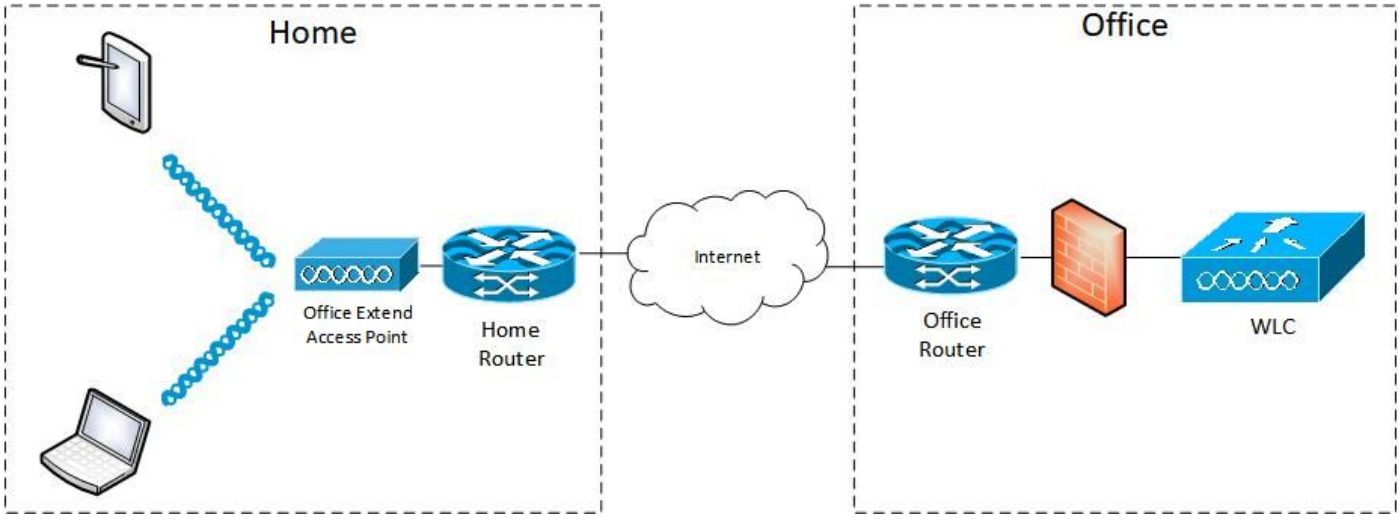
OEAP提供从Cisco WLC到远程位置的Cisco AP的安全通信，以便通过Internet将公司WLAN扩展到员工住所。用户在家庭办公室的体验与在公司办公室的体验完全相同。AP和控制器之间的数据报传输层安全(DTLS)加密可确保所有通信都具有最高级别的安全性。 FlexConnect模式下的任何室内AP都可以充当OEAP。

### 重要事实

- Cisco OEAP设计为在使用NAT的路由器或其他网关设备后工作。NAT允许设备（如路由器）充当Internet（公有）和个人网络（私有）之间的代理，这使整个计算机组可以用单个IP地址表示。在NAT设备后部署的Cisco OEAP数量没有限制。
- 除AP-700I、AP-700W和AP802系列AP外，所有支持的带集成天线的室内AP型号都可配置为OEAP。
- 所有OEAP必须位于同一AP组中，且该组必须包含不超过15个无线LAN。AP组中具有OEAP的控制器仅向每个连接的OEAP发布最多15个WLAN，因为它为个人服务集标识符(SSID)保留一个WLAN。

## 配置

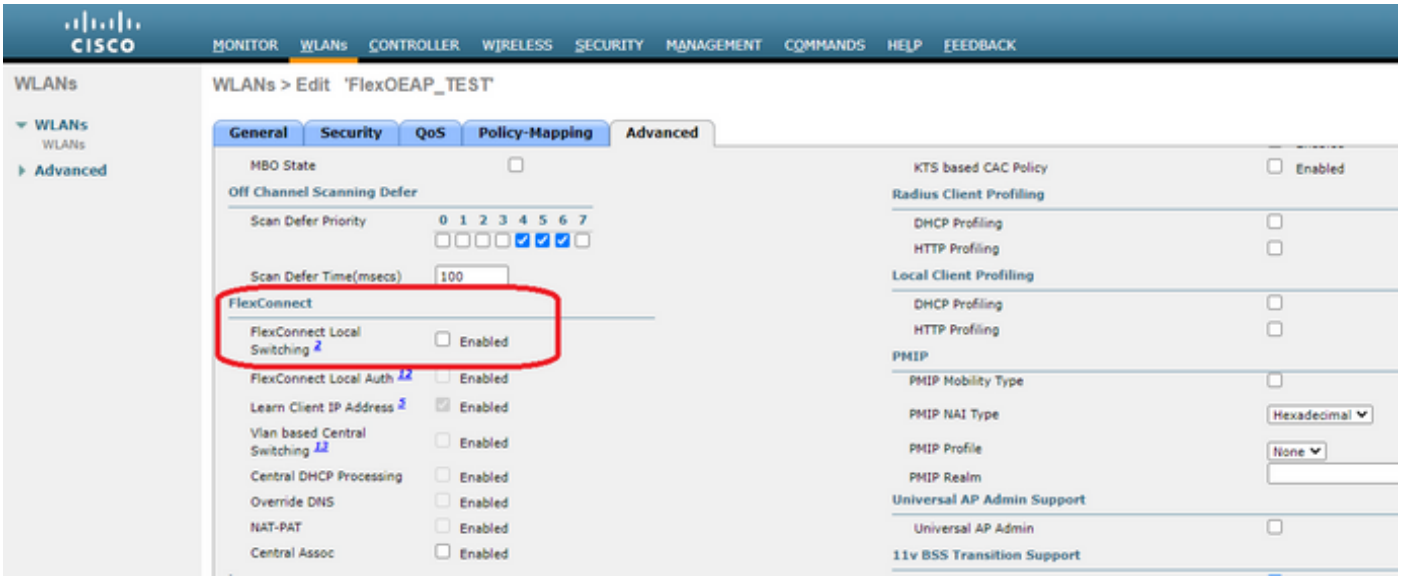
### 网络图



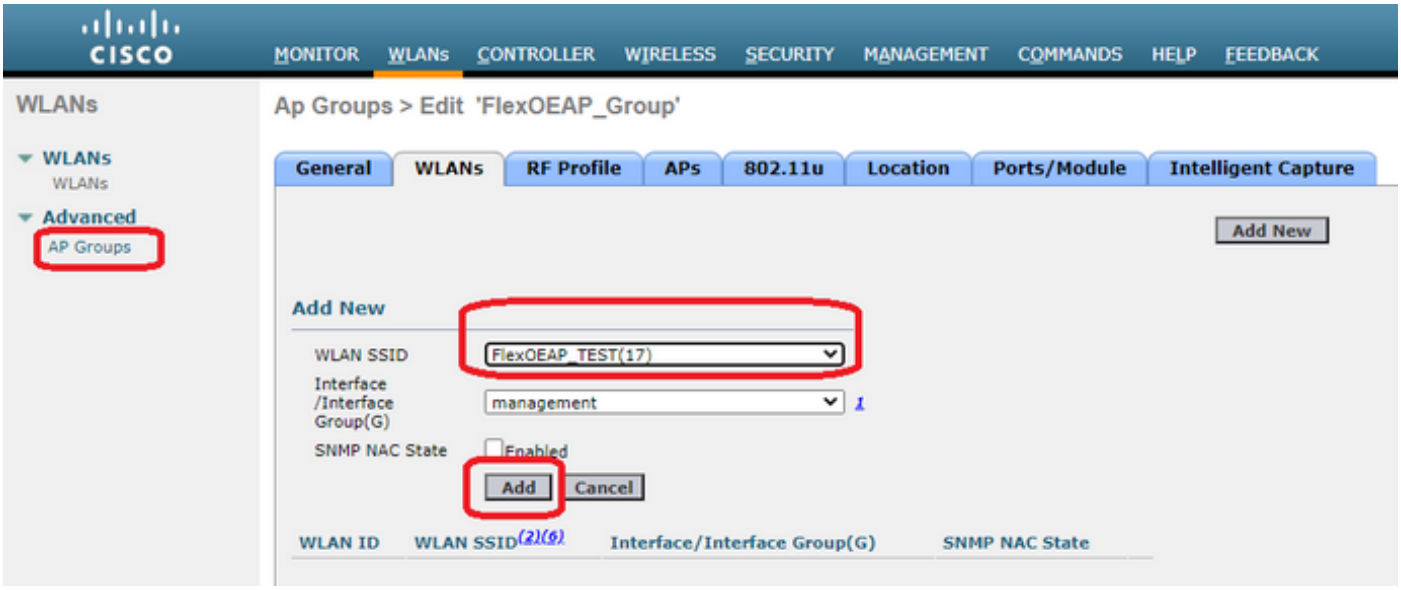

### 配置

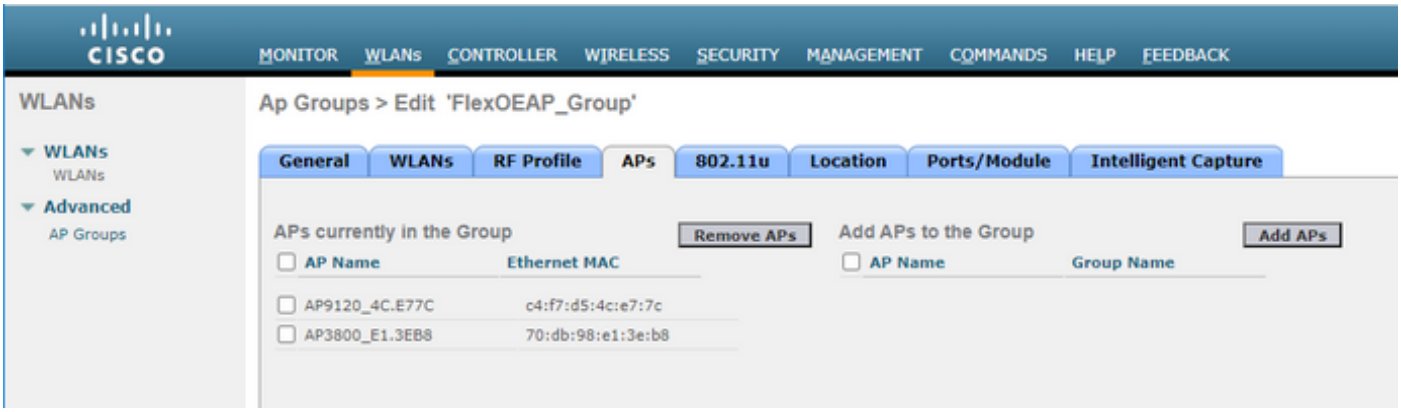
#### WLAN 配置

步骤1.创建WLAN以分配给AP组。您无需为此WLAN启用FlexConnect本地交换选项。




步骤2.创建AP组。在WLANs选项卡上，选择WLAN SSID，然后单击Add添加WLAN。转到AP选项卡并添加FlexConnect OEAP。

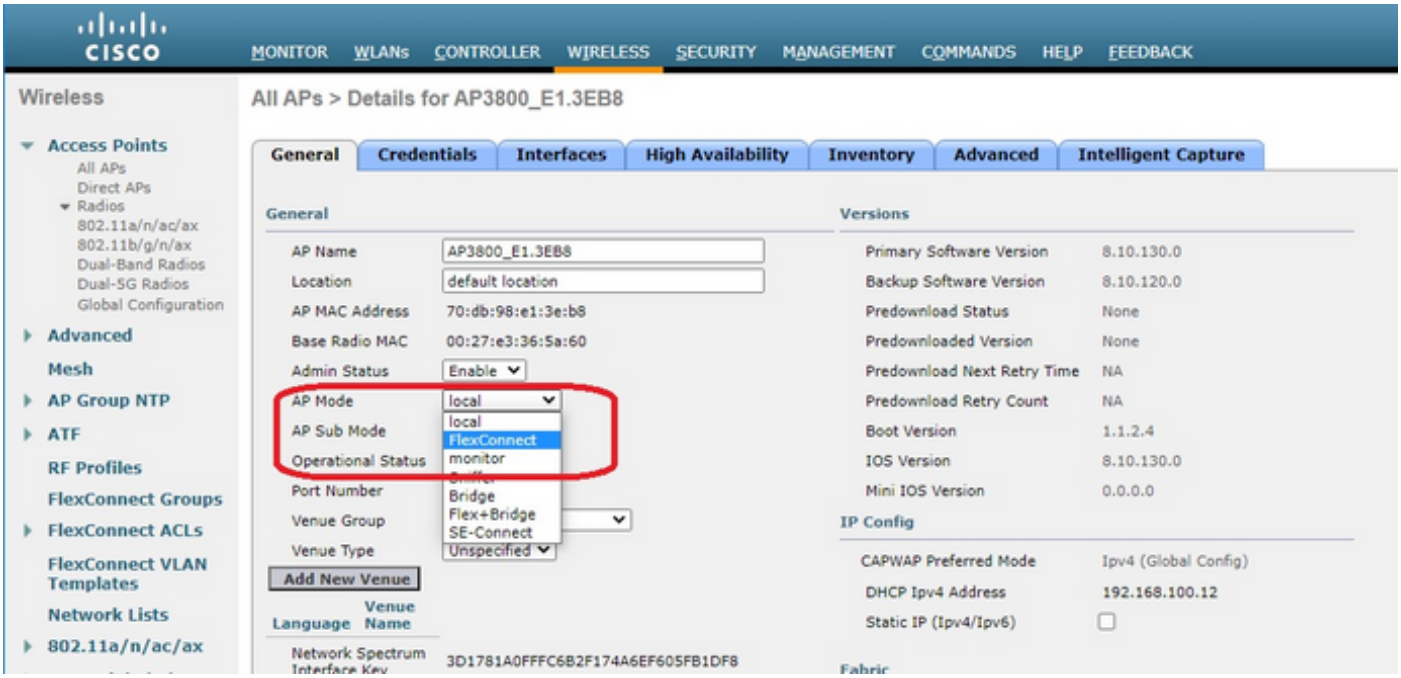


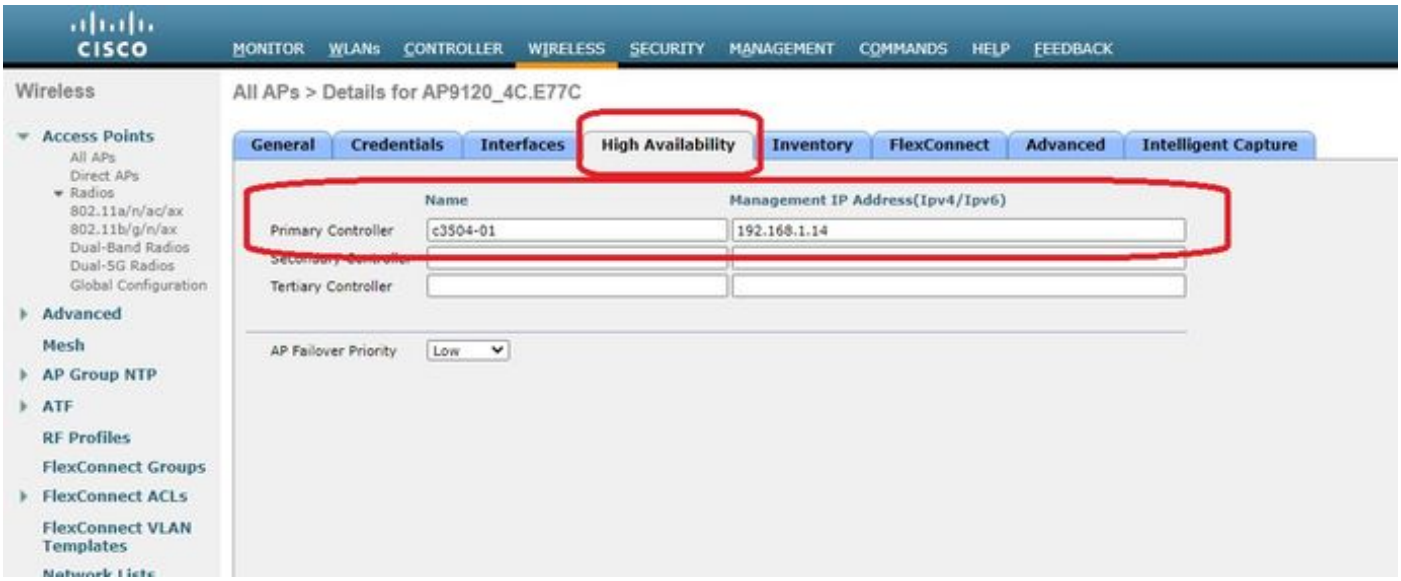

**无线接入点配置**

AP在FlexConnect模式下与控制器关联后，可将其配置为OEAP。

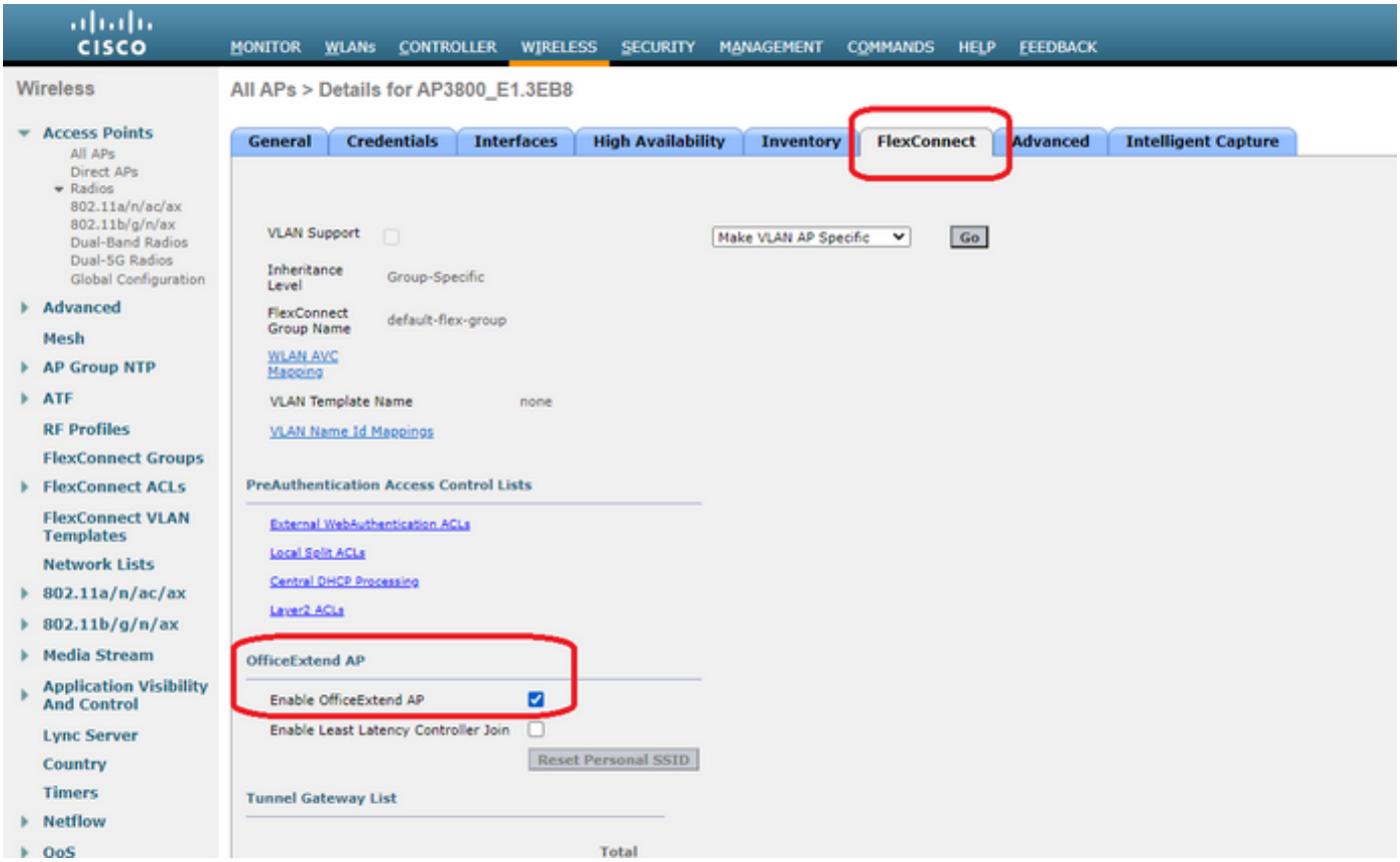
步骤1.在AP加入WLC后，将AP模式更改为FlexConnect，然后单击“应用”。



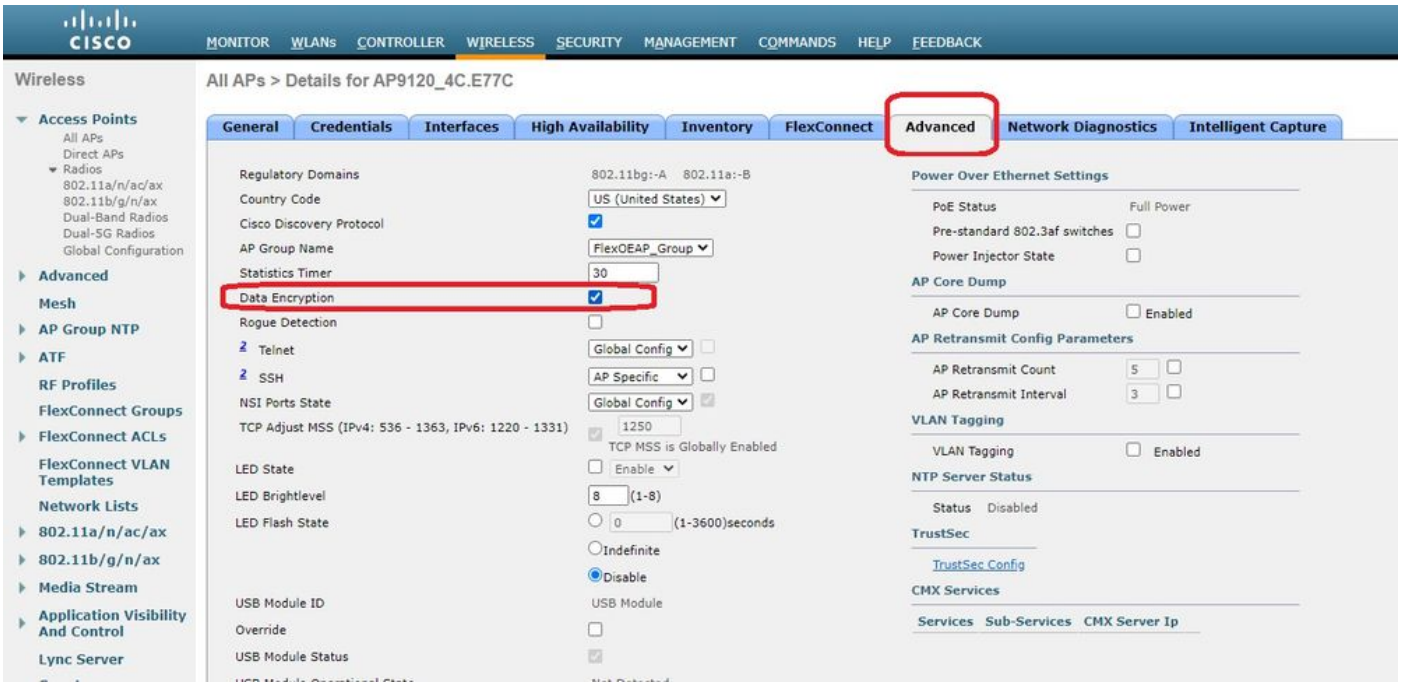

步骤2.确保在High Availability（高可用性）选项卡中至少配置了主WLC:




步骤3.转到FlexConnect选项卡并选中Enable **OfficeExtend AP**复选框。




为AP启**用OfficeExtend模**式时，DTLS数据加密将自动启用。但是，您可以启用或禁用特定AP的DTLS数据加密。为此，请选中（启用）或取消选中（禁用）“所有AP”>“[选定AP]的详细信息”>“高级”选项卡上的“数据加密”复选框：




**注意**：当您为AP启用OfficeExtend模式时，Telnet和SSH访问会自动禁用。但是，您可以启用或禁用特定AP的Telnet或SSH访问。为此，请选中（启用）或取消选中（禁用）“所有AP”>“[选定AP]”>“高级”选项卡上的“Telnet或SSH”复选框。

**注意**：为AP启用OfficeExtend模式时，链路延迟会自动启用。但是，您可以启用或禁用特定AP的链路延迟。要执行此操作，请选中（启用）或取消选中（禁用）All APs > Details for

[selected AP] > Advanced选项卡上的Enable Link Latency复选框。

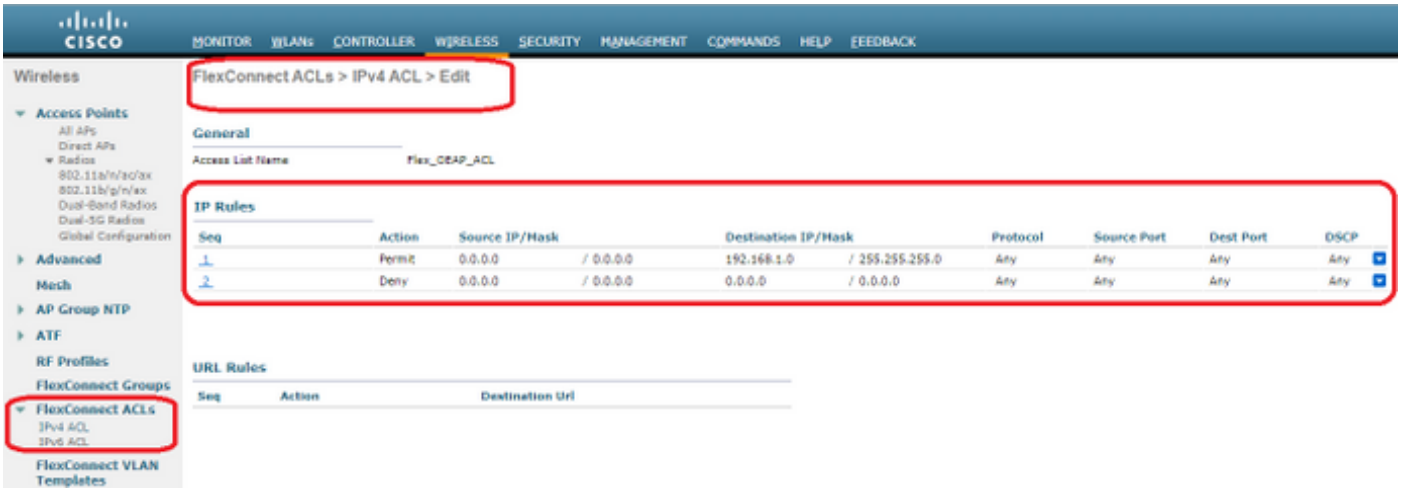
步骤3.选择“**应用**”。选择应用后，AP将重新加载。

步骤4. AP重新加入WLC后，AP处于OEAP模式。

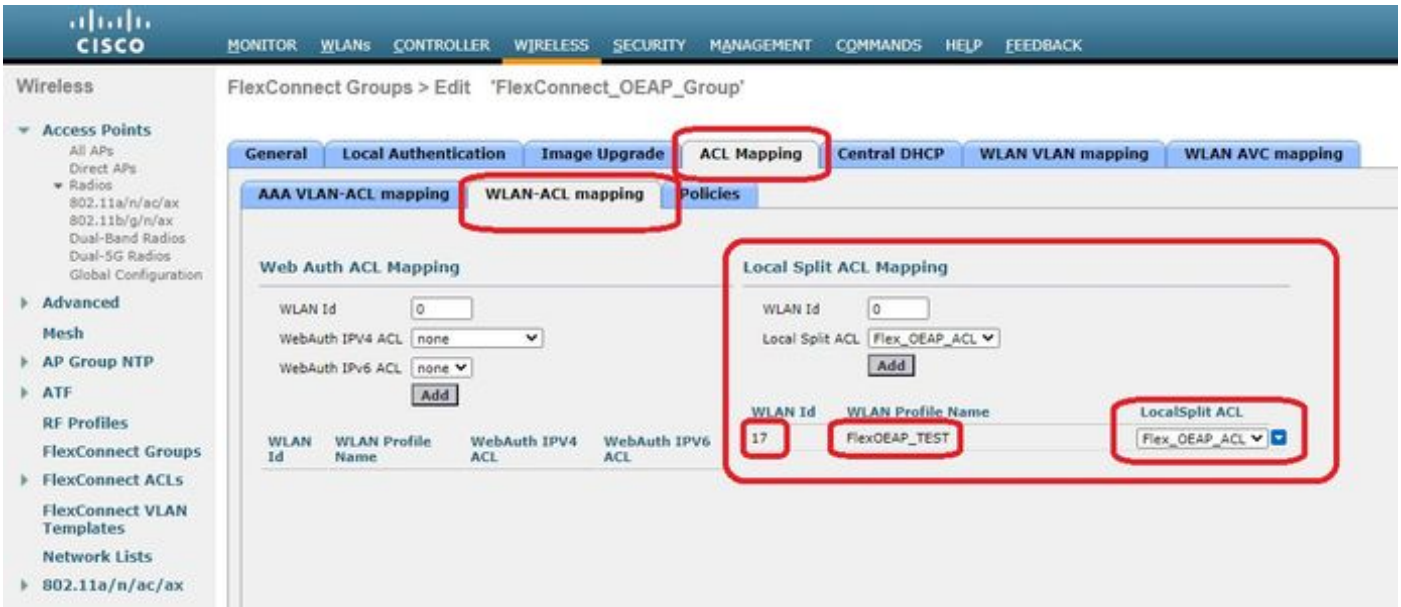
> **注意**：我们建议您配置AP加入安全（通常在AP策略下定义），以便只有授权AP才能加入WLC。您还可以使用本地有效证书(LSC)AP调配。

步骤5.创建FlexConnect访问控制列表(ACL)，以定义将集中交换（拒绝）和本地交换（允许）的流量。

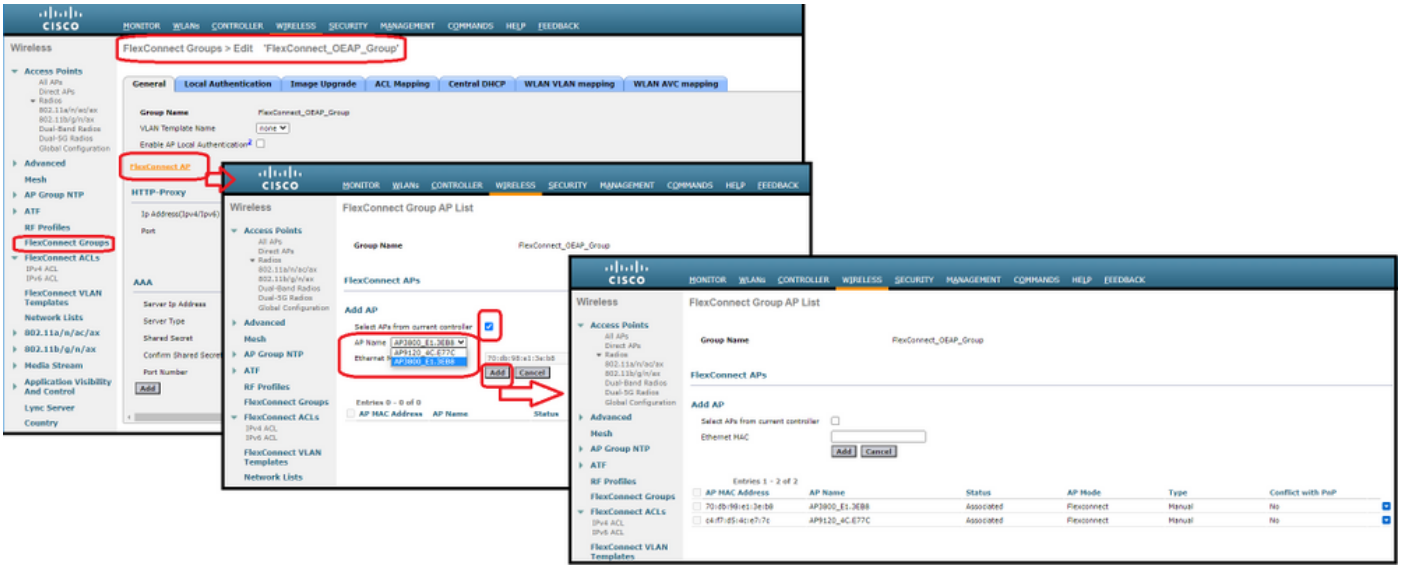
此处，您的目标是将所有流量本地交换到子网192.168.1.0/24。




步骤6.创建FlexConnect组，转到**ACL映射**，然后转**到WLAN-ACL映射**。在“本地拆分ACL映射”下，输入WLAN ID，然后选择FlexConnect ACL。然后单击添加。




步骤7.**将**AP添加到FlexConnect组：



# 验证

1.检验FlexConnect ACL状态和定义：

```
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.验证FlexConnect本地交换是否已禁用：

```
(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
...
```

### 3.验证FlexConnect组配置：

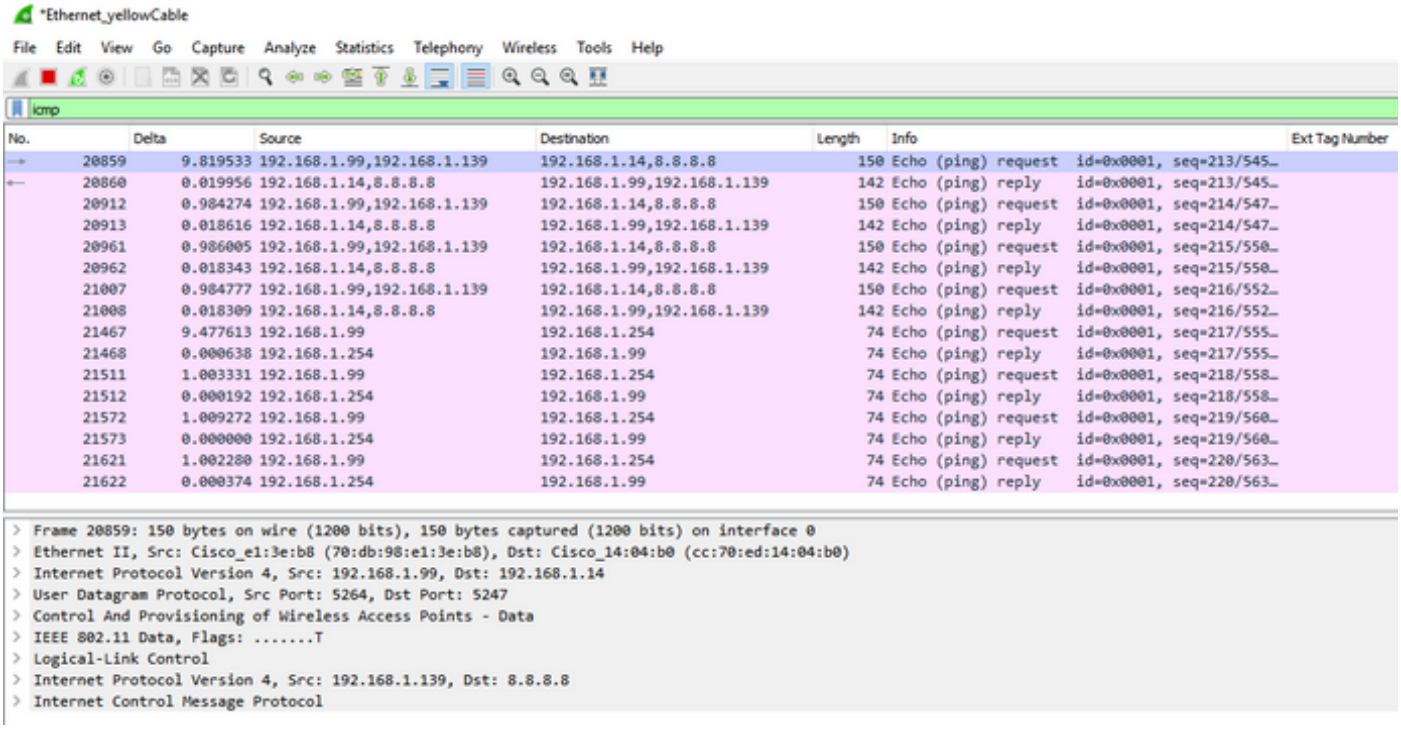
```
(c3504-01) >show flexconnect group summary

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................. 436973636f000000000000000000000000
Authority Info.............. Cisco A_ID
PAC Timeout.................. 0
HTTP-Proxy Ip Address.......
```

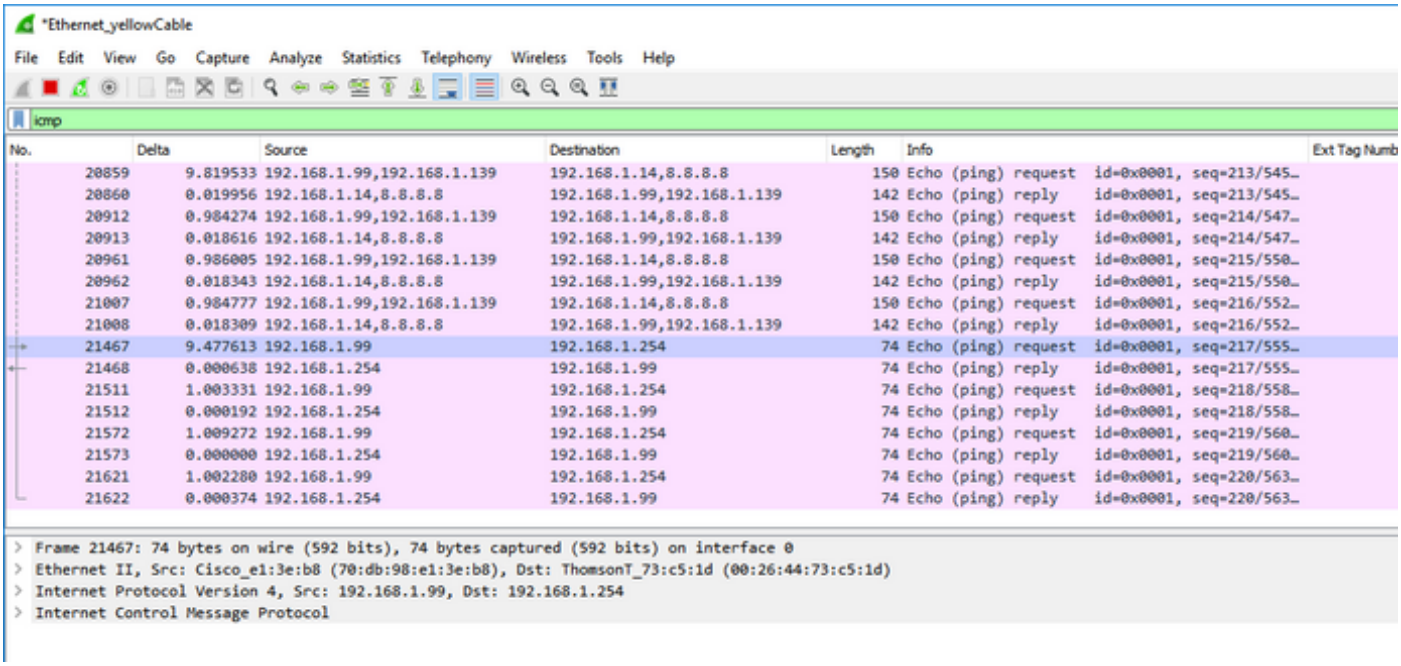
```
HTTP-Proxy Port.............. 0
Multicast on Overridden interface config: Disabled
DHCP Broadcast Overridden interface config: Disabled
Number of User's in Group: 0
FlexConnect Vlan-name to Id Template name: none
Group-Specific FlexConnect Local-Split ACLs :

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
```

您可以捕获AP接口上的流量，以验证流量是否在AP上拆分。

**提示**：出于故障排除目的，您可以禁用DTLS加密，以便查看封装在capwap中的数据流量。

此数据包捕获示例显示与指向WLC的ACL“deny”语句匹配的数据流量，以及与ACL“permit”语句匹配的数据流量，这些语句在AP本地交换：



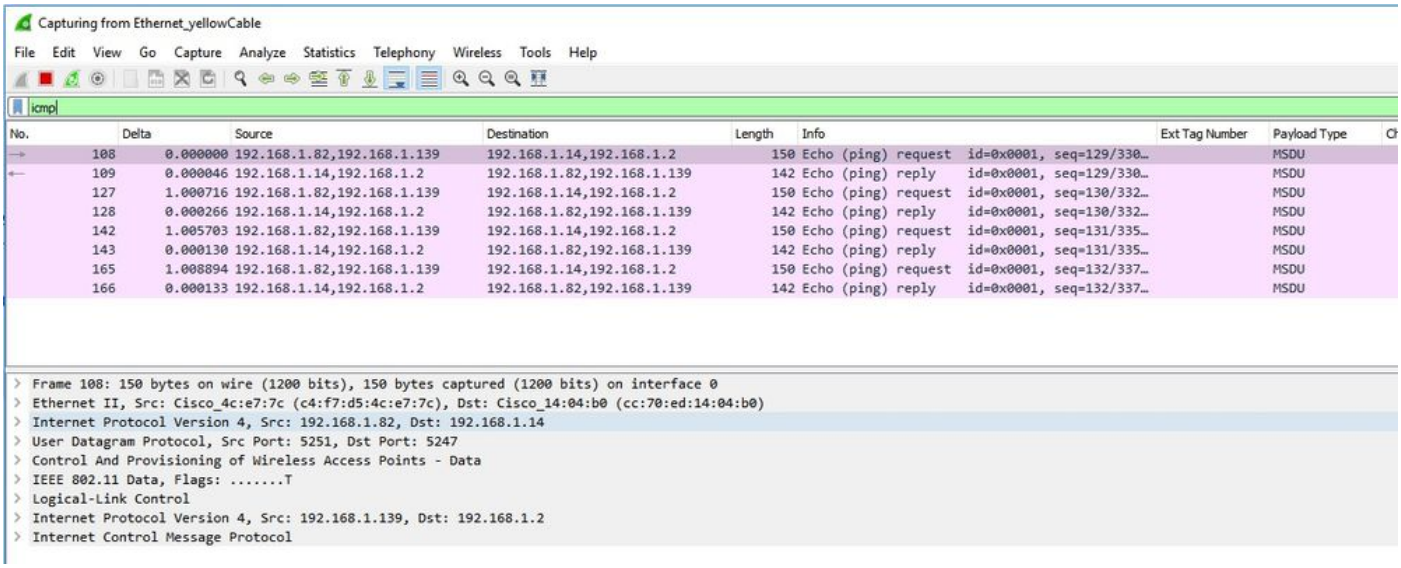



**注意**：在正常情况下，AP会转换本地交换流量的网络地址，因为客户端子网属于办公室网络，而家庭办公室的本地设备不知道如何到达客户端子网。AP使用本地家庭办公室子网中定义的IP地址来转换客户端流量。

为了验证AP是否执行了NAT，您可以连接到AP终端并发出“***show ip nat translations***”命令。示例：

```
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
```

如果删除分割隧道，则所有流量都在WLC中集中交换。本示例显示在capwap隧道内到192.168.1.2目的地的Internet控制消息协议(ICMP):


Capturing from Ethernet_yellowCable
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp
No. Delta Source Destination Length Info Ext Tag Number Payload Type
108 0.000000 192.168.1.82,192.168.1.139 192.168.1.14,192.168.1.2 150 Echo (ping) request id=0x0001, seq=129/330… MSDU
109 0.000046 192.168.1.14,192.168.1.2 192.168.1.82,192.168.1.139 142 Echo (ping) reply id=0x0001, seq=129/330… MSDU
127 1.000716 192.168.1.82,192.168.1.139 192.168.1.14,192.168.1.2 150 Echo (ping) request id=0x0001, seq=130/332… MSDU
128 0.000266 192.168.1.14,192.168.1.2 192.168.1.82,192.168.1.139 142 Echo (ping) reply id=0x0001, seq=130/332… MSDU
142 1.005703 192.168.1.82,192.168.1.139 192.168.1.14,192.168.1.2 150 Echo (ping) request id=0x0001, seq=131/335… MSDU
143 0.000130 192.168.1.14,192.168.1.2 192.168.1.82,192.168.1.139 142 Echo (ping) reply id=0x0001, seq=131/335… MSDU
165 1.008894 192.168.1.82,192.168.1.139 192.168.1.14,192.168.1.2 150 Echo (ping) request id=0x0001, seq=132/337… MSDU
166 0.000133 192.168.1.14,192.168.1.2 192.168.1.82,192.168.1.139 142 Echo (ping) reply id=0x0001, seq=132/337… MSDU
Frame 108: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
Ethernet II, Src: Cisco_4c:e7:7c (c4:f7:d5:4c:e7:7c), Dst: Cisco_14:04:b0 (cc:70:ed:14:04:b0)
Internet Protocol Version 4, Src: 192.168.1.82, Dst: 192.168.1.14
User Datagram Protocol, Src Port: 5251, Dst Port: 5247
Control And Provisioning of Wireless Access Points - Data
IEEE 802.11 Data, Flags: .......T
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.1.139, Dst: 192.168.1.2
Internet Control Message Protocol