使用分割隧道配置FlexConnect OEAP

目錄

簡介

本文說明如何將室記憶體取點(AP)設定為FlexConnect Office Extend AP(OEAP)模式，以及如何啟用分割通道，以便您可以定義哪些流量必須在家庭辦公室本地交換，哪些流量必須在無線區域網路控制器(WLC)集中交換。

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

必要條件

需求

本檔案中的組態假設已在已啟用網路位址轉譯(NAT)的非軍事區(DMZ)中設定WLC，且AP可從總部加入WLC。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 使用AireOS 8.10(130.0)軟體的WLC。
- Wave1 AP:1700/2700/3700 .
- Wave2 AP:1800/2800/3800/4800和Catalyst 9100系列。

本文中的資訊是根據特定實驗室環境內的裝置所建立。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

概觀

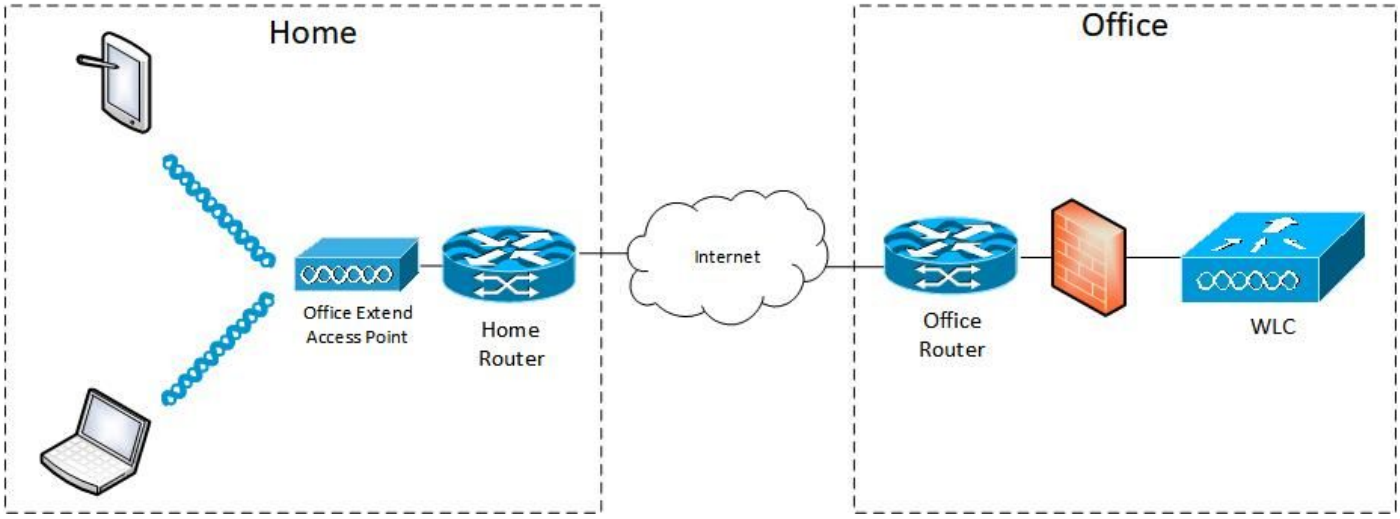
OEAP提供從Cisco WLC到遠端位置的Cisco AP的安全通訊，以便通過Internet將公司WLAN擴展到員工住所。使用者在家庭辦公室中的體驗與在公司辦公室中的體驗完全相同。AP和控制器之間的資料包傳輸層安全(DTLS)加密可確保所有通訊都具有最高級別的安全性。 FlexConnect模式下的任何室內AP都可以充當OEAP。

重要事實

- Cisco OEAP設計用於在使用NAT的路由器或其他網關裝置後工作。NAT允許裝置（如路由器）在Internet（公共）和個人網路（私有）之間充當代理，從而允許用單個IP地址代表整個電腦組。您可以在NAT裝置之後部署的Cisco OEAP數量沒有限制。
- 除AP-700I、AP-700W和AP802系列AP外，所有受支援的帶整合天線的室內AP型號均可配置為OEAP。
- 所有OEAP必須位於同一個AP組中，並且該組包含的無線LAN不能超過15個。在AP組中具有OEAP的控制器僅向每個連線的OEAP發佈最多15個WLAN，因為它為個人服務集識別符號(SSID)保留一個WLAN。

設定

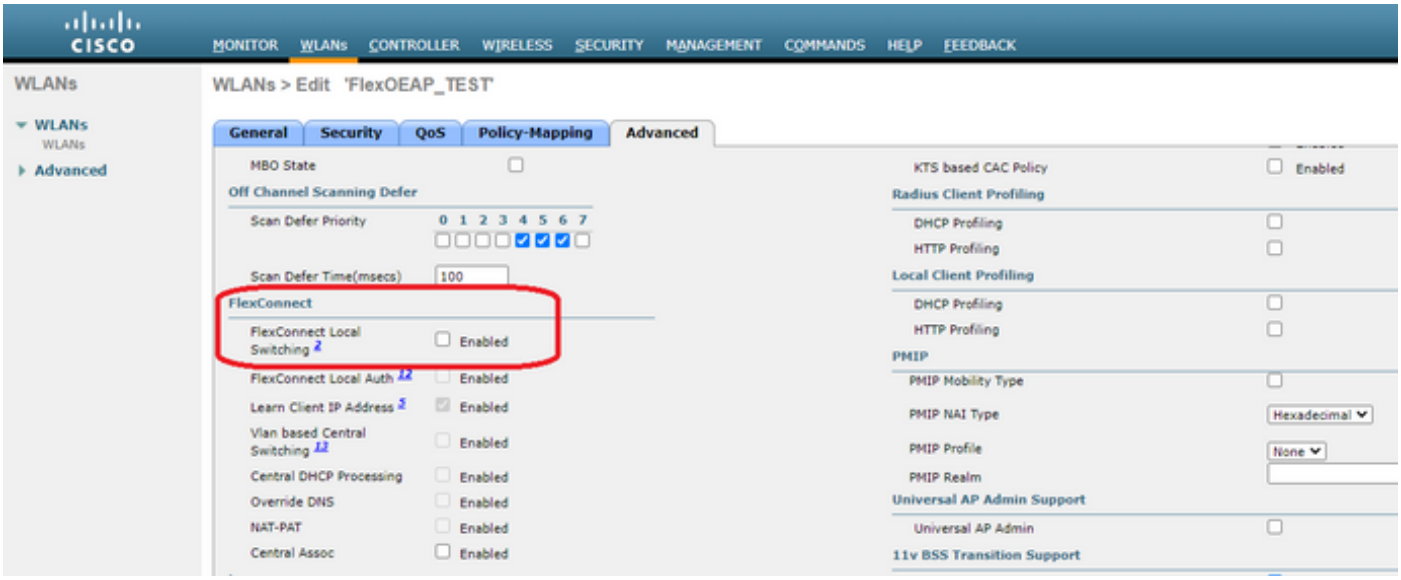
網路圖表



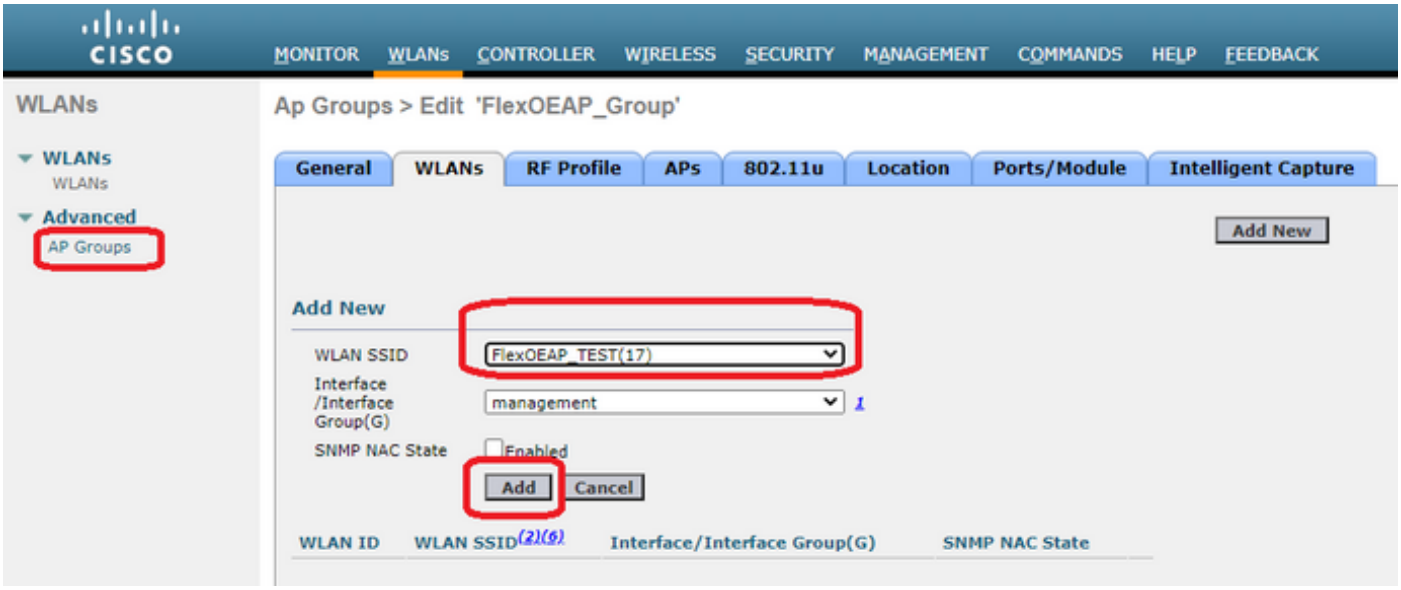
組態

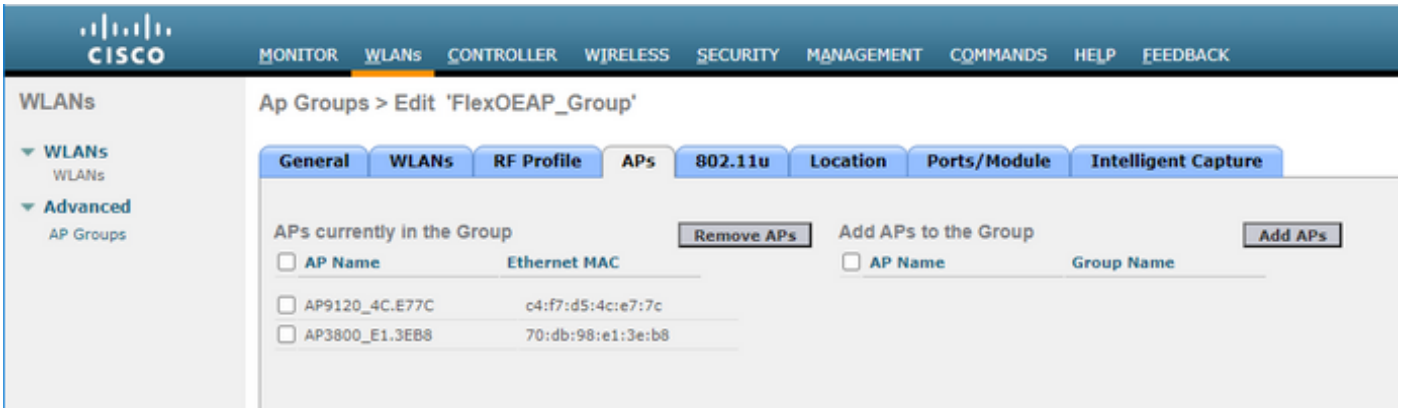
WLAN配置

步驟1.建立分配給AP組的WLAN。您無需為此WLAN啟用FlexConnect本地交換選項。



步驟2.建立AP組。在**WLANs**頁籤上，選擇WLAN SSID，然後按一下**Add**以新增WLAN。轉到**APs**頁籤並**新增** FlexConnect OEAP。

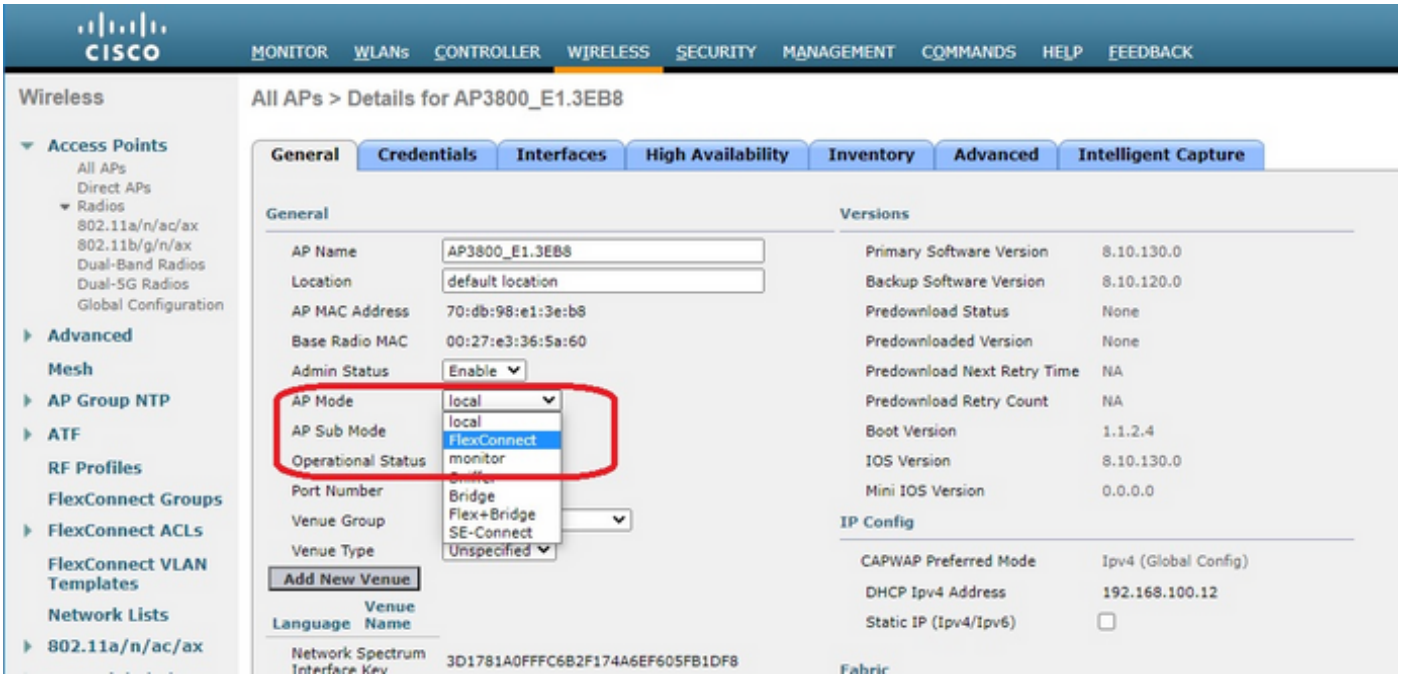




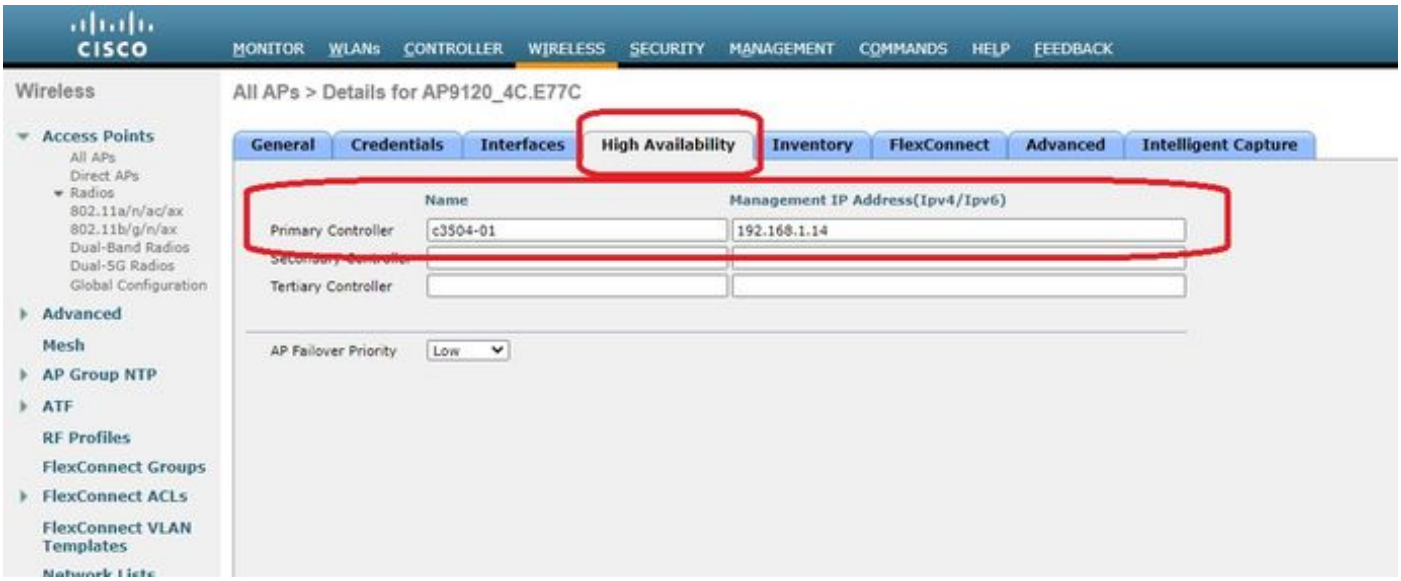
AP配置

在FlexConnect模式下，AP與控制器關聯後，您可以將其配置為OEAP。

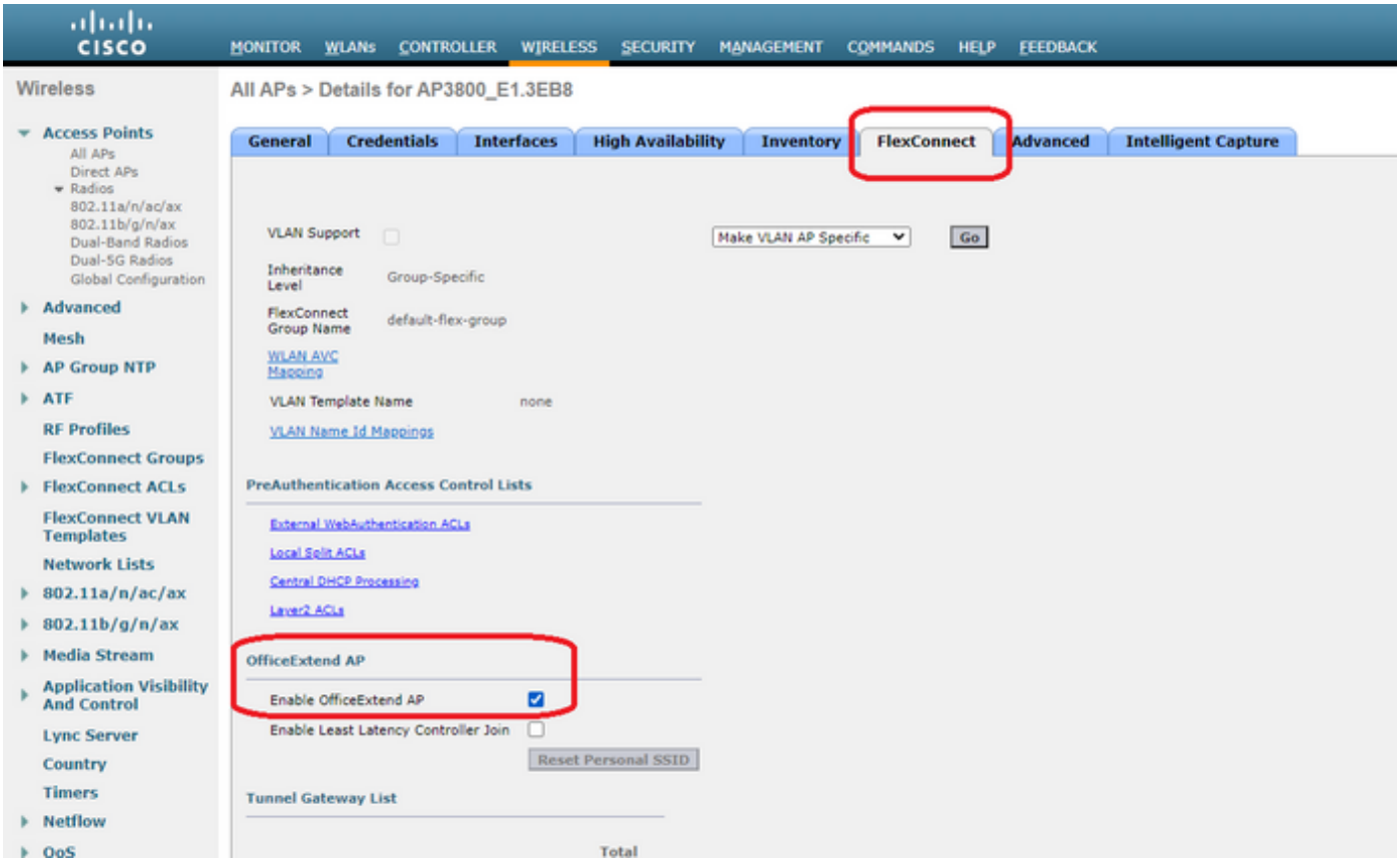
步驟1。AP加入WLC後，將AP模式更改為**FlexConnect**，然後按一下**Apply**。



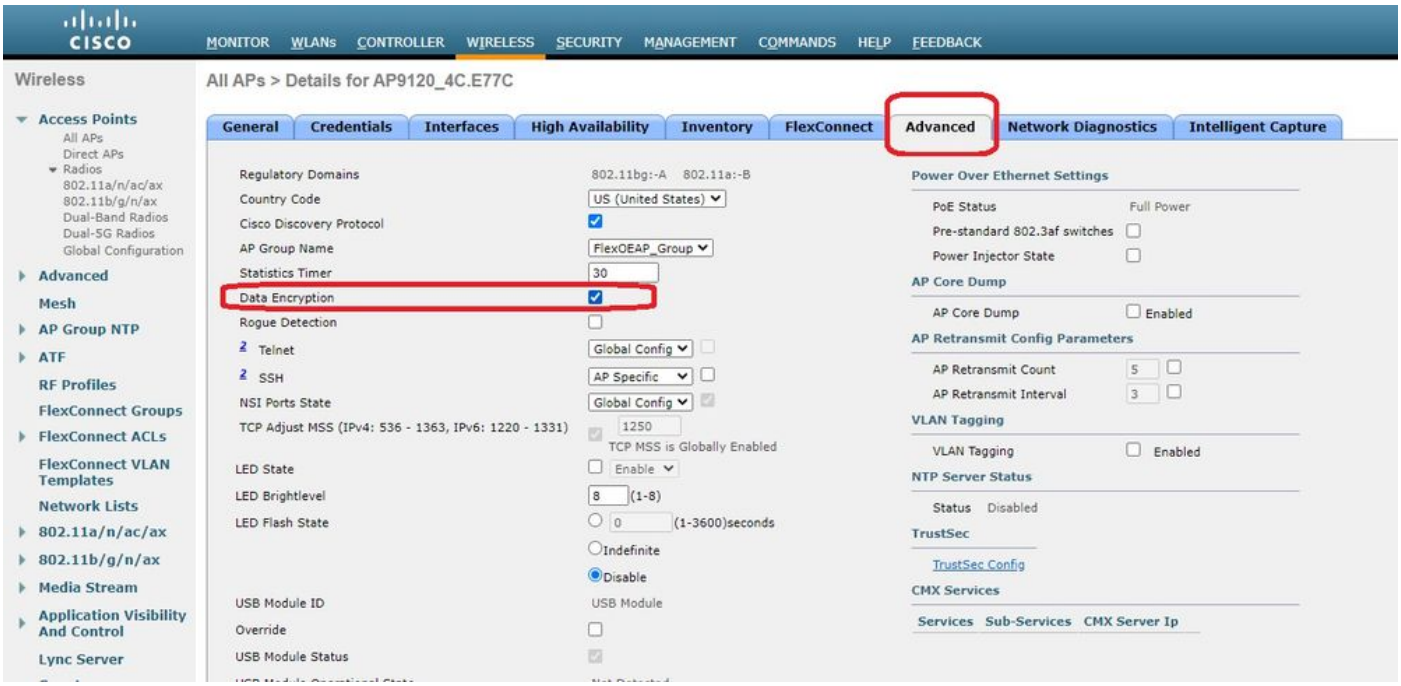
步驟2.確保在「High Availability（高可用性）」頁籤中至少配置了一個主WLC:



步驟3.轉到FlexConnect頁籤並選中**Enable OfficeExtend AP**覈取方塊。



為AP啟用OfficeExtend模式時，將自動啟用DTLS **Data Encryption**。但是，您可以啟用或禁用特定AP的DTLS資料加密。為此，請選中（啟用）或取消選中（禁用）所有AP > [選定AP]的詳細資訊>「高級」頁籤上的**Data Encryption**覈取方塊：



附註：為AP啟用OfficeExtend模式時，將自動禁用Telnet和SSH訪問。但是，您可以啟用或禁用特定AP的Telnet或SSH訪問。為此，請選中（啟用）或取消選中（禁用）所有AP > [選定AP]的詳細資訊>「高級」頁籤上的Telnet或SSH覈取方塊。

附註：為AP啟用OfficeExtend模式時，會自動啟用鏈路延遲。但是，您可以啟用或禁用特定AP的鏈路延遲。要執行此操作，請選中（啟用）或取消選中（禁用）所有AP > [選定AP] >

Advanced頁籤的Enable Link Latency覈取方塊。

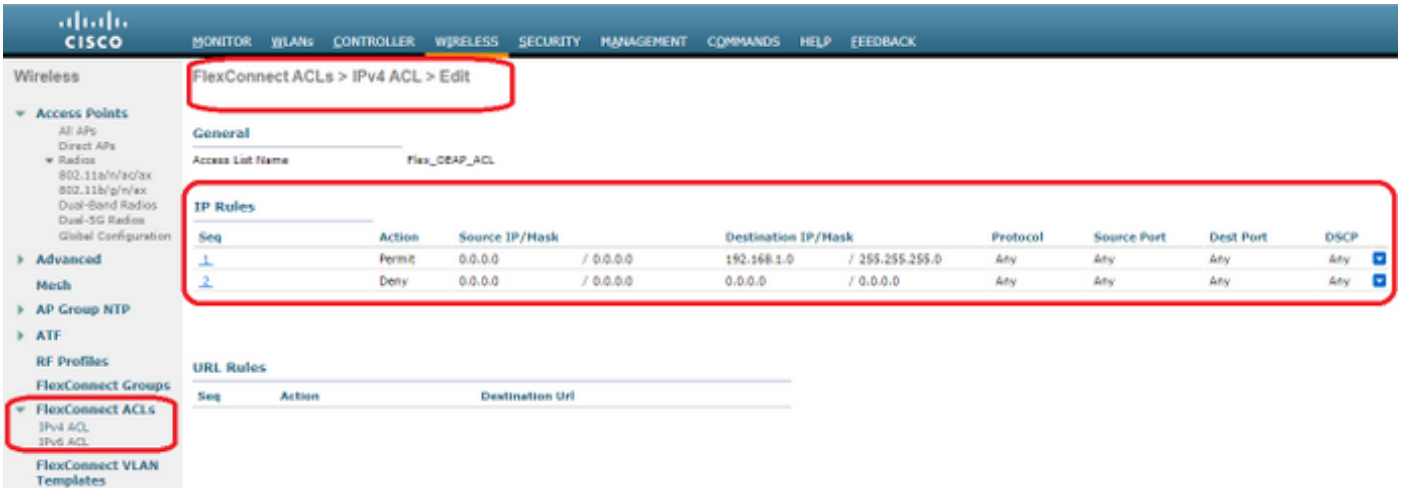
步驟3.選擇**Apply**。選擇「應用」後，AP將重新載入。

步驟4. AP重新加入WLC後，AP處於OEAP模式。

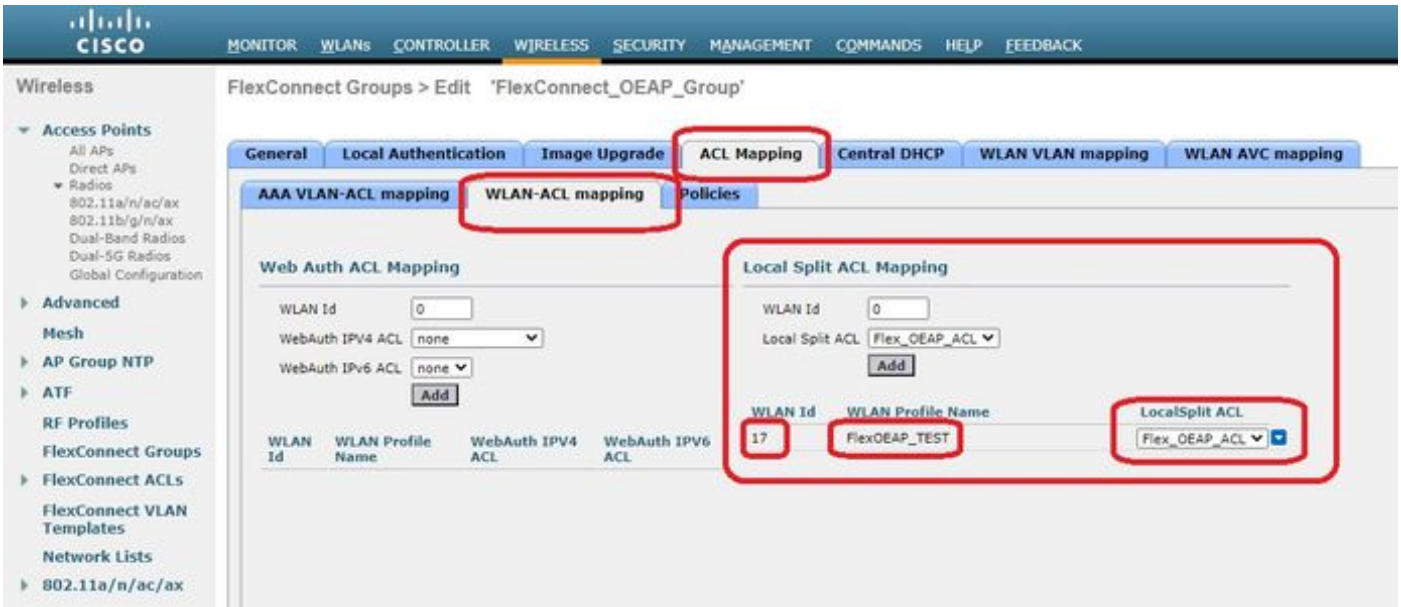
> **附註**：我們建議您配置AP加入安全性（通常在AP策略下定義），以便只有經過授權的AP可以加入WLC。您還可以使用本地重要證書(LSC)AP調配。

步驟5.建立FlexConnect存取控制清單(ACL)，定義哪些流量將集中交換（拒絕）和在本地交換（允許）。

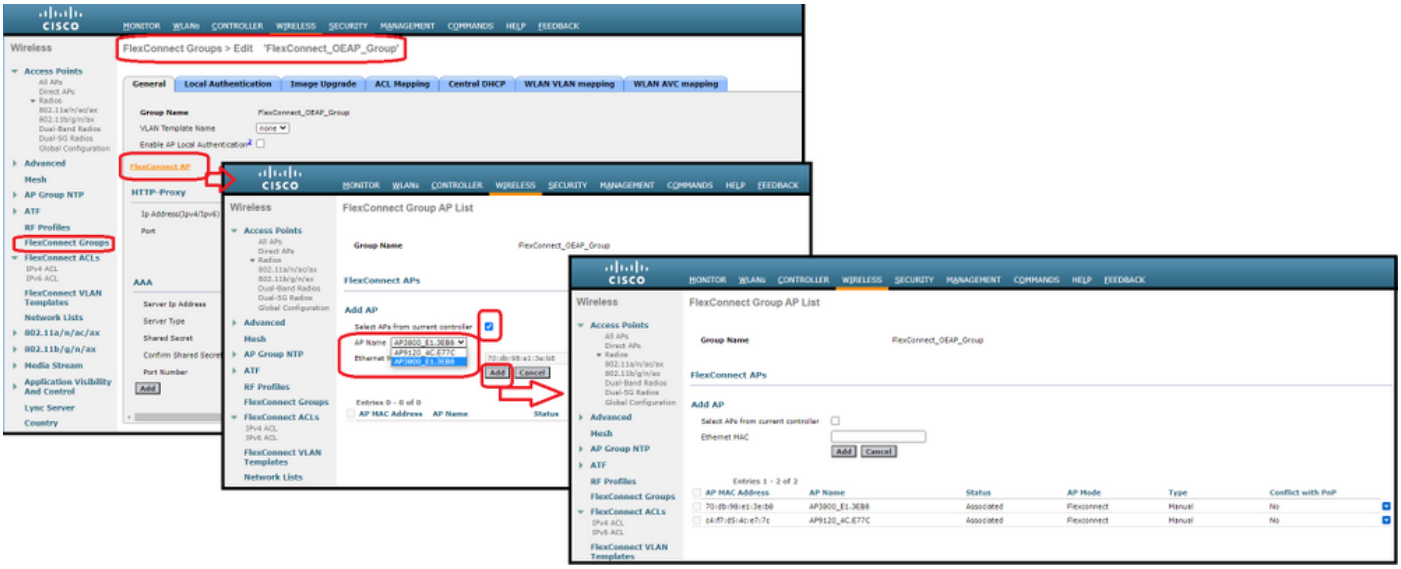
在這裡，您的目標是將本地所有流量切換到子網192.168.1.0/24。



步驟6.建立FlexConnect組，轉到**ACL對映**，然後轉到**WLAN-ACL對映**。在「本地拆分ACL對映」下，輸入WLAN ID並選擇FlexConnect ACL。然後按一下**「Add」**。



步驟7. **將AP**新增到FlexConnect群組：



驗證

1.驗證FlexConnect ACL狀態和定義：

```
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.驗證FlexConnect本地交換是否已禁用：

```
(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.驗證FlexConnect組配置：

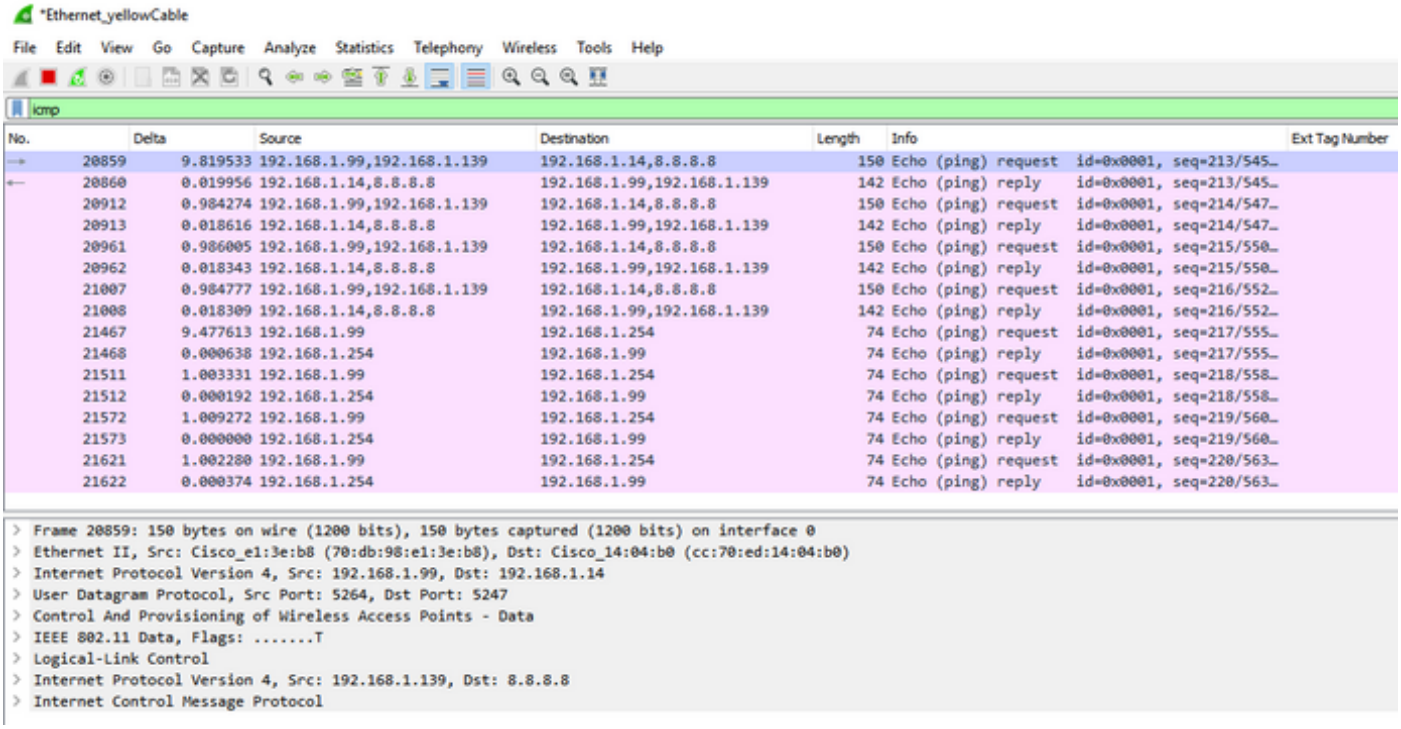
```
(c3504-01) >show flexconnect group summary

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.......
```

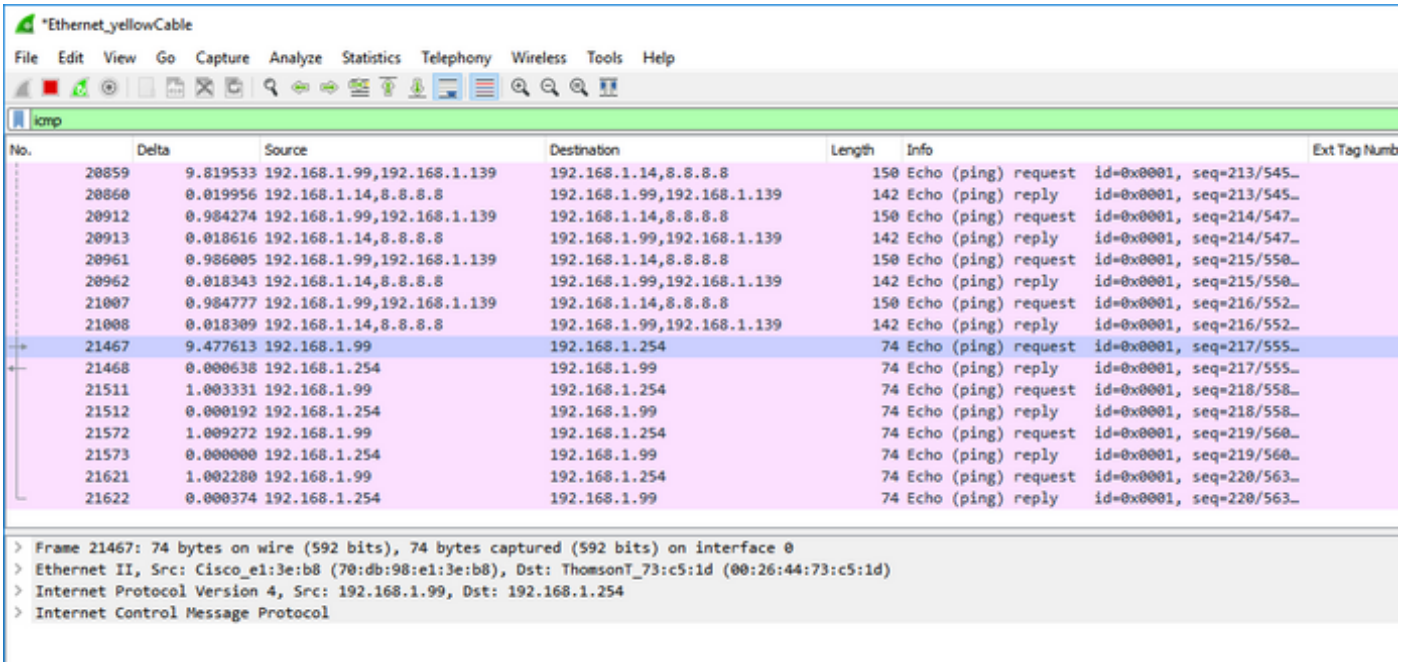
```
HTTP-Proxy Port.............. 0
Multicast on Overridden interface config: Disabled
DHCP Broadcast Overridden interface config: Disabled
Number of User's in Group: 0
FlexConnect Vlan-name to Id Template name: none
Group-Specific FlexConnect Local-Split ACLs :

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
```

您可以在AP介面捕獲流量，以驗證流量是否在AP進行分割。

提示：出於故障排除目的，您可以禁用DTLS加密以檢視封裝在capwap內的資料流量。

此封包擷取範例顯示與導向到WLC的ACL「deny」陳述式相符的資料流量，以及與AP本機上交換的ACL「permit」陳述式相符的資料流量：



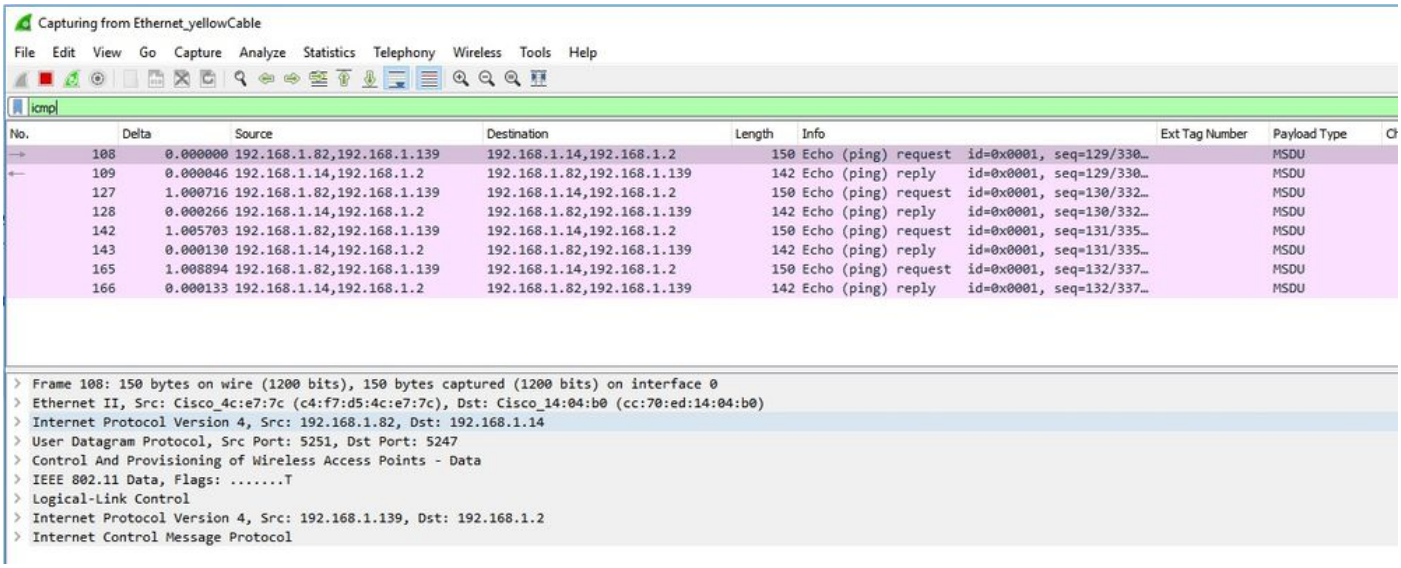


附註：在正常情況下，AP會轉換本地交換流量的網路地址，因為客戶端子網屬於辦公室網路，而家庭辦公室的本地裝置不知道如何到達客戶端子網。AP使用本地家庭辦公室子網中定義的IP地址來轉換客戶端流量。

為了驗證AP是否執行了NAT，您可以連線到AP終端機並發出「***show ip nat translations***」命令。範例：

```
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
```

如果移除分割通道，則會在WLC集中交換所有流量。此範例顯示capwap通道中到192.168.1.2目的地的網際網路控制訊息通訊協定(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