스플릿 터널링을 사용하여 FlexConnect OEAP 구성

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[개요](#)
[중요한 사실](#)
[구성](#)
[네트워크 다이어그램](#)
[구성](#)
[WLAN 컨피그레이션](#)
[AP 컨피그레이션](#)
[다음을 확인합니다.](#)

소개

이 문서에서는 실내 AP(Access Point)를 FlexConnect Office Extend AP(OEAP) 모드로 구성하는 방법 및 홈 오피스에서 로컬로 스위칭해야 하는 트래픽과 WLC(Wireless LAN Controller)에서 중앙 집중식으로 전환해야 하는 트래픽을 정의할 수 있도록 스플릿 터널링을 활성화하는 방법에 대해 설명합니다.

기고자: Tiago Antunes, Nicolas Darchis Cisco TAC 엔지니어

사전 요구 사항

요구 사항

이 문서에는 WLC가 NAT(Network Address Translation)가 활성화된 DMZ(Demilitarized Zone)에 이미 구성되어 있고 AP가 홈 오피스에서 WLC에 조인할 수 있다고 가정합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 버전 AireOS 8.10(130.0) 소프트웨어가 포함된 WLC
- Wave1 AP: 1700/2700/3700 .
- Wave2 AP: 1800/2800/3800/4800 및 Catalyst 9100 시리즈입니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 네트워크가 작동 중인 경우 모든 명령의

잠재적인 영향을 이해해야 합니다.

개요

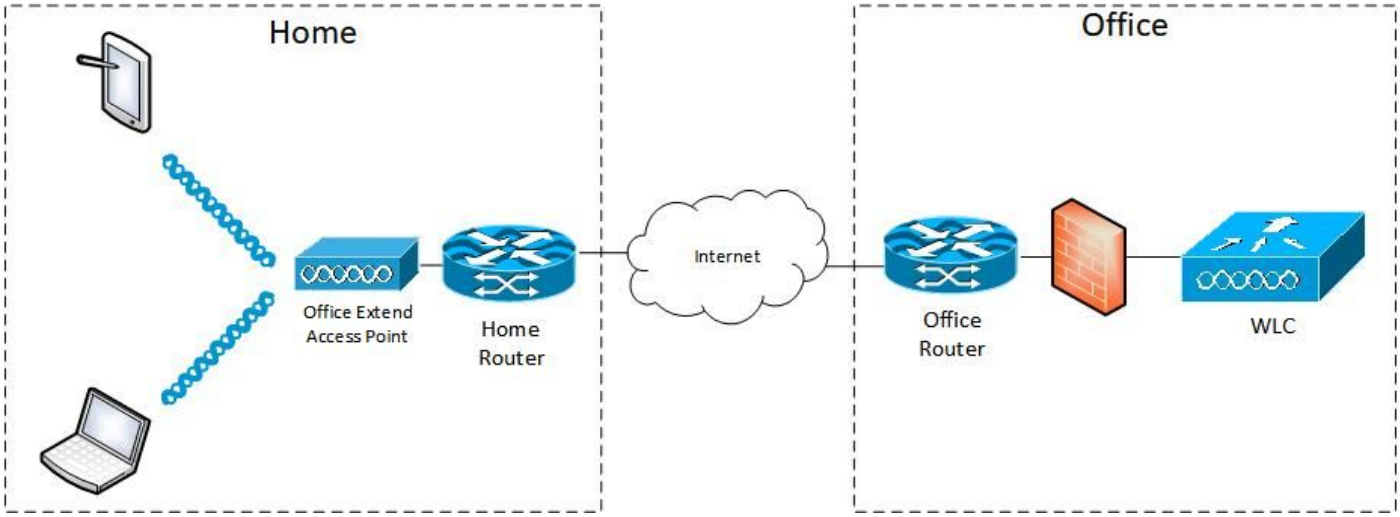
OEAP는 인터넷을 통해 기업 WLAN을 직원 거주지로 확장하기 위해 Cisco WLC에서 원격 위치의 Cisco AP로 안전한 통신을 제공합니다. 홈 오피스에서 사용하는 사용자의 경험은 기업 사무실에서와 정확히 동일합니다. AP와 컨트롤러 간의 DTLS(Datagram Transport Layer Security) 암호화는 모든 통신에서 최고 수준의 보안을 보장합니다. FlexConnect 모드의 모든 실내 AP는 OEAP로 작동할 수 있습니다.

중요한 사실

- Cisco OEAP는 NAT를 사용하는 라우터 또는 기타 게이트웨이 디바이스에서 작동하도록 설계되었습니다. NAT를 사용하면 라우터와 같은 장치가 인터넷(공용)과 개인 네트워크(사설) 사이에서 에이전트 역할을 할 수 있습니다. 이 경우 전체 컴퓨터 그룹을 단일 IP 주소로 나타낼 수 있습니다. NAT 디바이스 뒤에 구축할 수 있는 Cisco OEAP 수에는 제한이 없습니다.
- 통합 안테나를 사용하는 지원되는 모든 실내 AP 모델은 AP-700I, AP-700W 및 AP802 시리즈 AP를 제외하고 OEAP로 구성할 수 있습니다.
- 모든 OEAP는 동일한 AP 그룹에 있어야 하며, 해당 그룹은 15개 이하의 무선 LAN을 포함해야 합니다. AP 그룹에 OEAP가 있는 컨트롤러는 연결된 각 OEAP에 최대 15개의 WLAN만 게시합니다. 개인 SSID(Service Set Identifier)에 대해 하나의 WLAN을 예약하기 때문입니다.

구성

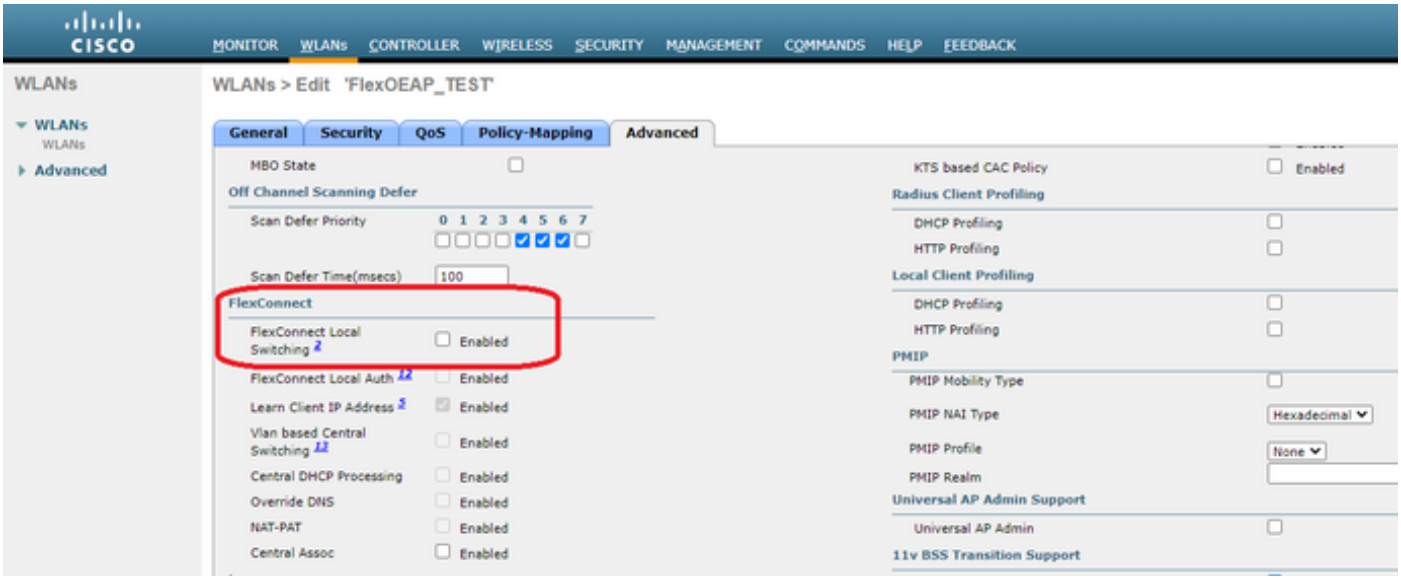
네트워크 다이어그램



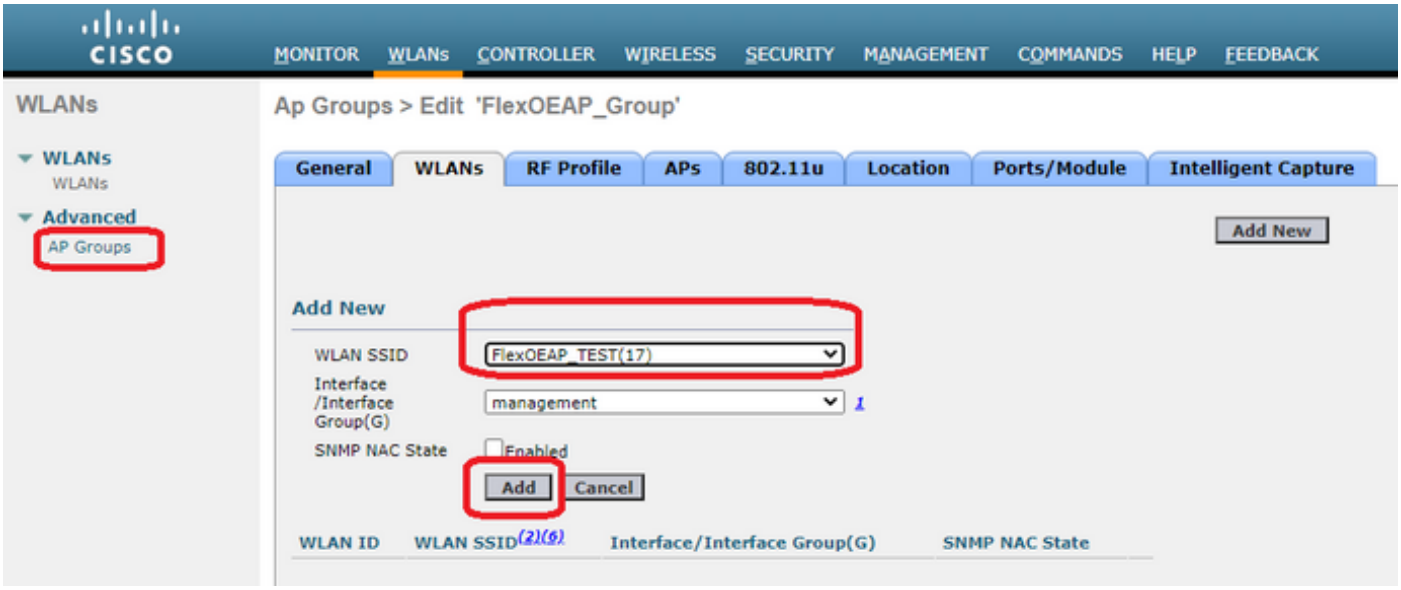
구성

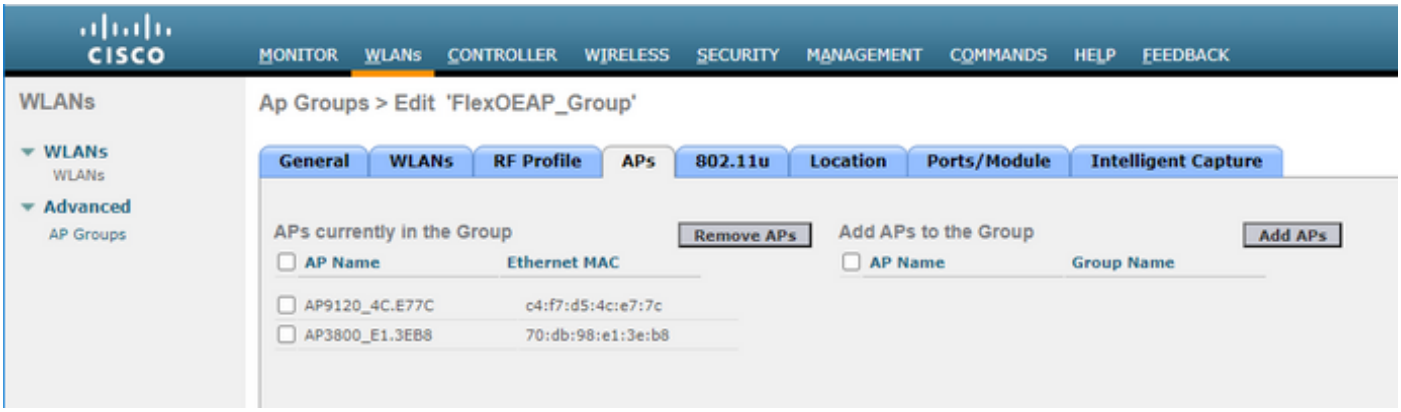
WLAN 컨피그레이션

1단계. AP 그룹에 할당할 WLAN을 생성합니다. 이 WLAN에 대해 FlexConnect Local Switching 옵션을 활성화할 필요가 없습니다.



2단계. AP 그룹을 생성합니다. WLANs(**WLANs**) 탭에서 WLAN SSID를 선택한 다음 Add(**추가**)를 클릭하여 WLAN을 추가합니다. APs(**APs**) 탭**으로** 이동하여 FlexConnect OEAP 추가.

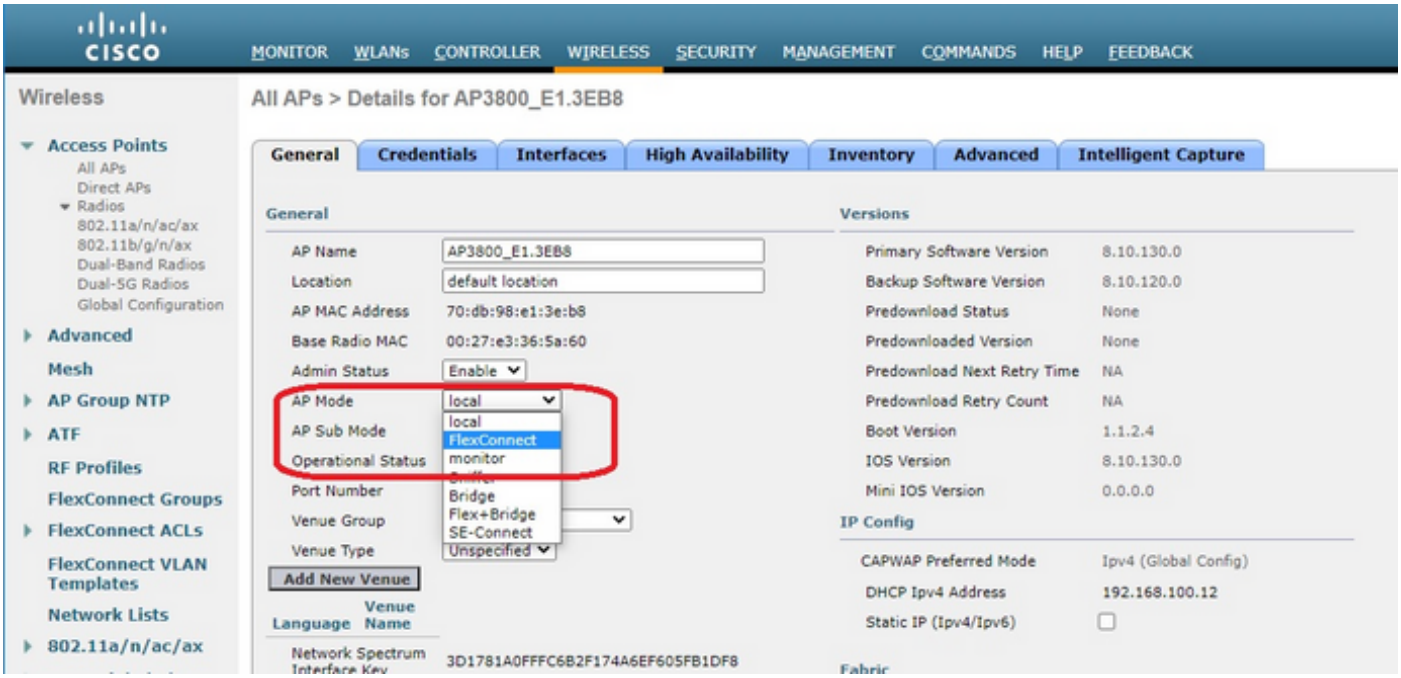




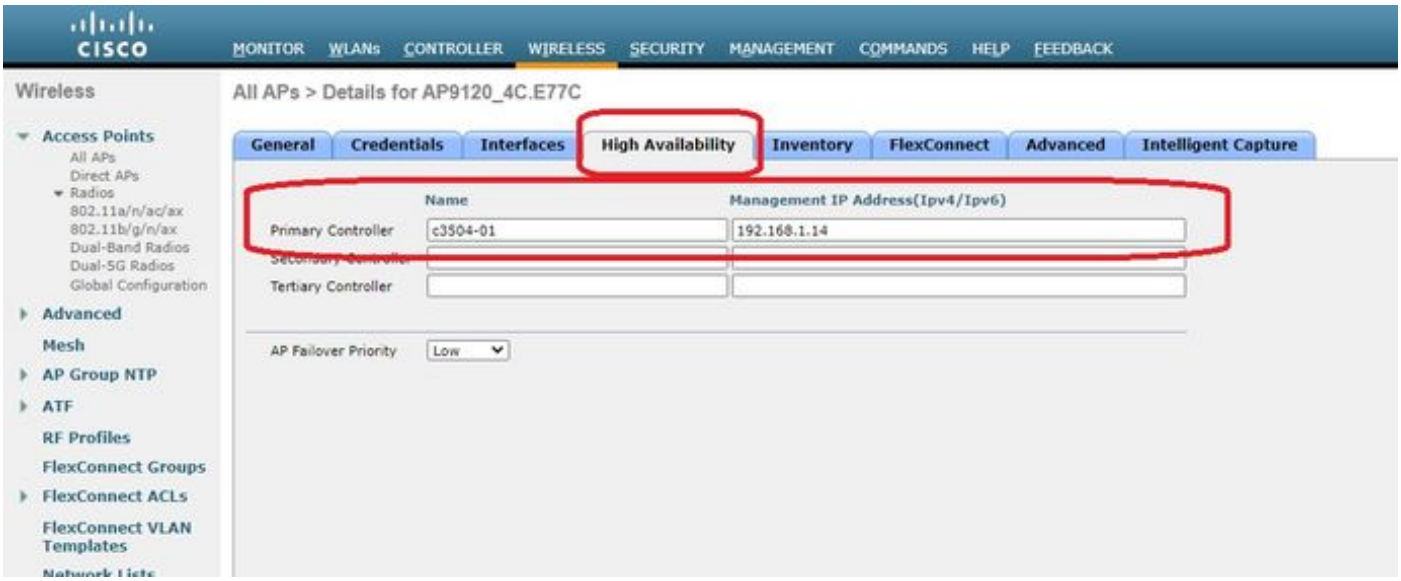
AP 컨피그레이션

AP가 FlexConnect 모드에서 컨트롤러에 연결되면 이를 OEAP로 구성할 수 있습니다.

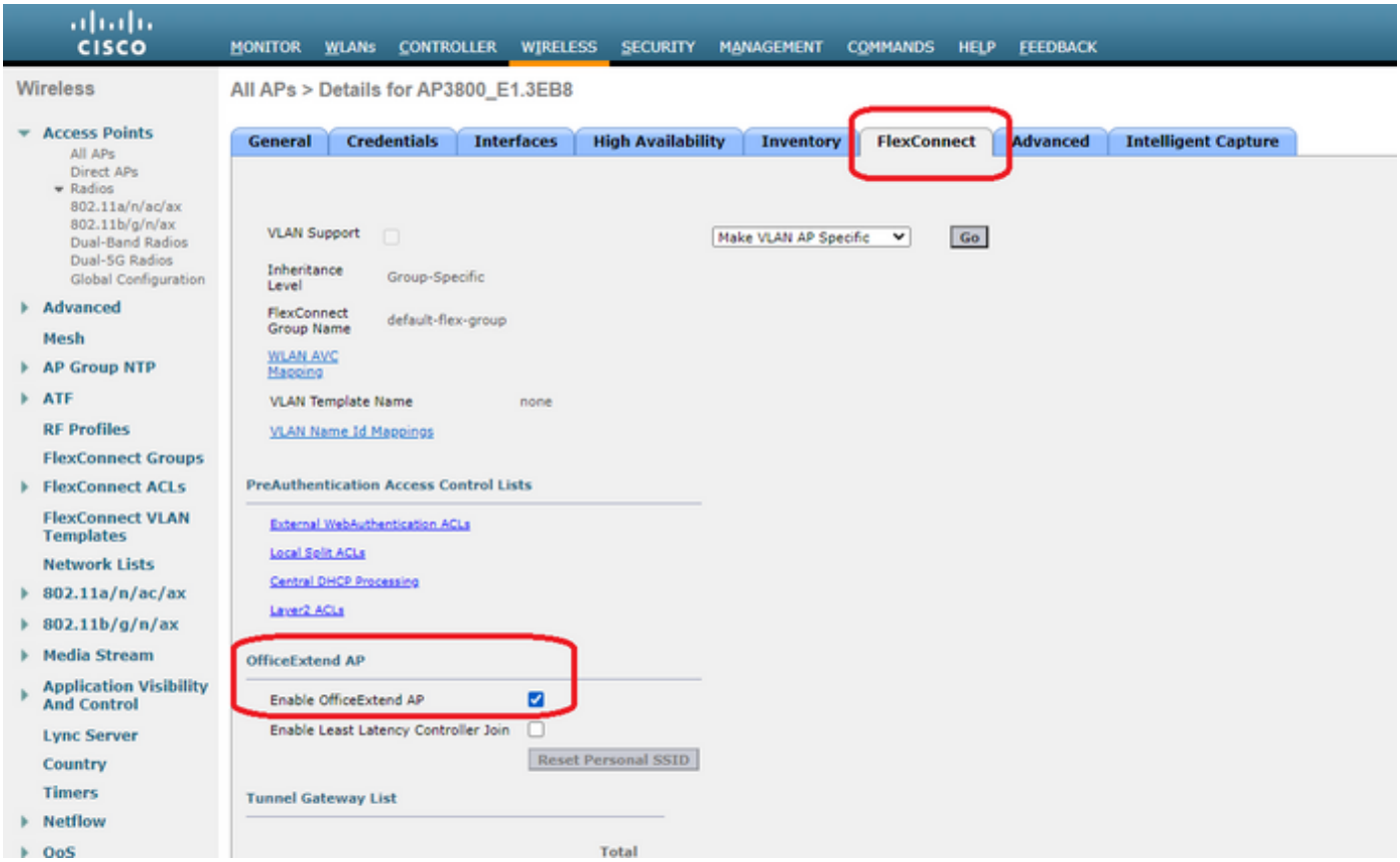
1단계. AP가 WLC에 가입하면 AP 모드를 FlexConnect로 변경하고 Apply(적용)를 **클릭합니다**.



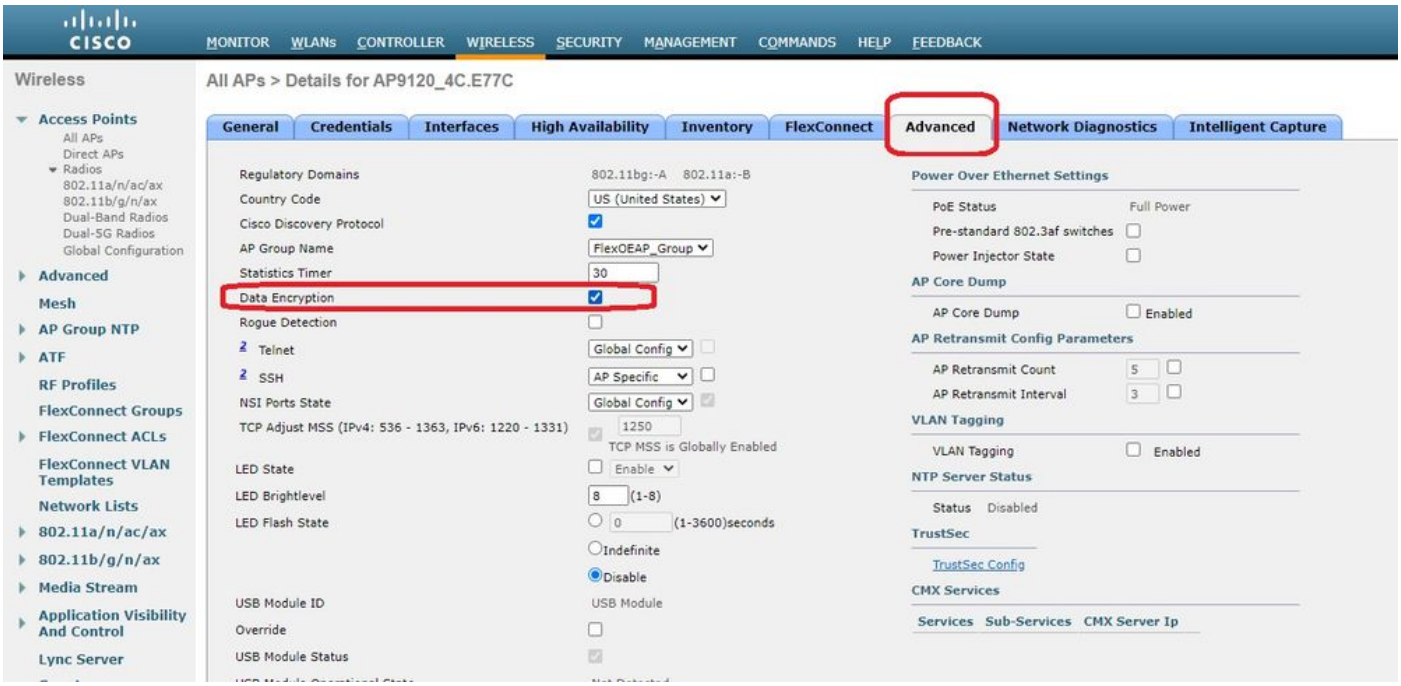
2단계. High Availability(고가용성) 탭에 최소 1차 WLC가 구성되어 있는지 확인합니다.



3단계. FlexConnect 탭으로 이동하여 OfficeExtend **AP 사용** 확인란을 선택합니다.



AP**에** 대해 OfficeExtend 모드를 활성화하면 DTLS 데이터 암호화가 자동으로 활성화됩니다. 그러나 특정 AP에 대해 DTLS 데이터 암호화를 활성화하거나 비활성화할 수 있습니다. 이렇게 하려면 [선택한 AP]에 대한 [세부 정보] > [고급] 탭의 [모든 AP] > [**데이터 암호화**] 확인란을 선택(활성화) 또는 선택 취소(비활성화)(비활성화)합니다.



참고: AP에 대해 OfficeExtend 모드를 활성화하면 텔넷 및 SSH 액세스가 자동으로 비활성화됩니다. 그러나 특정 AP에 대해 텔넷 또는 SSH 액세스를 활성화 또는 비활성화할 수 있습니다. 이렇게 하려면 [선택한 AP] > [고급] 탭의 [모든 AP] > [세부 정보]에서 텔넷 또는 SSH 확인란을 선택(활성화)하거나 선택 취소(비활성화)합니다.

참고: AP에 대해 OfficeExtend 모드를 활성화하면 링크 레이턴시가 자동으로 활성화됩니다. 그러나 특정 AP에 대해 링크 레이턴시를 활성화하거나 비활성화할 수 있습니다. 이렇게 하려면 All APs(모든 AP) > Details for [selected AP](선택한 AP] > Advanced(고급) 탭에서 Enable Link Latency(링크 레이턴시 활성화) 확인란을 선택(활성화) 또는 선택 취소(비활성화)합니다.

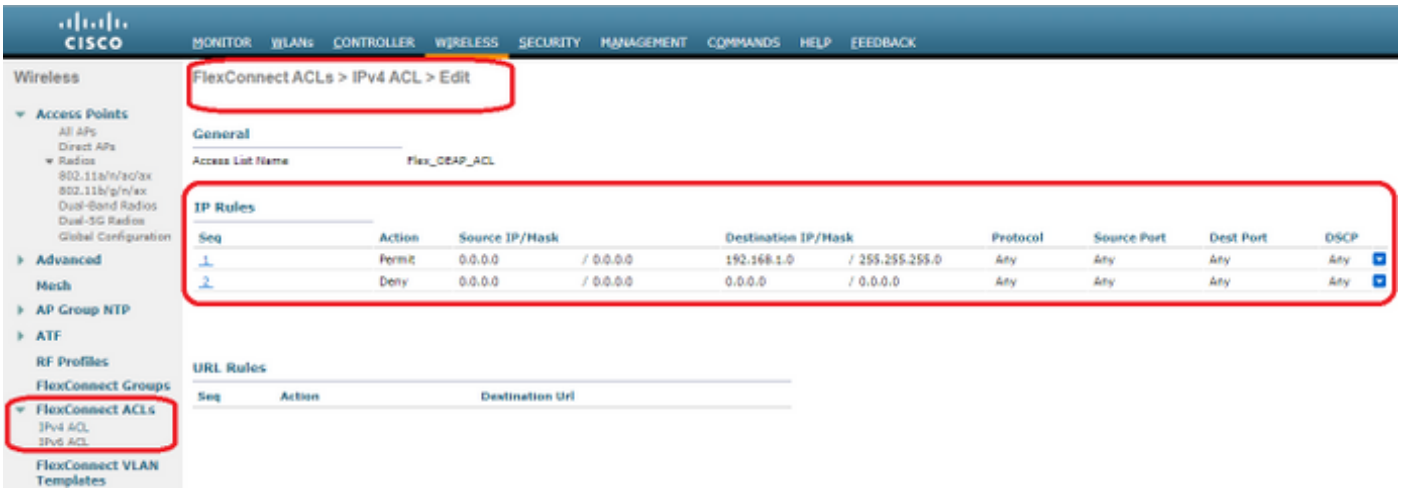
3단계. 적용을 **선택합니다**. Apply(적용)를 선택하면 AP가 다시 로드됩니다.

4단계. AP가 WLC에 다시 연결되면 AP는 OEAP 모드에 있습니다.

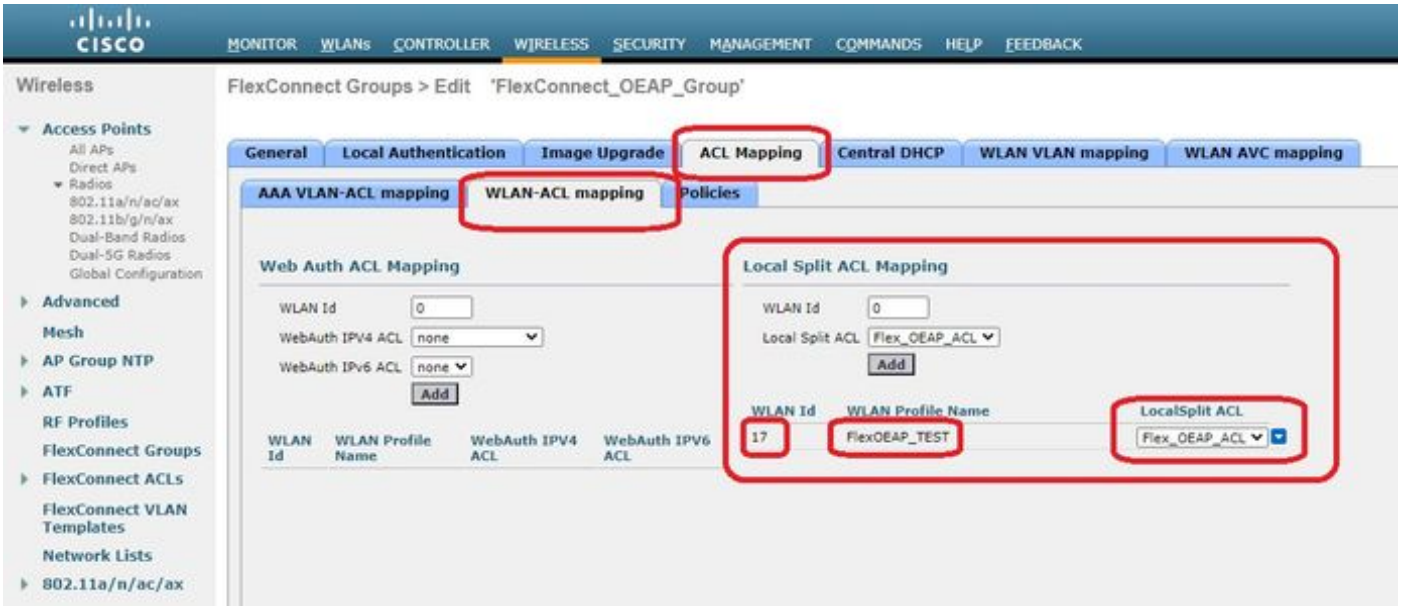
참고: 인증된 AP만 WLC에 참여할 수 있도록 AP 가입 보안(일반적으로 AP Policies에 정의됨)을 구성하는 것이 좋습니다. LSC(Locally Significant Certificate) AP 프로비저닝을 사용할 수도 있습니다.

5단계. FlexConnect ACL(Access Control List)을 생성하여 중앙에서(거부) 및 로컬로(허용)로 전환할 트래픽을 정의합니다.

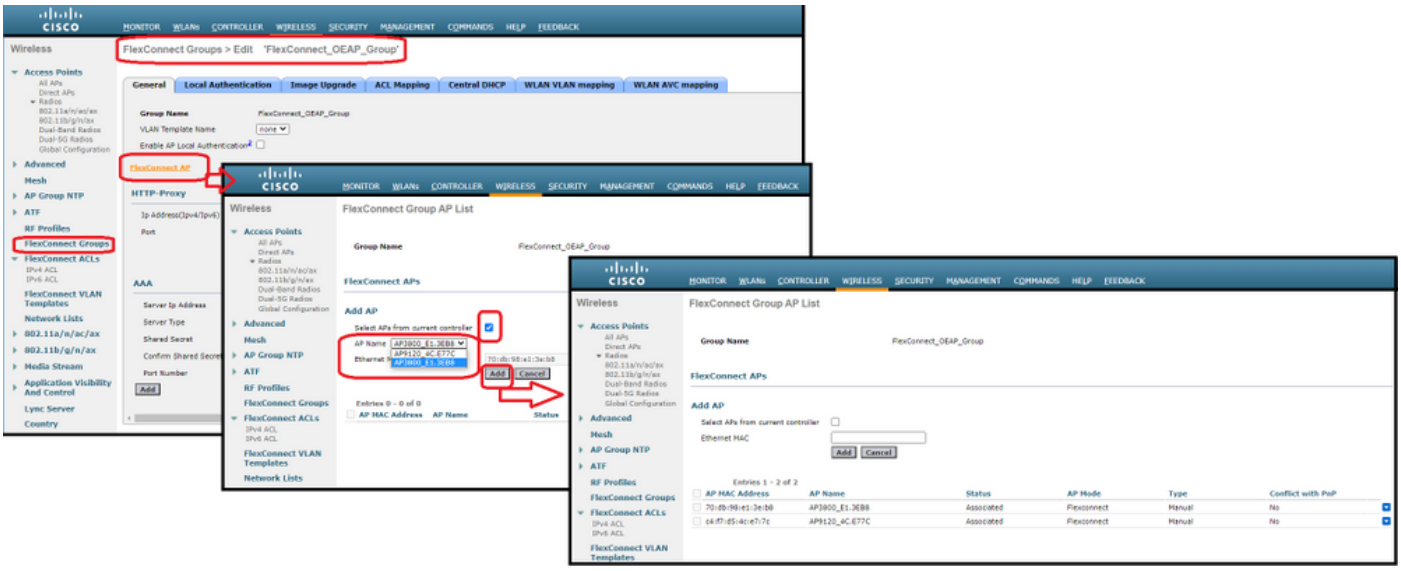
여기에서는 모든 트래픽을 서브넷 192.168.1.0/24으로 로컬로 스위칭하는 것을 목표로 합니다.



6단계. FlexConnect 그룹을 생성하고 **ACL 매핑**으로 이동한 다음 **WLAN-ACL 매핑으로 이동합니다**. "Local Split ACL Mapping(로컬 스플릿 ACL 매핑)"에서 WLAN ID를 입력하고 FlexConnect ACL을 선택합니다. 그런 다음 **Add를** 클릭합니다.



7단계. FlexConnect 그룹에 AP를 추가합니다.



다음을 확인합니다.

1. FlexConnect ACL 상태 및 정의를 확인합니다.

```
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. FlexConnect 로컬 스위칭이 비활성화되었는지 확인합니다.

```
(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. FlexConnect 그룹 구성을 확인합니다.

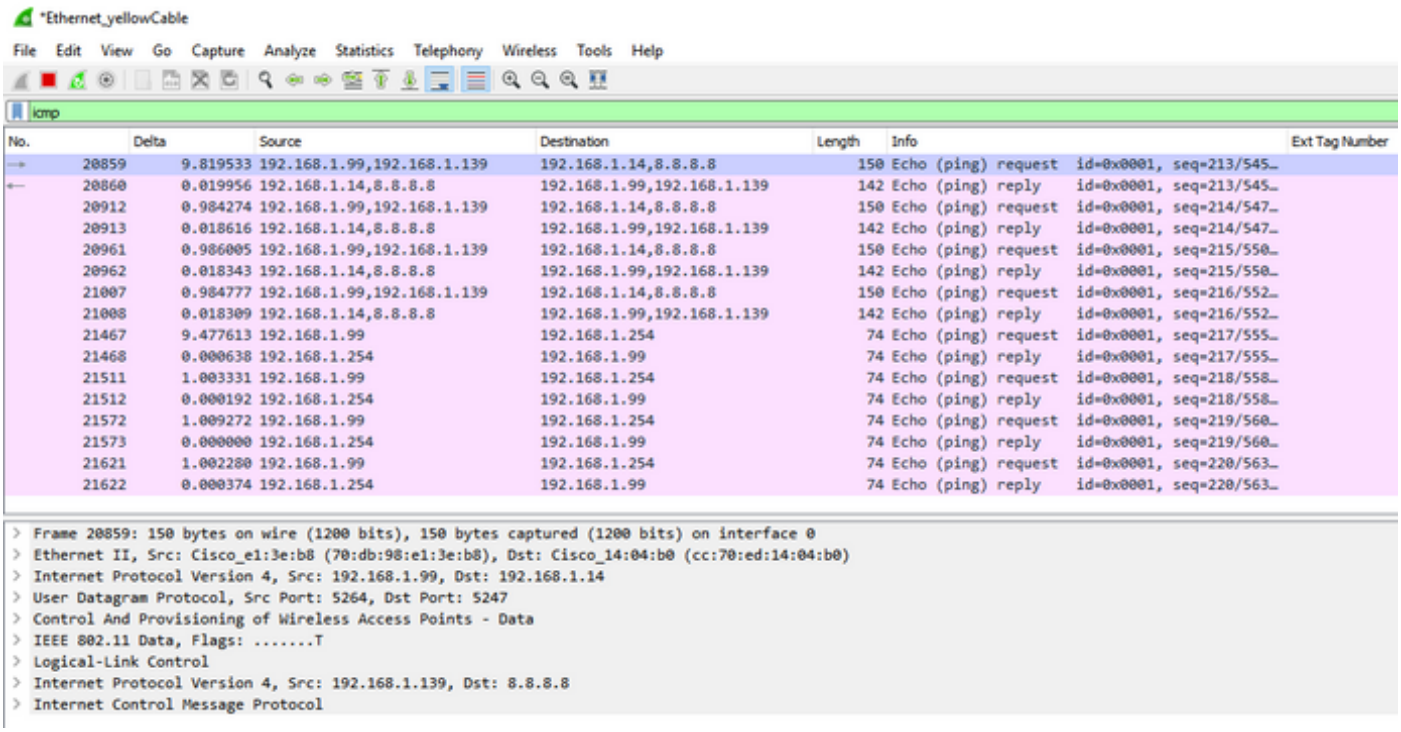
```
(c3504-01) >show flexconnect group summary

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................ 436973636f00000000000000000000
```

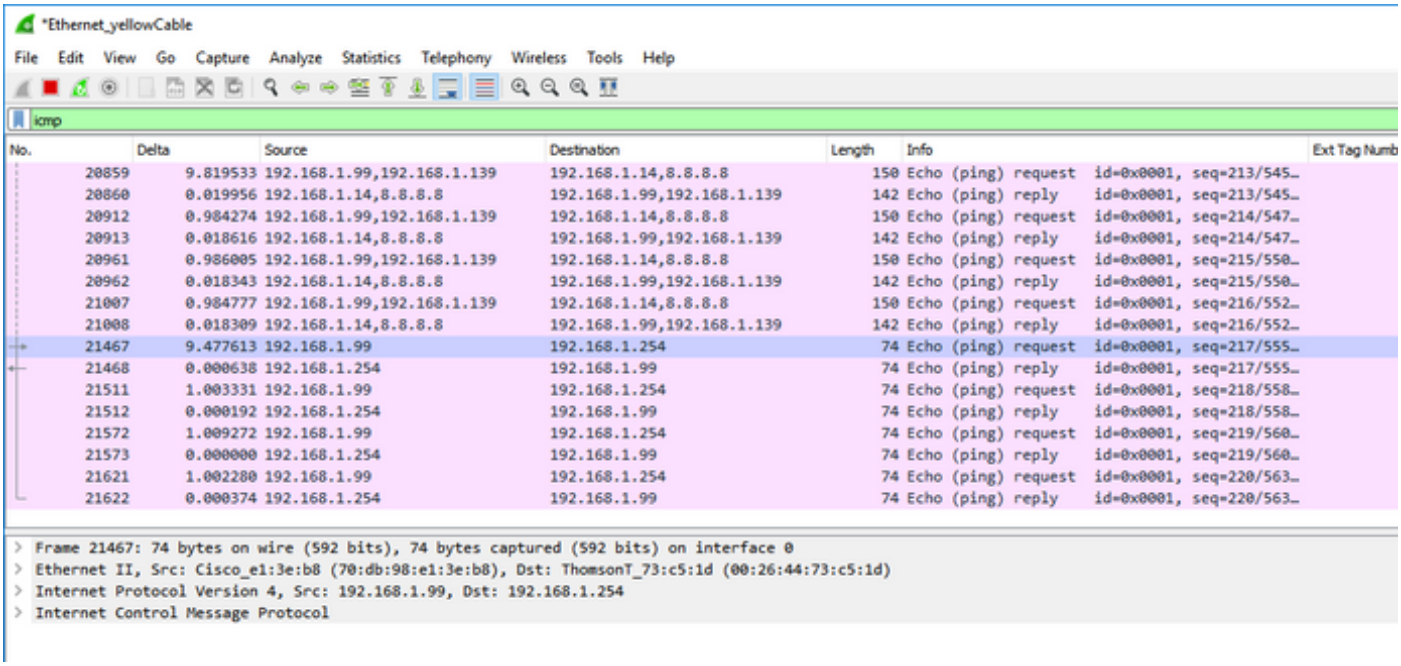
```
Authority Info.............. Cisco A_ID
PAC Timeout................. 0
HTTP-Proxy Ip Address.......
HTTP-Proxy Port............. 0
Multicast on Overridden interface config: Disabled
DHCP Broadcast Overridden interface config: Disabled
Number of User's in Group: 0
FlexConnect Vlan-name to Id Template 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
```

AP 인터페이스에서 트래픽을 캡처하여 트래픽이 AP에서 분할되었는지 확인할 수 있습니다.

> **팁**: 문제 해결을 위해 DTLS 암호화를 비활성화하면 CAPWAP 내에서 캡슐화된 데이터 트래픽을 볼 수 있습니다.

이 패킷 캡처 예에서는 WLC로 전달되는 ACL "deny" 문과 일치하는 데이터 트래픽과 AP에서 로컬로 전환된 ACL "permit" 문과 일치하는 데이터 트래픽을 보여줍니다.



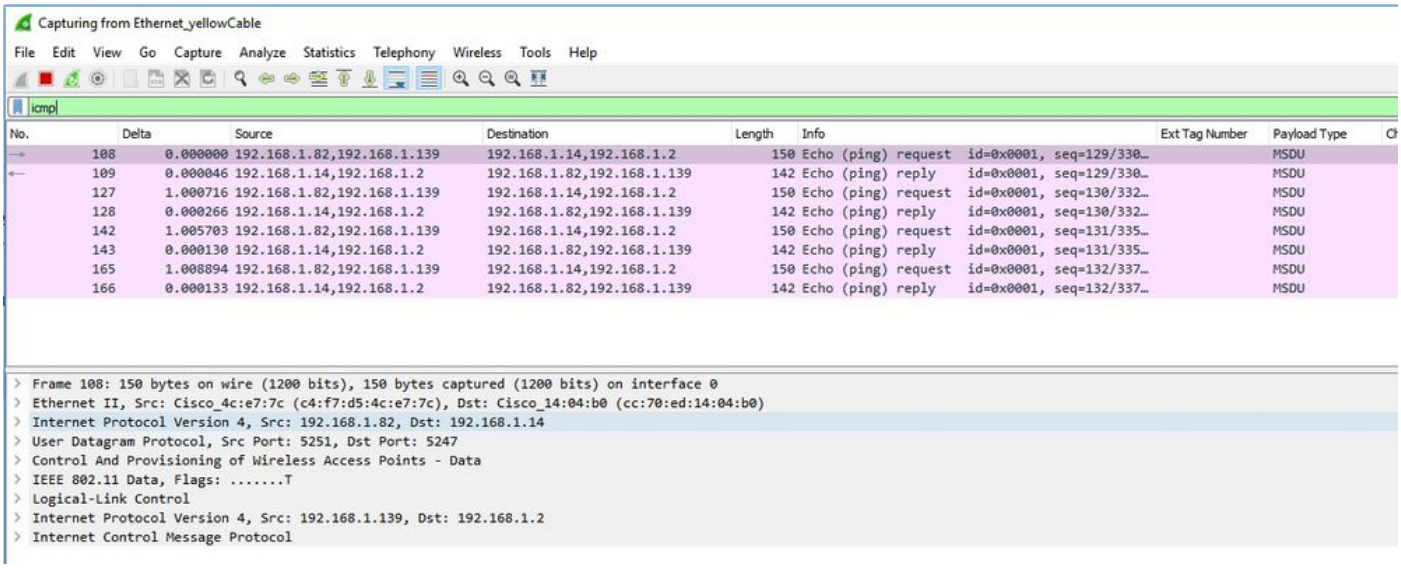


참고: 일반적인 시나리오에서 AP는 클라이언트 서브넷이 사무실 네트워크에 속하고, 홈 오피스의 로컬 디바이스는 클라이언트 서브넷에 도달하는 방법을 모르기 때문에 로컬로 스위칭된 트래픽의 네트워크 주소를 변환합니다. AP는 로컬 홈 오피스 서브넷에 정의된 IP 주소를 사용하여 클라이언트 트래픽을 변환합니다.

AP가 NAT를 수행했는지 확인하기 위해 AP 터미널에 연결하고 "***show ip nat translations***" 명령을 실행할 수 있습니다. 예:

```
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
```

스플릿 터널링을 제거하면 WLC에서 모든 트래픽이 중앙에서 전환됩니다. 다음 예에서는 capwap 터널 내부의 192.168.1.2 대상에 대한 ICMP(Internet Control Message Protocol)를 보여 줍니다.


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