Configure FlexConnect OEAP with Split Tunnelling

Contents

Introduction

This document describes how to configure an indoor Access Point (AP) as a FlexConnect Office Extend AP (OEAP) mode and how to enable split tunneling so that you can define what traffic must be switched locally at the home office and what traffic must be switched centrally at the Wireless LAN Controller (WLC).

Contributed by Tiago Antunes, Nicolas Darchis Cisco TAC Engineers.

Prerequisites

Requirements

There configuration on this document assumes that the WLC is already configured in a Demilitarized Zone (DMZ) with Network Address Translation (NAT) enabled and that the AP is able to join the WLC from the home office.

Components Used

The information in this document is based on these software and hardware versions:

- WLCs with version AireOS 8.10(130.0) Software.
- Wave1 APs: 1700/2700/3700.
- Wave2 APs: 1800/2800/3800/4800, and Catalyst 9100 series.

The information in this document was created from the devices in a specific lab environment.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

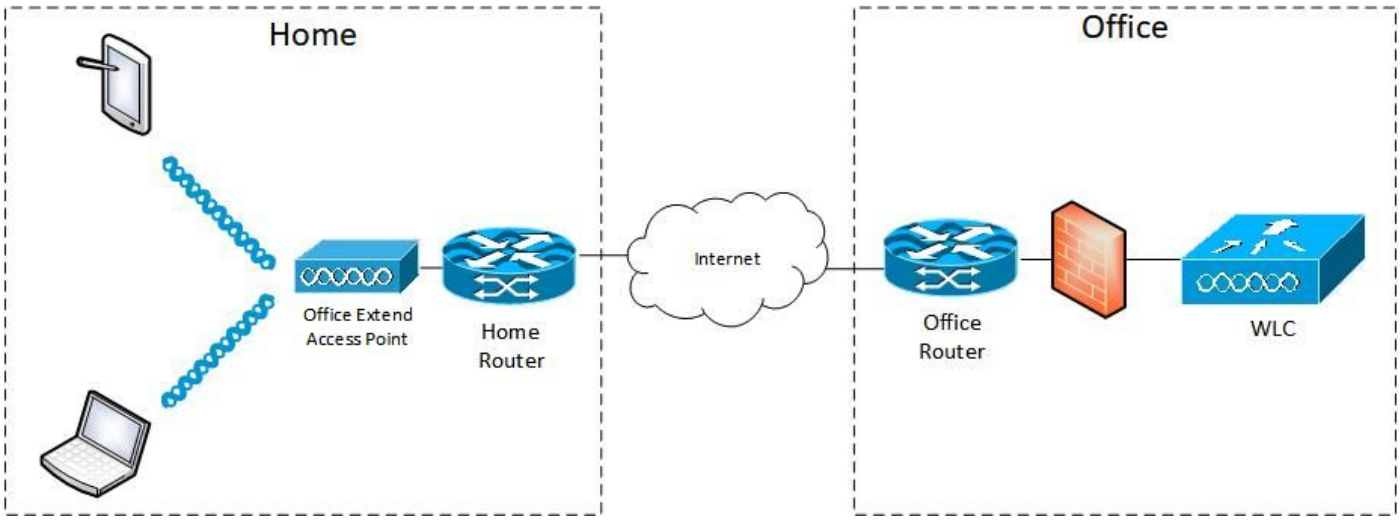
An OEAP provides secure communications from a Cisco WLC to a Cisco AP at a remote location, in order to extend the corporate WLAN over the Internet to an employee's residence. The user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the AP and the controller ensures that all communications have the highest level of security. Any indoor AP in FlexConnect mode can act as an OEAP.

Important Facts

- Cisco OEAPs are designed to work behind a router or other gateway device that uses NAT. NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), which enables an entire group of computers to be represented by a single IP address. There is no limit to the number of Cisco OEAPs that you can deploy behind a NAT device.
- All the supported indoor AP models with integrated antenna can be configured as an OEAP except the AP-700I, AP-700W, and AP802 series APs.
- All OEAPs must be in the same AP group, and that group must contain no more than 15 Wireless LANs. A controller with OEAPs in an AP group publishes only up to 15 WLANs to each connected OEAP because it reserves one WLAN for the personal Service Set Identifier (SSID).

Configure

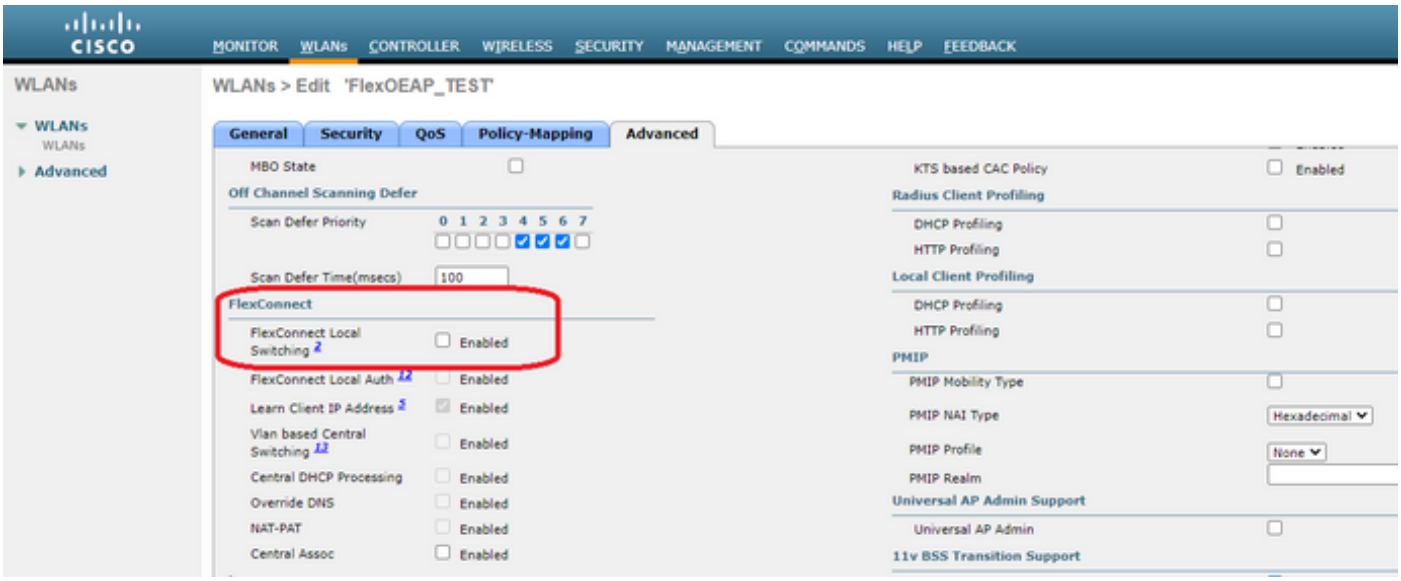
Network Diagram



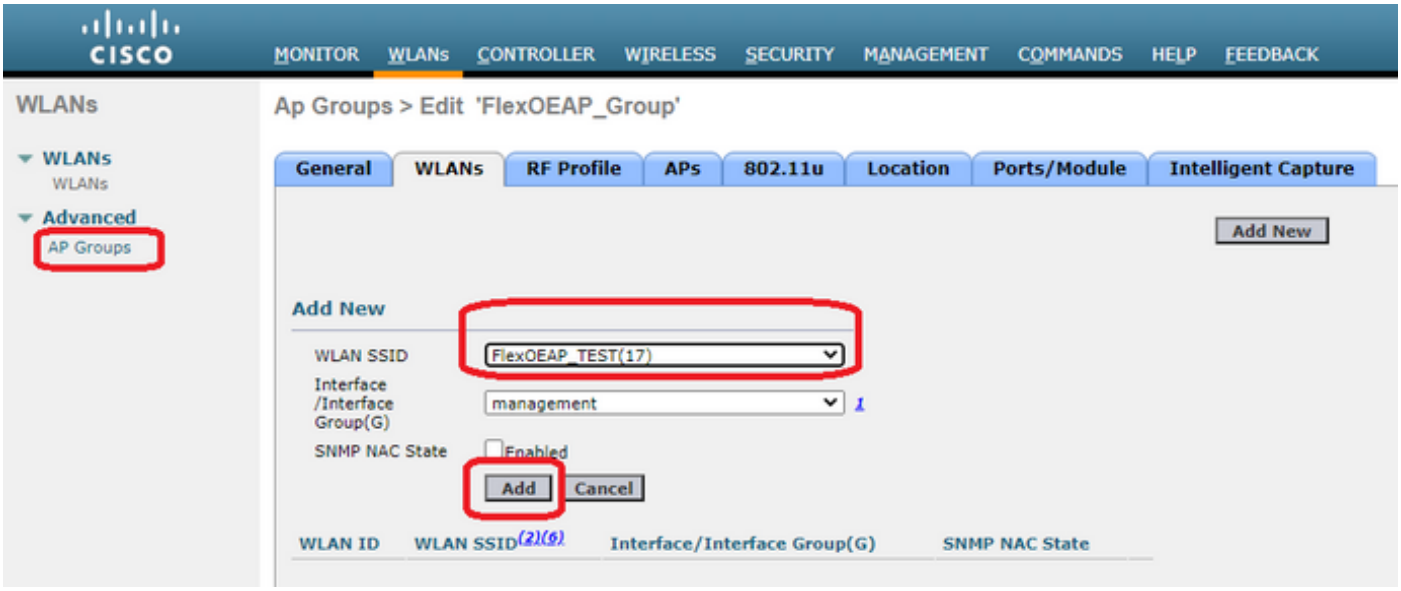
Configurations

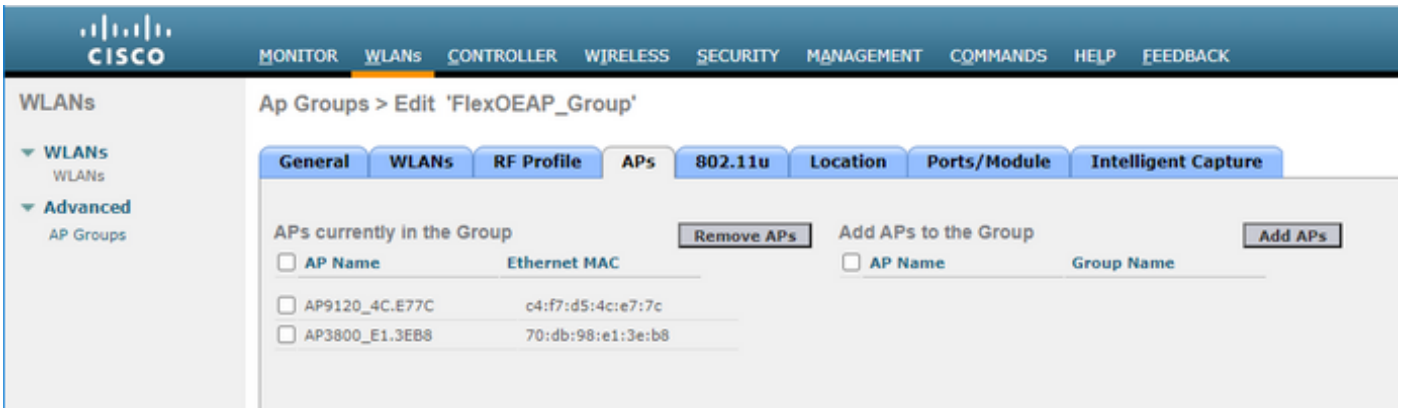
WLAN configuration

Step 1. Create a WLAN to assign to the AP Group. You do not need to enable the FlexConnect Local Switching option for this WLAN.



Step 2. Create an AP group. On the **WLANs** tab, choose the WLAN SSID and then click **Add** to add the WLAN. Go to the **APs** tab and **Add** the FlexConnect OEAP.



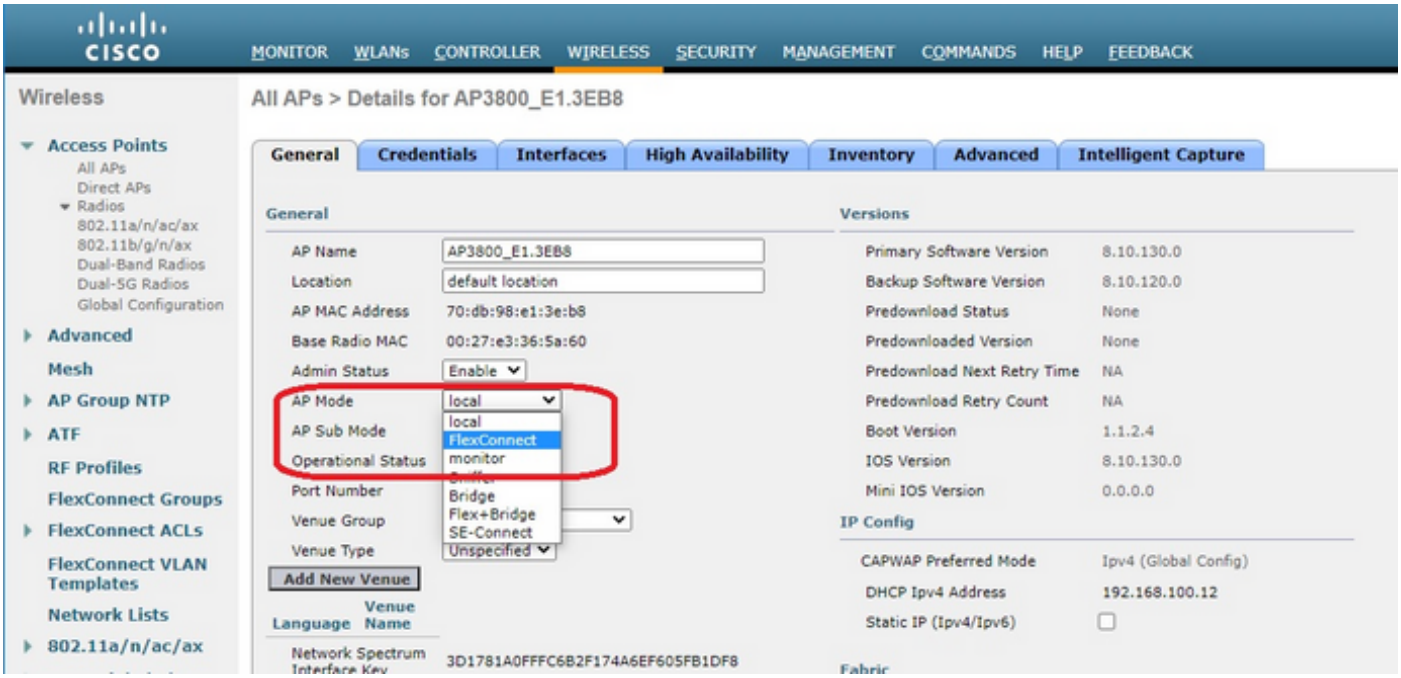


AP Configuration

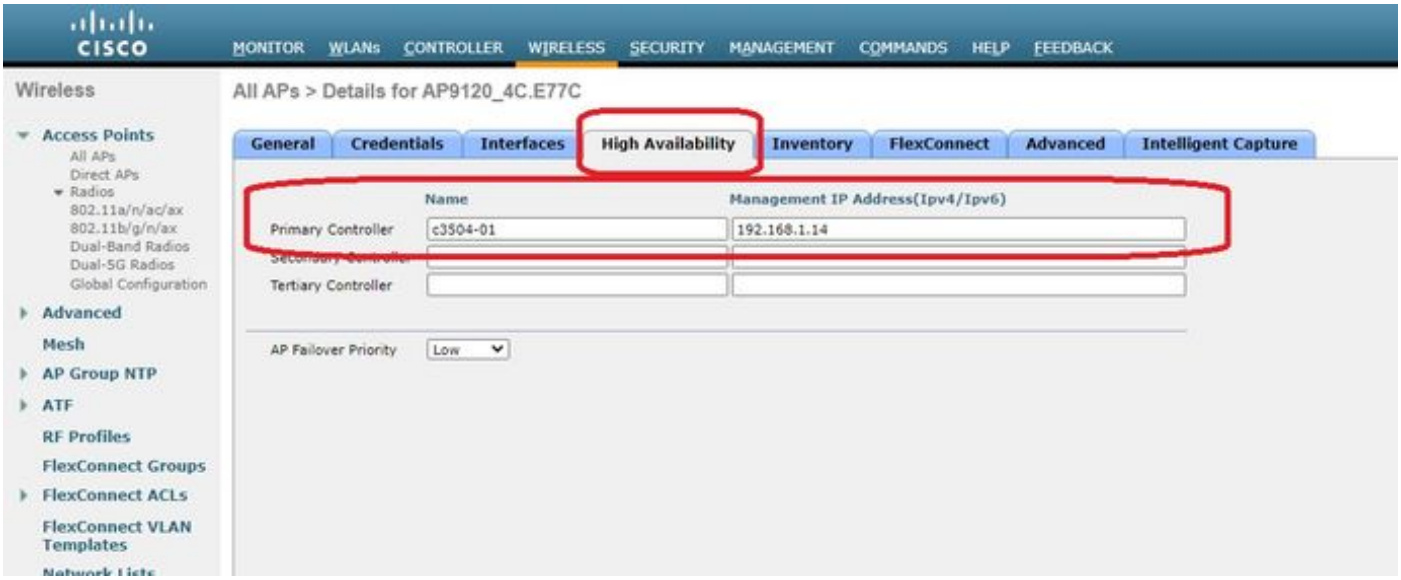
After the AP has associated with the controller in FlexConnect mode, you can configure it as an

OEAP.

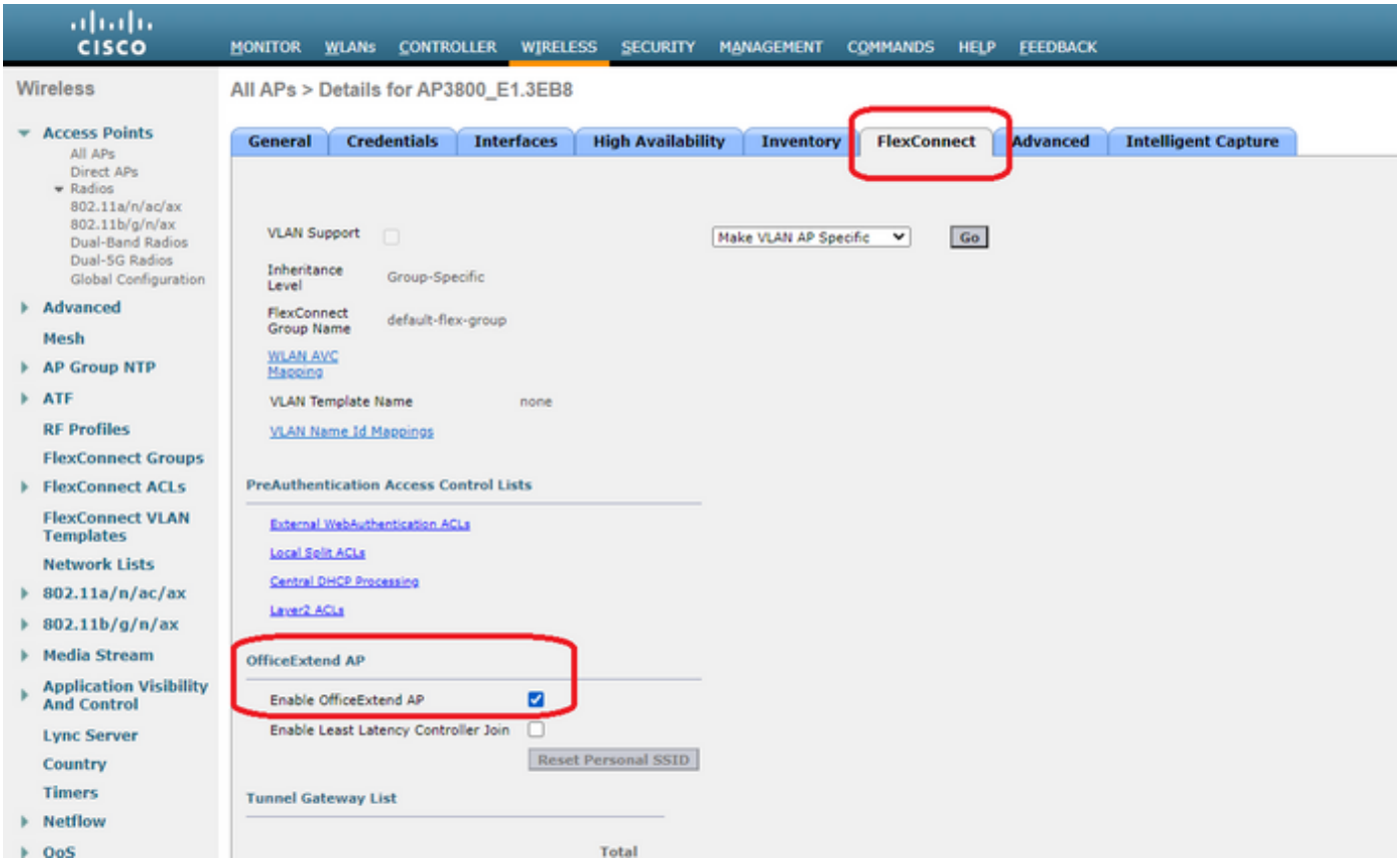
Step 1. After the AP joins the WLC, change the AP mode to **FlexConnect** and click **Apply**.



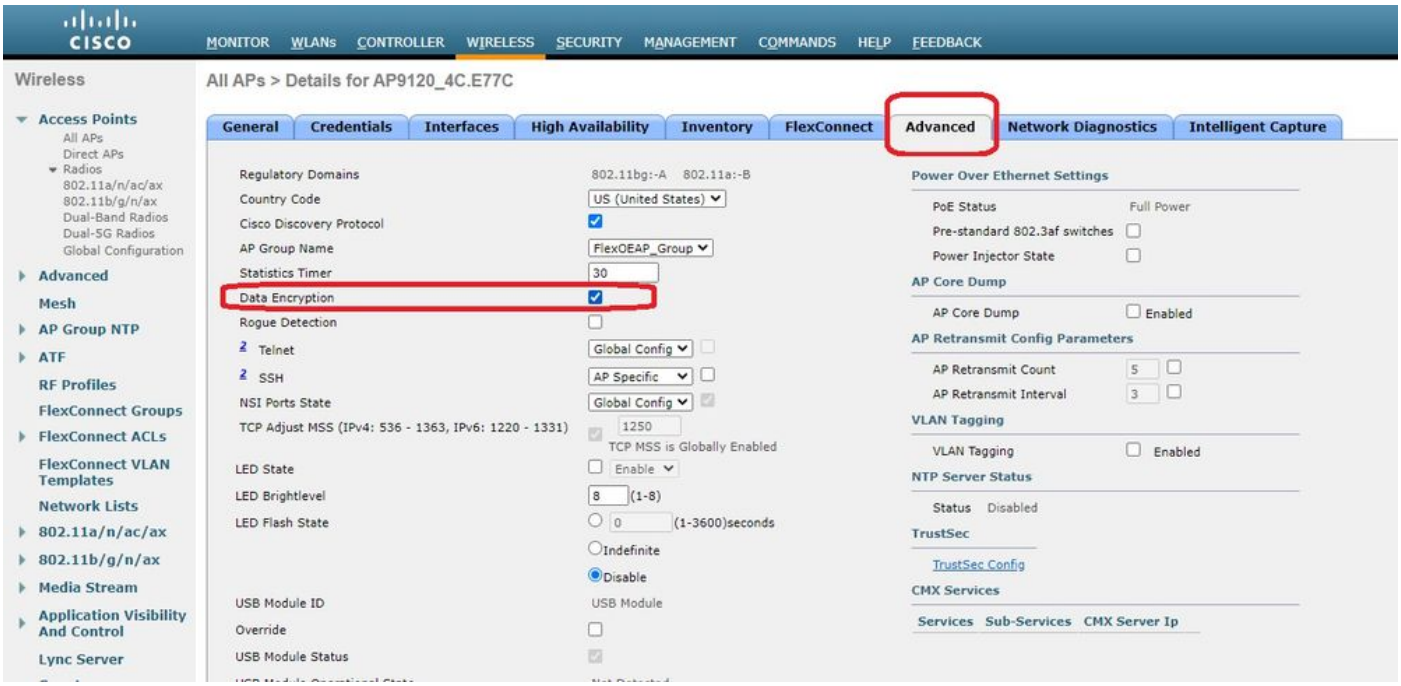
Step 2. Make sure you have at least a Primary WLC configured in the High Availability tab:



Step 3. Go to the FlexConnect tab and check the **Enable OfficeExtend AP** check box.



DTLS **Data Encryption** is enabled automatically when you enable the OfficeExtend mode for an AP. However, you can enable or disable DTLS data encryption for a specific AP. To do so, check (enable) or uncheck (disable) the **Data Encryption** check box on the All APs > Details for [selected AP] > Advanced tab:



Note: Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an AP. However, you can enable or disable Telnet or SSH access for a specific AP. To do so, check (enable) or uncheck (disable) the Telnet or SSH check box on the All APs > Details for [selected AP] > Advanced tab.

Note: Link latency is enabled automatically when you enable the OfficeExtend mode for an AP. However, you can enable or disable link latency for a specific AP. To do so, check (enable) or uncheck (disable) the Enable Link Latency check box on the All APs > Details for [selected AP] > Advanced tab.

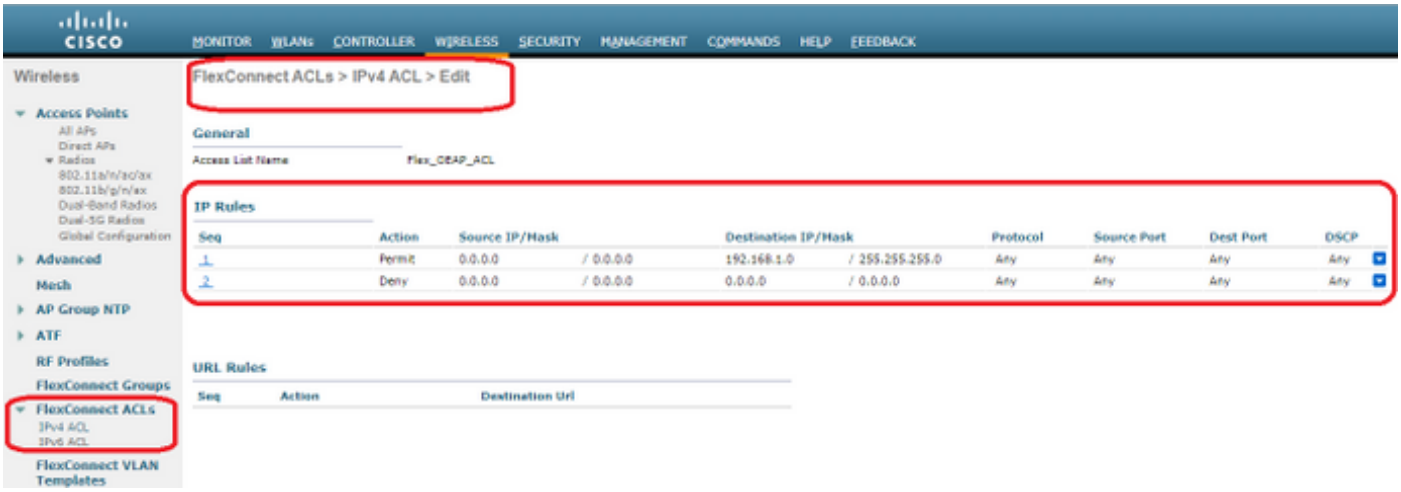
Step 3. Select **Apply**. After you select Apply, the AP reloads.

Step 4. After the AP rejoins the WLC, the AP is in OEAP mode.

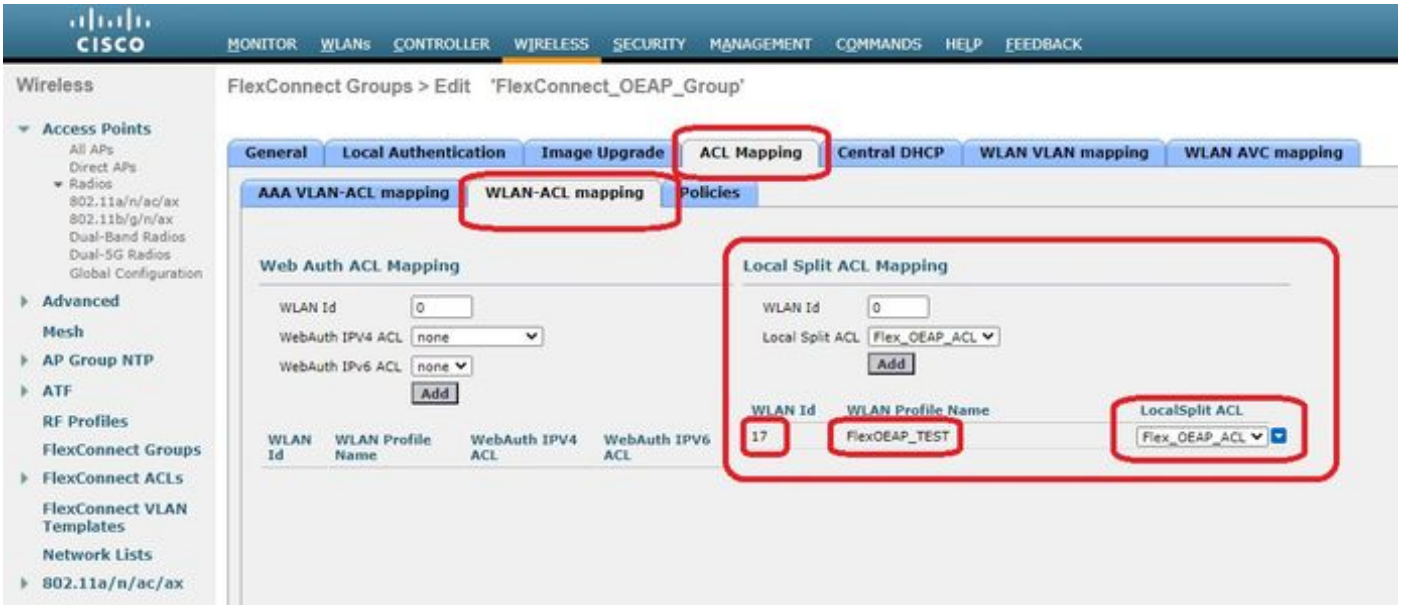
Note: We recommend that you configure AP join security (commonly defined under AP Policies) so that only authorized APs can join the WLC. You can also use Locally Significant Certificate (LSC) AP provisioning.

Step 5. Create a FlexConnect Access Control List (ACL) to define which traffic will be switched centrally (Deny) and locally (Permit).

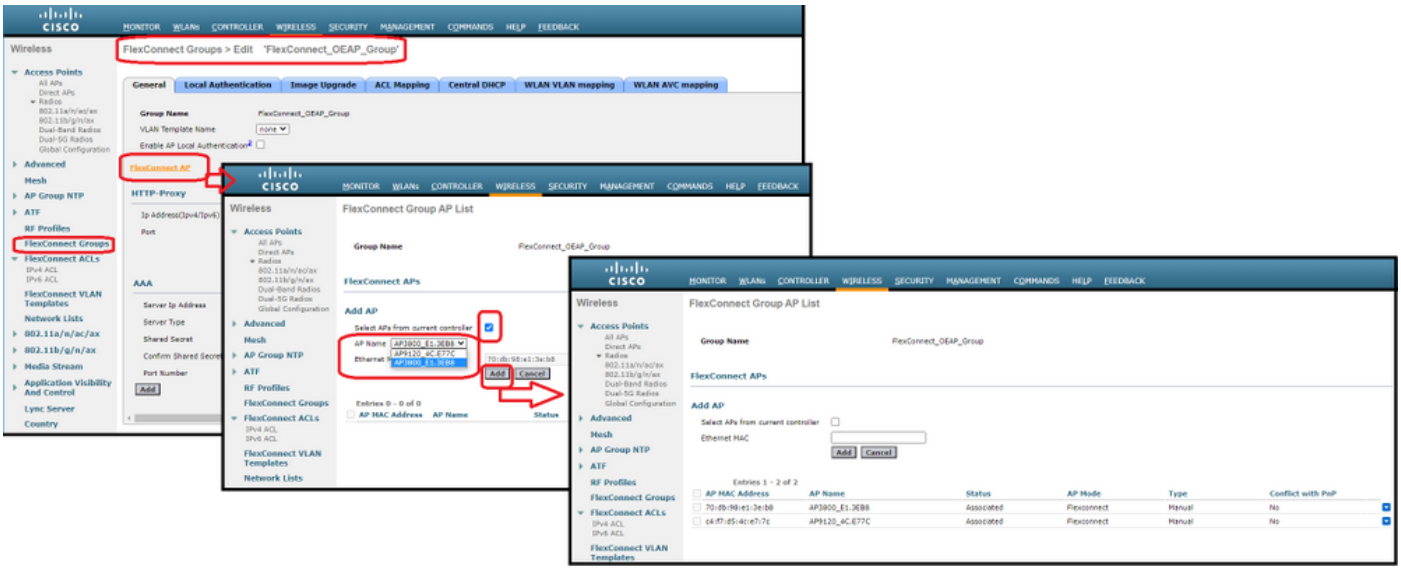
Here, you have the goal of switching locally all traffic to the subnet 192.168.1.0/24.



Step 6. Create a FlexConnect Group, go to **ACL Mapping**, and then go to **WLAN-ACL Mapping**. Under "Local Split ACL Mapping," enter the WLAN ID and choose the FlexConnect ACL. Then click **Add.**



Step 7. **Add** the AP to the FlexConnect group:



Verify

1. Verify the FlexConnect ACL status and definition:

```
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. Verify that FlexConnect local switching is disabled:

```
(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. Verify the FlexConnect Group configuration:

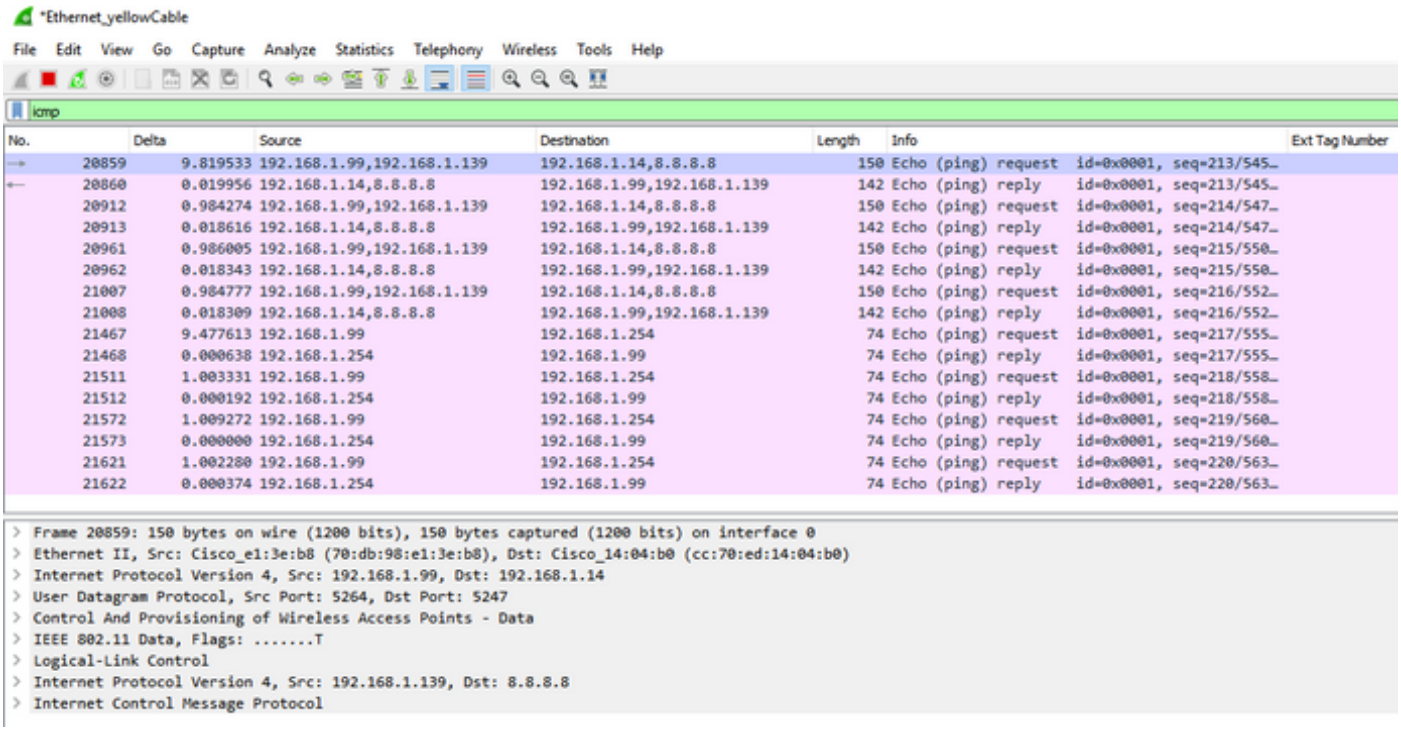
```
(c3504-01) >show flexconnect group summary

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
```

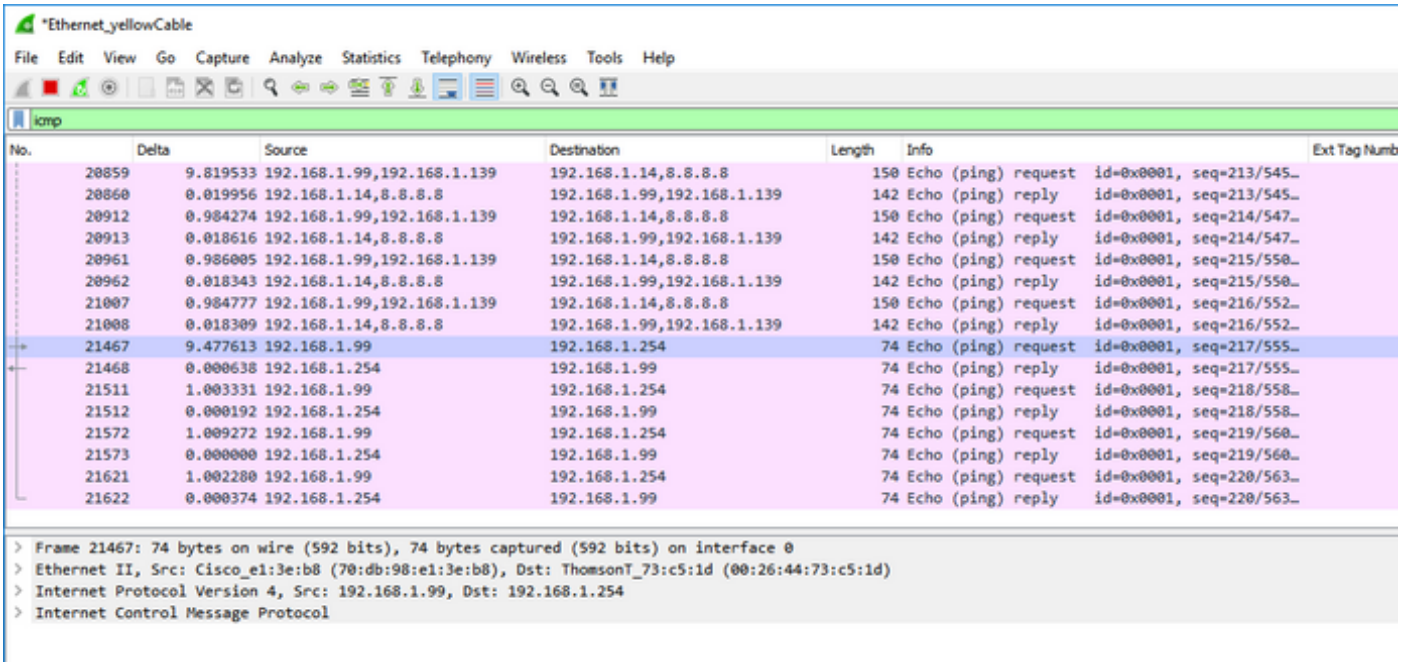
```
Authority Info.............. Cisco A_ID
PAC Timeout................. 0
HTTP-Proxy Ip Address.......
HTTP-Proxy Port............. 0
Multicast on Overridden interface config: Disabled
DHCP Broadcast Overridden interface config: Disabled
Number of User's in Group: 0
FlexConnect Vlan-name to Id Template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

You can capture the traffic at the AP interface in order to verify that the traffic is split at the AP.

> **Tip**: For troubleshooting purposes, you can disable DTLS encryption in order to see the data traffic encapsulated inside capwap.

This packet capture example shows data traffic that matches the ACL "deny" statements directed to the WLC, and data traffic that matches the ACL "permit" statements switched locally at the AP:



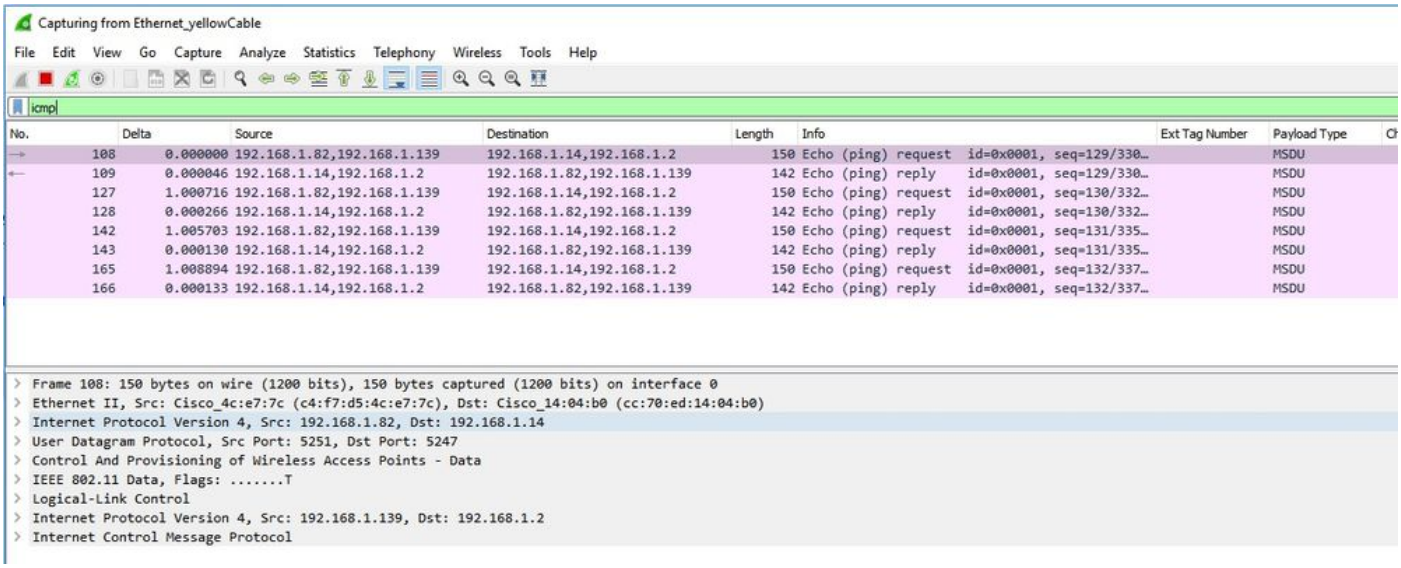


> **Note**: In normal scenarios, the AP translates network addresses for locally switched traffic because the client subnet belongs to the office network, and local devices at the home office do not know how to reach the client subnet. The AP uses the IP address that is defined in the local home office subnet to translate the client traffic.

In order to verify that the AP performed the NAT, you can connect to the AP terminal and issue the "***show ip nat translations***" command. Example:

```
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
```

If you remove split tunneling, then all traffic is switched centrally at the WLC. This example shows the Internet Control Message Protocol (ICMP) to the 192.168.1.2 destination, inside the capwap tunnel:


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