

Configuración de FlexConnect OEAP con tunelización dividida

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Overview](#)

[Hechos importantes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[configuración WLAN](#)

[Configuración de AP](#)

[Verificación](#)

Introducción

Este documento describe cómo configurar un punto de acceso interior (AP) como modo de punto de acceso de extensión de oficina (OEAP) de FlexConnect y cómo habilitar la tunelización dividida para que pueda definir qué tráfico debe conmutarse localmente en la oficina doméstica y qué tráfico debe conmutarse centralmente en el controlador de LAN inalámbrica (WLC).

Colaborado por Tiago Antunes, Nicolas Darchis Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Hay configuración en este documento que asume que el WLC ya está configurado en una zona desmilitarizada (DMZ) con traducción de direcciones de red (NAT) habilitada y que el AP puede unirse al WLC desde la oficina principal.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- WLC con la versión AireOS 8.10(130.0) Software.
- AP Wave1: 1700/2700/3700.
- AP Wave2: 1800/2800/3800/4800 y Catalyst serie 9100.

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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Overview

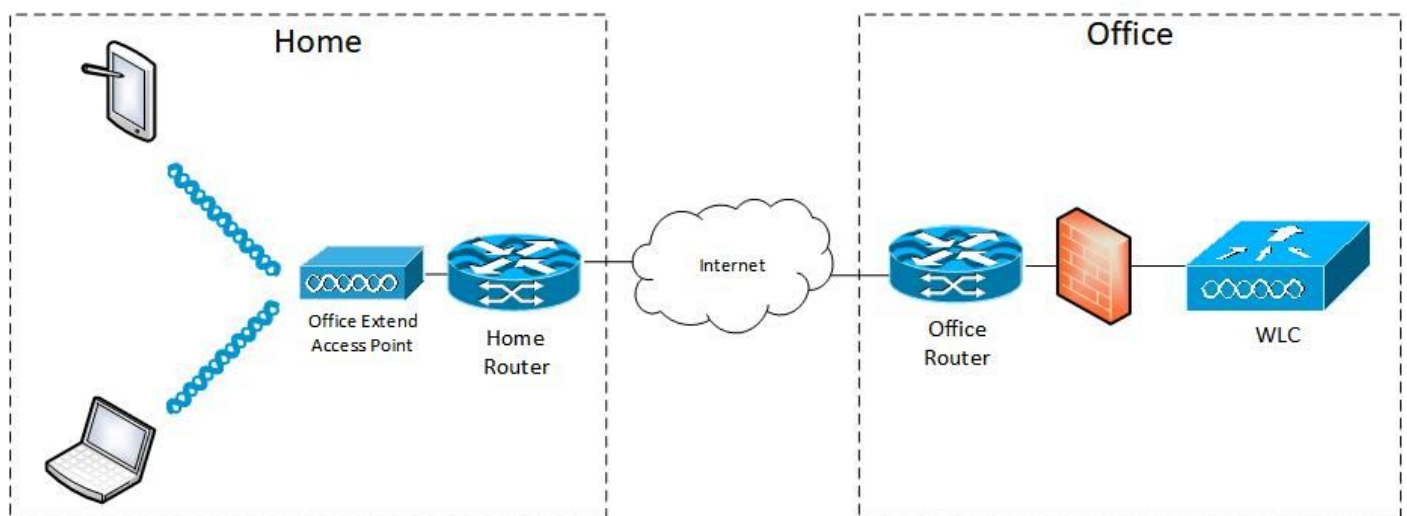
Un OEAP proporciona comunicaciones seguras de un WLC de Cisco a un AP de Cisco en una ubicación remota, para extender la WLAN corporativa a través de Internet a la residencia de un empleado. La experiencia del usuario en la oficina doméstica es exactamente la misma que en la oficina corporativa. El cifrado de seguridad de la capa de transporte del datagrama (DTLS) entre el punto de acceso y el controlador garantiza que todas las comunicaciones tengan el mayor nivel de seguridad. Cualquier punto de acceso interior en modo FlexConnect puede actuar como OEAP.

Hechos importantes

- Los OEAP de Cisco están diseñados para funcionar detrás de un router u otro dispositivo de gateway que utilice NAT. NAT permite que un dispositivo, como un router, actúe como agente entre Internet (pública) y una red personal (privada), lo que permite que un grupo completo de ordenadores se represente mediante una única dirección IP. No hay límite en el número de OEAP de Cisco que puede implementar detrás de un dispositivo NAT.
- Todos los modelos de AP interiores soportados con antena integrada se pueden configurar como OEAP excepto los AP-700I, AP-700W y los AP802 series AP.
- Todos los OEAP deben estar en el mismo grupo AP y ese grupo no debe contener más de 15 LAN inalámbricas. Un controlador con OEAP en un grupo AP publica sólo hasta 15 WLAN a cada OEAP conectado porque reserva una WLAN para el identificador personal del conjunto de servicios (SSID).

Configurar

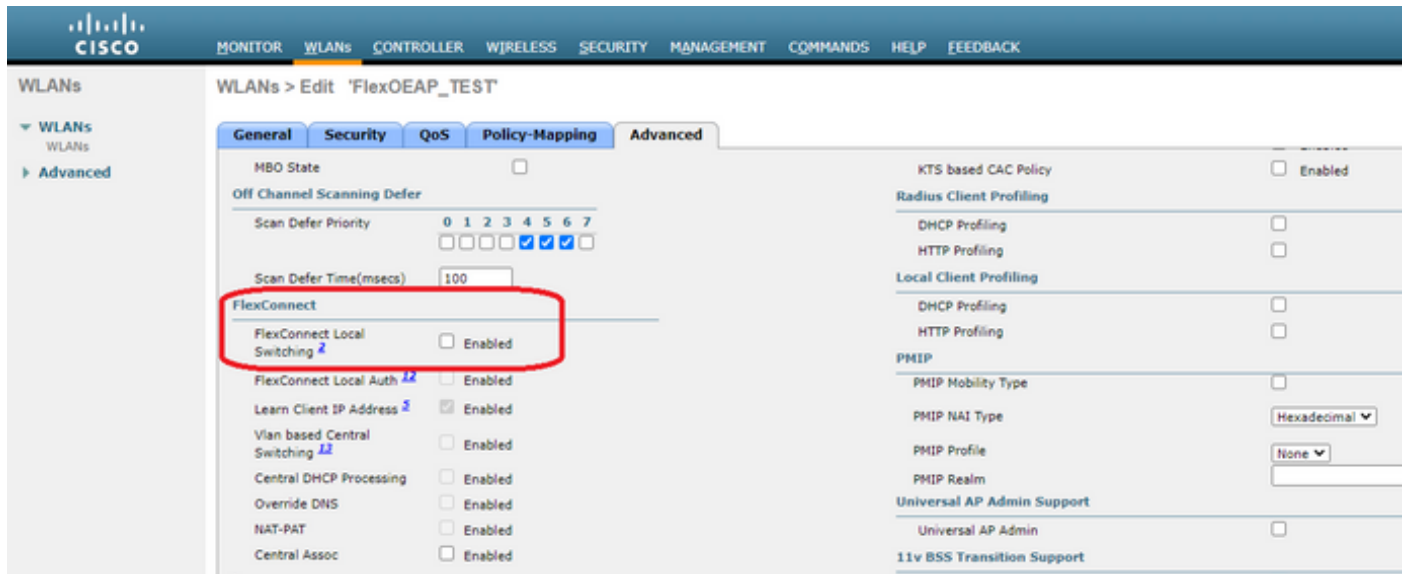
Diagrama de la red



Configuraciones

configuración WLAN

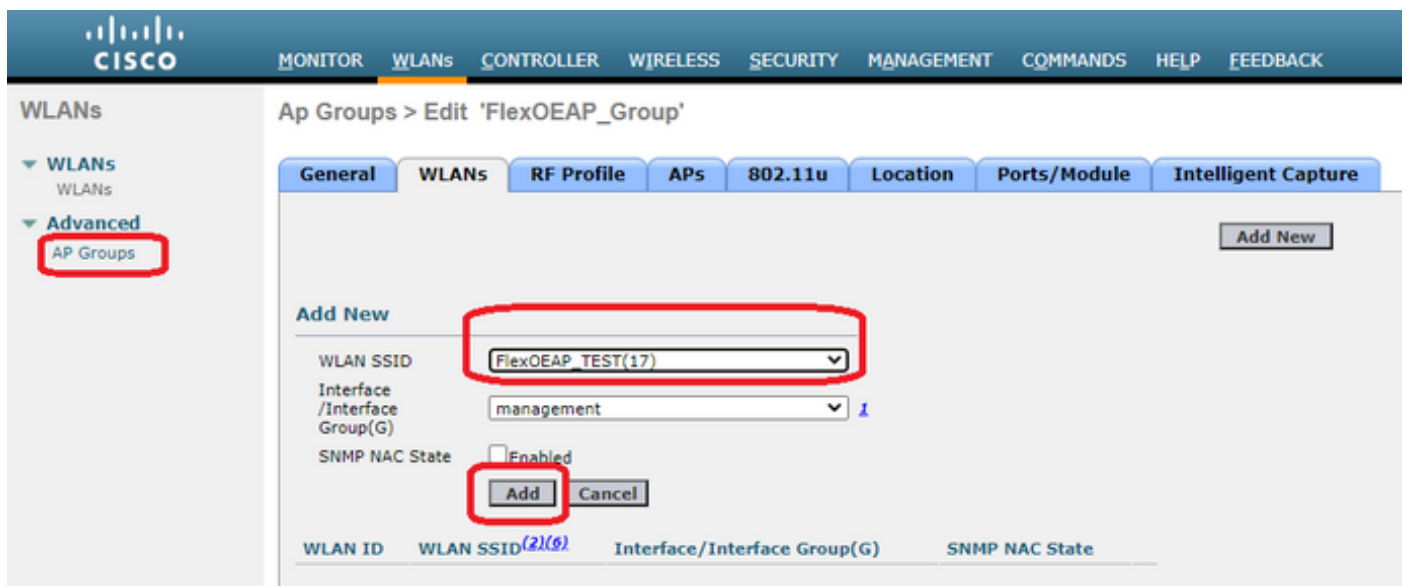
Paso 1. Cree una WLAN para asignar al grupo AP. No necesita habilitar la opción FlexConnect Local Switching para esta WLAN.



The screenshot shows the Cisco WLAN configuration interface for 'FlexOEAP_TEST'. The 'FlexConnect' section is highlighted with a red box. The 'FlexConnect Local Switching' option is set to 'Enabled'.

Option	State
FlexConnect Local Switching	Enabled
FlexConnect Local Auth	Enabled
Learn Client IP Address	Enabled
Vlan based Central Switching	Enabled
Central DHCP Processing	Enabled
Override DNS	Enabled
NAT-PAT	Enabled
Central Assoc	Enabled

Paso 2. Cree un grupo AP. En la pestaña **WLANs**, elija el WLAN SSID y luego haga clic en **Add** para agregar la WLAN. Vaya a la pestaña **APs** y **Agregar** el OEAP FlexConnect.



The screenshot shows the Cisco AP Groups configuration interface for 'FlexOEAP_Group'. The 'Add New' section is highlighted with a red box. The 'WLAN SSID' dropdown is set to 'FlexOEAP_TEST(17)'. The 'Add' button is also highlighted with a red box.

WLAN ID	WLAN SSID(2/6)	Interface/Interface Group(G)	SNMP NAC State
	FlexOEAP_TEST(17)	management	Enabled



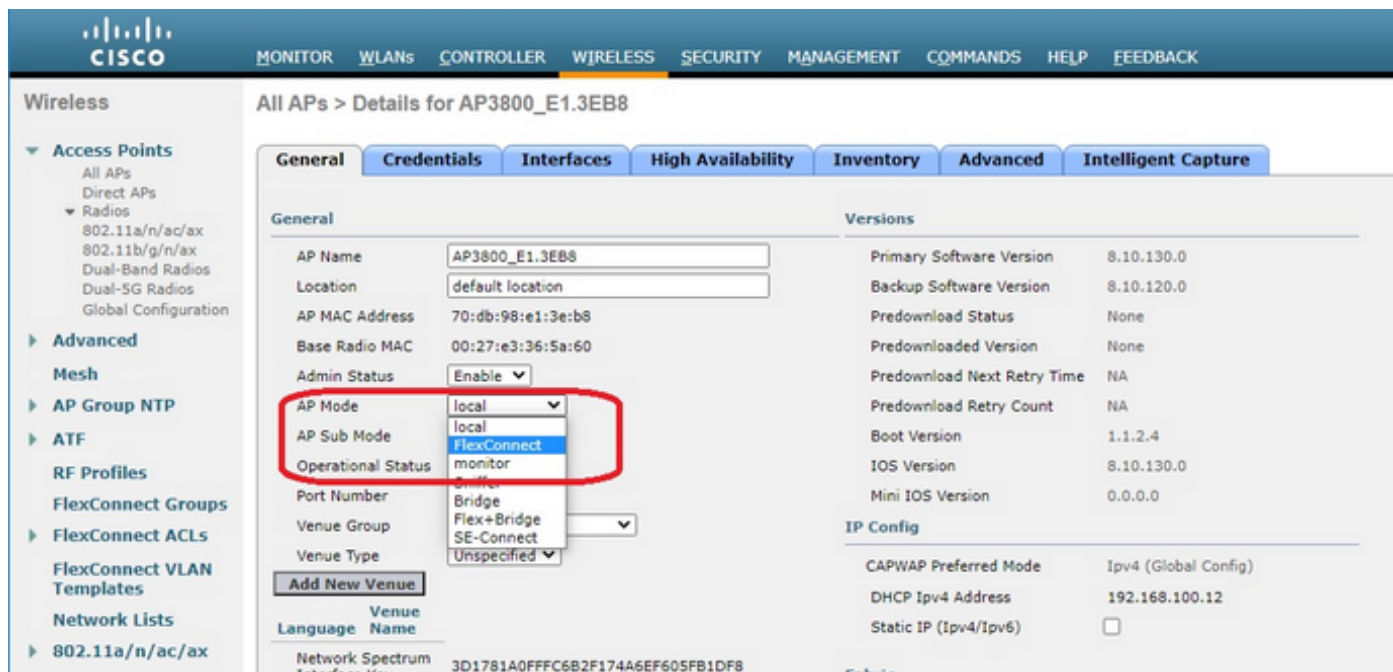
The screenshot shows the Cisco AP Groups configuration interface for 'FlexOEAP_Group'. The 'APs currently in the Group' section is highlighted with a red box. The table lists the APs and their Ethernet MAC addresses.

AP Name	Ethernet MAC
AP9120_4C.E77C	c4:f7:d5:4c:e7:7c
AP3800_E1.3EB8	70:db:98:e1:3e:b8

Configuración de AP

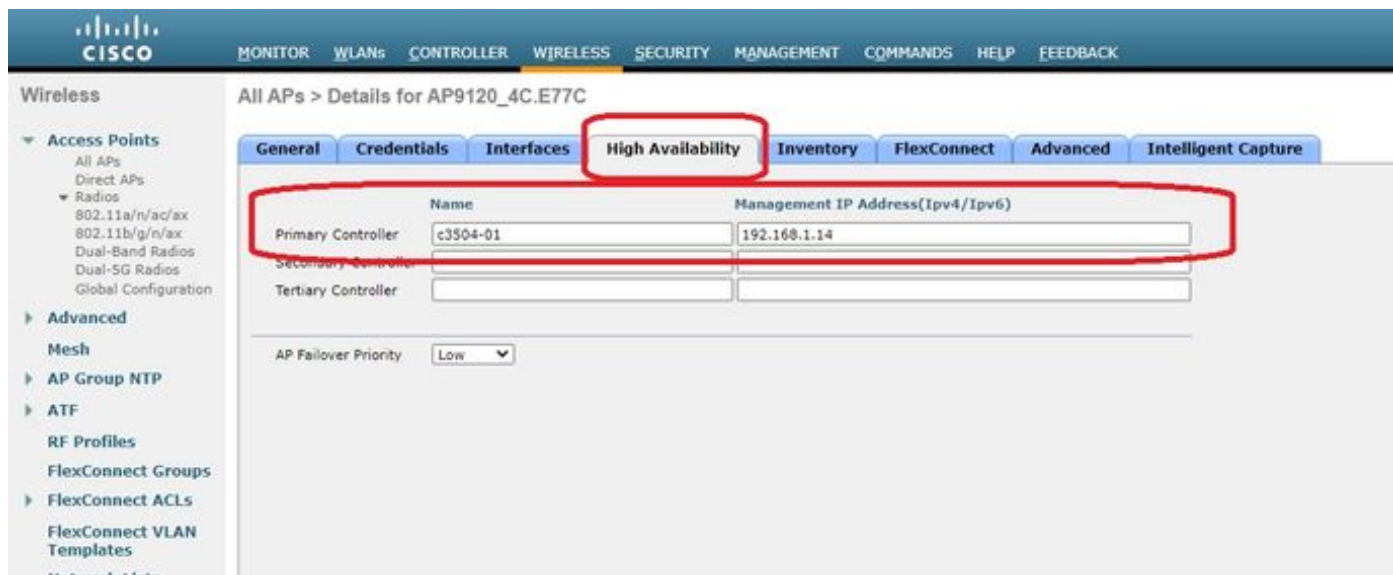
Después de que el AP se haya asociado con el controlador en el modo FlexConnect, puede configurarlo como OEAP.

Paso 1. Después de que el AP se una al WLC, cambie el modo AP a **FlexConnect** y haga clic en **Aplicar**.



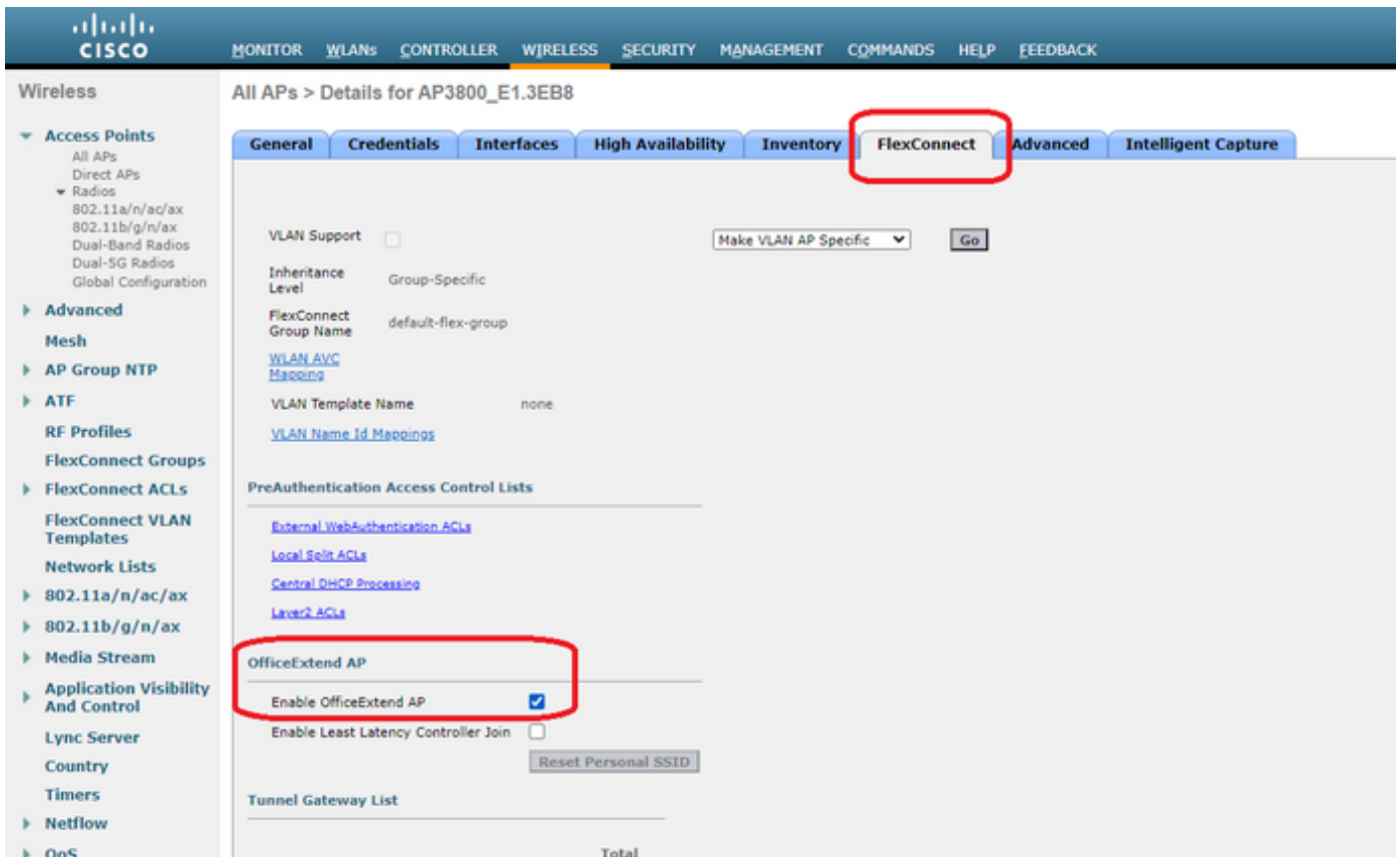
The screenshot shows the configuration page for AP3800_E1.3EB8. The 'General' tab is active. The 'AP Mode' dropdown menu is open, and 'FlexConnect' is selected. Other fields include AP Name (AP3800_E1.3EB8), Location (default location), AP MAC Address (70:db:98:e1:3e:b8), Base Radio MAC (00:27:e3:36:5a:60), Admin Status (Enable), and various version and IP configuration details.

Paso 2. Asegúrese de tener al menos un WLC primario configurado en la pestaña Alta Disponibilidad:

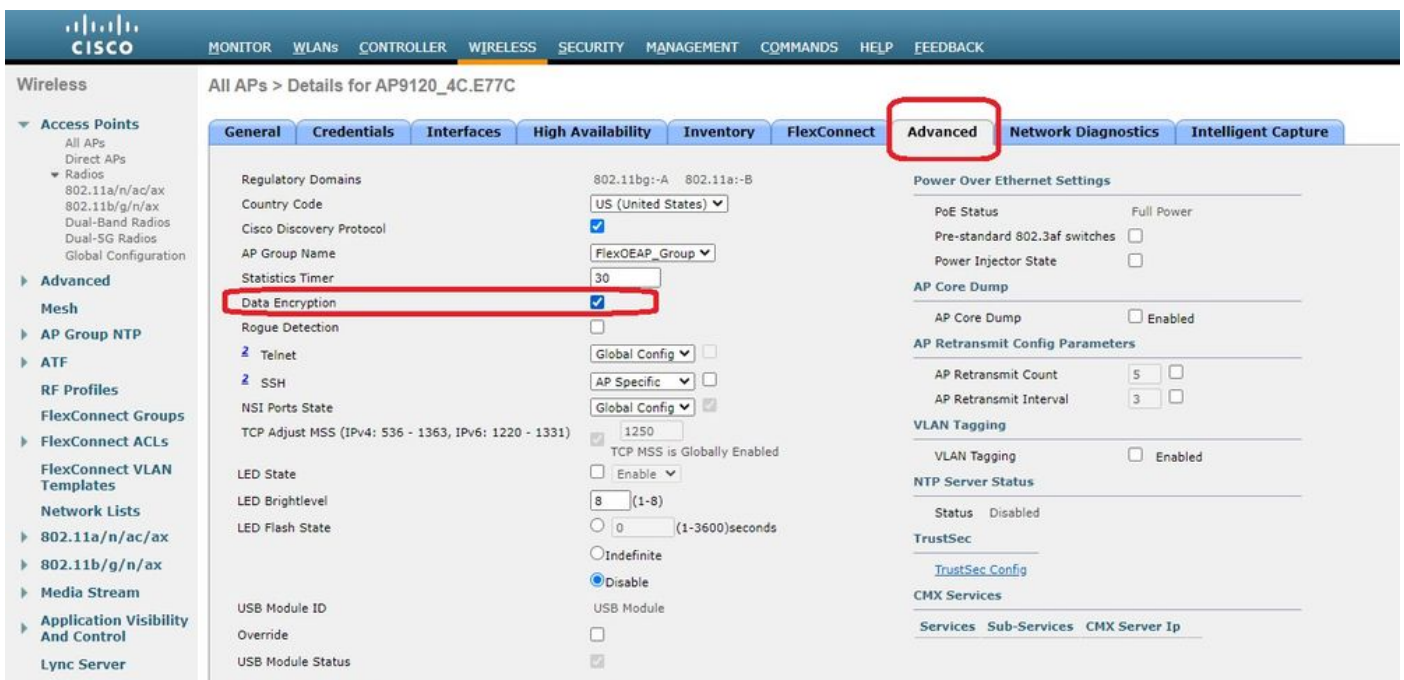


The screenshot shows the configuration page for AP9120_4C.E77C. The 'High Availability' tab is active. The 'Primary Controller' field is highlighted with a red box. The 'Primary Controller' field contains the name 'c3504-01' and the 'Management IP Address' is '192.168.1.14'. Other fields include Secondary Controller, Tertiary Controller, and AP Failover Priority (Low).

Paso 3. Vaya a la ficha FlexConnect y marque la casilla de verificación **Enable OfficeExtend AP**.



El cifrado de datos DTLS se habilita automáticamente cuando habilita el modo OfficeExtend para un AP. Sin embargo, puede habilitar o inhabilitar el cifrado de datos DTLS para un AP específico. Para hacerlo, marque (activar) o desmarque (desactivar) la casilla de verificación **Cifrado de datos** en la ficha Todos los AP > Detalles para [AP seleccionado] > Opciones avanzadas:



Nota: El acceso Telnet y SSH se desactivan automáticamente cuando habilita el modo OfficeExtend para un AP. Sin embargo, puede habilitar o inhabilitar el acceso Telnet o SSH para un AP específico. Para hacerlo, marque (activar) o desmarque (desactivar) la casilla de verificación Telnet o SSH en la pestaña All APs > Detalles for [selected AP] > Advanced .

Nota: La latencia de link se habilita automáticamente cuando habilita el modo OfficeExtend para un AP. Sin embargo, puede habilitar o inhabilitar la latencia de link para un AP específico. Para hacerlo, marque (activar) o desmarque (desactivar) la casilla de verificación Activar latencia de link en la pestaña Todos los AP > Detalles para [AP seleccionado] > Avanzado.

Paso 3. Seleccione **Aplicar**. Después de seleccionar Apply (Aplicar), el AP se recarga.

Paso 4. Después de que el AP se reúne al WLC, el AP está en el modo OEAP.

Nota: Recomendamos que configure la seguridad de unión de AP (definida comúnmente en Políticas de AP) para que solamente los AP autorizados puedan unirse al WLC. También puede utilizar el aprovisionamiento de puntos de acceso con certificado de importancia local (LSC).

Paso 5. Cree una lista de control de acceso (ACL) de FlexConnect para definir qué tráfico se conmutará de forma centralizada (Denegar) y local (Permitir).

Aquí, tiene el objetivo de cambiar localmente todo el tráfico a la subred 192.168.1.0/24.

FlexConnect ACLs > IPv4 ACL > Edit

General

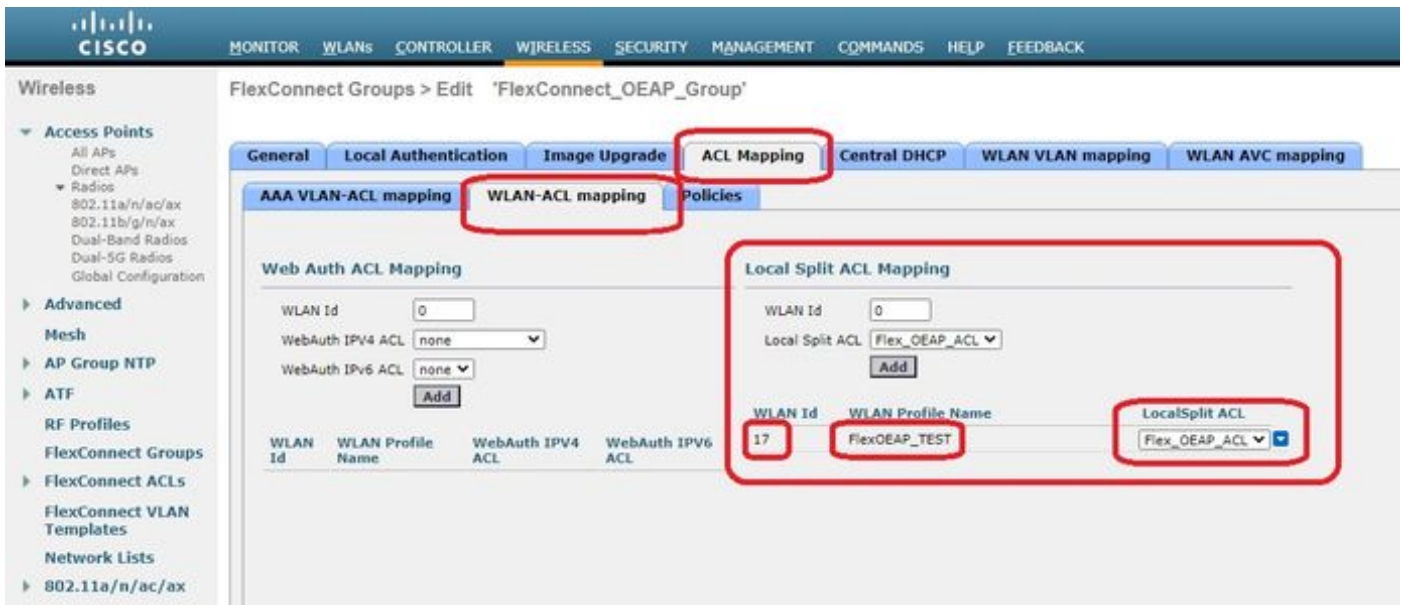
Access List Name Flex_OEAP_ACL

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	192.168.1.0 / 255.255.255.0	Any	Any	Any	Any
2	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any

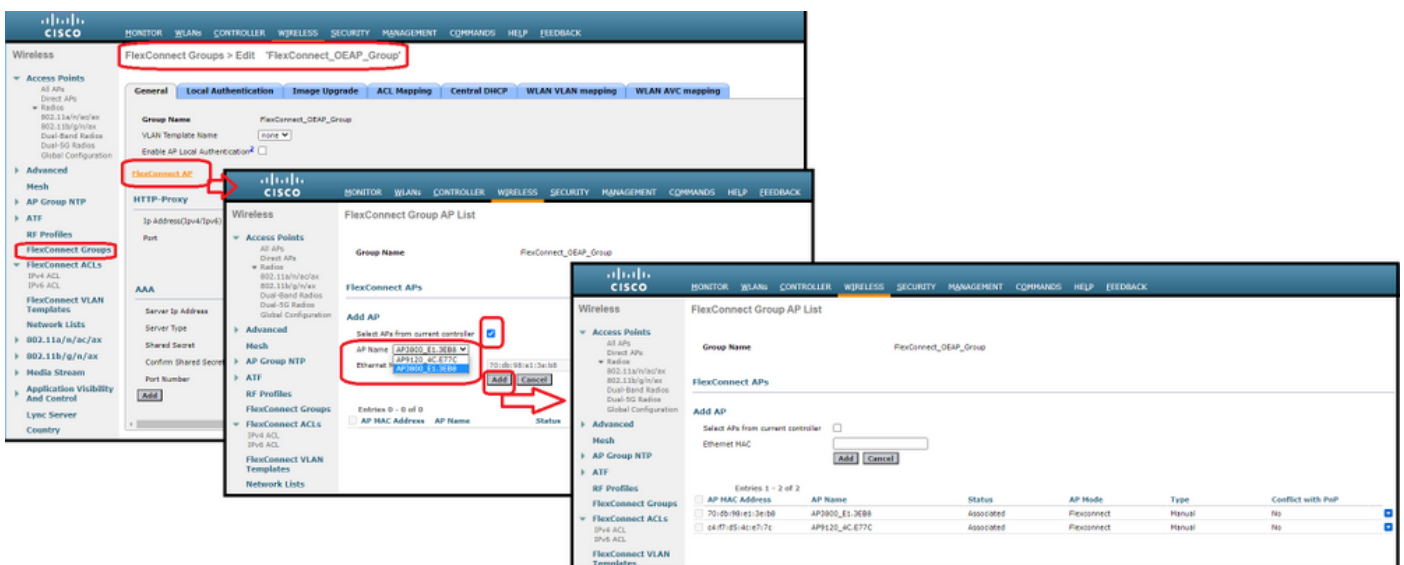
URL Rules

Seq	Action	Destination Url
-----	--------	-----------------

Paso 6. Cree un grupo FlexConnect, vaya al **mapeo ACL** y luego vaya al **mapeo de WLAN-ACL**. En "Local Split ACL Mapping" (Asignación de ACL dividida local), introduzca la ID de WLAN y elija la ACL de FlexConnect. A continuación, haga clic en **Agregar**.



Paso 7. Agregue el AP al grupo FlexConnect:



Verificación

1. Verifique el estado y la definición de FlexConnect ACL:

```
(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. Verifique que la conmutación local de FlexConnect esté inhabilitada:

```
(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. Verifique la configuración del grupo FlexConnect:

```
(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

```

Puede capturar el tráfico en la interfaz AP para verificar que el tráfico se divide en el AP.

Sugerencia: Para solucionar problemas, puede inhabilitar el cifrado DTLS para ver el tráfico de datos encapsulado dentro del capwap.

Este ejemplo de captura de paquetes muestra el tráfico de datos que coincide con las sentencias ACL "deny" dirigidas al WLC, y el tráfico de datos que coincide con las sentencias ACL "permit" conmutadas localmente en el AP:

*Ethernet_yellowCable

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Delta	Source	Destination	Length	Info	Ext Tag Number
20859	9.819533	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request id=0x0001, seq=213/545...	
20860	0.019956	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=213/545...	
20912	0.984274	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request id=0x0001, seq=214/547...	
20913	0.018616	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=214/547...	
20961	0.986005	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request id=0x0001, seq=215/550...	
20962	0.018343	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=215/550...	
21007	0.984777	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request id=0x0001, seq=216/552...	
21008	0.018309	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=216/552...	
21467	9.477613	192.168.1.99	192.168.1.254	74	Echo (ping) request id=0x0001, seq=217/555...	
21468	0.000638	192.168.1.254	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=217/555...	
21511	1.003331	192.168.1.99	192.168.1.254	74	Echo (ping) request id=0x0001, seq=218/558...	
21512	0.000192	192.168.1.254	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=218/558...	
21572	1.009272	192.168.1.99	192.168.1.254	74	Echo (ping) request id=0x0001, seq=219/560...	
21573	0.000000	192.168.1.254	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=219/560...	
21621	1.002280	192.168.1.99	192.168.1.254	74	Echo (ping) request id=0x0001, seq=220/563...	
21622	0.000374	192.168.1.254	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=220/563...	

> Frame 20859: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
 > Ethernet II, Src: Cisco_e1:3e:b8 (70:db:98:e1:3e:b8), Dst: Cisco_14:04:b0 (cc:70:ed:14:04:b0)
 > Internet Protocol Version 4, Src: 192.168.1.99, Dst: 192.168.1.14
 > User Datagram Protocol, Src Port: 5264, 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: 8.8.8.8
 > Internet Control Message Protocol

*Ethernet_yellowCable

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Delta	Source	Destination	Length	Info	Ext Tag Number
20859	9.819533	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request id=0x0001, seq=213/545...	
20860	0.019956	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=213/545...	
20912	0.984274	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request id=0x0001, seq=214/547...	
20913	0.018616	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=214/547...	
20961	0.986005	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request id=0x0001, seq=215/550...	
20962	0.018343	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=215/550...	
21007	0.984777	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request id=0x0001, seq=216/552...	
21008	0.018309	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply id=0x0001, seq=216/552...	
21467	9.477613	192.168.1.99	192.168.1.254	74	Echo (ping) request id=0x0001, seq=217/555...	
21468	0.000638	192.168.1.254	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=217/555...	
21511	1.003331	192.168.1.99	192.168.1.254	74	Echo (ping) request id=0x0001, seq=218/558...	
21512	0.000192	192.168.1.254	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=218/558...	
21572	1.009272	192.168.1.99	192.168.1.254	74	Echo (ping) request id=0x0001, seq=219/560...	
21573	0.000000	192.168.1.254	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=219/560...	
21621	1.002280	192.168.1.99	192.168.1.254	74	Echo (ping) request id=0x0001, seq=220/563...	
21622	0.000374	192.168.1.254	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=220/563...	

> Frame 21467: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 > Ethernet II, Src: Cisco_e1:3e:b8 (70:db:98:e1:3e:b8), Dst: ThomsonT_73:c5:1d (00:26:44:73:c5:1d)
 > Internet Protocol Version 4, Src: 192.168.1.99, Dst: 192.168.1.254
 > Internet Control Message Protocol

Nota: En escenarios normales, el AP traduce las direcciones de red para el tráfico conmutado localmente porque la subred del cliente pertenece a la red de la oficina, y los dispositivos locales en la oficina doméstica no saben cómo alcanzar la subred del cliente. El AP utiliza la dirección IP definida en la subred de la oficina local para traducir el tráfico del cliente.

Para verificar que el AP realizó la NAT, puede conectarse al terminal AP y ejecutar el comando **"show ip nat translations"**. Ejemplo:

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
```

Si elimina la tunelización dividida, todo el tráfico se conmuta centralmente en el WLC. Este ejemplo muestra el protocolo de mensajes de control de Internet (ICMP) al destino 192.168.1.2, dentro del túnel capwap:

The screenshot shows a Wireshark capture of ICMP traffic. The main pane displays a list of packets with columns for No., Delta, Source, Destination, Length, Info, Ext Tag Number, and Payload Type. The packets are numbered 108 through 166. Packets 108, 127, 142, 143, 165, and 166 are ping requests, while packets 109, 128, 144, 145, 166, and 167 are ping replies. The source and destination IP addresses are 192.168.1.82 and 192.168.1.14, and 192.168.1.14 and 192.168.1.82 respectively. The info column shows 'Echo (ping) request' and 'Echo (ping) reply' with sequence numbers.

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

The bottom pane shows the packet details for frame 108:

- > 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