

# FlexConnect OEAP met splitter-tunneling configureren

## Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[Belangrijke feiten](#)

[Configureren](#)

[Netwerkdigram](#)

[Configuraties](#)

[WLAN-configuratie](#)

[AP-configuratie](#)

[Verifiëren](#)

## Inleiding

In dit document wordt beschreven hoe u een access point (AP) binnen kunt configureren als een FlexConnect Office Extend AP (OEAP)-modus en hoe u splitsingen kunt inschakelen zodat u kunt definiëren wat er lokaal moet worden geschakeld op het thuishkantoor en welk verkeer centraal moet worden geschakeld op de draadloze LAN-controller (WLC).

Bijgedragen door Tiago Antunes, Nicolas Darchis Cisco TAC-engineers.

## Voorwaarden

### Vereisten

Bij de configuratie van dit document wordt ervan uitgegaan dat de WLC al is geconfigureerd in een gedemilitariseerde zone (DMZ) met netwerkadresomzetting (NAT) en dat AP vanuit het thuishkantoor aan de WLC kan deelnemen.

### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- WLC's met versie AireOS 8.10(130.0) software.
- Wave1 AP's: 1700/2700/3700.
- Wave2 access points: 1800/2800/3800/4800 en Catalyst 9100 Series.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

## Overzicht

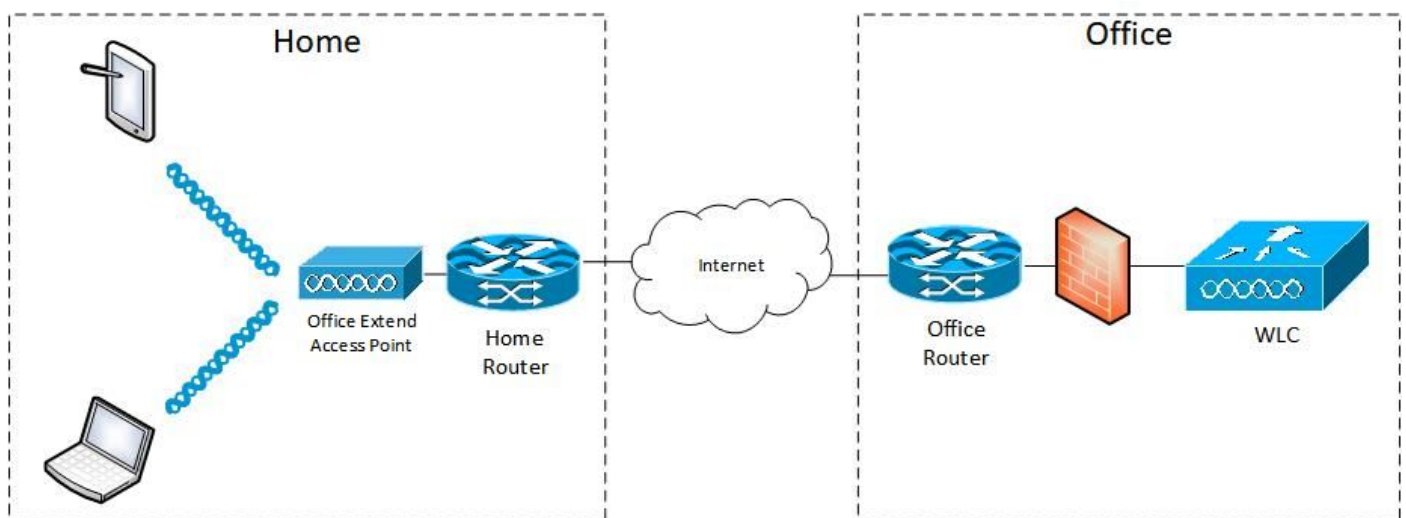
Een OEAP biedt veilige communicatie van een Cisco WLC naar een Cisco AP op een verre plaats, om de bedrijfsWLAN via het internet naar de verblijfplaats van een werknemer uit te breiden. De ervaring van de gebruiker op het thuishkantoor is precies dezelfde als bij het hoofdkantoor. Datagram Transport Layer Security (DTLS)-encryptie tussen de AP en de controller zorgt ervoor dat alle communicatie het hoogste beveiligingsniveau heeft. Elke AP binnen in FlexConnect modus kan als een OEAP fungeren.

## Belangrijke feiten

- Cisco OEAP's zijn ontworpen om achter een router of ander gateway-apparaat te werken dat NAT gebruikt. NAT staat een apparaat, zoals een router, toe om als agent tussen het internet (publiek) en een persoonlijk netwerk (privé) te handelen, wat een gehele groep computers toe om door één enkel IP adres vertegenwoordigd te zijn. Er is geen limiet aan het aantal MAP's van Cisco dat u achter een NAT-apparaat kunt implementeren.
- Alle ondersteunde modellen binnen AP met geïntegreerde antenne kunnen als OEAP worden geconfigureerd behalve AP-700I, AP-700W en AP802 reeks AP's.
- Alle OEAP's moeten in dezelfde AP-groep vallen en die groep mag niet meer dan 15 draadloze LAN's bevatten. Een controller met OEAP's in een AP-groep publiceert slechts 15 WLAN's bij elke aangesloten OEAP omdat deze één WLAN-server behoudt voor de persoonlijke serviceset (SSID).

## Configureren

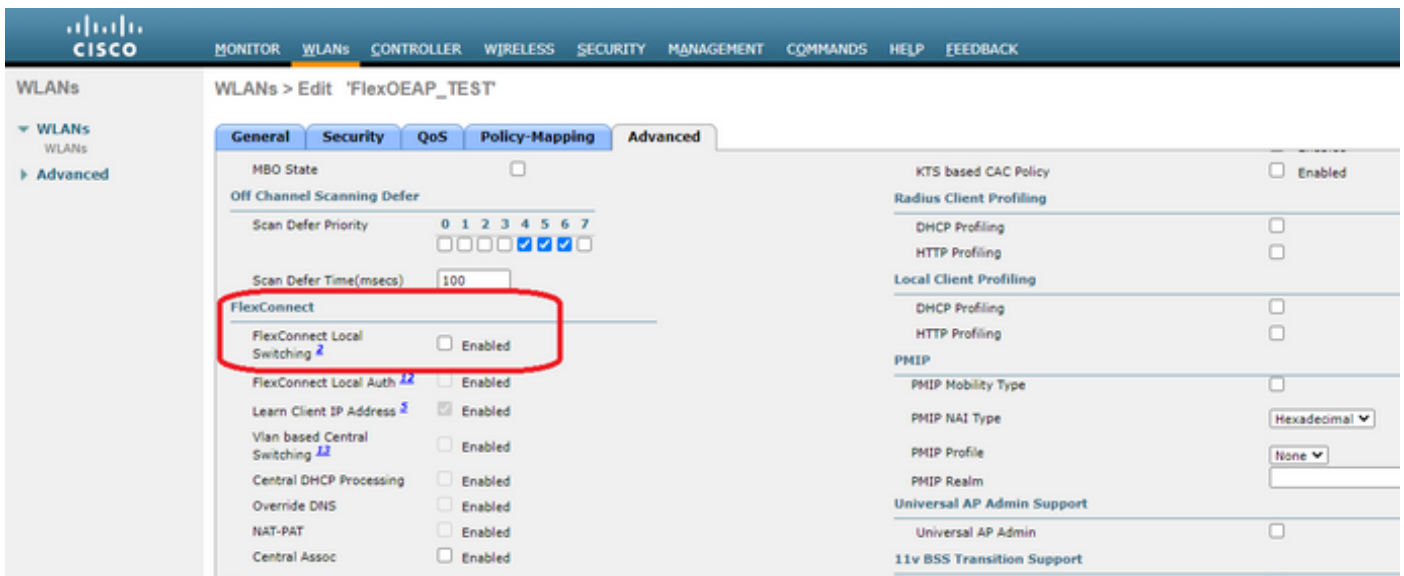
### Netwerkdigram



### Configuraties

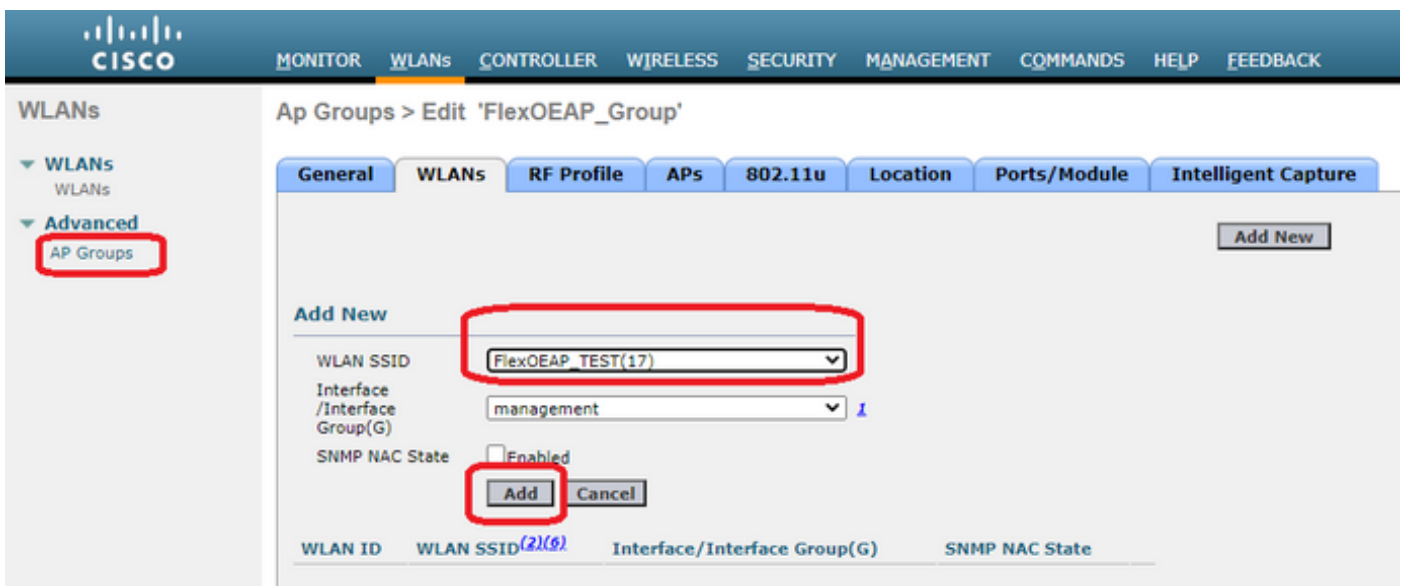
## WLAN-configuratie

Stap 1. Maak een WLAN-functie om aan de AP-groep toe te wijzen. U hoeft de FlexConnect Local Switching optie niet in te schakelen voor dit WLAN.



The screenshot shows the Cisco WLAN configuration interface for 'FlexOEAP\_TEST'. The 'Advanced' tab is selected, and the 'FlexConnect' section is highlighted with a red box. The 'FlexConnect Local Switching' option is set to 'Enabled'. Other options like 'FlexConnect Local Auth', 'Learn Client IP Address', and 'Vlan based Central Switching' are also visible.

Stap 2. Maak een AP-groep. Kies in het tabblad WLAN de WLAN-sid en klik vervolgens op **Add** om de WLAN-functie toe te voegen. Ga naar het tabblad AP en Voeg FlexConnect toe.



The screenshot shows the Cisco AP Groups configuration interface for 'FlexOEAP\_Group'. The 'WLANs' tab is selected, and the 'Add New' section is highlighted with a red box. The 'WLAN SSID' dropdown is set to 'FlexOEAP\_TEST(17)'. The 'Interface /Interface Group(G)' dropdown is set to 'management'. The 'Add' button is also highlighted with a red box.

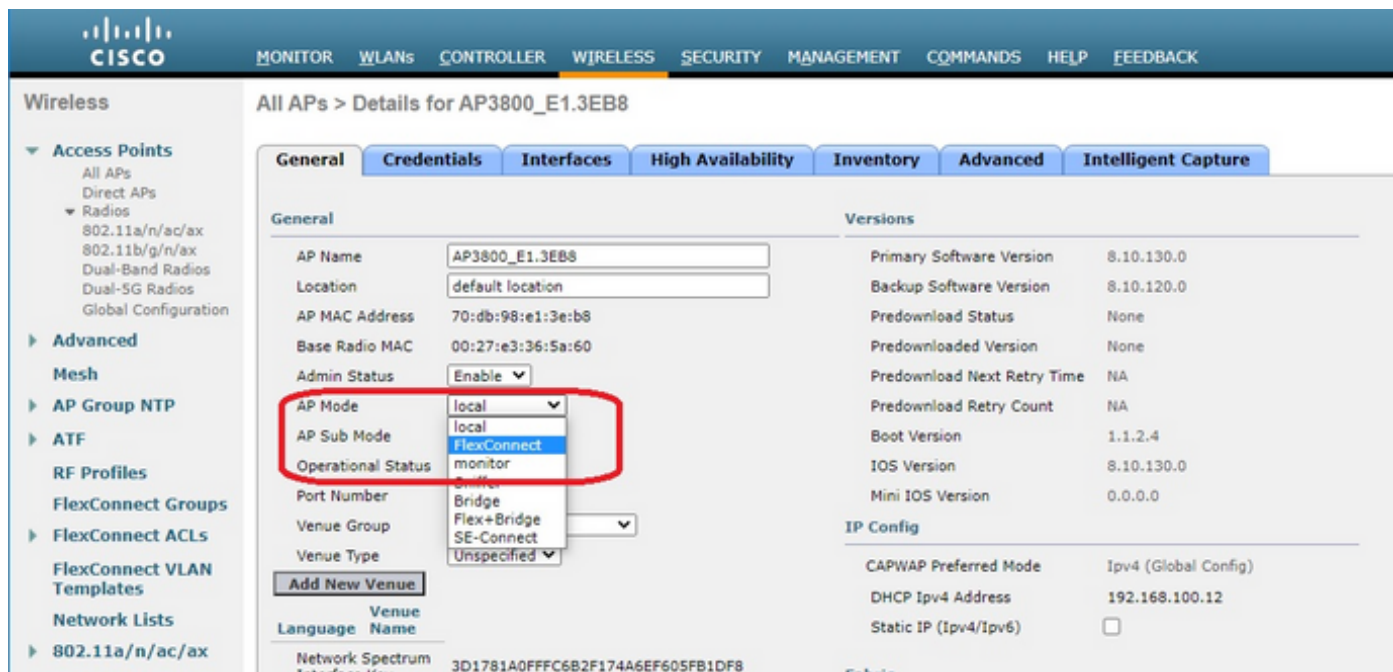


The screenshot shows the Cisco AP Groups configuration interface for 'FlexOEAP\_Group'. The 'APs' tab is selected, and the 'APs currently in the Group' section is visible. The table lists two APs: AP9120\_4C.E77C with Ethernet MAC c4:f7:d5:4c:e7:7c, and AP3800\_E1.3EB8 with Ethernet MAC 70:db:98:e1:3e:b8. The 'Add APs' button is highlighted with a red box.

## AP-configuratie

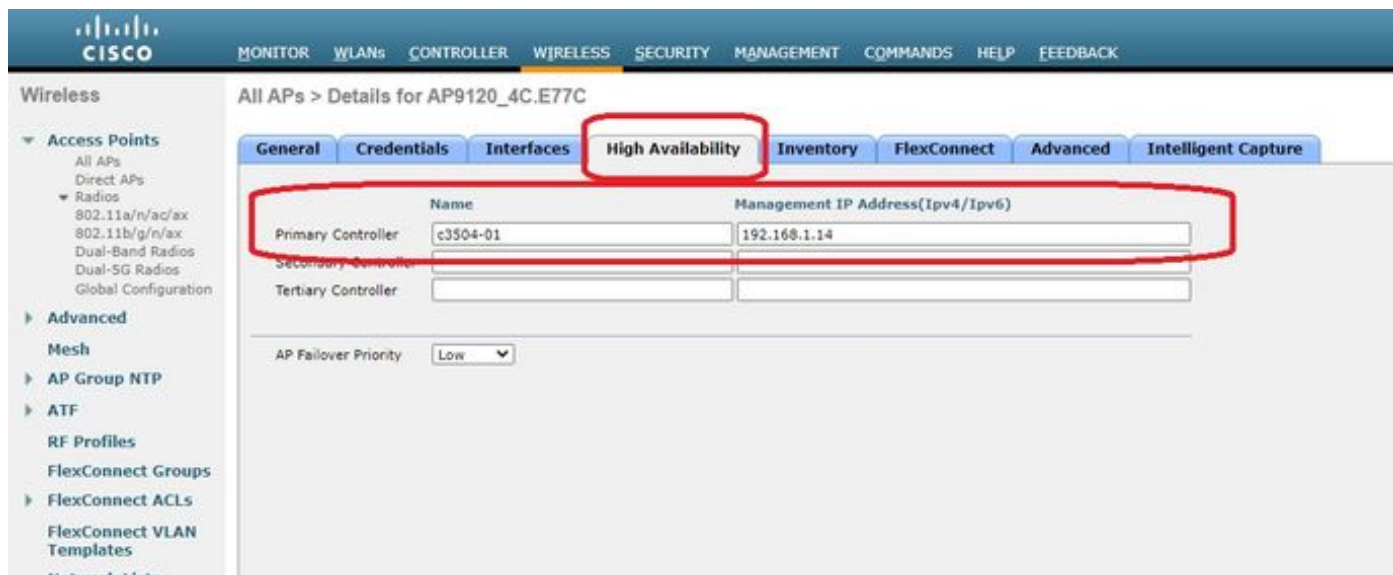
Nadat de AP met de controller in FlexConnect-modus is gekoppeld, kunt u deze als een OEAP configureren.

Stap 1. Nadat u zich bij de WLC hebt aangesloten, wijzigt u de AP-modus in **FlexConnect** en klikt u op **Toepassen**.



The screenshot shows the Cisco WLC configuration interface for AP3800\_E1.3EB8. The 'General' tab is active, and the 'AP Mode' dropdown menu is open, with 'FlexConnect' selected. The 'Operational Status' is set to 'monitor'. The 'AP Sub Mode' is also set to 'FlexConnect'. The 'Venue Group' is set to 'Flex+Bridge'. The 'Venue Type' is set to 'Unspecified'. The 'Add New Venue' button is visible. The 'Versions' section shows the Primary Software Version as 8.10.130.0 and the Backup Software Version as 8.10.120.0. The 'IP Config' section shows the CAPWAP Preferred Mode as Ipv4 (Global Config) and the DHCP Ipv4 Address as 192.168.100.12.

Stap 2. Zorg ervoor dat u minimaal een Primaire WLC hebt ingesteld op het tabblad Hoge beschikbaarheid:



The screenshot shows the Cisco WLC configuration interface for AP9120\_4C.E77C. The 'High Availability' tab is active, and the 'Primary Controller' field is highlighted with a red box. The 'Management IP Address' for the Primary Controller is 192.168.1.14. The 'AP Failover Priority' is set to 'Low'.

Stap 3. Ga naar het tabblad FlexConnect en controleer het vakje **OfficeExtend access point**.

The screenshot shows the Cisco Wireless Management interface for AP3800\_E1.3EB8. The 'FlexConnect' tab is highlighted with a red box. In the 'OfficeExtend AP' section, the 'Enable OfficeExtend AP' checkbox is checked and highlighted with a red box. Other visible settings include 'VLAN Support' (unchecked), 'Inheritance Level' (Group-Specific), and 'FlexConnect Group Name' (default-flex-group).

DTLS **Data Encryption** is automatisch ingeschakeld wanneer u de OfficeExtend-modus voor een AP inschakelen. U kunt echter wel DTLS-gegevensencryptie voor een specifieke AP in- of uitschakelen. Hiervoor controleert u (schakelt u) het aanvinkvakje **Data Encryption** uit op alle AP's > Details voor [geselecteerd AP] > tabblad Advanced:

The screenshot shows the Cisco Wireless Management interface for AP9120\_4C.E77C. The 'Advanced' tab is highlighted with a red box. In the 'Data Encryption' section, the 'Data Encryption' checkbox is checked and highlighted with a red box. Other visible settings include 'Regulatory Domains' (802.11bg:-A 802.11a:-B), 'Country Code' (US (United States)), and 'Cisco Discovery Protocol' (checked).

**Opmerking:** Telnet en SSH de toegang worden automatisch uitgeschakeld wanneer u de OfficeExtend modus voor een AP kunt inschakelen. U kunt echter telnet of SSH-toegang voor een specifieke AP in- of uitschakelen. Schakel dit in (schakelt) of uit (schakelt) het selectietekent van telnet of SSH uit op alle AP's > Details voor [geselecteerd AP] > Geavanceerd tabblad.

**Opmerking:** De latentie van de verbinding wordt automatisch geactiveerd wanneer u de modus OfficeExtend voor een AP toelaat. U kunt echter wel de link latency voor een bepaalde AP inschakelen of uitschakelen. Schakel om dit te doen de optie Link Latency inschakelen in (uitschakelen) of uit het vakje Enable Link Latency in op alle AP's > Details voor [geselecteerde AP] > Geavanceerd tabblad.

Stap 3. Selecteer **Toepassen**. Nadat u Toepassen hebt geselecteerd, herladen de AP opnieuw.

Stap 4. Nadat het AP zich bij de WLC herhaalt, is het AP in de OEAP modus.

**Opmerking:** We raden u aan om AP aan te sluiten bij veiligheid (algemeen gedefinieerd onder AP Beleid) zodat slechts geautoriseerde AP's zich bij de WLC kunnen aansluiten. U kunt ook LSC AP-voorziening (Local Significant certificaatlevering) gebruiken.

Stap 5. Maak een FlexConnect Access Control List (ACL) om te definiëren welk verkeer centraal (Jeans) en lokaal (Permit) zal worden geschakeld.

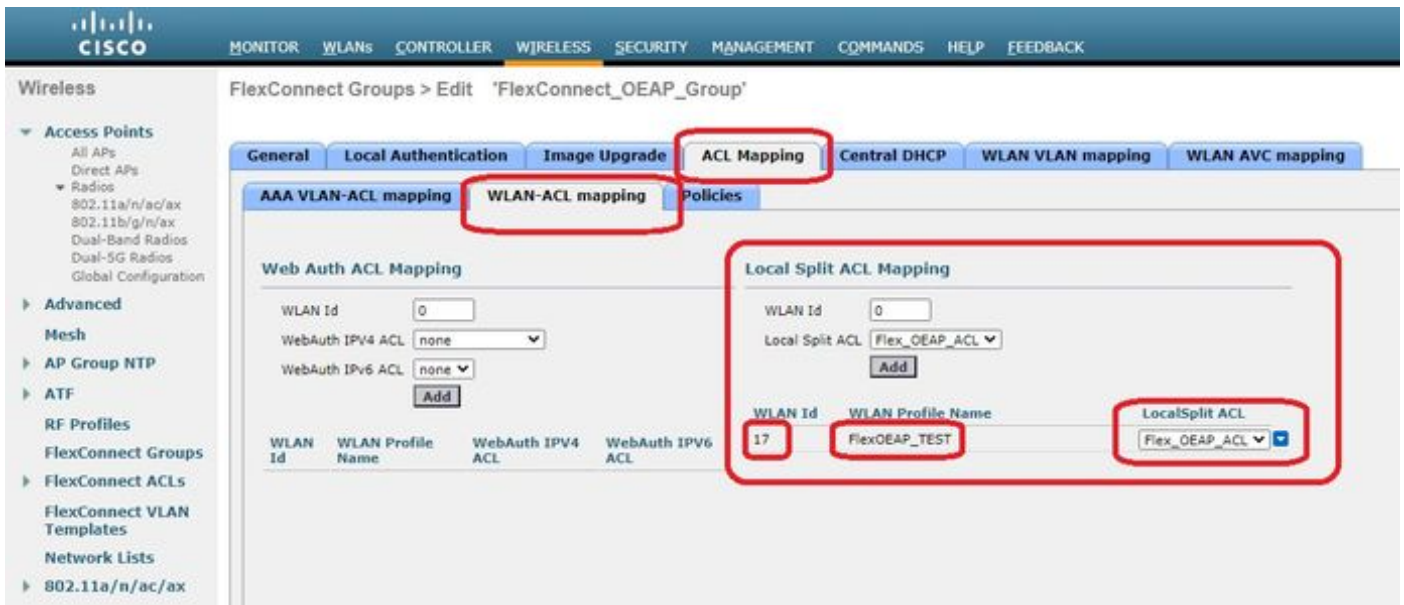
Hier, hebt u het doel om lokaal al verkeer naar het netto 192.168.1.0/24 te veranderen.

The screenshot shows the Cisco Wireless configuration interface. The breadcrumb navigation at the top reads "FlexConnect ACLs > IPv4 ACL > Edit". The main content area is titled "General" and shows "Access List Name" as "Flex\_OEAP\_ACL". Below this is a table of "IP Rules" with the following data:

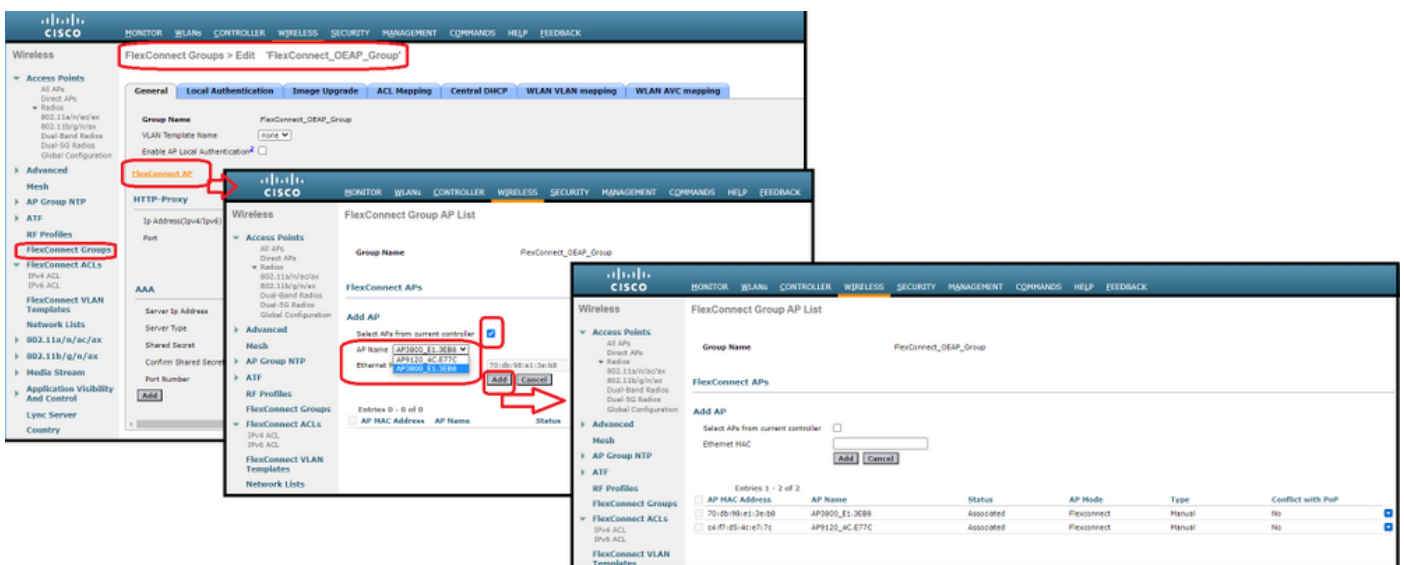
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	192.168.1.0 / 255.255.255.0	Any	Any	Any	Any
2	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any

The left sidebar shows the "FlexConnect ACLs" menu item highlighted with a red box. Below it are "IPv4 ACL" and "IPv6 ACL".

Stap 6. Maak een FlexConnect-groep, ga naar **ACL-afbeelding** en ga vervolgens naar **WLAN-ACL-making**. Typ onder "Local Split ACL mapping" de WLAN-id en kies FlexConnect ACL. Klik vervolgens op **Toevoegen**.



Stap 7. Voeg AP aan de groep FlexConnect toe:



## Verifiëren

1. Controleer de status en definitie van 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. Controleer dat FlexConnect lokale switching is uitgeschakeld:

```
(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. Controleer de configuratie van de FlexConnect-groep:

```
(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

U kunt het verkeer opnemen op de AP-interface om te controleren of het verkeer gesplitst is op de AP.

**Tip:** voor probleemoplossing kunt u DTLS-encryptie uitschakelen om het gegevensverkeer in de capwap te zien insluiten.

Dit voorbeeld van de pakketvastlegging toont gegevensverkeer dat de "ontken" van ACL overeenkomt met de verklaringen die op WLC zijn gericht en gegevensverkeer dat de "vergunning" van ACL overeenkomt die lokaal op AP zijn geschakeld:

\*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

**Opmerking:** In normale scenario's, vertaalt AP netwerkadressen voor lokaal geschakeld verkeer omdat klink aan het netwerk van het bureau behoort, en de lokale apparaten bij het huisbureau weten niet hoe te om de cliëntesubnet te bereiken. AP gebruikt het IP adres dat in het lokale dienstvoorwerp van het huisbureau wordt gedefinieerd om het clientverkeer te vertalen.

Om te verifiëren dat AP de NAT uitvoerde, kunt u met de AP terminal verbinden en de "*toon ip nat vertalingen*" opdracht geven. Voorbeeld:

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
```

Als u een gesplitste tunneling verwijdert, is al het verkeer centraal via de WLC geschakeld. Dit voorbeeld toont het Internet Control Message Protocol (ICMP) aan de bestemming 192.168.1.2, binnen de Capwap-tunnel:

The image shows a Wireshark packet capture window titled "Capturing from Ethernet\_yellowCable". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main display area shows a list of captured packets, with the first packet selected. The packet list table is as follows:

No.	Delta	Source	Destination	Length	Info	Ext Tag Number	Payload Type	C
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	

Below the packet list, the details pane for the selected packet (Frame 108) is expanded, showing the following layers:

- > 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