

Configurazione di FlexConnect OEAP con split tunneling

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Panoramica](#)

[Fatti importanti](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione della WLAN](#)

[Configurazione AP](#)

[Verifica](#)

Introduzione

Questo documento descrive come configurare un access point interno (AP) come modalità FlexConnect Office Extend AP (OEAP) e come abilitare il tunneling suddiviso in modo da poter definire quale traffico deve essere commutato localmente nell'ufficio di casa e quale traffico deve essere commutato centralmente sul controller WLC.

Contributo di Tiago Antunes, Nicolas Darchis Cisco TAC Engineers.

Prerequisiti

Requisiti

Nella configurazione di questo documento si presume che il WLC sia già configurato in una zona demilitarizzata (DMZ) con Network Address Translation (NAT) abilitato e che l'AP sia in grado di collegarsi al WLC dall'ufficio di casa.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Panoramica

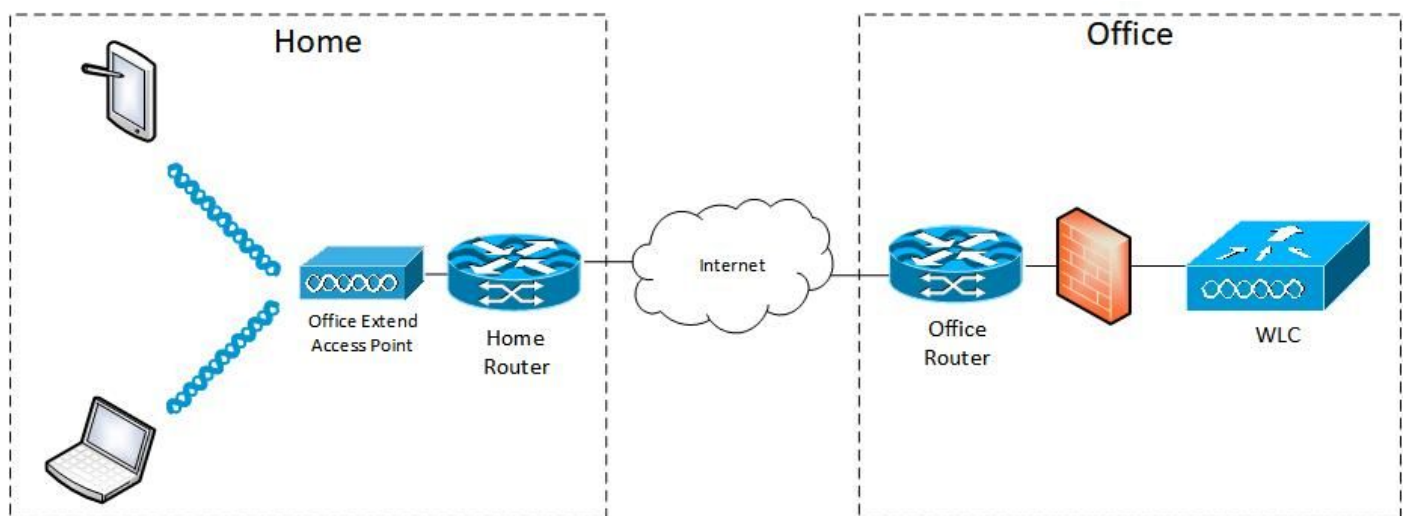
Un OEAP consente di comunicare in modo sicuro da un WLC Cisco a un AP Cisco in una posizione remota, in modo da estendere la WLAN aziendale tramite Internet alla residenza di un dipendente. L'esperienza dell'utente al suo domicilio è esattamente la stessa che si avrebbe al suo ufficio aziendale. La crittografia Datagram Transport Layer Security (DTLS) tra l'access point e il controller assicura che tutte le comunicazioni abbiano il massimo livello di sicurezza. Qualsiasi access point interno in modalità FlexConnect può funzionare come OEAP.

Fatti importanti

- I Cisco OEAP sono progettati per funzionare dietro un router o un altro dispositivo gateway che usa NAT. Il protocollo NAT consente a un dispositivo, ad esempio un router, di fungere da agente tra Internet (pubblico) e una rete personale (privata), consentendo a un intero gruppo di computer di essere rappresentato da un unico indirizzo IP. Non ci sono limiti al numero di Cisco OEAP che è possibile distribuire dietro un dispositivo NAT.
- Tutti i modelli di punti di accesso interni supportati con antenna integrata possono essere configurati come OEAP, ad eccezione dei punti di accesso serie AP-700I, AP-700W e AP802.
- Tutti gli OEAP devono trovarsi nello stesso gruppo di access point e tale gruppo non deve contenere più di 15 LAN wireless. Un controller con OEAP in un gruppo AP pubblica solo fino a 15 WLAN su ciascun OEAP connesso perché riserva una WLAN per l'SSID (Personal Service Set Identifier).

Configurazione

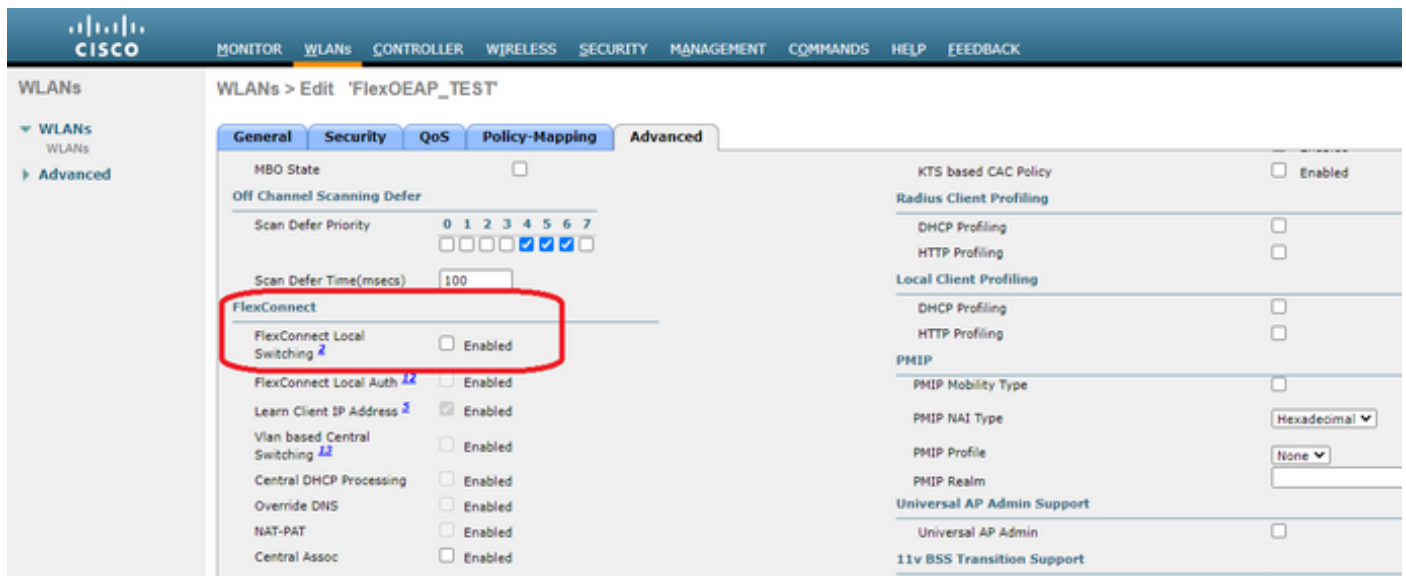
Esempio di rete



Configurazioni

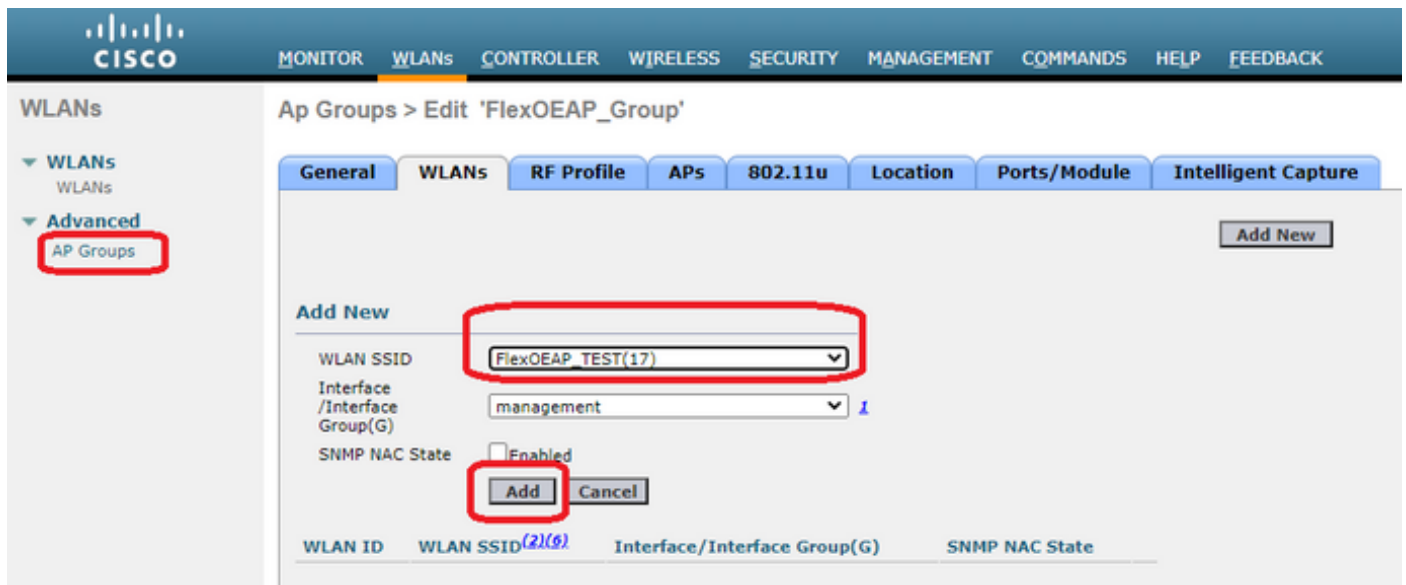
Configurazione della WLAN

Passaggio 1. Creare una WLAN da assegnare al gruppo AP. non è necessario abilitare l'opzione di switching locale FlexConnect per questa WLAN.



The screenshot shows the Cisco configuration interface for a WLAN named 'FlexOEAP_TEST'. The 'Advanced' tab is selected, and the 'FlexConnect' section is highlighted with a red box. The 'FlexConnect Local Switching' option is disabled. Other options in the 'FlexConnect' section include 'FlexConnect Local Auth', 'Learn Client IP Address', 'Vlan based Central Switching', 'Central DHCP Processing', 'Override DNS', 'NAT-PAT', and 'Central Assoc', all of which are enabled. The 'FlexConnect Local Switching' option is disabled.

Passaggio 2. Creare un gruppo PA. Nella scheda **WLAN**, selezionare il SSID della WLAN, quindi fare clic su **Add** (Aggiungi) per aggiungere la WLAN. Andare alla scheda **AP** e aggiungere il protocollo OEAP FlexConnect.



The screenshot shows the Cisco configuration interface for an AP Group named '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 'Add' button is also highlighted with a red box. The 'Interface /Interface Group(G)' dropdown is set to 'management'. The 'SNMP NAC State' option is disabled.



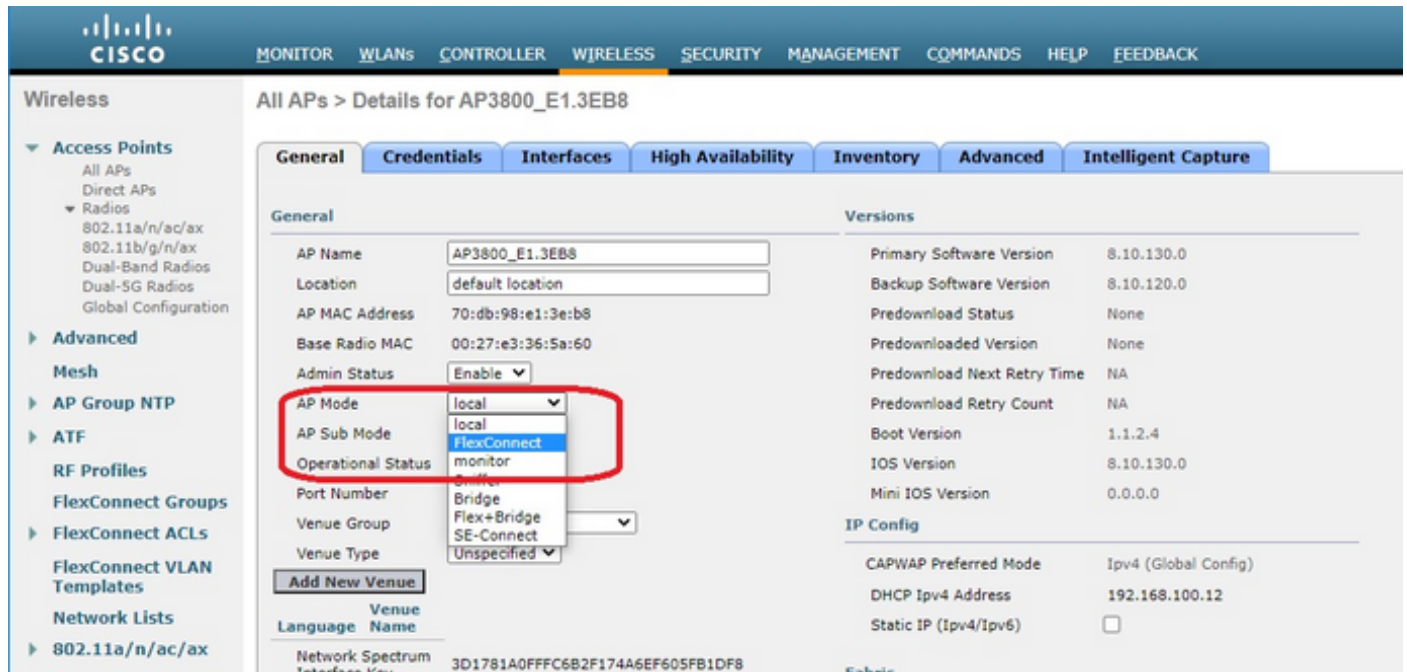
The screenshot shows the Cisco configuration interface for an AP Group named 'FlexOEAP_Group'. The 'APs' tab is selected, and the 'APs currently in the Group' section is highlighted with a red box. The table shows two APs: AP9120_4C.E77C and AP3800_E1.3EB8. The 'Add APs to the Group' section is also visible, with an 'Add APs' button.

AP Name	Ethernet MAC
<input type="checkbox"/> AP9120_4C.E77C	c4:f7:d5:4c:e7:7c
<input type="checkbox"/> AP3800_E1.3EB8	70:db:98:e1:3e:b8

Configurazione AP

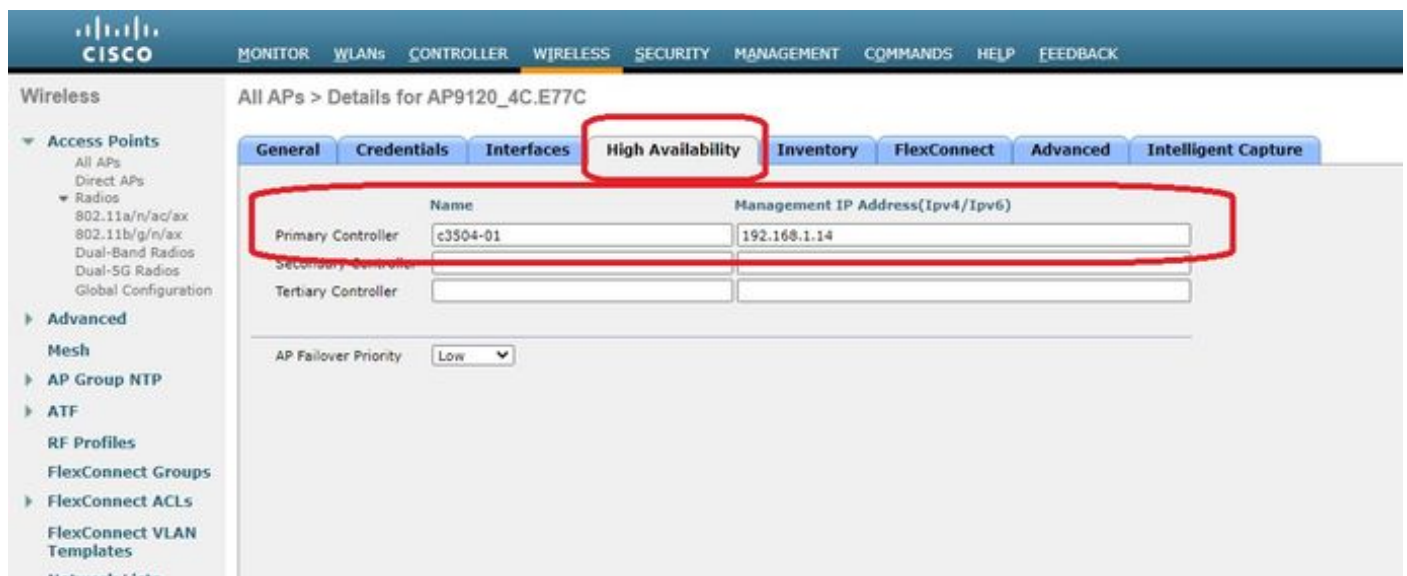
Dopo che l'access point è stato associato al controller in modalità FlexConnect, è possibile configurarlo come OEAP.

Passaggio 1. Dopo che l'access point si è unito al WLC, modificare la modalità AP in **FlexConnect** e fare clic su **Apply**.



The screenshot shows the Cisco Wireless configuration interface for AP3800_E1.3EB8. The 'General' tab is selected, and the 'AP Mode' dropdown menu is open, with 'FlexConnect' highlighted. The 'Operational Status' is set to 'monitor'. 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), Port Number, Venue Group, Venue Type (Unspecified), Add New Venue, Language, and Network Spectrum (3D1781A0FFFC6B2F174A6EF605FB1DF8). The 'Versions' section shows Primary Software Version (8.10.130.0), Backup Software Version (8.10.120.0), and other software-related details. The 'IP Config' section shows CAPWAP Preferred Mode (Ipv4 (Global Config)), DHCP Ipv4 Address (192.168.100.12), and Static IP (Ipv4/Ipv6) (unchecked).

Passaggio 2. Verificare che nella scheda Alta disponibilità sia configurato almeno un WLC primario:



The screenshot shows the Cisco Wireless configuration interface for AP9120_4C.E77C. The 'High Availability' tab is selected, and the 'Primary Controller' field is highlighted with a red box. The 'Name' is 'c3504-01' and the 'Management IP Address (Ipv4/Ipv6)' is '192.168.1.14'. The 'Secondary Controller' and 'Tertiary Controller' fields are empty. The 'AP Failover Priority' is set to 'Low'.

Passaggio 3. Andare alla scheda FlexConnect e selezionare la casella di controllo **Abilita OfficeExtend AP**.

The screenshot shows the Cisco Wireless Controller configuration interface for an AP3800_E1.3EB8. The 'FlexConnect' tab is highlighted with a red box. Under the 'OfficeExtend AP' section, the 'Enable OfficeExtend AP' checkbox is checked and also highlighted with a red box. Other visible settings include 'VLAN Support' (unchecked), 'Inheritance Level' (Group-Specific), and 'FlexConnect Group Name' (default-flex-group).

La **crittografia dei dati** DTLS viene attivata automaticamente quando si attiva la modalità OfficeExtend per un access point. Tuttavia, è possibile abilitare o disabilitare la crittografia dei dati DTLS per un punto di accesso specifico. A tale scopo, selezionare (abilitare) o deselegionare (disabilitare) la casella di controllo **Crittografia dati** nella scheda Tutti i punti di accesso > Dettagli per [punto di accesso selezionato] > Avanzate:

The screenshot shows the Cisco Wireless Controller configuration interface for an AP9120_4C.E77C. The 'Advanced' tab is highlighted with a red box. Under the 'Data Encryption' section, the 'Data Encryption' checkbox is checked and also 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).

Nota: L'accesso Telnet e SSH vengono disabilitati automaticamente quando si abilita la modalità OfficeExtend per un access point. Tuttavia, è possibile abilitare o disabilitare l'accesso Telnet o SSH per un access point specifico. A tale scopo, selezionare (abilitare) o deselegionare (disabilitare) la casella di controllo Telnet o SSH nella scheda Tutti gli access point > Dettagli per [access point selezionato] > Avanzate.

Nota: La latenza del collegamento viene attivata automaticamente quando si attiva la modalità OfficeExtend per un punto di accesso. Tuttavia, è possibile abilitare o disabilitare la latenza del collegamento per un access point specifico. A tale scopo, selezionare (abilitare) o deselezionare (disabilitare) la casella di controllo Abilita latenza collegamento nella scheda Tutti gli access point > Dettagli per [access point selezionato] > Avanzate.

Passaggio 3. Selezionare **Applica**. Dopo aver selezionato Applica, l'access point viene ricaricato.

Passaggio 4. Dopo che l'access point si è unito nuovamente al WLC, è in modalità OEAP.

Nota: Si consiglia di configurare la sicurezza dell'join AP (comunemente definita nei criteri AP) in modo che solo gli AP autorizzati possano unirsi al WLC. È inoltre possibile utilizzare il provisioning AP LSC (Locally Significant Certificate).

Passaggio 5. Creare un elenco di controllo di accesso (ACL) FlexConnect per definire il traffico da commutare a livello centrale (Nega) e locale (Autorizza).

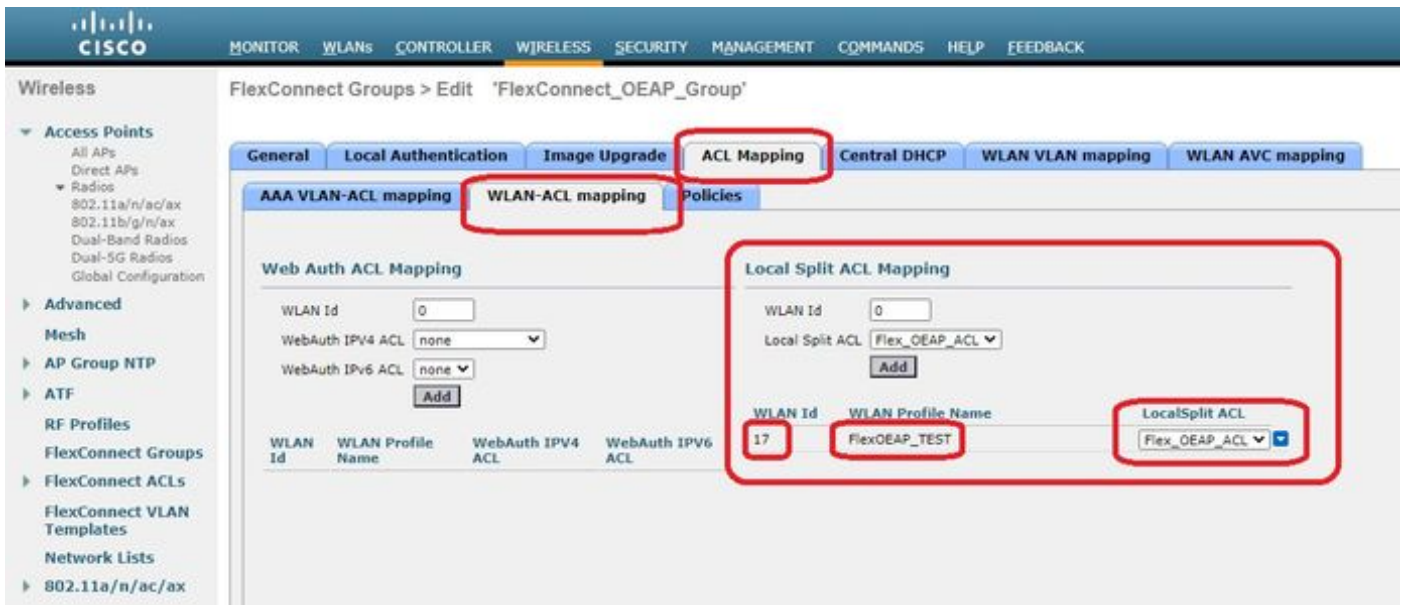
In questo caso, l'obiettivo è passare localmente tutto il traffico alla subnet 192.168.1.0/24.

The screenshot shows the Cisco WLC configuration interface. The top navigation bar includes: MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, FEEDBACK. The left sidebar shows the configuration tree with 'FlexConnect ACLs' selected. The main content area is titled 'FlexConnect ACLs > IPv4 ACL > Edit'. Under the 'General' tab, the 'Access List Name' is 'Flex_OEAP_ACL'. The 'IP Rules' section contains a table with two rules:

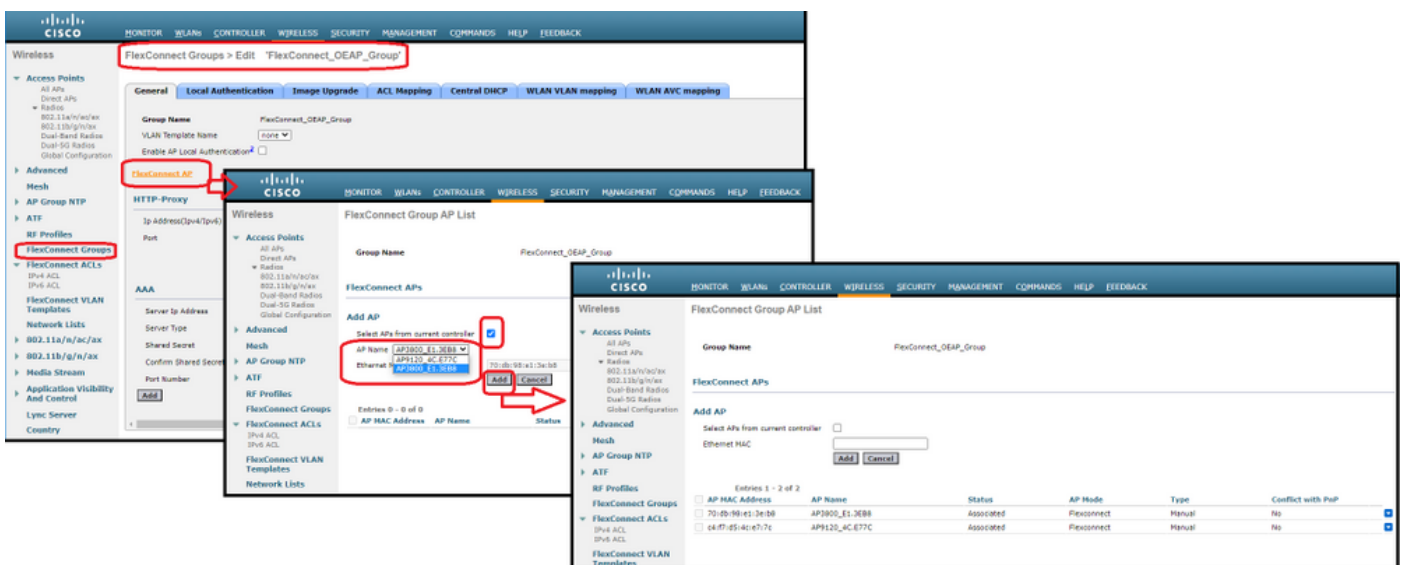
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	192.168.1.0 / 255.255.255.0	Any	Any	Any	Any
2	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any

The 'URL Rules' section is currently empty.

Passaggio 6. Creare un gruppo FlexConnect, andare su **Mapping ACL**, quindi su **Mapping WLAN-ACL**. In "Local Split ACL Mapping", immettere l'ID WLAN e scegliere l'ACL FlexConnect. Quindi fare clic su **Aggiungi**.



Passaggio 7. Aggiungere l'access point al gruppo FlexConnect:



Verifica

1. Verificare lo stato e la definizione dell'ACL di FlexConnect:

```
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. Verificare che la commutazione locale di FlexConnect sia disabilitata:

```
(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. Verificare la configurazione del gruppo 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

```

È possibile acquisire il traffico sull'interfaccia dell'access point per verificare che venga suddiviso sull'access point.

Suggerimento: per risolvere il problema, è possibile disabilitare la crittografia DTLS per visualizzare il traffico di dati incapsulato in capwap.

Nell'esempio di acquisizione di pacchetti viene mostrato il traffico di dati che corrisponde alle istruzioni "deny" dell'ACL dirette al WLC e il traffico di dati che corrisponde alle istruzioni "allow" dell'ACL commutate localmente all'access point:

*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: In scenari normali, l'access point converte gli indirizzi di rete per il traffico commutato localmente perché la subnet client appartiene alla rete aziendale e i dispositivi locali dell'ufficio domestico non sanno come raggiungere la subnet client. L'access point utilizza l'indirizzo IP definito nella subnet dell'ufficio domestico locale per convertire il traffico client.

Per verificare che l'access point abbia eseguito il NAT, è possibile connettersi al terminale dell'access point e usare il comando "**show ip nat translations**". Esempio:

```
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:

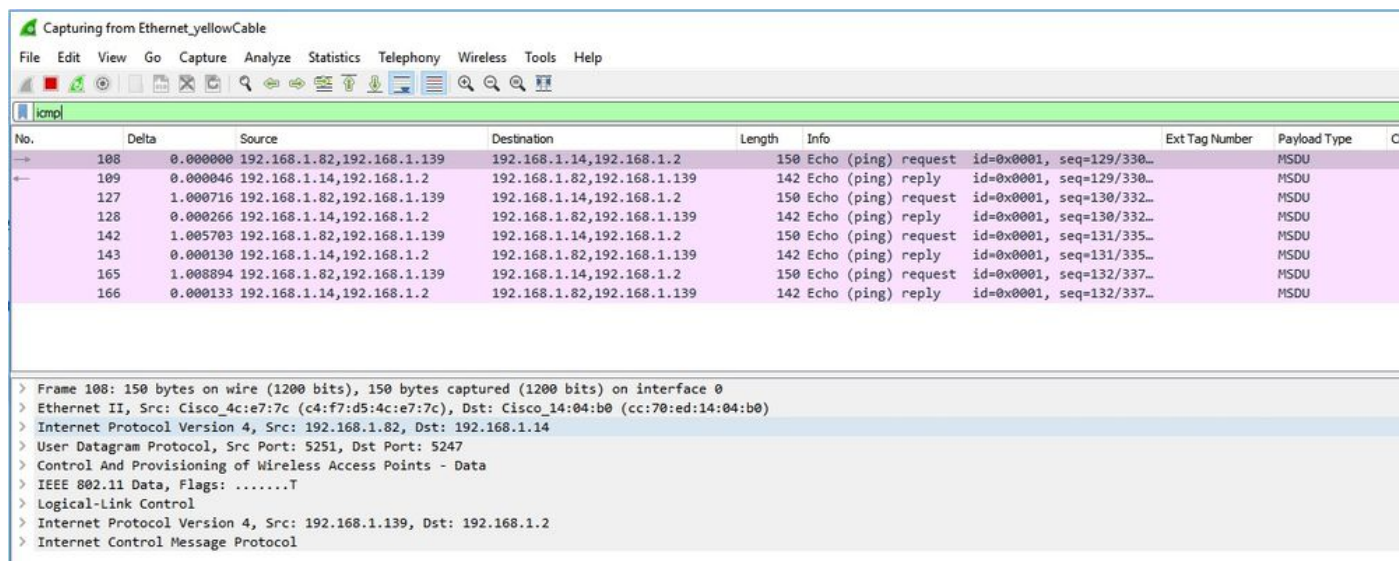
```
(192.168.1.2, 5000, 192.168.1.99, 1223) => (192.168.1.2, 5000, 192.168.1.139, 1223)
```

```
[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
```

Se si rimuove il tunneling suddiviso, tutto il traffico viene commutato centralmente sul WLC. Nell'esempio viene mostrato il protocollo ICMP (Internet Control Message Protocol) sulla destinazione 192.168.1.2, all'interno del tunnel capwap:



The screenshot shows a Wireshark 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 selected packet (No. 108) expanded to show its protocol layers.

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	

The expanded packet details for frame 108 are as follows:

- > 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