# Configurazione di Catalyst 9800 e FlexConnect OEAP Split Tunneling

### Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Panoramica Premesse Configurazione Esempio di rete Configurazioni Definizione di una lista di controllo dell'accesso per il tunneling ripartito Collegamento di un criterio ACL all'ACL definito Configurazione di un criterio di profilo wireless e di un nome ACL MAC diviso Mappatura di una WLAN a un profilo delle policy Configurazione di un profilo di aggiunta AP e associazione con il tag del sito Associazione di un tag di criteri e di siti a un punto di accesso Verifica Documentazione correlata

## Introduzione

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

## Prerequisiti

#### Requisiti

La configurazione di questo documento presume che il WLC sia già configurato in una DMZ con 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:

- Wireless LAN Controller 9800 con software Cisco IOS-XE 17.3.1.
- 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. 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 Cisco OfficeExtend Access Point (Cisco OEAP) fornisce comunicazioni sicure da un WLC Cisco a un Cisco AP in una postazione remota, estendendo senza problemi la WLAN aziendale su Internet fino 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 il punto di accesso 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.

#### Premesse

FlexConnect si riferisce alla capacità di un punto di accesso (AP) di gestire client wireless in postazioni remote, ad esempio su una WAN. Possono anche decidere se il traffico proveniente dai client wireless viene immesso direttamente sulla rete a livello di punto di accesso (switching locale) o se il traffico viene centralizzato sul controller 9800 (switching centrale) e inviato nuovamente sulla WAN, per singola WLAN.

Per informazioni dettagliate su FlexConnect, consultare il documento <u>Understand FlexConnect on</u> <u>Catalyst 9800 Wireless Controller</u>.

La modalità OEAP è un'opzione disponibile in un access point FlexConnect per consentire funzionalità aggiuntive, ad esempio un SSID locale personale per l'accesso a casa, e può anche fornire la funzione di tunneling suddiviso, per una maggiore granularità e definire quale traffico deve essere commutato localmente nell'ufficio di casa e quale traffico deve essere commutato centralmente nel WLC, su una singola WLAN

## Configurazione

Esempio di rete



#### Configurazioni

Definizione di una lista di controllo dell'accesso per il tunneling ripartito

Passaggio 1. Scegliere Configurazione > Sicurezza > ACL. Selezionare Aggiungi.

Passaggio 2. Nella finestra di dialogo Add ACL Setup, immettere il nome dell'ACL, scegliere il tipo di ACL dall'elenco a discesa ACL Type (Tipo ACL), quindi immettere il numero di sequenza nelle impostazioni Rules. Scegliere quindi Azione come Consenti o Nega.

Passaggio 3. Scegliere il tipo di origine richiesto dall'elenco a discesa Tipo di origine.

Se si sceglie il tipo di origine Host, è necessario immettere il nome host/IP.

Se si sceglie il tipo di origine Rete, è necessario specificare l'indirizzo IP di origine e la maschera del carattere jolly di origine.

Nell'esempio, tutto il traffico tra un host e la subnet 192.168.1.0/24 viene commutato centralmente (negazione) e tutto il resto del traffico viene commutato localmente (autorizzazione).

Cisco Cisco	Catalyst 9800-CL Wireless C	Controller	Welcome admin	5000 4 8 8	Search APs and Clients Q
Q Search Menu Itams	Configuration - > Security	-> ACL			
Dashboard	+ Add X Delete	Associate Interfaces			×
	ACL Name*	HomeOffice_ACL	ACL Type	IPv4 Extended	
	Rules				
	> Sequence*	1	Action	deny 🔹	
C Licensing	Source Type	any 🔻			
Y Troubleshooting	Destination Type	Network			
	Destination IP*	192.168.1.0	Destination Wildcard*	0.0.0.255	
	Log	0	DSCP	None	
	+ Add × Delete				
	Sequence ~	<ul> <li>Source IP</li> <li>Wildcard</li> </ul>	Destination ~ Destination IP Wildcard	Protocol ~ Port	Port DSCP v Log v
	⊲ ⊲ 0 ⊳ ⊳	10 🔹 items per page			No items to display
	D Cancel				Apply to Device

Passaggio 4. Selezionare la casella di controllo Registro se si desidera visualizzare i registri e selezionare Aggiungi.

Passaggio 5. Aggiungere le altre regole e selezionare Applica a dispositivo.

🛄 Apps 📙 My 📄 PersonalAdmin 📃 W	VorkAndVac 🧧 WebMons 🔒	Shifts Community PS	HTTS Wir 11AX el	WLC 🚺 DNA 📃 LAB 🛄	Home Lab 🧧 WNBU 🚺 Ad	C »
Cisco Cisco Catalyst	9800-CL Wireless Co	ontroller	Welcome admin 🛛 縃 🤻		Soarch APs and Cliente C	2 🛛
Q. Sisarch Meno Items	nfiguration * > Security * + Add × Delete	ACL     Associate Interfaces				
Ad	ld ACL Setup					×
C Monitoring	ACL Name*	HomeOffice_ACL	ACL Type	IPv4 Extended 🔹 👻		
Sconfiguration	Rules					
€ Administration →	Sequence*	ī ī	Action	permit 🗸		
C Licensing	Source Type	any				
💥 Troubleshooting	Destination Type	any 👻				
e e e e e e e e e e e e e e e e e e e	Protocol	ahp 🔹				
	.og	0	DSCP	None 🖌		
	+ Add X Delete	1				
	Sequence ~ Action	v IP Source v Wildcard	Destination ~ Destination ~ Wildcard	Protocol ~ Port	Destination ~ Port DSCP ~	Log ~
	O 1 deny	any	192.168.1.0 0.0.0.255	ip None	None None	Enabled
	O 2 permit	any	any	ip None	None None	Disabled
	4 4 1 ⊨ ⊨	10 🔻 items per page			1 - 2 of	2 items
	Cancel				Apply to	Device

Collegamento di un criterio ACL all'ACL definito

Passaggio 1. Creare un nuovo profilo Flex. Andare a Configurazione > Tag e profili > Flex.

selezionare Aggiungi.

Passaggio 2. Inserire un nome e abilitare OEAP. Inoltre, verificare che l'ID della VLAN nativa sia quello indicato sulla porta dello switch AP.

Cisco Cata	lyst 9800-CL	Wireless Controller			Welcome admin	* * 8 0 3	0 C See	Parat Cleme Q
Conference of the second secon	Configuration + Add Flex Pr C TagoFi C default	Tags & Profiles * > Flex     Figure 1 - Flex     Add Flex Profile     General     Local Authentica	tion Policy ACL VLAN	4 Umbrella		×		
<ul> <li>(c) Administration →</li> <li>(c) Licensing</li> <li>(c) Troubleshooting</li> </ul>	18 4 <b>1</b>	Name* Description Nativo VLAN ID HTTP Praxy Part HTTP-Praxy IP Address CTS Policy Inline Tagging SGACL Enforcement CTS Profile Name	HomeOffice_FlexProfile Enter Description   Enter Description     O  O  O  O  O  O  O  O  O  O  O  O	Fatback Radio Shut Flex Rosilient ARP Caching Efficient Image Upgrade Office Extend AP Join Minimum Latency mDNS Flex Profile	O O O O Search or Soliect •			7 - 2 di 2 form
		Cancel				Apply to Device		

**Nota:** Quando si attiva la modalità Office-Extend, anche la crittografia del collegamento viene attivata per impostazione predefinita e non può essere modificata anche se si disattiva la crittografia del collegamento nel profilo di join AP.

Passaggio 3. Passare alla scheda ACL criterio e selezionare Aggiungi. Aggiungere qui l'ACL al profilo e applicarlo al dispositivo.

¢	cisco	Cisco Catalyst 9800-CL Wirel	ess Controller	Welcome admin	*	<b>*</b>	•	3 6	00	
Q	Search Menu h	Configuration * > Ta	ags & Profiles * > Flex							
		Add Flex Profile								×
		General Local Authenticatio	n Policy ACL VLAN	Umbrella						
		ACL Name	Pre / Central Web Auth	Auth URL 🗸						
		O HomeOffice_ACL	Disabled							
© v		4 <b>4 1</b> ▶ ▶  <u>10 v</u> it	ems per page 1 -	1 of 1 items				C		
66		Cancel								Apply to Device

#### Configurazione di un criterio di profilo wireless e di un nome ACL MAC diviso

Passaggio 1. Creare un profilo WLAN. In questo esempio viene utilizzato un SSID denominato HomeOffice con protezione WPA2-PSK.

Passaggio 2. Creare un profilo criteri. Andare a Configurazione > Tag > Criterio e selezionare

Aggiungi. In Generale, assicurarsi che questo profilo sia centralizzato, come mostrato nell'esempio:

Contrib Lines Roma				
cearch wend terns	General Access Policies	QOS and AVC Mobility	Advanced	
Dashboard	A Configur	ing in enabled state will result in loss of	of connectivity for clients associated with	h this profile.
Monitoring >				
Configuration >	Name*	HomeOfficePolicy	WLAN Switching Policy	
Administration	Description	Enter Description	Central Switching	ENABLED
	Status		Central Authentication	ENABLED
licensing	Passive Client	DISABLED	Central DHCP	
Froubleshooting	Encrypted Traffic Analytics	DISABLED	Central Association	DISABLED
	CTS Policy		Flex NAT/PAT	DISABLED
	Inline Tagging	0		
	SGACL Enforcement	0		
	Default SGT	2-65519		

Passaggio 3. All'interno del profilo della policy, accedere a Policy di accesso e definire la VLAN per il traffico da commutare centralmente. I client ricevono un indirizzo IP nella subnet assegnata a questa VLAN.

Q. Search Menu Items	Configur	ation * > Tags & Profi	Edit Policy Profile					
Dashboard	+ Ad	d 🛛 🗙 Delete	General Access Policies RADIUS Profiling	QOS and AVC Mobility	Advanced	WLAN ACL		
Monitoring >	Stat	Policy Profile Nam	HTTP TLV Caching	o		IPv4 ACL	Search or Select	•
Configuration		F	DHCP TLV Caching	0		IPv6 ACL	Search or Select	•
Administration		• • • • • • • •	Global State of Device Classification	Disabled (i)		URL Filters	Search or Select	
X Troubleshooting	14 4	1 🕨 🕪 🔤 10 ,	Local Subscriber Policy Name	Search or Select	•	Post Auth	Search or Select	
			VLAN					
			VLAN/VLAN Group Multicast VLAN	Enter Multicast VLAN	<u> </u>			
							-	

Passaggio 4. Per configurare il tunneling con split locale su un access point, è necessario

verificare che il protocollo DCHP richiesto sia stato abilitato sulla WLAN. In questo modo, il client che si sta associando alla WLAN suddivisa non eseguirà il DHCP. È possibile attivare questa opzione nella scheda Profilo criterio in Avanzate. Selezionare la casella di controllo DHCP IPv4 richiesto. Nelle impostazioni dei criteri Flex della WLAN, selezionare l'ACL MAC suddiviso creato in precedenza dall'elenco a discesa ACL MAC suddiviso. Selezionare Applica a dispositivo:

Cisco Catalys	st 9800-CL Wireless Cont	roller We	elcome admin 🛛 🌴 🐔 💾 🕯	0000	Search APs and Clients Q
Q Search Menu Items	Configuration * > Tags & Profil	Edit Policy Profile			×
	+ Add × Delete	Idle Threshold (bytes)	0	User Defined (Priva	ite) Network
Dashboard		Client Exclusion Timeout (sec)	Ø 60	Status	0
Monitoring >	Status ~ Policy Profile Nam	Guest LAN Session Timeout	0	Status	0
2	O O HomeOfficePolic	DHCP		Drop Unicast	U
Configuration >	O 🔮		-	Umbrella	
O Administration		IPv4 DHCP Required	•	Umbrella Parameter Map	Not Configured
C Licensing		DHCP Server IP Address			Clear
NG Tranklashastian		Show more >>>		Flex DHCP Option for DNS	ENABLED
Troubleshooting		AAA Policy		DNS Traffic Redirect	IGNORE
		Allow AAA Override	o	WLAN Flex Policy	
		NAC State	0	VLAN Central Switch	ing Ø
		Policy Name	default-aaa-policy x	Split MAC ACL	HomeOffice_ACU x v
		Accounting List	Search or Select 🔹	Air Time Fairness P	Policies
				2.4 GHz Policy	Search or Select
				5 GHz Policy	Search or Select
		D Cancel			Update & Apply to Device

**Nota:** Affinché il tunneling suddiviso funzioni, i client Apple iOS devono impostare l'opzione 6 (DNS) nell'offerta DHCP.

#### Mappatura di una WLAN a un profilo delle policy

Passaggio 1. Scegliere Configurazione > Tag e profili > Tag. Nella scheda Criterio selezionare Aggiungi.

Passaggio 2. Immettere il nome del Tag Policy e in WLAN-POLICY Maps scheda, selezionare Add.

Passaggio 3. Selezionare il profilo WLAN dall'elenco a discesa Profilo WLAN e scegliere il profilo Policy dall'elenco a discesa Profilo policy. Selezionare l'icona Tick, quindi Applica al dispositivo.

Cisco Cisco	o Catalyst 9	9800-C	CL Wireless Contr	oller 🛛 🕅	elcome admin 🛛 🐐		O C Snarch APs and	Clients Q
Q. Search Menu items	Cor	nfiguratio	on* > Tags & Profile	s* > Tags				
Dashboard	Pol	licy	Site RF AP					
Monitoring     Manitoring	-> <mark>-</mark>	+ Add	Add Policy Tag				×	
	>	Polk	Name*	HomeOfficePolicyTag				*
	>	C Locz	Description	Enter Description				
C Licensing		O RLA	V WLAN-POLI	CY Maps: 0			_	
X Troubleshooting		o defa	+ Add × D	Delete				1 - 5 of 5 items
			WLAN Profile		<ul> <li>Policy Profile</li> </ul>		*	
			4 4 0 ⊨ 1	I 10 V items per page		No iti	ems to display	
			Map WLAN and F	Policy				
			WLAN Profile*	HomeOffice	Policy Profile*	HomeOfficePo		
			> RLAN-POLIC	CY Maps: 0				
			Cancel				pply to Device	

#### Configurazione di un profilo di aggiunta AP e associazione con il tag del sito

Passaggio 1. Passare a Configurazione > Tag e profili > AP Join e selezionare Aggiungi. Inserire un nome. È possibile abilitare il protocollo SSH per consentire la risoluzione dei problemi e disabilitarlo in seguito, se non necessario.

Passaggio 2. Scegliere Configurazione > Tag e profili > Tag. Nella scheda Sito selezionare Aggiungi.

Passaggio 3. Inserire il nome del tag della sede, deselezionare Abilita sede locale, quindi selezionare Profilo di aggiunta AP e Profilo flessibile (creato in precedenza) dagli elenchi a discesa. Quindi Applica al dispositivo.

Cisco	Cisco Cataly	/st 9800-1	CL Wireless Controlle	ər	Welcome admin	<b>* *</b> B	* * • *	Search APs and Clients Q	•
Q Search Menu Ite	ms (	Configurati	on * → Tags & Profiles *	> Tags					
Dashboard		Policy	Site RF AP						
Monitoring	×	+ Add	Add Site Tag						×
	>	O Tiag	oc Name*	HomeOficeSite					
() Administratio	n 💦	o defa	Description	Enter Description					
C Licensing			AP Join Profile	HomeOfficeAP	<u>.</u>				
Troubleshoot	ing		Flex Profile	HomeOffice_FlexPro					
			Enable Local Site						
			Cancel	_				Apply to Dev	ice

Associazione di un tag di criteri e di siti a un punto di accesso

Opzione 1. Questa opzione richiede la configurazione di 1 access point alla volta. Andare a Configurazione > Wireless > Access Point. Selezionare il punto di accesso che si desidera spostare nella home office, quindi selezionare i tag della home office. Selezionare Aggiorna e Applica al dispositivo:

Cisco Cat	talyst 9800-CL Wireless Conti	roller	Welcome admin	C 0 0 0 0 0	Search APs and Clients Q	•
Q. Search Menu Items	Configuration * > Wireless * >	Edit AP				×
Dashboard  Monitoring  Configuration	All Access Points Number of AP(s): 1	Admin Status AP Mode Operation Status	ENABLED	Boot Version IOS Version Mini IOS Version	1.1.2.4 17.3.1.9 0.0.0.0	
Image: Construction       Image: Construction         Image: Constret       Image: Construct	AP9120_4C.E77C C0120AXI- B 5 GHz Radios 2.4 GHz Radios	Fabric Status LED State LED Brightness Level CleanAir <u>NSI Key</u> <b>Tags</b>	Disabled  ENABLED  8	CAPWAP Preferred Mode DHCP IPv4 Address Static IP (IPv4/IPv6) Time Statistics Up Time	IPv4 192.168.100.29 0 days 5 hrs 6 mins 48 secs	
	<ul> <li>Dual-Band Radios</li> <li>Country</li> <li>LSC Provision</li> </ul>	A Changing Tags will lose associatio Policy Site RF	Cause the AP to momentarily in with the Controller.       HomeOfficePolicyTat       TiagoOfficeSite       Idefault-rf-tag	Controller Association Latenc	ry 2 mins 41 secs	to Device

Si consiglia inoltre di configurare un controller primario in modo che l'access point conosca l'IP/il nome del WLC da raggiungere una volta distribuito nell'home office. A tale scopo, è possibile modificare il punto di accesso passando direttamente alla scheda Alta disponibilità:

	Name		Managem	ent IP Address (IP	v4/IPv6)		
mary Controller	eWLC-9800-01		192.16	8.1.15		]	
condary Controller							
rtiary Controller						]	
	C. C						
failover priority	1LOW						
failover priority	LOW	•					
allover priority	row	•					
allover priority	LOW	•					
over priority	LOW	•					
failover priority	LOW	•					
allover priority	LOW	•					
failover priority	LOW	•					
failover priority	LOW	•					
failover priority	LOW	•					
fallover priority	LOW	•					
failover priority	LOW	•					
fallover priority	LOW	•					
failover priority	LOW	•					



Opzione 2. Questa opzione consente di configurare più access point contemporaneamente. Selezionare Configurazione > Wireless Setup > Avanzate > Tag AP. Selezionare le etichette create in precedenza e scegliere Applica a dispositivo.

Cisco Catalyst 9800-C	L Wireless Controller		Welcome admin 🛛 🗰 🧒 🕲 🕲 🕲 🕲 🕄 Search Mit and Danie Q
Q. Search Menu tamo	n* > Wireless Setup* > Advance		
Deshboard	) Tome & Probles	+ Tag APs Number of APs: 2 Selected Number of APs: 2	
Configuration > 0	WLAN Profile	AP ~ AP AP ~ Admin ~ Admin ~ Admin ~ Model AP MAC ~ Mode Status	Operation - RF - Hyperfocat Status PolicyTag - Site Tag - Tag Location - Country - Method
Administration >	Policy Profile	AR- AP3805_E13EB8 AP38021. 0027 e335 5a60 Piex Enabled K3	Registered HomeOfficePolicyTag HomeOficeSite default default PT Shared rad
C Leonsing	Policy Tag 🕜 🔳 👔	O AP9120_4C E77C 09120A00 0064 e422 1790 Fiex Disabled	Registered HomeOfficePolicyTag TageOfficeSite default default US Dedicated
Troubleshooting	AP-sori Profile	Tag APs Tags Policy HomeOfficePolicyTa Policy HomeOfficePolicyTa RF default-rf-tag Changing AP Tag(s) will cause associated AP(s) to meco	nect Apply to Device

Gli AP si riavviano e si uniscono nuovamente al WLC con le nuove impostazioni.

### Verifica

Èpossibile verificare la configurazione tramite GUI o CLI. Questa è la configurazione risultante nella CLI:

```
1
ip access-list extended HomeOffice_ACL
1 deny ip any 192.168.1.0 0.0.0.255 log
2 permit ip any any log
1
wireless profile flex HomeOffice_FlexProfile
acl-policy HomeOffice_ACL
office-extend
1
wireless profile policy HomeOfficePolicy
no central association
aaa-override
flex split-mac-acl HomeOffice_ACL
flex vlan-central-switching
ipv4 dhcp required
vlan default
no shutdown
1
wireless tag site HomeOficeSite
flex-profile HomeOffice_FlexProfile
no local-site
!
wireless tag policy HomeOfficePolicyTag
wlan HomeOffice policy HomeOfficePolicy
wlan HomeOffice 5 HomeOffice
security wpa psk set-key ascii 0 xxxxxx
no security wpa akm dot1x
security wpa akm psk
no shutdown
1
```

```
ap 70db.98e1.3eb8
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
ap c4f7.d54c.e77c
policy-tag HomeOfficePolicyTag
site-tag HomeOficeSite
!
```

Controllo configurazione punto di accesso:

eWLC-9800-01#show ap name AP3800\_E1.3EB8 config general Cisco AP Name : AP3800\_E1.3EB8 Cisco AP Identifier : 0027.e336.5a60 . . . MAC Address : 70db.98e1.3eb8 IP Address Configuration : DHCP IP Address : 192.168.1.99 IP Netmask : 255.255.255.0 Gateway IP Address : 192.168.1.254 . . . SSH State : Enabled Cisco AP Location : default location Site Tag Name : HomeOficeSite RF Tag Name : default-rf-tag Policy Tag Name : HomeOfficePolicyTag AP join Profile : HomeOfficeAP Flex Profile : HomeOffice\_FlexProfile Primary Cisco Controller Name : eWLC-9800-01 Primary Cisco Controller IP Address : 192.168.1.15 . . . AP Mode : FlexConnect AP VLAN tagging state : Disabled AP VLAN tag : 0 CAPWAP Preferred mode : IPv4 CAPWAP UDP-Lite : Not Configured AP Submode : Not Configured Office Extend Mode : Enabled

Épossibile connettersi direttamente all'access point e verificare la configurazione:

AP3800\_E1.3EB8#show ip access-lists Extended IP access list HomeOffice\_ACL 1 deny ip any 192.168.1.0 0.0.0.255 2 permit ip any any AP3800\_E1.3EB8#show capwap client detailrcb SLOT 0 Config SSID : HomeOffice Vlan Id : 0 Status : Enabled ... otherFlags : DHCP\_REQUIRED VLAN\_CENTRAL\_SW ... Profile Name : HomeOffice ...

```
AP3800_E1.3EB8#show capwap client config
AdminState : ADMIN_ENABLED(1)
Name : AP3800_E1.3EB8
Location : default location
Primary controller name : eWLC-9800-01
Primary controller IP : 192.168.1.15
Secondary controller name : c3504-01
Secondary controller IP : 192.168.1.14
Tertiary controller name :
ssh status : Enabled
ApMode : FlexConnect
ApSubMode : Not Configured
Link-Encryption : Enabled
OfficeExtend AP : Enabled
Discovery Timer : 10
Heartbeat Timer : 30
```

Di seguito è riportato un esempio di acquisizioni di pacchetti che mostrano il traffico modificato localmente. Il test è stato eseguito effettuando un "ping" tra un client con IP 192.168.1.98 e il server DNS Google, quindi 192.168.1.254. L'ICMP ha origine con l'IP dell'indirizzo IP dell'access point 192.168.1.99 inviato al DNS Google a causa del NAT dell'access point che gestisce il traffico a livello locale. Non è disponibile alcun protocollo icmp per 192.168.1.254 in quanto il traffico viene crittografato nel tunnel DTLS e vengono visualizzati solo i frame dati dell'applicazione.

	*Ethernet_yellowCable												
File	File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help												
4		💿 📘 🖪	X C 9 00 0	≝ 7 <b>8 . . . . . . . . . .</b>									
	imp												
No.	1	Delta	Source	Destination	Length Inf	fo				Ext Tag Number			
	825	0.000000	192.168.1.99	8.8.8.8	74 Ec	ho (ping)	request	id=0x0001,	seq=13/3328				
4	831	0.018860	8.8.8.8	192.168.1.99	74 Ec	ho (ping)	reply	id=0x0001,	seq=13/3328				
	916	0.991177	192.168.1.99	8.8.8	74 Ec	ho (ping)	request	id=0x0001,	seq=14/3584				
	920	0.018004	8.8.8.8	192.168.1.99	74 Ec	ho (ping)	reply	id=0x0001,	seq=14/3584				
	951	1.009921	192.168.1.99	8.8.8	74 Ec	ho (ping)	request	id=0x0001,	seq=15/3840				
	954	0.017744	8.8.8.8	192.168.1.99	74 Ec	ho (ping)	reply	id=0x0001,	seq=15/3840				
	1010	1.000264	192.168.1.99	8.8.8	74 Ec	ho (ping)	request	id=0x0001,	seq=16/4096				
L	1011	0.018267	8.8.8.8	192.168.1.99	74 Ec	ho (ping)	reply	id=0x0001,	seq=16/4096				

Frame 825: 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: 8.8.8.8

> Internet Control Message Protocol

**Nota:** Il traffico che viene commutato localmente è NAT dal punto di accesso perché in scenari normali, la subnet client appartiene alla rete Office e i dispositivi locali dell'ufficio domestico non sanno come raggiungere la subnet client. Il punto di accesso converte il traffico del client utilizzando l'indirizzo IP del punto di accesso che si trova nella subnet dell'ufficio locale.

Èpossibile accedere alla GUI OEAP aprendo un browser e digitando nell'URL l'indirizzo IP dell'access point. Le credenziali predefinite sono admin/admin ed è necessario modificarle all'accesso iniziale.



Dopo aver effettuato l'accesso, è possibile accedere alla GUI:

ahaha	HOME CONFIGURATION	EVENT LOG NETWORK	HELP			Befresh Logout
CISCO		- DIAGNOSTICS				TELEWORKER
AP Info	Home: Summary					
SSID						
Client	General Information					
onen	AP Name	AP3800_E1.3EB8				
	AP IP Address	192.168.1.99				
	AP Mode	FlexConnect				
	AP MAC Address	70:db:98:e1:3e:b8				
	AP Uptime	0 days, 0 hours, 52 minutes, 25 seconds				
	AP Software Version	17.3.1.9				
	WLC Info	[eWLC-9800-01][192.168.1.15]				
	CAPWAP Status	Run				
	WAN Gateway Status	Good				
	AP Statistics					
	Radio	Admin Status	Chan/BW	Tx Power	Pkts In/Out	
	2.4 GHz	Enabled	1/20MHz	14d8m	22338/145430	
	5 GHz	Enabled	36/40MHz	18dBm	0/0	
	LAN Port					
	Port No	Admin Status	Port Type	Link Status	Pkts In/Out	
	1	Disabled	Local	Blocked	0/0	
	2	Disabled	Local	Blocked	0/0	
	3	Disabled	Local	Blocked	0/0	
	4	Disabled	Local	Blocked	0/0	
	62010 - 2016 Casco Systems Inc. Al nytha reserved.					

Èpossibile accedere alle informazioni tipiche di un OEAP, come le informazioni dell'access point, gli SSID e i client connessi:

cisco	Номе	CONFIGURATION	EVENT_LOG	NETWORK DIAGNOSTICS	HELP			Befresh   Logout TELEWORKER
AP Info	Associatio	on						Show all
5510	Local Clier	ate						
Client	Client MAC		Client IP		WLAN SSID	Radio/LAN	Association Time	Pkts In/Out
	Corporate	Clients						
	Client MAC		Client IP		WLAN SSID	Radio/LAN	Association Time	Pkts In/Out
	98:22:EF:D4	:D1:09	192.168.1.98		HomeOffice	2.4GHz	00d:00h:00m:19s	46/2
	82010 - 2016 Cisco Sy	stems inc. All rights reserved.						

## Documentazione correlata

Informazioni su FlexConnect su Catalyst 9800 Wireless Controller

Tunneling ripartito per FlexConnect

Configurazione di OEAP e RLAN su Catalyst 9800 WLC