Configuración de la Tunelización Dividida de Catalyst 9800 y FlexConnect OEAP

Contenido

Introducción **Prerequisites** Requirements **Componentes Utilizados Overview Antecedentes** Configurar Diagrama de la red Configuraciones Definición de una Lista de Control de Acceso para la Tunelización Dividida Vinculación de una Política ACL a la ACL Definida Configuración de una Política de Perfil Inalámbrico y un Nombre MAC ACL Dividido Asignación de una WLAN a un Perfil de Política Configuración de un Perfil de Unión AP y Asociación con la Etiqueta del Sitio Asociación de una etiqueta de política y una etiqueta de sitio a un punto de acceso Verificación Documentación relacionada

Introducción

Este documento describe cómo configurar un punto de acceso interior (AP) como FlexConnect Office Extend (OEAP) y cómo habilitar la tunelización dividida para que pueda definir qué tráfico se puede conmutar localmente en la oficina doméstica y qué tráfico se debe conmutar centralmente en el WLC.

Prerequisites

Requirements

La configuración en este documento asume que el WLC ya está configurado en una DMZ con NAT habilitado 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.

- Wireless LAN Controllers 9800 que ejecuta Cisco IOS-XE 17.3.1 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. 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 punto de acceso Cisco OfficeExtend (Cisco OEAP) proporciona comunicaciones seguras desde un Cisco WLC a un Cisco AP en una ubicación remota, ampliando sin problemas 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.

Antecedentes

FlexConnect hace referencia a la capacidad de un punto de acceso (AP) para gestionar clientes inalámbricos mientras se trabaja en ubicaciones remotas, por ejemplo, a través de una WAN. También pueden decidir si el tráfico de los clientes inalámbricos se coloca directamente en la red en el nivel AP (conmutación local) o si el tráfico se centraliza en el controlador 9800 (conmutación central) y se envía de vuelta a través de la WAN, por WLAN.

Consulte este documento <u>Comprender FlexConnect en el controlador inalámbrico Catalyst 9800</u> para obtener información detallada sobre FlexConnect.

El modo OEAP es una opción disponible en un punto de acceso FlexConnect, para permitir funcionalidad adicional, por ejemplo, un SSID local personal para el acceso doméstico, y también puede proporcionar una función de tunelización dividida, para obtener una mayor granularidad para definir qué tráfico debe conmutarse localmente en la oficina doméstica y qué tráfico debe conmutarse centralmente en el WLC, a través de una sola WLAN

Configurar

Diagrama de la red



Configuraciones

Definición de una Lista de Control de Acceso para la Tunelización Dividida

Paso 1. Elija Configuration > Security > ACL. Seleccione Agregar.

Paso 2. En el cuadro de diálogo Add ACL Setup (Agregar configuración de ACL), introduzca el nombre de la ACL, elija el tipo de ACL en la lista desplegable ACL Type (Tipo de ACL) y, en Rules settings (Parámetros de reglas), introduzca el número de secuencia. A continuación, elija la acción como permit o deny.

Paso 3. Elija el tipo de origen requerido en la lista desplegable Tipo de Origen.

Si elige el tipo de origen como Host, debe introducir el nombre de host/IP.

Si elige el tipo de origen como Red, debe especificar la dirección IP de origen y la máscara de comodín de origen.

En este ejemplo, todo el tráfico desde cualquier host a la subred 192.168.1.0/24 se conmuta centralmente (deny) y todo el resto del tráfico se conmuta localmente (permit).

Cisco Catal	yst 9800-CL Wireless C	Controller	Welcome admin		Search APs and Clients Q
Q. Search Menu Items	Configuration* > Security	-> ACL			
Dashboard	+ Add X Delete	Associate Interfaces			
	Add ACL Setup				× .
Monitoring >	ACL Name*	HomeOffice_ACL	ACL Type	IPv4 Extended	
Configuration	Rules				
(c) Administration →	Sequence*	1	Action	deny 🔹	
© Licensing	Source Type	any			
X Troubleshooting	Destination Type	Network			
	Destination IP*	192.168.1.0	Destination Wildcard*	0.0.0.255	
	Protocol	Ip 💌			
	Log	Ø	DSCP	None	
	+ Add × Delete				
	Sequence ~ Action	✓ Source IP ✓ Source ✓ Wildcard	Destination · Destination IP Wildcard	 Source ~ Protocol ~ Port 	Port DSCP v Log v
	4 4 0 b b	10 🔻 items per page			No items to display
	Cancel				Apply to Device

Paso 4. Marque la casilla de verificación Registro si desea los registros y seleccione Agregar.

Paso 5. Agregue el resto de las reglas y seleccione Aplicar al dispositivo.

🛄 Apps 🦲 My 📒 PersonalAdmin	📙 WorkAndVac 📒 WebMons 📙	Shifts 📙 Community 📙 PS	HTTS 📴 Wir 🛄 11AX 🚺 el	WLC 🚺 DNA 🛄 LAB 🛄	Home Lab 🛄 WNBU 📃 AC 🛛 😕
Cisco Cata	lyst 9800-CL Wireless Cr	ontroller	Welcome admin 🛛 縃 🤻		Soarch APs and Cliente Q
Q. Search Menu Items	Configuration * > Security *	> ACL			
Daabhaard	+ Add × Detete	Associate Interfaces			
Dashboard	Add ACL Setup				×
Monitoring >	ACL Name*	HomeOffice_ACL	ACL Type	IPv4 Extended 🔹 👻	
Configuration	Rules				
Administration	Sequence*		Action	permit 🔹	
© Licensing	Source Type	any			
X Troubleshooting	Destination Type	any 🔹			
	Protocol	ahp 🔹			
	Log	0	DSCP	None	
	+ Add × Delete				
	Sequence ~ Action	Source ~ Source ~ ~ IP 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
	H 4 1 H H	10 🔹 items per page			1 - 2 of 2 items
	S Cancel				Apply to Device

Vinculación de una Política ACL a la ACL Definida

Paso 1. Cree un nuevo perfil flexible. Vaya a Configuration > Tags & Profiles > Flex. seleccione Agregar.

Paso 2. Introduzca un nombre y active OEAP. Además, asegúrese de que el ID de VLAN nativo sea el del switchport de AP.

Cisco Catalyst 9800-Cl	. Wireless Controller			Welcome admin	1 0 B 7 N	0 C Search Africa	Cares Q (P
Configuration C	Tags & Profiles * > Flow	ation Policy ACL VLAN	Umbrella		×		
Administration Licensing Troubleshooting	Name* Description Native VLAN ID HTTP Praxy Port HTTP-Praxy IP Address CTS Policy Inline Tagging SGACL Enforcement GTS Profile Name	HomeOffice_FlexProfile Enter Description 1 0 0.0.0.0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	Falback Realio Shut Flex Realient ARP Caching Efficient Image Upgrade Office Extend AP Join Minimum Latency mDNS Flex Profile	C C C C C C C C C C C C C C C C C C C			
	3 Cancel				Apply to Device		

Nota: Cuando habilita el modo Office-Extend, el Link-Encryption también se habilita de forma predeterminada y no se puede cambiar aunque inhabilite Link Encryption en el AP Join Profile.

Paso 3. Vaya a la ficha Policy ACL (Política de ACL) y seleccione Add (Agregar). Aquí agregue la ACL al perfil y aplíquela al dispositivo.

¢	cisco	Cisco Catalyst 9800-CL Wirele	ss Controller	Welcome admin	* *	. 8	• 3	02	
0	Search Menu It	Configuration * > Tag	Is & Profiles * > Flex						
		Add Flex Profile							×
		General Local Authentication	Policy ACL VLAN	Umbrella					
			Pre A	uth URL 🗸					
		HomeOffice_ACL	Disabled						
C		4 4 1 ▶ ▶ 10 ↓ iter	ns per page 1 -	1 of 1 items					
×		D Cancel						ľ	Apply to Device

Configuración de una Política de Perfil Inalámbrico y un Nombre MAC ACL Dividido

Paso 1. Cree un perfil WLAN. En este ejemplo, se utilizó un SSID denominado HomeOffice con seguridad WPA2-PSK.

Paso 2. Cree un perfil de política. Vaya a Configuration > Tags > Policy y seleccione Add . En General, asegúrese de que este perfil sea una política conmutada centralmente como se muestra en este ejemplo:

Search Menu Items	General Access Policies	QOS and AVC Mobility	Advanced	
Dashboard	A Config	uring in enabled state will result in loss	of connectivity for clients associated wi	th this profile.
	Name*	HomeOfficePolicy	WLAN Switching Policy	
	Description	Enter Description	Central Switching	
	Status Passive Client		Central Authentication Central DHCP	ENABLED
	Encrypted Traffic Analytics	DISABLED	Central Association	DISABLED
	CTS Policy		Flex NAT/PAT	DISABLED
	Inline Tagging	0		
	SGACL Enforcement	0		
	Default SGT	2-65519		

Paso 3. Dentro del perfil de política, vaya a Políticas de acceso y defina la VLAN para que el tráfico se conmute centralmente. Los clientes obtienen una dirección IP en la subred asignada a esta VLAN.

Cisco Cataly	yst 9800-CL Wireless Con	troller Weld	come admin 🛛 🕷 📽 🖺 🏟 🔯 🥝	C Search APs and Clients Q
Q, Search Menu Items	Configuration • > Tags & Prof	Edit Policy Profile	OOS and AVC Mobility Advanced	×
Dashboard	+ Add × Delete Status × Policy Profile Nam	RADIUS Profiling	0	WLAN ACL
Monitoring >		HTTP TLV Caching	0	IPv4 ACL Search or Select
Configuration >	O ⊘ F	DHCP TLV Caching	0	IPv6 ACL Search or Select 🔹
O Administration	C C Finglinian and	WLAN Local Profiling		URL Filters
C Licensing	IA A 1 P PI 10	Global State of Device Classification	Disabled (1)	Pre Auth Search or Select 👻
X Troubleshooting		Local Subscriber Policy Name	Search or Select	Post Auth Search or Select 👻
		VLAN		
		VLAN/VLAN Group	default	
		Multicast VLAN	Enter Multicast VLAN	
		Cancel		Update & Apply to Device

Paso 4. Para configurar la tunelización dividida local en un AP, debe asegurarse de haber habilitado el DCHP requerido en la WLAN. Esto asegura que el cliente que se asocia con la WLAN dividida haga DHCP. Puede activar esta opción en el perfil de política en la ficha Opciones avanzadas. Active la casilla de verificación IPv4 DHCP Required. En la configuración de la política flexible de WLAN, elija la ACL MAC dividida creada anteriormente en la lista desplegable Dividir ACL MAC. Seleccione Aplicar al dispositivo:

Cisco Cisco	Catalyst 9800-CL Wireless C	ontroller Welcome admin	A TO D O C Search APs and Clients Q
Q. Search Menu Items	Configuration * > Tags & P	rofil Edit Policy Profile	×
	+ Add × Delete	Idle Threshold (bytes)	User Defined (Private) Network
Dashboard	Status y Policy Profile	Client Exclusion Timeout (sec) 60	Status O
		Guest LAN Session Timeout	Drop Unicast
	B S HomeOfficePe	DHCP	Umbrella
	0 0	IPv4 DHCP Required	
205 Administration		DHCP Server IP Address	Umbrella Parameter Map
C Licensing		0	Flex DHCP Option
💥 Troubleshooting		Show more >>>	for DNS
		AAA Policy	DNS Traffic Redirect
		Allow AAA Override Ø	WLAN Flex Policy
		NAC State O	VLAN Central Switching
		Policy Name default-aaa	-policy x Split MAC ACL HomeOffice_ACU x
		Accounting List Search or S	elect 🔹 🛈 Air Time Fairness Policies
			2.4 GHz Policy Search or Select 🔹
			5 GHz Policy Search or Select V
		Cancel	Update & Apply to Device

Nota: Los clientes Apple iOS necesitan que la opción 6 (DNS) se configure en la oferta DHCP para que funcione la tunelización dividida.

Asignación de una WLAN a un Perfil de Política

Paso 1. Elija Configuration > Tags & Profiles > Tags. En la ficha Política, seleccione Agregar.

Paso 2. Introduzca el nombre de la política de etiquetas y, en la ficha WLAN-POLICY Maps (Mapas de POLÍTICA WLAN), seleccione Add (Agregar).

Paso 3. Elija el perfil WLAN de la lista desplegable Perfil WLAN y elija el perfil de política de la lista desplegable Perfil de política. Seleccione el icono Marcar y, a continuación, Aplicar al dispositivo.

Cisco Catalyst 9800-	-CL Wireless Controller	Welcome admin 🛛 🔗 🐔	B & D O C Snarch	APs and Dirents Q
Q Search Menu Itams	tion * > Tags & Profiles * > Tags			
Dashboard	Site RF AP			_
(Monitoring ,	Add Policy Tag		×	
Configuration	Name* HomeOfficePolicyT	ag		~
(i) Administration	Description Enter Description			
C Licensing O RL	WLAN-POLICY Maps: 0			
Troubleshooting	a Add × Delete			1 - 5 of 5 items
	WLAN Profile	 Policy Profile 	~	
	i≪ ≪ 0 ⊨ ⊨i 10 v items ;	ber page	No items to display	
	Map WLAN and Policy			
	WLAN Profile* HomeOffice	Policy Profile*	HomeOfficePolicy	
	RLAN-POLICY Maps: 0			
	Cancel		Apply to Device	

Configuración de un Perfil de Unión AP y Asociación con la Etiqueta del Sitio

Paso 1. Vaya a Configuration > Tags & Profiles > AP Join y seleccione Add . Introduzca un nombre. Opcionalmente, puede habilitar SSH para permitir la resolución de problemas y después desactivarla si no es necesario.

Paso 2. Elija Configuration > Tags & Profiles > Tags. En la ficha Sitio, seleccione Agregar.

Paso 3. Ingrese el nombre de la etiqueta del sitio, desmarque Enable Local Site (Activar sitio local) y, a continuación, seleccione el perfil de conexión de AP y el perfil flexible (creado antes) en las listas desplegables. A continuación, aplique al dispositivo.

	co Catalys	t 9800-	-CL Wireless Controll	er	Welcome admin	* * *	 Search APa and Clients Q	
Q. Search Menu Items		Configura	tion * > Tags & Profiles *	> Tags				
Dashboard		Policy	Site RF AP					
Monitoring		+ A(Add Site Tag					×
	*	O Tia	ge Name*	HomeOficeSite				
	~	O de	fau Description	Enter Description				
C Licensing			AP Join Profile	HomeOfficeAP				
Y Troubleshooting			Flex Profile	HomeOffice_FlexPro				
			Fabric Control Plane Na					
			Cancel				Apply to Dev	ice

Asociación de una etiqueta de política y una etiqueta de sitio a un punto de acceso

Opción 1. Esta opción requiere que configure 1 AP a la vez. Vaya a Configuration > Wireless > Access Points (Configuración > Tecnología inalámbrica > Puntos de acceso). Seleccione el AP que desea mover al Home Office y luego seleccione las Etiquetas del Home Office. Seleccione Actualizar y Aplicar al dispositivo:

Cisco Cataly	st 9800-CL Wireless Contr	oller	Welcome admin 🛛 倄	C O Ø \$ 4 8 7	Search APs and Clients Q	•
Q Search Menu Items	Configuration * > Wireless * >	Edit AP				×
Dashboard Monitoring Monitoring Configuration Administration Configuration	All Access Points Number of AP(s): 1 AP Name AP Model AP9120_4C.E77C B 1 1 1 1 1 1 1 1 1 1 1 1	Admin Status AP Mode Operation Status Fabric Status LED State LED Brightness Level	ENABLED	Boot Version IOS Version Mini IOS Version IP Config CAPWAP Preferred Mode DHCP IPv4 Address Static IP (IPv4 /IPv6)	1.1.2.4 17.3.1.9 0.0.0.0 IPv4 192.168.100.29	
X Troubleshooting	> 5 GHz Radios	CleanAir <u>NSI Key</u>		Time Statistics		- 1
	2.4 GHz RadiosDual-Band Radios	Tags Changing Tags will c lose association	ause the AP to momentarily with the Controller.	Up Time Controller Association Later	0 days 5 hrs 6 mins 48 secs ncy 2 mins 41 secs	
	> Country	Policy	HomeOfficePolicyTat +)		- 1
	LSC Provision	Site RF	TiagoOfficeSite • default-rf-tag •	J		
and the second se		Cancel			🗄 Update & Apply to	Device

También se recomienda configurar un controlador primario para que el AP conozca la IP/Nombre del WLC para alcanzar una vez que se implementa en el Home Office. Puede hacer esto editando el AP directamente a la pestaña Alta Disponibilidad:

General	Interfaces	High Availability	Inventory BLE ICap Advanced	
		Name	Management IP Address (IPv4/IPv6)	
Primary Contro	Hor eW	.C-9800-01	192.168.1.15	
Secondary Cor	ntroller			
Tertiary Contro	iller			
AP failover pric	ority Low	•		

Opción 2. Esta opción le permite configurar varios AP simultáneamente. Vaya a Configuration > Wireless Setup > Advanced > Tag AP. Seleccione las etiquetas creadas anteriormente y seleccione Aplicar al dispositivo.

Update & Apply to Device

⁵ Cancel

Cisco Catalyst 9800-	CL Wireless Controller		Welcome admin 🖌 🤻 🖺 🔕 🕃 😡 😂 Seven Min and Davis Q
Q. Search Menu tants	ion* > Wireless Setup* > Advance		
Deshboard	n) Tags & Prohiles	+ Tog APs Number of APs: 2 Selected Number of APs: 2	
Configuration > 0	WLAN Profile	O AP Name - Model AP MAC - Mode Status	Operation - Policy Tag - Site Tag - Tag Location - Country - Method
Administration	Policy Profile	AP3800_E1.3EB8 AP38021. 0027.e336.5a80 Fiex Enabled K9	Registered HomeOfficePolicyTag HomeOfficeSite default default PT Shared rad rf-tag location PT Shared rad
C Licensing	Policy Tag 🧳 🔳 👔	AP9120_40_E770 B Dtabled	Registered HomeOfficePolicyTag TiageOfficeSte default default US Dedicated rt-tag location US Dedicated
Troubleshooting	AP-Join Profile Pers Profile Set Trg IF Profile SF Trg Apply Trg APa	Tag APS Tags Policy HomeOfficePolicyTat BF default-rf-tag • Changing AP Tag(s) will cause associated AP(s) to recon	viect Apply to Device

Los APs se reinician y se reunen al WLC con las nuevas configuraciones.

Verificación

Puede verificar la configuración mediante GUI o CLI. Esta es la configuración resultante en CLI:

```
!
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
!
wireless profile flex HomeOffice_FlexProfile
acl-policy HomeOffice_ACL
office-extend
!
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
!
wireless tag site HomeOficeSite
flex-profile HomeOffice_FlexProfile
no local-site
!
wireless tag policy HomeOfficePolicyTag
wlan HomeOffice policy HomeOfficePolicy
1
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 !

Verificación de la configuración de AP:

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 . . .

Puede conectarse directamente al AP y también verificar la configuración:

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
. . .
```

Este es un ejemplo de capturas de paquetes que muestran el tráfico conmutado localmente. Aquí, la prueba realizada fue un "ping" de un cliente con IP 192.168.1.98 al servidor DNS de Google y luego a 192.168.1.254. Puede ver el ICMP originado con la IP de la dirección IP AP 192.168.1.99 enviada al DNS de Google debido a que el AP NATing el tráfico localmente. No hay icmp a 192.168.1.254 porque el tráfico se cifra en el túnel DTLS y sólo se ven tramas de datos de aplicación.

```
*Ethernet_yellowCable
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools
                                                                     Help
🛋 🔳 🧟 💿 📙 🛅 🕱 📴 🤇 🗢 🗢 🕾 🗿 🖢 🚍 🔍 Q, Q, 🏨
icmp
       Delta
                                                   Destination
                                                                                                                                       Ext Tag Number
No.
                   Source
                                                                                  Length
                                                                                         Info
    825 0.000000 192.168.1.99
                                                                                       74 Echo (ping) request id=0x0001, seq=13/3328...
                                                   8.8.8.8
   831 0.018860 8.8.8.8
916 0.991177 192.168
                                                                                                            id=0x0001, seq=13/3328...
                                                   192.168.1.99
                                                                                       74 Echo (ping) reply
          0.991177 192.168.1.99
                                                   8.8.8.8
                                                                                       74 Echo (ping) request id=0x0001, seq=14/3584...
         0.018004 8.8.8.8
                                                  192.168.1.99
                                                                                       74 Echo (ping) reply
                                                                                                              id=0x0001, seq=14/3584...
    920
   951 1.009921 192.168.1.99
                                                   8.8.8.8
                                                                                       74 Echo (ping) request id=0x0001, seq=15/3840...
   954
         0.017744 8.8.8.8
                                                  192,168,1,99
                                                                                       74 Echo (ping) reply
                                                                                                              id=0x0001, seq=15/3840...
   1010
         1.000264 192.168.1.99
                                                   8.8.8.8
                                                                                       74 Echo (ping) request id=0x0001, seq=16/4096...
  1011 0.018267 8.8.8.8
                                                  192.168.1.99
                                                                                       74 Echo (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: El tráfico que se conmuta localmente es NATed por el AP porque en escenarios normales, la subred del cliente pertenece a la red de Office y los dispositivos locales en la oficina doméstica no saben cómo alcanzar la subred del cliente. El AP traduce el tráfico del cliente usando la dirección IP AP que está en la subred de la oficina local.

Puede acceder a la GUI de OEAP abriendo un navegador y escribiendo la URL de la dirección IP de AP. Las credenciales predeterminadas son admin/admin y debe cambiarlas en el inicio de sesión inicial.

C C A Not secure 192.168.1.99	
	ahaha
	CISCO
	OfficeExtend Access Point
	Welcome! Please click the login button to enter your user name and password
	Login
	© 2016 - 2019 Cisco Systems, Inc. All rights reserved. Cisco, the Cisco logo, and Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in
	the united states and certain other countries. All third party trademarks are the property of their respective owners.

Una vez que inicie sesión, tendrá acceso a la GUI:

ahaha		EVENT LOG	NETWORK	UCID				Befresh Logout
CISCO	Boar Contrologiton	Eveni_coo	DIAGNOSTICS	Berty				TELEWORKER
AP Info	Home: Summany							
	Home: Summary							
SSID								
Cilent	General Information							
	AP Name AP3800_E1.3EB8							
	AP IP Address	192.108.1.99						
	AP Mode	FlexConnect	sinect					
	AP MAC Address	AP Lintime 0 days 0 hours 52 minu		2				
	AP Optime	where Version 17.3 t 0						
	WLC Info [eWLC-9800-01][192.168.1.15]							
	CADWAD Status	Run Good						
	WAN Gateway Status							
	and standard and							
	AP Statistics	101010-0000			Contraction of the Contraction o	29233301		
	Radio Admin Status		C	han/BW	Tx Power	Pkts In/Out		
	2.4 GHz	Enabled		1,	2001H2	14d8m	22338/145430	
	5 GHZ	Enabled		3	o/40MHz	1808m	0/0	
	LAN Port							
	Port No	Admin Stat	tus	P	ort Type	Link Status	Pkts In/Out	
	1	Disabled		Lo	scal	Blocked	0/0	
	2	Disabled		L	ocal	Blocked	0/0	
	3	Disabled		L	scal	Blocked	0/0	
	4	Disabled		L	ocal	Blocked	0/0	
	62010 - 2016 Cisco Systems Inc. All rights reserved.							

Tiene acceso a información típica en un OEAP, como información de AP, SSID y clientes conectados:

cisco	HOME	CONFIGURATION	EVENT_LOG	NETWORK DIAGNOSTICS	Herb			Refresh Logout TELEWORKER
AP Info SSID	Associatio	on						Show all
Client	Local Clier Client MAC	nts	Client IP		WLAN SSID	Radio/LAN	Association Time	Pkts In/Out
	Corporate Client MAC	Clients	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
	62010 - 2016 Cisco Sy	stems inc. All rights reserved.						

Documentación relacionada

Introducción a FlexConnect en el controlador inalámbrico Catalyst 9800

Tunelización dividida para FlexConnect

Configuración de OEAP y RLAN en el WLC Catalyst 9800