Configuration de la tunnellisation fractionnée OEAP Catalyst 9800 et FlexConnect

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Aperçu Informations générales Configuration Diagramme du réseau Configurations Définition d'une liste de contrôle d'accès pour la transmission tunnel partagée Liaison d'une stratégie de liste de contrôle d'accès à la liste de contrôle d'accès définie Configuration d'une stratégie de profil sans fil et d'un nom de liste de contrôle d'accès MAC partagée Mappage d'un WLAN à un profil de stratégie Configuration d'un profil de jointure AP et association avec la balise de site Fixation d'une balise de stratégie et d'une balise de site à un point d'accès Vérification Documentation associée

Introduction

Ce document décrit comment configurer un point d'accès intérieur (AP) en tant que FlexConnect Office Extend (OEAP) et comment activer la transmission tunnel partagée afin que vous puissiez définir quel trafic peut être commuté localement au bureau à domicile et quel trafic doit être commuté centralement au WLC.

Conditions préalables

Conditions requises

La configuration de ce document suppose que le WLC est déjà configuré dans une DMZ avec NAT activé et que l'AP est capable de rejoindre le WLC depuis le bureau à domicile.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

• Contrôleurs LAN sans fil 9800 exécutant le logiciel Cisco IOS-XE 17.3.1.

- Points d'accès Wave1 : 1700/2700/3700 .
- Points d'accès Wave2 : Gammes 1800/2800/3800/4800 et Catalyst 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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Aperçu

Un point d'accès Cisco OfficeExtend (Cisco OEAP) fournit des communications sécurisées d'un WLC Cisco à un point d'accès Cisco sur un site distant, étendant de manière transparente le WLAN d'entreprise via Internet à la résidence d'un employé. L'expérience de l'utilisateur au bureau à domicile est exactement la même que celle du bureau de l'entreprise. Le chiffrement DTLS (Datagram Transport Layer Security) entre le point d'accès et le contrôleur garantit que toutes les communications ont le niveau de sécurité le plus élevé. Tout point d'accès intérieur en mode FlexConnect peut agir en tant qu'OEAP.

Informations générales

FlexConnect désigne la capacité d'un point d'accès (AP) à gérer des clients sans fil lorsqu'ils fonctionnent sur des sites distants, par exemple, sur un WAN. Ils peuvent également décider si le trafic des clients sans fil est directement placé sur le réseau au niveau du point d'accès (commutation locale) ou si le trafic est centralisé sur le contrôleur 9800 (commutation centrale) et renvoyé sur le WAN, par WLAN.

Consultez ce document <u>Comprendre FlexConnect sur le contrôleur sans fil Catalyst 9800</u> pour obtenir des informations détaillées sur FlexConnect.

Le mode OEAP est une option disponible dans un point d'accès FlexConnect, pour permettre des fonctionnalités supplémentaires, par exemple, un SSID local personnel pour l'accès domestique, et peut également fournir une fonctionnalité de tunnellisation partagée, pour une granularité plus grande pour définir le trafic devant être commuté localement au bureau à domicile et le trafic devant être commuté centralement au WLC, sur un seul WLAN

Configuration

Diagramme du réseau



Configurations

Définition d'une liste de contrôle d'accès pour la transmission tunnel partagée

Étape 1. Choisissez Configuration > Security > ACL. Sélectionnez Ajouter.

Étape 2. Dans la boîte de dialogue Ajouter une configuration de liste de contrôle d'accès, saisissez le nom de la liste de contrôle d'accès, sélectionnez le type de liste dans la liste déroulante Type de liste de contrôle d'accès et, sous les paramètres Règles, saisissez le numéro de séquence. Choisissez ensuite l'action comme autorisation ou refus.

Étape 3. Choisissez le type de source requis dans la liste déroulante Type de source.

Si vous choisissez le type source comme Hôte, vous devez entrer le nom d'hôte/l'adresse IP.

Si vous choisissez le type de source comme Réseau, vous devez spécifier l'adresse IP source et le masque générique source.

Dans cet exemple, tout le trafic de n'importe quel hôte vers le sous-réseau 192.168.1.0/24 est commuté de manière centralisée (deny) et tout le reste du trafic est commuté localement (permit).

	o Catalyst 9800-CL Wireless C	Controller	Welcome admin		Search APs and Clients Q
Q Search Menu Items	Configuration * > Security	-> ACL			
Dashboard	+ Add × Delete	Associate Interfaces			
Monitoring	Add ACL Setup 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	
	Protocol				
		0	DSCP	None	
	Sequence ~	Source ~	Destination · Destination	- Source - I	Destination ~
	Action	 ✓ Source IP ✓ Wildcard 10 ✓ Items per page 	IP Wildcard	Protocol ~ Port	Port DSCP v Log v No items to display
	D Cancel				Apply to Device

Étape 4. Cochez la case Log (Journal) si vous souhaitez afficher les journaux, puis sélectionnez Add (Ajouter).

Étape 5. Ajoutez le reste des règles et sélectionnez Appliquer au périphérique.

🛄 Apps 📙 My 📙 PersonalAdmin	📙 WorkAndVac 📒 WebMons 📒	Shifts 📙 Community 📙 PS	HTTS 📙 Wir 🛄 11AX 🛄 e	WLC 🚺 DNA 📒 LAB 📙	Home Lab 🧧 WNBU 📃 AC 🛛 🛸
Cisco Catal	yst 9800-CL Wireless C	ontroller	Welcome admin 🛛 🐐 🤻		Search APs and Cliente Q
Q. Snarch Menu Items	Configuration * > Security *	ACL			
	+ Add × Delete	Associate Interfaces			
Dashboard	Add ACL Setup				×
Monitoring >	ACL Name*	HomeOffice_ACL	ACL Type	IPv4 Extended 🔹 👻	
Configuration >	Rules				
O 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 → Wildcard 	Destination ~ Destination ~ Wildcard	Protocol v 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
	∈ ∈ 1 ⊨ ⊨ [10 🔻 items per page			1 - 2 of 2 items
	Cancel				Apply to Device

Liaison d'une stratégie de liste de contrôle d'accès à la liste de contrôle d'accès définie

Étape 1. Créez un profil flexible. Accédez à Configuration > Tags & Profiles > Flex. sélectionnez

Ajouter.

Étape 2. Entrez un nom et activez OEAP. Vérifiez également que l'ID de VLAN natif est celui du port de commutation AP.

Cisco Catalyst 9800	-CL Wireless Controller			Welcome admin	e e a ≉ a	0 C Search Alls and Claren	Q
Configur Configur Dashboard Monitoring	tion * > Tagis & Profiles * > Fler	ation Policy ACL VLAN	Umbrella		×		
Configuration	1 Name* Description Native VLANID HTTP Proxy IP Address CTS Policy Inline Tagging SGACL Enforcement CTS Profile Name	HomeOffice_FlexProfile Enter Description	Falback Radio Shut Flex Resilient ARP Caching Efficient Image Upgrade Office Extend AP Join Minimum Latency mDNS Flex Profile	0 0 0 0 0 0			1 - 2 of 2 horn
	Cancel				Apply to Device		

Note: Lorsque vous activez le mode Office-Extend, le chiffrement de liaison est également activé par défaut et ne peut pas être modifié même si vous désactivez le chiffrement de liaison dans le profil de jointure AP.

Étape 3. Accédez à l'onglet Liste de contrôle d'accès de stratégie et sélectionnez Ajouter. Ajoutez la liste de contrôle d'accès au profil et appliquez-la au périphérique.

¢	cisco	Cisco Catalyst 9800-CL	Wireless Controller	Welcome admin	*	•	• 0	0	8	
٩	Search Menu It	Configuration	* > Tags & Profiles * > Flex							
		Add Flex Profile								×
G		General Local Authe	ntication Policy ACL VLAN	Umbrella						
Z,			Pre /	Auth URL 🗸						
Ś		ACL Name HomeOffice_ACL	Central Web Auth Filter Disabled	t.						
C		4 4 1 ⊨ ⊨ 10	tems per page 1 -	1 of 1 items						
X		Cancel							8 A	Apply to Device

Configuration d'une stratégie de profil sans fil et d'un nom de liste de contrôle d'accès MAC partagée

Étape 1. Créez un profil WLAN. Dans cet exemple, il a utilisé un SSID nommé HomeOffice avec la sécurité WPA2-PSK.

Étape 2. Créez un profil de stratégie. Accédez à Configuration > Tags > Policy et sélectionnez Add. Sous Général, assurez-vous que ce profil est des stratégies commutées de manière centralisée comme indiqué dans cet exemple :

irch Menu items	General Access Polic	cies QOS and AVC Mobility	Advanced	
	A C	onfiguring in enabled state will result in los	is of connectivity for clients associated w	th this profile.
	Name*	HomeOfficePolicy	WLAN Switching Policy	
ministration >	Description	Enter Description	Central Switching	
	Status		Central Authentication	
	Passive Client Encrypted Traffic Analy	DISABLED DISABLED	Central DHCP Central Association	ENABLED DISABLED
	CTS Policy		Flex NAT/PAT	DISABLED
	Inline Tagging	O		
	SGACL Enforcement	o		
	Default SGT	2-65519		

Étape 3. Dans le profil de stratégie, accédez à Politiques d'accès et définissez le VLAN pour le trafic à commuter de manière centralisée. Les clients obtiennent une adresse IP dans le sous-réseau attribué à ce VLAN.

Cisco Cataly	/st 9800-CL	_ Wireless Contr	roller Wei	lcome admin 🛛 🗌 🐔 😭	¢ 🖲 O	C Search	APs and Clients Q	•
Q. Search Menu Items	Configuration	 Tags & Profil 	Edit Policy Profile	COS and AVC Mobility	Advenced			×
Dashboard	+ Add	× Delete	RADIUS Profiling	QUS and AVC MODILITY	Advanced	WLAN ACL		
Monitoring >		Policy Profile Nam	HTTP TLV Caching	o		IPv4 ACL	Search or Select	T•
Configuration >	0 0	F,	DHCP TLV Caching	0		IPv6 ACL	Search or Select	•
Administration	0 0	Faragination add	Global State of Device	Disabled ①		URL Filters		
C Licensing	I4 4 1	▶ ⊪ 10 •	Classification Local Subscriber Policy Name	Search or Select 🔹		Pre Auth	Search or Select	
o w			VLAN		١	Post Autri	Stoll bill for Science	
			VLAN/VLAN Group	default	J			
			Multicast VLAN	Enter Multicest VLAN				
			Cancel				🗄 Update & Apply	to Device

Étape 4. Pour configurer la transmission tunnel partagée locale sur un point d'accès, vous devez vous assurer que vous avez activé DCHP Required sur le WLAN. Cela garantit que le client associé au WLAN partagé fait le DHCP. Vous pouvez activer cette option dans le profil de stratégie sous l'onglet Avancé. Activez la case à cocher IPv4 DHCP Required. Sous Paramètres de stratégie flexible WLAN, sélectionnez la liste de contrôle d'accès MAC fractionnée créée précédemment dans la liste déroulante Liste de contrôle d'accès MAC fractionnée. Sélectionnez Appliquer au périphérique :

Cisco Cataly	yst 9800-CL Wireless Cont	roller We	elcome admin 🛛 縃 📽 🖺 🐇	000	Search APs and Clients Q
O Search Menu Items	Configuration * > Tags & Profil	Edit Policy Profile			×
	+ Add X Delete	Idle Threshold (bytes)	0	User Defined (Priva	te) Network
Dashboard		Client Exclusion Timeout (sec)	Ø 60		0
	Status v Policy Profile Nam	Guest LAN Session Timeout	0	Status	0
				Drop Unicast	0
Configuration >		DHCP		Umbrella	
(O) Administration	0	IPv4 DHCP Required	0	Umbrella	Not Configured
		DHCP Server IP Address		Parameter Map	Clear
CLICENSING	≪ 1 ⊨ ⊨ 10 •	Show more >>>		Flex DHCP Option for DNS	ENABLED
X Troubleshooting				DND T	(Change)
		AAA Policy		Redirect	I DINURE
		Allow AAA Override	0	WLAN Flex Policy	
		NAC State	O	VLAN Central Switchi	ng 🖸
		Policy Name	default-aaa-policy x	Split MAC ACL	HomeOffice_ACU x v
		Accounting List	Search or Select 🔹	Air Time Fairness P	olicies
				2.4 GHz Policy	Search or Select
				5 GHz Policy	Search or Select
		Cancel			Update & Apply to Device

Note: Les clients Apple iOS ont besoin de l'option 6 (DNS) à définir dans l'offre DHCP pour que la tunnellisation partagée fonctionne.

Mappage d'un WLAN à un profil de stratégie

Étape 1. Choisissez Configuration > Tags & Profiles > Tags. Dans l'onglet Stratégie, sélectionnez Ajouter.

Étape 2. Saisissez le nom de la stratégie de balise et sous l'onglet WLAN-POLICY Maps, sélectionnez Ajouter.

Étape 3. Choisissez le profil WLAN dans la liste déroulante WLAN Profile et choisissez le profil Policy dans la liste déroulante Policy Profile. Sélectionnez l'icône de sélection, puis Appliquer au périphérique.

Cisco Cisco	o Catalyst 9	9800-C	L Wireless Contro	viler v	Velcome admin	e 🛛 🕈 🕅	0 C Search APs an	d Dilema Q
Q. Search Menu kems	Cor	nfiguratio	in * > Tags & Profiles	* > Tags				
Dashboard	Pol	licy	Site RF AP					_
(C) Monitoring	-> <mark>-</mark>	+ Add	Add Policy Tag				×	
	>	Polk	Name*	HomeOfficePolicyTag				*
	>		Description	Enter Description				
C Licensing		O RLA	V WLAN-POLIC	CY Maps: 0			_	
X Troubleshooting		o defa	+ Add × Da	alete			_	1 - 5 of 5 items
			WLAN Profile		 Policy Profile 		~	
			4 4 0 ⊨ ⊨	I 10 v items per page		No	tems to display	
			Map WLAN and P	olicy				
			WLAN Profile*	HomeOffice	Policy Profile*	HomeOffice	Policy	
			> RLAN-POLIC	Y Maps: 0				
			Cancel			(B /	Apply to Device	

Configuration d'un profil de jointure AP et association avec la balise de site

Étape 1. Naviguez jusqu'à Configuration > Tags & Profiles > AP Join et sélectionnez Add. Saisissez un nom. Vous pouvez éventuellement activer SSH pour autoriser le dépannage et, ultérieurement, le désactiver si nécessaire.

Étape 2. Choisissez Configuration > Tags & Profiles > Tags. Dans l'onglet Site, sélectionnez Ajouter.

Étape 3. Entrez le nom de la balise de site, décochez Activer le site local, puis sélectionnez le profil de jointure AP et le profil flexible (créés avant) dans les listes déroulantes. Appliquez ensuite au périphérique.

e dialo	Cisco Catal	lyst 9800-0	CL Wireless Controller		Welcome admin	# 10 13	0 0 0 0	Search APa and Clients Q	•
Q. Search Menu	Items	Configuratio	n * > Tags & Profiles * >	Tags					
Dashboard		Policy	Site RF AP						
Monitoring	,	+ Add	Add Site Tag						×
	on 🔸	D Tiago	Name*	HomeOficeSite					
	tion 🔉	O defa	Description	Enter Description					
C Licensing			AP Join Profile	HomeOfficeAP					
Troublesho	ooting		Flex Profile	HomeOffice_FlexPro					
			Fabric Control Plane Name	0					
			Cancel					Apply to Devi	ice

Fixation d'une balise de stratégie et d'une balise de site à un point d'accès

Option 1. Cette option nécessite que vous configuriez 1 point d'accès à la fois. Accédez à Configuration > Wireless > Access Points. Sélectionnez le point d'accès à déplacer vers le bureau à domicile, puis sélectionnez les balises du bureau à domicile. Sélectionnez Mettre à jour et appliquer au périphérique :

Cisco Cata	alyst 9800-CL Wireless Contr	oller	Welcome admin	500 0 4 a 7	Search APs and Clients Q	
Q. Search Menu Items	Configuration * > Wireless * >	Edit AP				×
Image: Dashboard Image: Dashboard	All Access Points Number of AP(s): 1 AP Name AP Model AP9120_4C.E77C B C B C C B C C C C C C C C C C C	Admin Status AP Mode Operation Status Fabric Status LED State LED Brightness Level CleanAir <u>NSI Key</u>	ENABLED	Boot Version IOS Version Mini IOS Version IP Config CAPWAP Preferred Mode DHCP IPv4 Address 1 Static IP (IPv4/IPv6)	1.1.2.4 17.3.1.9 0.0.0.0 Pv4 192.168.100.29	
	> 5 GHZ RAdios	Tags		Time Statistics		- 1
	 2.4 GHz Radios Dual-Band Radios 	Changing Tags will o	cause the AP to momentarily n with the Controller.	Up Time Controller Association Latency	0 days 5 hrs 6 mins 48 secs 2 mins 41 secs	
	> Country	Policy	HomeOfficePolicyTas	ר		
	LSC Provision	Site RF	TiagoOfficeSite	J		
		Cancel			Update & Apply to	Device

Il est également recommandé de configurer un contrôleur principal de sorte que le point d'accès connaisse l'adresse IP/nom du WLC à atteindre une fois qu'il est déployé dans le bureau à domicile. Vous pouvez modifier le point d'accès directement en accédant à l'onglet Haute disponibilité :

	Name		Management IP	Address (IPv4/	1Pv6)	
Primary Controller	eWLC-9800-01		192.168.1.1	5		
Secondary Controller						
Tertiary Controller						
AP failover priority	Low					
Charles and the state of the second state of t		1.1.1				



Option 2. Cette option vous permet de configurer plusieurs points d'accès simultanément. Accédez à Configuration > Wireless Setup > Advanced > Tag APs. Sélectionnez les balises créées précédemment et sélectionnez Appliquer au périphérique.

Cisco Catalyst 9800-CL Wit	reless Controller			Nelcome admin 📔 🐐 🤻 🖺	0 0 0 0	Search Alls and Chem. Q	
Q. Search Menu Itama	Wreless Setup* > Advanced	_					
Dashboard Star	* + 1sg Number of A Selected Ma	s 2 ber of APs 2					
Configuration > 0	Tags & Profiles	AP ~ Nodel AP M	AP ~ Admin ~	Operation - Statua Policy Tag -	Site Tag - Tag	Location ~ Country ~	Hyperlocat Method
Administration	Policy Profile	AIR- _E1.3EB8 AP38021, 0027. K9	e336.5a60 Flex Enabled	Registered HomeOfficePolicyTag	HomeOficeSite default- rf-tag	default pt location	Shared rad
C Licensing	Policy Tag / D AP91:	4C.E77C 0 0064	e422 1790 Flex Disabled	Registered HomeOfficePolicyTag	TagoOfficeSite default - rt-tag	default US	Dedicated :
Troubleshooting	AP Join Profile	Tag APs Tags Policy Site Changing AP Tags	HameOfficePolicyTa HomeOfficePolicyTa default=rf-tag (s) will cause associated AP(s) to reconn	ect			

Les AP redémarrent et rerejoignent le WLC avec les nouveaux paramètres.

Vérification

Vous pouvez vérifier la configuration via l'interface utilisateur graphique ou l'interface de ligne de commande. Voici la configuration résultante dans l'interface de ligne de commande :

```
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
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
!
```

Vérification de la configuration du point d'accès :

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

Vous pouvez vous connecter directement au point d'accès et vérifier également la configuration :

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
```

Voici un exemple de capture de paquets montrant le trafic commuté localement. Ici, le test effectué était un ping d'un client avec IP 192.168.1.98 vers le serveur DNS de Google, puis vers 192.168.1.254. Vous pouvez voir l'ICMP provenant de l'adresse IP de l'AP 192.168.1.99 envoyée au DNS Google en raison de la NAT de l'AP qui effectue le trafic localement. Il n'y a pas de icmp vers 192.168.1.254, car le trafic est chiffré dans le tunnel DTLS et seules les trames de données d'application sont vues.

4	*Ethernet_yellowCable											
File	Edit	View Go	Capture Analyz	ze Statistics Telephony Wirel	ess Tools Help							
4		💿 📙 🔚	े 🗙 🖸 🤉 👄	🗢 🕾 T 🛓 📃 🔍 🤆	Q. 🖳 🎹							
i i	imp											
No.	C	Delta	Source	Destination		Length	Info					Ext Tag Number
7*	825	0.000000	192.168.1.99	8.8.8.8		74	Echo	(ping)	request	id=0x0001,	seq=13/3328	
4-	831	0.018860	8.8.8.8	192.168.1	.99	74	Echo	(ping)	reply	id=0x0001,	seq=13/3328	
	916	0.991177	192.168.1.99	8.8.8.8		74	Echo	(ping)	request	id=0x0001,	seq=14/3584	
	920	0.018004	8.8.8.8	192.168.1	.99	74	Echo	(ping)	reply	id=0x0001,	seq=14/3584	
	951	1.009921	192.168.1.99	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	
5	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

Note: Le trafic qui est commuté localement est NATed par le point d'accès, car dans des scénarios normaux, le sous-réseau du client appartient au réseau Office et les périphériques locaux du bureau à domicile ne savent pas comment atteindre le sous-réseau du client. Le point d'accès traduit le trafic client à l'aide de l'adresse IP du point d'accès qui se trouve dans le sous-réseau du bureau à domicile local.

Vous pouvez accéder à l'interface utilisateur graphique OEAP en ouvrant un navigateur et en tapant l'URL de l'adresse IP AP. Les informations d'identification par défaut sont admin/admin et vous devez les modifier lors de la connexion initiale.



Une fois connecté, vous avez accès à l'interface utilisateur graphique :

սիսիս		NETWORK				Befresh Logout
CISCO	HOME CONFIGURATION	EVENT_LDG DIAGNOSTICS	Here			TELEWORKER
AP Info	Hama: Bumman					
50ID	Home: Summary					
5510	Constal Information					
Client	General Information	403000 51 3550				
	AD ID Address	102 168 1 00				
	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	
		Disabled	Local	Biocked	0/0	
	62010 - 2016 Cisco Systems Inc. All rights reserved					

Vous avez accès aux informations standard d'un OEAP, telles que les informations de point d'accès, les SSID et les clients connectés :

cisco	Номе	CONFIGURATION	EVENT_LOG	NETWORK DIAGNOSTICS	Herb			Refresh Logout TELEWORKER
AP Info SSID	Associatio	on						Show all
Client	Local Clients Client MAC		Client IP		WLAN SSID Rodio/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	:01:09	192.168.1.98		HomeOffice	2.4GHz	00d:00h:00m:19s	46/2
	62010 - 2016 Cisco Sy	stems inc. All rights reserved.						

Documentation associée

Comprendre FlexConnect sur le contrôleur sans fil Catalyst 9800

Fractionnement de la transmission tunnel pour FlexConnect

Configurer OEAP et RLAN sur le WLC Catalyst 9800