使用分割隧道配置FlexConnect OEAP

目錄

<u>驗證</u>

簡介

本文說明如何將室記憶體取點(AP)設定為FlexConnect Office Extend AP(OEAP)模式,以及如何啟 用分割通道,以便您可以定義哪些流量必須在家庭辦公室本地交換,哪些流量必須在無線區域網路 控制器(WLC)集中交換。

作者: Tiago Antunes、Nicolas Darchis Cisco TAC工程師。

必要條件

需求

本檔案中的組態假設已在已啟用網路位址轉譯(NAT)的非軍事區(DMZ)中設定WLC,且AP可從總部加入WLC。

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 使用AireOS 8.10(130.0)軟體的WLC。
- Wave1 AP:1700/2700/3700 .
- Wave2 AP:1800/2800/3800/4800和Catalyst 9100系列。

本文中的資訊是根據特定實驗室環境內的裝置所建立。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

恐觷

OEAP提供從Cisco WLC到遠端位置的Cisco AP的安全通訊,以便通過Internet將公司WLAN擴展到 員工住所。使用者在家庭辦公室中的體驗與在公司辦公室中的體驗完全相同。AP和控制器之間的資 料包傳輸層安全(DTLS)加密可確保所有通訊都具有最高級別的安全性。 FlexConnect模式下的任何 室內AP都可以充當OEAP。

重要事實

- Cisco OEAP設計用於在使用NAT的路由器或其他網關裝置後工作。NAT允許裝置(如路由器)在Internet(公共)和個人網路(私有)之間充當代理,從而允許用單個IP地址代表整個電腦組。您可以在NAT裝置之後部署的Cisco OEAP數量沒有限制。
- •除AP-700I、AP-700W和AP802系列AP外,所有受支援的帶整合天線的室內AP型號均可配置為 OEAP。
- 所有OEAP必須位於同一個AP組中,並且該組包含的無線LAN不能超過15個。在AP組中具有 OEAP的控制器僅向每個連線的OEAP發佈最多15個WLAN,因為它為個人服務集識別符號 (SSID)保留一個WLAN。

設定

網路圖表



組態

WLAN配置

步驟1.建立分配給AP組的WLAN。您無需為此WLAN啟用FlexConnect本地交換選項。

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMAND	DS HELP EEEDBACK
WLANs	WLANs > Edit 'FlexOEAP_TEST'	
VLANS	General Security QoS Policy-Mapping Advanced	
Advanced	MBO State	KTS based CAC Policy Enabled
	Off Channel Scanning Defer	Radius Client Profiling
	Scan Defer Priority 0 1 2 3 4 5 6 7	DHCP Profiling
		HTTP Profiling
	Scan Defer Time(msecs) 100	Local Client Profiling
	FlexConnect	DHCP Profiling
	FlexConnect Local Enabled	HTTP Profiling
	Switching 2 Chables	PMIP
	FlexConnect Local Auth 22 Enabled	PMIP Mobility Type
	Learn Client IP Address 2 🖾 Enabled	PMIP NAI Type Hexadecimal ¥
	Vian based Central Enabled	PMIP Profile
	Central DHCP Processing Enabled	PMIP Realm
	Override DNS Enabled	Universal AP Admin Support
	NAT-PAT Enabled	Universal AP Admin
	Central Assoc Enabled	11v BSS Transition Support

步驟2.建立AP組。在**WLANs**頁籤上,選擇WLAN SSID,然後按一下**Add**以新增WLAN。轉到**APs**頁 籤並**新增** FlexConnect OEAP。

 cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
VLANs	General WLANS RF Profile APs 802.11u Location Ports/Module Intelligent Capture
Advanced AP Groups	Add New
	Add New WLAN SSID FlexOEAP_TEST(17) Interface
	VIAN ID WLAN SSID ⁽²⁾⁽⁶⁾ Interface Group(G) SNMP NAC State
սիսիս cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
VLANS WLANS	General WLANS RF Profile APS 802.11u Location Ports/Module Intelligent Capture
 Advanced AP Groups 	APs currently in the Group Remove APs Add APs to the Group Add APs AP Name Ethernet MAC AP Name Group Name
	AP9120_4C.E77C c4:f7:d5:4c:e7:7c AP3800_E1.3EB8 70:db:98:e1:3e:b8

AP配置

在FlexConnect模式下,AP與控制器關聯後,您可以將其配置為OEAP。

步驟1。AP加入WLC後,將AP模式更改為FlexConnect,然後按一下Apply。

ဂျက်က င၊sco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY M	IANAGEMENT COMMANDS HELP	<u>F</u> EEDBACK
Wireless	All APs > Details f	or AP3800_E1.3EB8		
Access Points All APs	General Crede	ntials Interfaces High Availability	Inventory Advanced I	ntelligent Capture
Direct APs ▼ Radios 802.11a/n/ac/ax	General		Versions	
802.11b/g/n/ax	AP Name	AP3800_E1.3E88	Primary Software Version	8.10.130.0
Dual-SG Radios	Location	default location	Backup Software Version	8.10.120.0
Global Configuration	AP MAC Address	70:db:98:e1:3e:b8	Predownload Status	None
Advanced	Base Radio MAC	00:27:e3:36:5a:60	Predownloaded Version	None
Mesh	Admin Status	Enable ¥	Predownload Next Retry Time	NA
AP Group NTP	AP Mode	local V	Predownload Retry Count	NA
ATF	AP Sub Mode	local ElexConnect	Boot Version	1.1.2.4
RF Profiles	Operational Status	monitor	IOS Version	8.10.130.0
FlexConnect Groups	Port Number	Bridge	Mini IOS Version	0.0.0.0
FlexConnect ACLs	Venue Group	Flex+Bridge SE-Connect	IP Config	
FlexConnect VLAN	Venue Type	Unspecified V	CAPWAP Preferred Mode	Ipv4 (Global Config)
Templates	Add New Venue		DHCP Ipv4 Address	192.168.100.12
Network Lists	Language Name		Static IP (Ipv4/Ipv6)	
802.11a/n/ac/ax	Network Spectrum	3D1781A0FFFC6B2F174A6EF605FB1DF8	Fabric	

步驟2.確保在「High Availability(高可用性)」頁籤中至少配置了一個主WLC:

/ireless	All APs > Details for	AP9120_4C.E770					
Access Points All APs Direct APs	General Credent	ials Interfaces	High Availability	Inventory	FlexConnect	Advanced	Intelligent Capture
Direct APs ▼ Radios 802.11a/n/ac/ax		Name	Ма	nagement IP Ad	dress(Ipv4/Ipv6)		
802.11b/g/n/ax Dual-Band Radios	Primary Controller	c3504-01	19	2.168.1.14			
Dual-5G Radios Global Configuration	Tertiary Controller	6	- i				
Advanced							
Mesh	AP Failover Priority	Low ¥					
AP Group NTP							
ATF							
RF Profiles							
FlexConnect Groups							
FlexConnect ACLs							
FlexConnect VLAN Templates							
Mohumah Liete							

步驟3.轉到FlexConnect頁籤並選中Enable OfficeExtend AP覈取方塊。

	ဂါဂါဂ င၊sco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
W	ireless	All APs > Details for AP3800_E1.3EB8
Ŧ	Access Points All APs	General Credentials Interfaces High Availability Inventory FlexConnect Advanced Intelligent Capture
	 ■ Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios 	VLAN Support Make VLAN AP Specific V Go
	Dual-SG Radios Global Configuration	Inheritance Group-Specific
÷	Advanced Mesh	FlexConnect default-flex-group default-flex-group
÷	AP Group NTP	WILAN AVC Macong
÷	ATF	VLAN Template Name none
	RF Profiles	VLAN Name Id Mappings
	FlexConnect Groups	
÷	FlexConnect ACLs	PreAuthentication Access Control Lists
	FlexConnect VLAN Templates	External WebAuthentication ACLs
	Network Lists	Costel 2017 Acad
×	802.11a/n/ac/ax	Law 240 s
•	802.11b/g/n/ax	
×	Media Stream	OfficeExtend AP
÷	Application Visibility And Control	Enable OfficeExtend AP
	Lync Server	Enable Least Latency Controller Join
	Country	Reset Personal SSID
	Timers	Tunnel Gateway List
. •	Netflow	
	OoS	Total

為AP啟用OfficeExtend模式時,將自動啟用DTLS **Data Encryption**。但是,您可以啟用或禁用特定 AP的DTLS資料加密。為此,請選中(啟用)或取消選中(禁用)所有AP > [選定AP]的詳細資訊 >「高級」頁籤上的**Data Encryption**覈取方塊:

cisco	MONITOR WLA	ans <u>c</u> ontro	ULLER WIRELESS	5 <u>S</u> ECURITY M <u>A</u>	NAGEMENT	C <u>o</u> mmands	HELP	<u>F</u> EEDBACK		
Wireless	All APs > Deta	ails for AP91	120_4C.E77C				-			
 Access Points All APs Direct APs 	General	Credentials	Interfaces	High Availability	Inventory	FlexConn	ect A	Advanced	Network Diagnostics	5 Intelligent Capture
✓ Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Dual-SG Radios Global Configuration	Regulatory D Country Code Cisco Discove AP Group Nai	iomains e ery Protocol me		802.11bg:-/ US (United	A 802.11a:-B States) V		1	Power Over I PoE Status Pre-standa	Ethernet Settings Full and 802.3af switches	Power
Advanced Mesh	Statistics Tim Data Encrypt	ner ion		30				AP Core Dum		
AP Group NTP	Rogue Detect	tion		Global Conf	ig 🗸 🗌		1	AP Core Di	ump 🛄 E iit Config Parameters	nabled
RF Profiles FlexConnect Groups	SSH NSI Ports Sta	ste		AP Specific Global Conf				AP Retrans AP Retrans	mit Count 5 mit Interval 3	
FlexConnect ACLs	TCP Adjust M	ISS (IPv4: 536 -	1363, IPv6: 1220 -	1331) 🖾 1250 TCP MSS	is Globally Enab	led		VLAN Taggin VLAN Tagg	g ing 🗌	Enabled
Templates Network Lists	LED State	el		8 (1-8)	<u>×</u>		1	NTP Server S Status D	Status	
802.11a/n/ac/ax	LED Flash Sta	ite		O <u>0</u> OIndefinite	(1-3600)secon	ds		TrustSec		
Media Stream	USB Module II	D		Disable USB Module				TrustSec C CMX Services	ontig s	
Application Visibility And Control	Override	that up		0				Services S	ub-Services CMX Serve	r Ip
Lync Server	USB Module S			101						

附註:為AP啟用OfficeExtend模式時,將自動禁用Telnet和SSH訪問。但是,您可以啟用或禁 用特定AP的Telnet或SSH訪問。為此,請選中(啟用)或取消選中(禁用)所有AP > [選定 AP]的詳細資訊>「高級」頁籤上的Telnet或SSH覈取方塊。

附註:為AP啟用OfficeExtend模式時,會自動啟用鏈路延遲。但是,您可以啟用或禁用特定 AP的鏈路延遲。要執行此操作,請選中(啟用)或取消選中(禁用)所有AP > [選定AP] > Advanced頁籤的Enable Link Latency覈取方塊。

步驟3.選擇Apply。選擇「應用」後,AP將重新載入。

步驟4. AP重新加入WLC後, AP處於OEAP模式。

附註:我們建議您配置AP加入安全性(通常在AP策略下定義),以便只有經過授權的AP可以 加入WLC。您還可以使用本地重要證書(LSC)AP調配。

步驟5.建立FlexConnect存取控制清單(ACL),定義哪些流量將集中交換(拒絕)和在本地交換(允 許)。

|--|

	ျ၊ျ၊ cisco	MONITOR WLANS CON		WIRELESS SECU	RITY MANAGEMENT	COMMANDS HE	P EEEDBACK				
v	/ireless	FlexConnect ACLs > I	IPv4 ACL >	Edit							
Ĩ	All APs	General									
	V Radios 802.11a/n/ac/ax	Access List Name	flag.)	OBAP_ACL							
	802.11b/g/n/ex Dual-Band Radios Dual-3G Radios	IP Rules									
	Global Configuration	Seq	Action	Source IP/Has	k	Destination IP/	Hask	Protocol	Source Port	Dest Port	DSCP
	Advanced	1	Permit	0.0.0.0	/ 0.0.0.0	192.168.1.0	/ 255.255.255.0	Any	Any	Any	Any 🖬
	Mesh	2	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any 🖸
	AP Group NTP										
	ATF										
	RF Profiles	URL Rules									
0	FlexConnect Groups	Seq Action		Destination	Url						
Ľ	1Pv4 AQL 1Pv6 AQL										
	FlexConnect VLAN										

步驟6.建立FlexConnect組,轉到**ACL對映**,然後轉到**WLAN-ACL對映**。在「本地拆分ACL對映」下 ,輸入WLAN ID並選擇FlexConnect ACL。然後按一下**「Add」。**

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Vireless	FlexConnect Groups > Edit 'FlexConnect_OEAP_Group'
Access Points All APs Direct APs	General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping WLAN AVC mapping
 Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Dual-5G Radios Global Configuration 	AAA VLAN-ACL mapping WLAN-ACL mapping Policies Web Auth ACL Mapping Local Split ACL Mapping
Advanced Mesh	WLAN Id 0 WLAN Id 0 ULAN Id 0 ULAN Id CONTRACT OF CONT
ATF RF Profiles FlexConnect Groups	WebAuth IPv6 ACL none V Add WLAN WLAN Profile WebAuth IPV4 WebAuth IPV6 Id Name ACL ACL ACL Fiex_OEAP_ACL V
FlexConnect ACLs FlexConnect VLAN Templates Network Lists	
802.11a/n/ac/ax	

步驟7. 將AP新增到FlexConnect群組:



驗證

1.驗證FlexConnect ACL狀態和定義:

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 DSCP Action

--- ---- ------

1 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 Any 0-65535 0-65535 Any Deny

2.驗證FlexConnect本地交換是否已禁用:

(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.驗證FlexConnect組配置:

(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

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 您可以在AP介面捕獲流量,以驗證流量是否在AP進行分割。

提示:出於故障排除目的,您可以禁用DTLS加密以檢視封裝在capwap內的資料流量。

此封包擷取範例顯示與導向到WLC的ACL「deny」陳述式相符的資料流量,以及與AP本機上交換的ACL「permit」陳述式相符的資料流量:

*Ethernet_yellowCable

File	Edit View Go	Capture Analyze Statistics T	elephony Wireless Tools Help		
1	🛛 🔬 🛞 🗍 🗄	S C 9 🗢 🗢 🕾 🖡 🎍	🚍 📃 ९, ९, ९, 🎚		
	np				
No.	Delta	Source	Destination	Length Info	Ext Tag Number
+	28859	9.819533 192.168.1.99,192.1	58.1.139 192.168.1.14,8.8.8.8	150 Echo (ping) request	id=0x0001, seq=213/545_
e	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 192.168.1.99,192.1	58.1.139 192.168.1.14,8.8.8.8	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 192.168.1.99,192.1	58.1.139 192.168.1.14,8.8.8.8	150 Echo (ping) request	id=0x0001, seq=215/550_
	28962	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 192.168.1.99,192.1	58.1.139 192.168.1.14,8.8.8.8	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 20059: 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

4	*Ethernet_yellowCabl	le										
File	Edit View Go	Capture	Analyze Statistics Telephony	Wireless Tools	Help							
Æ.	📕 🔬 💿 📃 🛅	XD	९ 🗢 🗢 🕾 🗿 🛓 🚍 🔳	0,0,0,1								
	amp											
No.	Delta		Source	Destination		Length	Info					Ext Tag Numb
	28859	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_	
L	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

附註:在正常情況下,AP會轉換本地交換流量的網路地址,因為客戶端子網屬於辦公室網路 ,而家庭辦公室的本地裝置不知道如何到達客戶端子網。AP使用本地家庭辦公室子網中定義 的IP地址來轉換客戶端流量。

為了驗證AP是否執行了NAT,您可以連線到AP終端機並發出「*show ip nat translations*」命令。範 例:

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

如果移除分割通道,則會在WLC集中交換所有流量。此範例顯示capwap通道中到192.168.1.2目的 地的網際網路控制訊息通訊協定(ICMP):

File E	dit View G	o Capture	Analyze Statistics Telephony V Q @ @ @ 2 1 2 2 2 0 0	Vireless Tools Help Q Q III						
icmp										
No.	Delta	P	Source	Destination	Length	Info				
	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
-	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
	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
	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
	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
	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
	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
	166	0.000133	192,168,1,14,192,168,1,2	192,168,1,82,192,168,1,139	142	Echo	(ning)	reply	id=0x0001.	seg=132/337

Ext Tag Number

Payload Type

MSDU MSDU MSDU MSDU MSDU

MSDU MSDU

MSDU

Ch

> 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