使用分割隧道配置FlexConnect OEAP

目录

<u>简介</u> <u>先决条件</u> <u>要求</u> 使用的组件 概述 重事实 配置 配络图 配置 <u>WLAN 配置</u> <u>光线接入点配置</u> <u>验证</u>

简介

本文档介绍如何将室内接入点(AP)配置为FlexConnect Office Extend AP(OEAP)模式,以及如何启 用分割隧道,以便您可以定义哪些流量必须在家庭办公室本地交换,哪些流量必须在无线局域网控 制器(WLC)集中交换。

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

先决条件

要求

本文档中的配置假设WLC已在启用网络地址转换(NAT)的隔离区(DMZ)中配置,并且AP能够从家庭 办公室加入WLC。

使用的组件

本文档中的信息基于以下软件和硬件版本:

- •WLC,带AireOS 8.10(130.0)软件版本。
- Wave1 AP:1700/2700/3700 的多播地址发送一次邻居消息。
- 第2波AP:1800/2800/3800/4800和Catalyst 9100系列。

本文档中的信息都是基于特定实验室环境中的设备编写的。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

概述

OEAP提供从Cisco WLC到远程位置的Cisco AP的安全通信,以便通过Internet将公司WLAN扩展到 员工住所。用户在家庭办公室的体验与在公司办公室的体验完全相同。AP和控制器之间的数据报传 输层安全(DTLS)加密可确保所有通信都具有最高级别的安全性。 FlexConnect模式下的任何室内 AP都可以充当OEAP。

重要事实

- Cisco OEAP设计为在使用NAT的路由器或其他网关设备后工作。NAT允许设备(如路由器)充当Internet(公有)和个人网络(私有)之间的代理,这使整个计算机组可以用单个IP地址表示。在NAT设备后部署的Cisco OEAP数量没有限制。
- •除AP-700I、AP-700W和AP802系列AP外,所有支持的带集成天线的室内AP型号都可配置为 OEAP。
- 所有OEAP必须位于同一AP组中,且该组必须包含不超过15个无线LAN。AP组中具有OEAP的 控制器仅向每个连接的OEAP发布最多15个WLAN,因为它为个人服务集标识符(SSID)保留一 个WLAN。

配置

网络图



配置

WLAN 配置

步骤1.创建WLAN以分配给AP组。您无需为此WLAN启用FlexConnect本地交换选项。

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS	HELP <u>F</u> EEDBACK
WLANs	WLANs > Edit 'FlexOEAP_TEST'	
VILANS	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	HTTP Profiling
	Switching 2 C Ensoled	PMIP
	FlexConnect Local Auth 12 Enabled	PMIP Mobility Type
	Learn Client IP Address 2 🖾 Enabled	PMIP NAI Type Hexadecimal ¥
	Vlan 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

步骤2.创建AP组。在WLANs选**项**卡上,选择WLAN SSID,然后单击**Add**添加WLAN。转到AP**选项** 卡并添**加**FlexConnect OEAP。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
WLANS	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 management /Interface management SNMP NAC State Enabled Add Cancel
. cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
WLANs 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 APs Name Ethernet MAC Add APs to the Group Name
	AP9120_4C.E77C c4:f7:d5:4c:e7:7c AP3800_E1.3EB8 70:db:98:e1:3e:b8

无线接入点配置

AP在FlexConnect模式下与控制器关联后,可将其配置为OEAP。

步骤1.在AP加入WLC后,将AP模式更改为FlexConnect,然后单击"应用"。

iiliiilii cisco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY	NANAGEMENT COMMANDS HELP	FEEDBACK
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 Electonnect	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	IP Config	
FlexConnect VLAN	Venue Type	Unspecified ¥	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 Interface Key	3D1781A0FFFC6B2F174A6EF605FB1DF8	Fabric	

步骤2.确保在High Availability(高可用性)选项卡中至少配置了主WLC:

/ireless	All APs > Details for	AP9120_4C.E770					
* Access Points All 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		- i				
Advanced							
Mesh	AP Failover Priority	Low ¥					
AP Group NTP							
ATF							
RF Profiles							
FlexConnect Groups							
FlexConnect ACLs							
FlexConnect VLAN Templates							
Mohumah Liete							

步骤3.转到FlexConnect选项卡并选中Enable OfficeExtend AP复选框。

	ာါကျက cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
W	ïreless	All APs > Details for AP3800_E1.3EB8
*	Access Points All APs Direct APs Radios 802.11a/n/ac/ax	General Credentials Interfaces High Availability Inventory FlexConnect Advanced Intelligent Capture
	802.11b/g/n/ax Dual-Band Radios Dual-SG Radios Global Configuration	VLAN Support Make VLAN AP Specific Go
Þ	Advanced	FlexConnect Group Name default-flex-group
Þ	AP Group NTP	WLAN AVC Mapping
÷	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	Central DVCR Procession
×	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

为AP启**用OfficeExtend模**式时,DTLS数据加密将自动启用。但是,您可以启用或禁用特定AP的 DTLS数据加密。为此,请选中(启用)或取消选中(禁用)"所有AP">"[选定AP]的详细信息">"高 级"选项卡上的"数据加密"复选框:

cisco	MONITOR WLANS CONTROLLER WIRELESS SI	ecurity management commands help	P <u>F</u> EEDBACK
Wireless	All APs > Details for AP9120_4C.E77C		
Access Points All APs Direct APs Radios 802 11a/p/ac/ay	General Credentials Interfaces High Regulatory Domains	Availability Inventory FlexConnect 802.11bg:-A 802.11a:-B	Advanced Network Diagnostics Intelligent Capture Power Over Ethernet Settings
802.11b/g/n/ax Dual-Band Radios Dual-5G Radios Global Configuration	Country Code Cisco Discovery Protocol AP Group Name	US (United States) V FlexOEAP_Group V	PoE Status Full Power Pre-standard 802.3af switches Power Injector State
Advanced Mesh	Statistics Timer Data Encryption	30	AP Core Dump
AP Group NTP ATF	Rogue Detection ² Telnet	Global Config 💙	AP Retransmit Config Parameters
RF Profiles FlexConnect Groups	▲ SSH NSI Ports State	AP Specific V	AP Retransmit Count 5 AP Retransmit Interval 3 VI AN Tanging
FlexConnect ACLs FlexConnect VLAN	TCP Adjust MSS (IPv4: 536 - 1363, IPv6: 1220 - 1331) LED State	TCP MSS is Globally Enabled	VLAN Tagging Enabled
Network Lists	LED Brightlevel LED Flash State	8 (1-8) O 0 (1-3600)seconds	Status Disabled
802.11b/g/n/ax Media Stream		⊖Indefinite ©Disable	TrustSec Config
Application Visibility And Control	USB Module ID Override	USB Module	Services Sub-Services CMX Server Ip
Lync Server	USB Module Status		

注意:当您为AP启用OfficeExtend模式时,Telnet和SSH访问会自动禁用。但是,您可以启用 或禁用特定AP的Telnet或SSH访问。为此,请选中(启用)或取消选中(禁用)"所有 AP">"[选定AP]">"高级"选项卡上的"Telnet或SSH"复选框。

注意:为AP启用OfficeExtend模式时,链路延迟会自动启用。但是,您可以启用或禁用特定 AP的链路延迟。要执行此操作,请选中(启用)或取消选中(禁用)All APs > Details for [selected AP] > Advanced选项卡上的Enable Link Latency复选框。

步骤3.选择"应用"。选择应用后,AP将重新加载。

步骤4. AP重新加入WLC后,AP处于OEAP模式。

注意:我们建议您配置AP加入安全(通常在AP策略下定义),以便只有授权AP才能加入WLC。您还可以使用本地有效证书(LSC)AP调配。

步骤5.创建FlexConnect访问控制列表(ACL),以定义将集中交换(拒绝)和本地交换(允许)的流 量。

此处,您的目标是将所有流量本地交换到子网192.168.1.0/24。

	cisco	MONITOR	WLANS C	ONTROLLER	WIRELESS ;	SECURITY MANAGEMENT	COMMANDS HE	LP EEEDBACK				
v	Access Balats	FlexConne	ect ACLs :	> IPv4 ACL >	Edit							
Ť	All APs Direct APs	General										
	 Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios 	IP Rules	ina.	rao,	OBAP_ALL							
	Duel-SG Radios Global Configuration	Seq		Action	Source IP	/Mask	Destination IP/	/Hask	Protocol	Source Port	Dest Port	DSCP
'	Mesh	2		Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any Any	Any	Any Any	Any D
-	AP Group NTP ATF											
	RF Profiles	URL Rules										
ſ	FlexConnect ACLs IPv4 AOL IPv6 ACL	Seq	Action		Dextin	ation Url						
	FlexConnect VLAN											

步骤6.创建FlexConnect组,转到**ACL映射**,然后转**到WLAN-ACL映射**。在"本地拆分ACL映射"下 ,输入WLAN ID,然后选择FlexConnect ACL。然后单击添加。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Wireless	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-SG Radios Global Configuration 	AAA VLAN-ACL mapping WLAN-ACL mapping Policies Web Auth ACL Mapping Local Split ACL Mapping
Advanced Mesh	WLAN Id 0 WEAN Id 0 WebAuth IPV4 ACL none V Local Split ACL
 AP Group NTP ATF RF Profiles FlexConnect Groups 	WebAuth IPv6 ACL none V Add WLAN WLAN Profile WebAuth IPv4 WebAuth IPv6 ACL 17 Flex_OEAP_ACL V
 FlexConnect ACLs FlexConnect VLAN Templates Network Lists 	
▶ 802.11a/n/ac/ax	

步骤7.将AP添加到FlexConnect组:



验证

1.检验FlexConnect ACL状态和定义:

c3504-01) >show flexconnect acl summary

ACL Name Status

----- -----

Flex_OEAP_ACL Applied

(c3504-01) >show flexconnect acl detailed Flex_OEAP_ACL

Source Destination Source Port Dest Port Index IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action

1 0.0.0.0/0.0.0 192.168.1.0/255.255.255.0 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 哈证ElexConnect本地 奇俗目不已林田。

2.验证FlexConnect本地交换是否已禁用:

(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.验证FlexConnect组配置:

(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 您可以捕获AP接口上的流量,以验证流量是否在AP上拆分。

提示:出于故障排除目的,您可以禁用DTLS加密,以便查看封装在capwap中的数据流量。

此数据包捕获示例显示与指向WLC的ACL"deny"语句匹配的数据流量,以及与ACL"permit"语句匹配 的数据流量,这些语句在AP本地交换:

*Ethernet_yellowCable

File	Edit View Go	Capture Analyze Statis	tics Telephony Wireless To-	ols Help					
1	🗖 🧕 🕘 🗍 🗄	S 🖸 🤇 🗢 🗢 😫	Ŧ 🛓 🚍 📃 🍳 🍳 🦉	ž					
k	тр								
No.	Delta	Source	Destinati	n	Length B	nfo			Ext Tag Number
	28859	9.819533 192.168.1.99,	192.168.1.139 192.16	3.1.14,8.8.8.8	150 E	Echo (ping)	request id=00	0001, seq=213/545_	
e	20860	0.019956 192.168.1.14,	8.8.8.8 192.16	3.1.99,192.168.1.139	142 E	<pre>cho (ping)</pre>	reply id=00	0001, seq=213/545	
	20912	0.984274 192.168.1.99,	,192.168.1.139 192.16	8.1.14,8.8.8.8	150 E	icho (ping)	request id=0	0001, seq=214/547_	
	20913	0.018616 192.168.1.14,	8.8.8.8 192.16	3.1.99,192.168.1.139	142 E	Echo (ping)	reply id=00	0001, seq=214/547_	
	20961	0.986005 192.168.1.99,	,192.168.1.139 192.16	8.1.14,8.8.8.8	150 E	icho (ping)	request id=0	0001, seq=215/550	
	20962	0.018343 192.168.1.14,	8.8.8.8 192.16	3.1.99,192.168.1.139	142 E	Echo (ping)	reply id=8x	0001, seq=215/550_	
	21007	0.984777 192.168.1.99,	,192.168.1.139 192.16	3.1.14,8.8.8.8	150 E	icho (ping)	request id=0	0001, seq=216/552	
	21008	0.018309 192.168.1.14,	,8.8.8.8 192.16	3.1.99,192.168.1.139	142 E	Echo (ping)	reply id=80	0001, seq=216/552_	
	21467	9.477613 192.168.1.99	192.16	3.1.254	74 E	Echo (ping)	request id=0	0001, seq=217/555	
	21468	0.000638 192.168.1.254	192.16	3.1.99	74 E	icho (ping)	reply id=00	0001, seq=217/555_	
	21511	1.003331 192.168.1.99	192.16	3.1.254	74 E	Echo (ping)	request id=0)	0001, seq=218/558_	
	21512	0.000192 192.168.1.254	192.16	3.1.99	74 E	icho (ping)	reply id=00	0001, seq=218/558	
	21572	1.009272 192.168.1.99	192.16	3.1.254	74 E	Echo (ping)	request id=0)	00001, seq=219/560_	
	21573	0.000000 192.168.1.254	4 192.16	3.1.99	74 E	<pre>cho (ping)</pre>	reply id=0	0001, seq=219/560.	
	21621	1.002280 192.168.1.99	192.16	3.1.254	74 E	Echo (ping)	request id=0	0001, seq=220/563_	
	21622	0.000374 192.168.1.254	4 192.16	3.1.99	74 E	Echo (ping)	reply id=0	0001, 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	C *Ethernet_yellowCable												
Fil	le Edit View Go	Capture	Analyze Statistics Telephony	Wireless Tools	Help								
1	📕 🙇 💿 📃 🗔	XD	९ 👄 🗢 🕾 🗿 🛓 🚍 🔳	ର୍ ର୍ ଭ୍ 🎹									
	kmp												
No.	Delta		Source	Destination		Length	Info					Ext Tag Numb	
	20859	9.819533	192.168.1.99,192.168.1.139	192.168.1	.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=213/545_		
	20860	0.019956	192.168.1.14,8.8.8.8	192.168.1	.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=213/545_		
	20912	0.984274	192.168.1.99,192.168.1.139	192.168.1	.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=214/547_		
	20913	0.018616	192.168.1.14,8.8.8.8	192.168.1	.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=214/547_		
	20961	0.986005	192.168.1.99,192.168.1.139	192.168.1	.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=215/550_		
	20962	0.018343	192.168.1.14,8.8.8.8	192.168.1	.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=215/550_		
	21007	0.984777	192.168.1.99,192.168.1.139	192.168.1	.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=216/552_		
	21008	0.018309	192.168.1.14,8.8.8.8	192.168.1	.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=216/552_		
+	21467	9.477613	192.168.1.99	192.168.1	.254	74	Echo	(ping)	request	id=0x0001,	seq=217/555_		
+	21468	0.000638	192.168.1.254	192.168.1	.99	74	Echo	(ping)	reply	id=0x0001,	seq=217/555_		
	21511	1.003331	192.168.1.99	192.168.1	.254	74	Echo	(ping)	request	id=0x0001,	seq=218/558		
	21512	0.000192	192.168.1.254	192.168.1	.99	74	Echo	(ping)	reply	id=0x0001,	seq=218/558_		
	21572	1.009272	192.168.1.99	192.168.1	.254	74	Echo	(ping)	request	id=0x0001,	seq=219/560_		
	21573	0.000000	192.168.1.254	192.168.1	.99	74	Echo	(ping)	reply	id=0x0001,	seq=219/560		
	21621	1.002280	192.168.1.99	192.168.1	. 254	74	Echo	(ping)	request	id=0x0001,	seq=220/563_		
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

注意:在正常情况下,AP会转换本地交换流量的网络地址,因为客户端子网属于办公室网络 ,而家庭办公室的本地设备不知道如何到达客户端子网。AP使用本地家庭办公室子网中定义 的IP地址来转换客户端流量。

为了验证AP是否执行了NAT,您可以连接到AP终端并发出"*show ip nat translations"*命令。示例:

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

如果删除分割隧道,则所有流量都在WLC中集中交换。本示例显示在capwap隧道内到 192.168.1.2目的地的Internet控制消息协议(ICMP):

File E	dit View G	o Capture	Analyze Statistics Telephony V Q 🐵 🐵 🕸 🗿 💆 🚍 🧐	Vireless Tools Help						
icmp										
No.	Delta	18	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	(ping)	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