スプリットトンネリングを使用したFlexConnect OEAPの設定

内容

概要 <u>前提条件</u> <u>要件</u> 使用するコンポーネント 概要 重要な事実 <u>設定</u> <u>ネットワーク図</u> 設定 WLAN 設定 <u>AP の設定</u> 確認

概要

このドキュメントでは、FlexConnect Office Extend AP(OEAP)モードとして屋内アクセスポイン ト(AP)を設定する方法と、ホームオフィスでローカルにスイッチングするトラフィックとワイヤ レスLANコントローラ(WLC)で中央でスイッチングするトラフィックを定義する方法について説 明します。

著者: Cisco TACエンジニア、Nicolas Darchis

前提条件

要件

このドキュメントの設定では、WLCがネットワークアドレス変換(NAT)が有効な非武装地帯 (DMZ)にすでに設定されていて、APがホームオフィスからWLCに参加できることを前提としてい ます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- •バージョンAireOS 8.10(130.0)ソフトウェアを搭載したWLC。
- Wave1 AP:1700/2700/3700.
- Wave2 AP:1800/2800/3800/4800、およびCatalyst 9100シリーズ。
- このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド

キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してく ださい。

概要

OEAPは、企業WLANをインターネット経由で従業員の自宅まで拡張するために、Cisco WLCか らリモートロケーションのCisco APへのセキュアな通信を提供します。ホームオフィスでのユー ザエクスペリエンスは、企業オフィスでのユーザエクスペリエンスとまったく同じです。APとコ ントローラ間のDatagram Transport Layer Security(DTLS)暗号化により、すべての通信のセキュ リティが最高レベルになります。 FlexConnectモードの屋内APは、OEAPとして機能できます。

重要な事実

- Cisco OEAPは、NATを使用するルータやその他のゲートウェイデバイスの背後で動作するように設計されています。NATを使用すると、ルータなどのデバイスが、インターネット(パブリック)とパーソナルネットワーク(プライベート)の間のエージェントとして機能し、コンピュータのグループ全体を1つのIPアドレスで表すことができます。NATデバイスの背後に導入できるCisco OEAPの数に制限はありません。
- AP-700I、AP-700W、およびAP802シリーズのAPを除く、統合アンテナを備えたすべての屋 内APモデルをOEAPとして設定できます。
- すべてのOEAPは同じAPグループに属している必要があり、そのグループに含まれるワイヤレスLANは15以下である必要があります。APグループにOEAPを持つコントローラは、パーソナルService Set Identifier(SSID)に1つのWLANを予約するため、接続された各OEAPに対して最大15のWLANのみを公開します。

設定

ネットワーク図



設定

WLAN 設定

ステップ1:APグループに割り当てるWLANを作成します。このWLANのFlexConnectローカルスイッチングオプションを有効にする必要はありません。

ll cisco	MONITOR WLANS CONT	ROLLER WIJRELESS SEC	CURITY MANAGEMENT	COMMANDS	HELP FEEDBACK	_
WLANs	WLANs > Edit 'FlexOE	AP_TEST				
VLANS	General Security	QoS Policy-Mapping	Advanced			
Advanced	MBO State				KTS based CAC Policy	Enabled
	Off Channel Scanning Defe	r			Radius Client Profiling	
	Scan Defer Priority	0 1 2 3 4 5 6 7			DHCP Profiling	0
					HTTP Profiling	
	Scan Defer Time(msecs)	100			Local Client Profiling	
	FlexConnect				DHCP Profiling	0
	FlexConnect Local	Easter			HTTP Profiling	
	Switching 2				PMIP	
	FlexConnect Local Auth	Enabled			PMIP Mobility Type	
	Learn Client IP Address 2	Enabled			PMIP NAI Type	Hexadecimal ¥
	Vlan based Central Switching	Enabled			PMIP Profile	None V
	Central DHCP Processing	Enabled			PMIP Realm	
	Override DNS	Enabled			Universal AP Admin Support	
	NAT-PAT	Enabled			Universal AP Admin	0
	Central Assoc	Enabled			11v BSS Transition Support	

ステップ2:APグループを作成します。[WLANs]タ**ブで**、WLAN SSIDを選択し、[**Add**]をクリック してWLANを追加します。[APs]タブ**に移動**し、[FlexConnect OEAP]を追加します。

،،ا،،،ا،، cısco	MONITOR	<u>W</u> LANs		WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	EEEDBACK
WLANs	Ap Group	os > Edit	'FlexOEAP_	Group'					
VLANs WLANs	General	WLAI	Ns RF Profi	le APs	802.11u	Location	Ports/Module	Inte	lligent Capture
Advanced									Add New
	Add New WLAN S Interfac Group(G	V SSID ce ce 3)	FlexOEAP_TES	ST(17)	✓✓				
	WLAN IC	AC State	Add Car	icel Interface/In	terface Group	(G) SNM	P NAC State		

ll cısco	MONITOR WLANS	ONTROLLER WIRELESS	<u>S</u> ECURITY	MANAGEMENT	COMMANDS	HELP E	EEDBACK	
WLANs	Ap Groups > Edit 'I	FlexOEAP_Group'						
VLANS	General WLANs	RF Profile APs	802.11u	Location F	Ports/Module	Intellig	ent Capture	
 Advanced AP Groups 	APs currently in the	Group	Remove APs	Add APs to	the Group		Ad	d APs
	AP Name	Ethernet MAC		AP Nam	e	Group Nan	ne	
	AP9120_4C.E77C	c4:f7:d5:4c:e7:7c						
	AP3800_E1.3EB8	70:db:98:e1:3e:b8						

AP の設定

APをFlexConnectモードでコントローラに関連付けた後、OEAPとして設定できます。

o

ဂျက်က cisco	MONITOR WLANS	CONTROLLER WIRELESS SECURITY M	ANAGEMENT COMMANDS HELP	<u>F</u> EEDBACK
Vireless	All APs > Details f	or AP3800_E1.3EB8		
Access Points	General Crede	ntials Interfaces High Availability	Inventory Advanced I	ntelligent Capture
	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 Electropert	Boot Version	1.1.2.4
RE Profiles	Operational Status	monitor	IOS Version	8.10.130.0
ElexConnect Groups	Port Number	Bridge	Mini IOS Version	0.0.0.0
ElexConnect ACLs	Venue Group	Flex+Bridge	IP Config	
ElayConnact VI AN	Venue Type	Unspecified V	CAPWAP Preferred Mode	Inv4 (Global Confin)
Templates	Add New Venue		DHCP Invd Address	192 168 100 12
Network Lists	Venue Language Name		Static IP (Ipv4/Ipv6)	
802.11a/n/ac/ax	Network Spectrum	3D1781A0FFFC6B2F174A6EF605FB1DF8	Fabric	0

ステップ2:[High Availability]タブで少なくともプライマリWLCが設定されていることを確認しま す。

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
Wireless	All APs > Details for AP9120_4C.E77C
* Access Points All APs	General Credentials Interfaces High Availability Inventory FlexConnect Advanced Intelligent Capture
Direct APs * Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Dual-SG Radios	Name Management IP Address(Ipv4/Ipv6) Primary Controller c3504-01 Secondary Service 1
Advanced Mesh	AB Exilour Brinth Lon M
 AP Group NTP ATF RF Profiles 	
FlexConnect Groups FlexConnect ACLs FlexConnect VLAN Templates Network Lists	

ステップ3:[FlexConnect]タブに移動し、[**Enable OfficeExtend AP**]チェックボ**ックスをオン**にしま す。

	ဂါဂါဂ င၊sco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
W	ïreless	All APs > Details for AP3800_E1.3EB8
*	Access Points	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 Group Name default-flex-group
÷	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	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	
	005	Total

DTLSデー**タ暗号化**は、APのOfficeExtendモードを有効にすると自動的に有効になります。ただ し、特定のAPに対してDTLSデータ暗号化を有効または無効にできます。有効にするには、[All APs] > [Details for [selected AP] > [Advanced]タブで[**Data Encryption**]チェックボックスをオン (有効)またはオフ(無効)にします。

	cisco	MONITOR Y	WLANS CONTRO	OLLER WIRELESS	<u>s</u> ecurity m <u>a</u>	anagement q	OMMANDS HELP	P <u>F</u> EEDBACK					
W	ireless	All APs > D	etails for AP9	120_4C.E77C									
*	Access Points All APs	General	Credentials	Interfaces	High Availability	Inventory	FlexConnect	Advanced	Advanced Network Diagnostics Intelligent Capt				
	Direct APs Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual Baad Badies	Regulator Country C	ry Domains Code		802.11bg:-	A 802.11a:-B States) 🗸		Power Over PoE Statu	r				
	Dual-SG Radios Global Configuration	Cisco Disc AP Group	covery Protocol Name		FlexOEAP_0	Group 🗸		Pre-stand Power Inj	ard 802.3af switches ector State				
•	Advanced	Statistics	Timer		30			AP Core Dur	np				
	Mesh	Data Encr	ryption					AP Core D	ump	Enable	d		
•	AP Group NTP	Rogue De	etection		0			AP Retransmit Config Parameters					
•	ATF	² Telnet			Global Cont	fig 🗸							
	RF Profiles	2 SSH			AP Specific	•		AP Retran	smit Count				
	FlexConnect Groups	NSI Ports	State		Global Cont	fig 🗸 🖾							
•	FlexConnect ACLs	TCP Adjus	st MSS (IPv4: 536	- 1363, IPv6: 1220 -	1331) 🖾 1250 TCP MSS	is Globally Enable	d	VLAN Taggin	ig aina	Enabl	ed		
	FlexConnect VLAN Templates	LED State	1. 		Enable	~		NTP Server	Status				
	Network Lists	LED Bright	tlevel		8 (1-8)			Status (Disabled				
Þ	802.11a/n/ac/ax	LED Flash	State		0 0	(1-3600)second	s	TrustSec					
	802.11b/g/n/ax				OIndefinite			TrustSec (Config				
	Media Stream				Oisable			CMX Service	s.				
	Application Visibility	USB Modu	le ID		USB Module	1							
	And Control	Override						Services S	ub-services CMX S	erver Ip			
	Lync Server	USB Modu	ile Status		123								

注: TelnetおよびSSHアクセスは、APのOfficeExtendモードを有効にすると自動的に無効に なります。ただし、特定のAPに対してTelnetまたはSSHアクセスを有効または無効にでき ます。そのためには、[All APs] > [Details for [selected AP] > [Advanced]タブで[Telnet]また は[SSH]チェックボックスをオンまたはオフにします。 **注**: APのOfficeExtendモードを有効にすると、リンク遅延が自動的に有効になります。ただ し、特定のAPのリンク遅延を有効または無効にすることができます。そのためには、[All APs] > [Details for [selected AP] > [Advanced]タブの[Enable Link Latency]チェックボックス をオン(有効)またはオフ(無効)にします。

ステップ3:[Apply]を選択します。[Apply]を選択すると、APがリロードされます。

ステップ4:APがWLCに再接続した後、APはOEAPモードになります。

注:許可されたAPだけがWLCに加入できるように、AP加入セキュリティ(一般にAPポリ シーで定義)を設定することを推奨します。ローカルで有効な証明書(LSC)APプロビジョニ ングを使用することもできます。

ステップ5:FlexConnectアクセスコントロールリスト(ACL)を作成し、中央でスイッチングするト ラフィック(拒否)とローカルでスイッチングするトラフィック(許可)を定義します。

ここでは、すべてのトラフィックをサブネット192.168.1.0/24にローカルにスイッチングすることを目的としています。

	cisco	MONITOR WLANS CO	NTROLLER	WIRELESS SECURI	TY HANAGEMENT	COMMANDS HE	P EEEDBACK					
W	/ireless	FlexConnect ACLs >	IPv4 ACL >	Edit								
Ť	All APs	General										
	 Radios 802.11a/n/ac/ax 	Access List Name	flex.	OBAP_ACL								_
	802.11b/g/n/ex Dual-Band Radios Dual-5G Radios	IP Rules										٦
	Global Configuration	Seq	Action	Source IP/Hask		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	٥J
	AP Group NTP											-
	ATE											
	RF Profiles	URL Rules										
Ć	FlexConnect Groups FlexConnect ACLs JPv4 ACL JPv6 ACL	Seq Action		Destination U	4							
	Templates											

ステップ6:FlexConnectグループを作成し、[**ACL Mapping**]に移動し、[**WLAN-ACL Mapping**]に移 動**します**。[Local Split ACL Mapping]で、WLAN IDを入力し、FlexConnect ACLを選択します。次 に、[追加]をクリ**ックします。**

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
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 WLAN Id 0 WLAN Id 0
► AP Group NTP	WebAuth IPv6 ACL none V Add
ATF RF Profiles FlexConnect Groups	Add WLAN VLAN Profile WebAuth IPV4 WebAuth IPV6 VebAuth IPV6 ACL Flex_OEAP_ACL Flex_O
FlexConnect ACLs	
FlexConnect VLAN Templates	
Network Lists	
▶ 802.11a/n/ac/ax	

ステップ7:FlexConnect**グルー**プにAPを追加します。



確認

1. FlexConnect ACLのステータスと定義を確認します。

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 Any 0-65535 0-65535 Any Deny

2. FlexConnectローカルスイッチングが無効になっていることを確認します。

(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-quar.... 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. FlexConnectグループの設定を確認します。 (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 Group Radius/Local Auth Parameters : Group Radius AP Settings: AP RADIUS server..... Disabled EAP-FAST Auth..... Disabled LEAP Auth..... Disabled EAP-TLS Auth..... Disabled EAP-TLS CERT Download..... Disabled PEAP Auth..... Disabled Server Key Auto Generated... No Server Key..... <hidden> Authority Info..... Cisco A_ID PAC Timeout..... 0 HTTP-Proxy Ip Address..... 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 APインターフェイスでトラフィックをキャプチャして、トラフィックがAPで分割されていることを確認できます。

ヒント:トラブルシューティングの目的で、DTLS暗号化を無効にして、capwap内でカプセ ル化されたデータトラフィックを確認できます。

次のパケットキャプチャの例は、WLCに向けられたACL「deny」ステートメントに一致するデー タトラフィックと、APでローカルにスイッチングされたACL「permit」ステートメントに一致す るデータトラフィックを示しています。 Ethernet_yellowCable

File	Edit	View	Go	Capture	Analyze	Statistics	Telephony	Wireless	Tools	Help
11	. 1	@ [1.0%	52 (5)	Q	6 50 6	A = =	00	N G	

				units							
icmp											
No.	Delta		Source	Destination	Length	Info					Ext Tag Number
-+	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_	
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	192.168.1.99,192.168.1.139	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=219/568_	
	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

	Ethernet_yellowCable																			
File	Edit View	Go Ca	apture	Analyze	Statistics	Teleph	hony	Wireles	s Tools	Help										
A.	i 🧟			۹ 👄 👄	2 🖗	4 🗐		Q, Q,	् 👖											
	omp																			
No.		Delta		Source				D	estination				Length	Inf	fo					Ext Tag Numb
	20859	9.8	319533	192.168.	1.99,192	2.168.1	.139	19	92.168.	1.14,8.8	8.8.8		1	50 Ec	ho (p	oing)	request	id=0x0001,	seq=213/545_	
	20860	0.0	919956	192.168.3	1.14,8.8	8.8.8		19	92.168.	1.99,19	2.168.1.13	19	1	\$2 Ec	ho (p	oing)	reply	id=0x0001,	seq=213/545_	
	20912	0.9	984274	192.168.1	1.99,192	2.168.1	.139	19	92.168.	1.14,8.8	8.8.8		1	50 Ec	ho (p	oing)	request	id=0x0001,	seq=214/547_	
	20913	0.0	318616	192.168.	1.14,8.8	8.8.8		19	92.168.	1.99,193	2.168.1.13	9	1	\$2 Ec	ho (p	oing)	reply	id=0x0001,	seq=214/547_	
	20961	0.9	986005	192.168.	1.99,192	2.168.1	.139	19	92.168.	1.14,8.8	8.8.8		1	50 Ec	ho (p	oing)	request	id=0x0001,	seq=215/550_	
	20962	0.0	918343	192.168.1	1.14,8.8	8.8.8		19	92.168.	1.99,19	2.168.1.13	19	1	42 Ec	ho (p	oing)	reply	id=0x0001,	seq=215/550_	
	21007	0.9	984777	192.168.1	1.99,192	2.168.1	.139	19	92.168.	1.14,8.8	8.8.8		1	50 Ec	ho (p	oing)	request	id=0x0001,	seq=216/552_	
	21008	0.0	918309	192.168.	1.14,8.8	8.8.8		19	92.168.	1.99,193	2.168.1.13	9	1	\$2 Ec	ho (p	oing)	reply	id=0x0001,	seq=216/552_	
+	21467	9.4	477613	192.168.	1.99			19	92.168.	1.254				74 Ec	ho (p	oing)	request	id=0x0001,	seq=217/555_	
+	21468	0.0	900638	192.168.1	1.254			19	92.168.	1.99				74 Ec	ho (p	oing)	reply	id=0x0001,	seq=217/555_	
	21511	1.0	003331	192.168.1	1.99			19	92.168.	1.254				74 Ec	ho (p	oing)	request	id=0x0001,	seq=218/558	
	21512	0.0	300192	192.168.	1.254			19	92.168.	1.99				74 Ec	ho (p	oing)	reply	id=0x0001,	seq=218/558_	
	21572	1.0	309272	192.168.	1.99			19	92.168.	1.254				74 Ec	ho (p	oing)	request	id=0x0001,	seq=219/560_	
	21573	0.0	999999	192.168.1	1.254			19	92.168.	1.99				74 Ec	ho (p	oing)	reply	id=0x0001,	seq=219/560	
	21621	1.0	002280	192.168.1	1.99			19	92.168.	1.254				74 Ec	ho (p	oing)	request	id=0x0001,	seq=220/563_	
L	21622	0.0	300374	192.168.	1.254			19	92.168.	1.99				74 Ec	ho (p	oing)	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:通常のシナリオでは、クライアントサブネットがオフィスネットワークに属し、ホーム オフィスのローカルデバイスがクライアントサブネットに到達する方法を認識しないため、 APはローカルでスイッチングされるトラフィックのネットワークアドレスを変換します。 APは、ローカルホームオフィスのサブネットで定義されたIPアドレスを使用して、クライ アントトラフィックを変換します。

APがNATを実行したことを確認するには、AP端末に接続し、「*show ip nat translations*」コマン ドを発行します。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

スプリットトンネリングを削除すると、すべてのトラフィックがWLCで中央でスイッチングされ ます。次の例は、capwapトンネル内の192.168.1.2宛先へのインターネット制御メッセージプロ トコル(ICMP)を示しています。

Capturing from Ethernet_yellowCable																
File	Edit Vie	ew Go	Capture	Analyze Statistics	Telephony	Wireless Tools	Help									
1	■ ₫ ◎ 🗌 🗅 🕱 🖸 🔍 ⇔ ⇔ 🕾 🖉 💆 🚍 🗐				Q Q Q II											
	cmp															
No.		Delta		Source		Destination		Length	Info					Ext Tag Number	Payload Type	d
	10	8	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		MSDU	
+	10	9	0.000046	192.168.1.14,192	.168.1.2	192.168.1.4	82,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=129/330		MSDU	
	12	7	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		MSDU	
	12	8	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		MSDU	
	14	2	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		MSDU	
	14	3	0.000130	192.168.1.14,192	.168.1.2	192.168.1.1	82,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=131/335		MSDU	
	16	5	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		MSDU	
	16	6	0.000133	192.168.1.14,192	.168.1.2	192.168.1.	82,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=132/337		MSDU	

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