

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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[概要](#)

[重要な事実](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[WLAN 設定](#)

[AP の設定](#)

[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

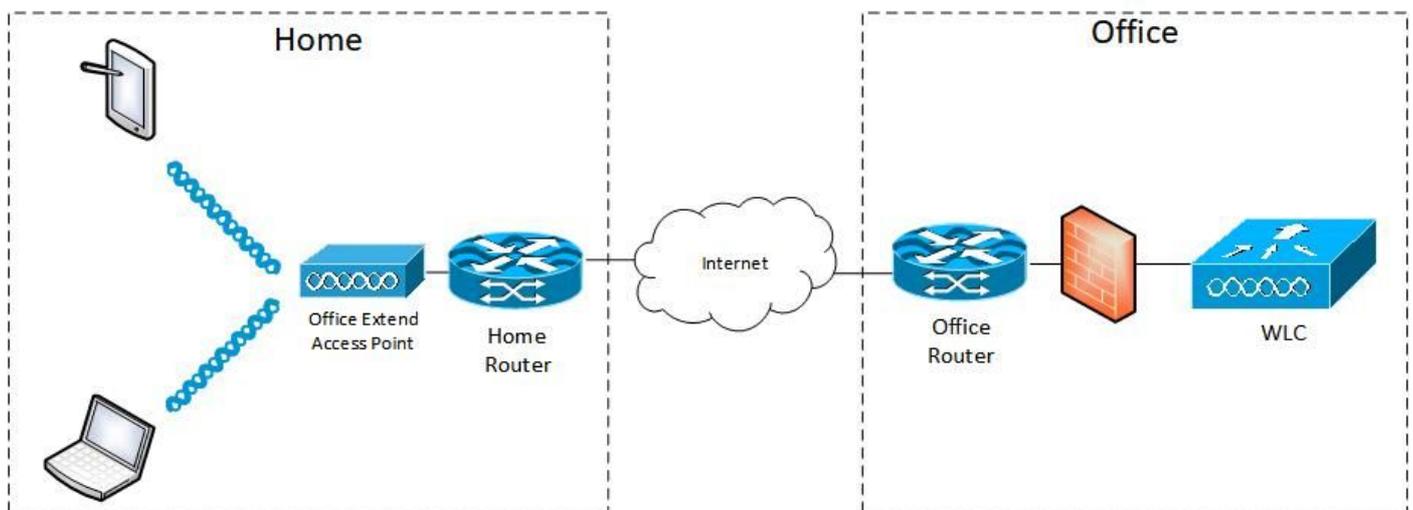
OEAPは、企業WLANをインターネット経由で従業員の自宅まで拡張するために、Cisco WLCからリモートロケーションのCisco APへのセキュアな通信を提供します。ホームオフィスでのユーザエクスペリエンスは、企業オフィスでのユーザエクスペリエンスとまったく同じです。APとコントローラ間のDatagram Transport Layer Security(DTLS)暗号化により、すべての通信のセキュリティが最高レベルになります。FlexConnectモードの屋内APは、OEAPとして機能できます。

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ます。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

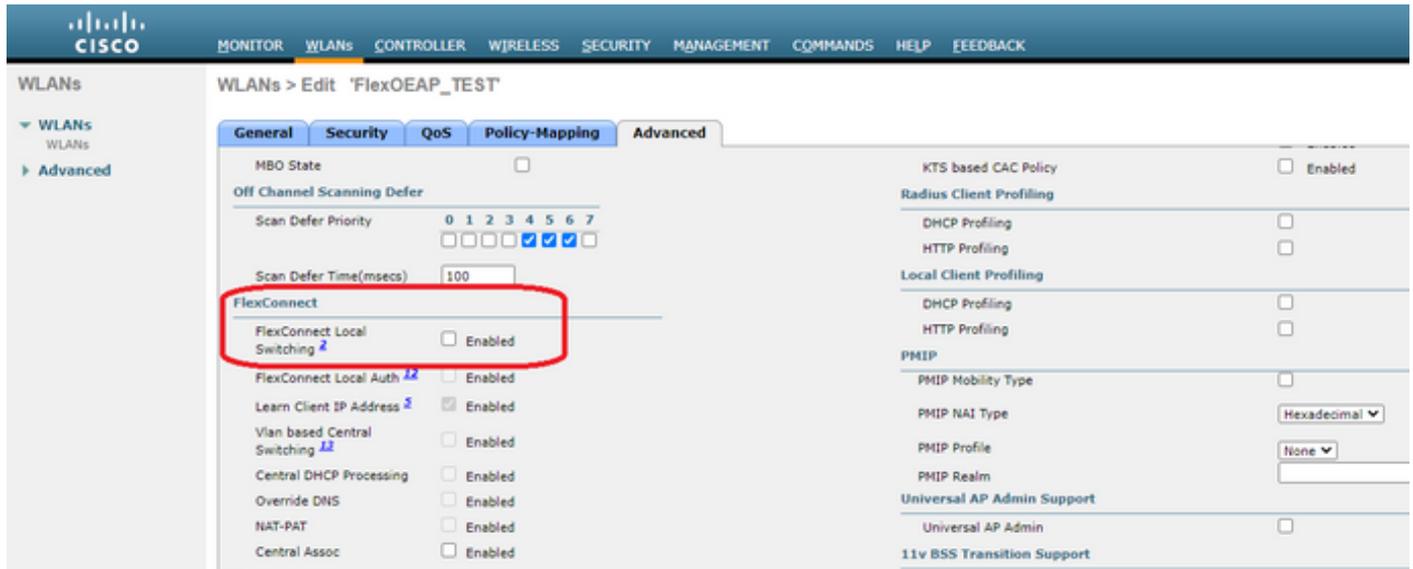
ネットワーク図



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。



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。



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。

ステップ1:APがWLCに加入した後、APモードをFlexConnectに変更し、[Apply]をクリックします。

Wireless

All APs > Details for AP3800_E1.3EB8

General Credentials Interfaces High Availability Inventory Advanced Intelligent Capture

General

AP Name AP3800_E1.3EB8

Location default location

AP MAC Address 70:db:98:e1:3e:b8

Base Radio MAC 00:27:e3:36:5a:60

Admin Status Enable

AP Mode local

AP Sub Mode local

Operational Status FlexConnect

Port Number

Venue Group

Venue Type

Add New Venue

Venue Name

Language

Network Spectrum Interface Key 3D1781A0FFFC6B2F174A6EF605FB1DF8

Versions

Primary Software Version 8.10.130.0

Backup Software Version 8.10.120.0

Predownload Status None

Predownload Version None

Predownload Next Retry Time NA

Predownload Retry Count NA

Boot Version 1.1.2.4

IOS Version 8.10.130.0

Mini IOS Version 0.0.0.0

IP Config

CAPWAP Preferred Mode Ipv4 (Global Config)

DHCP Ipv4 Address 192.168.100.12

Static IP (Ipv4/Ipv6)

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。

Wireless

All APs > Details for AP9120_4C.E77C

General Credentials Interfaces High Availability Inventory FlexConnect Advanced Intelligent Capture

Primary Controller c3504-01

Management IP Address(Ipv4/Ipv6) 192.168.1.14

Secondary Controller

Tertiary Controller

AP Failover Priority Low

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。

The screenshot shows the Cisco Wireless LAN Controller configuration interface. The 'FlexConnect' tab is highlighted with a red box. Under the 'OfficeExtend AP' section, the 'Enable OfficeExtend AP' checkbox is checked and also highlighted with a red box. Other tabs include General, Credentials, Interfaces, High Availability, Inventory, Advanced, and Intelligent Capture.

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。

The screenshot shows the Cisco Wireless LAN Controller configuration interface for AP9120_4C.E77C. The 'Advanced' tab is highlighted with a red box. In the 'Data Encryption' section, the checkbox is checked and also highlighted with a red box. Other tabs include General, Credentials, Interfaces, High Availability, Inventory, FlexConnect, Network Diagnostics, and Intelligent Capture.

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。

FlexConnect ACLs > IPv4 ACL > Edit

General

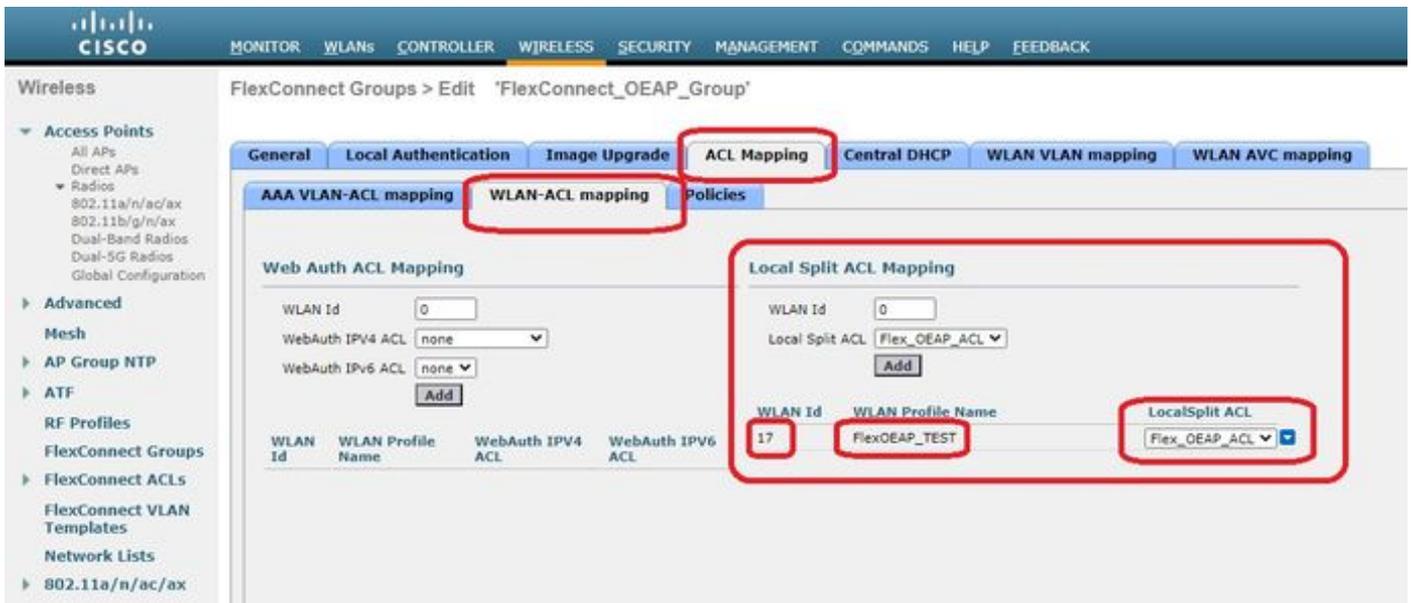
Access List Name Flex_OEAP_ACL

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP
1	Permit	0.0.0.0 / 0.0.0.0	192.168.1.0 / 255.255.255.0	Any	Any	Any	Any
2	Deny	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any

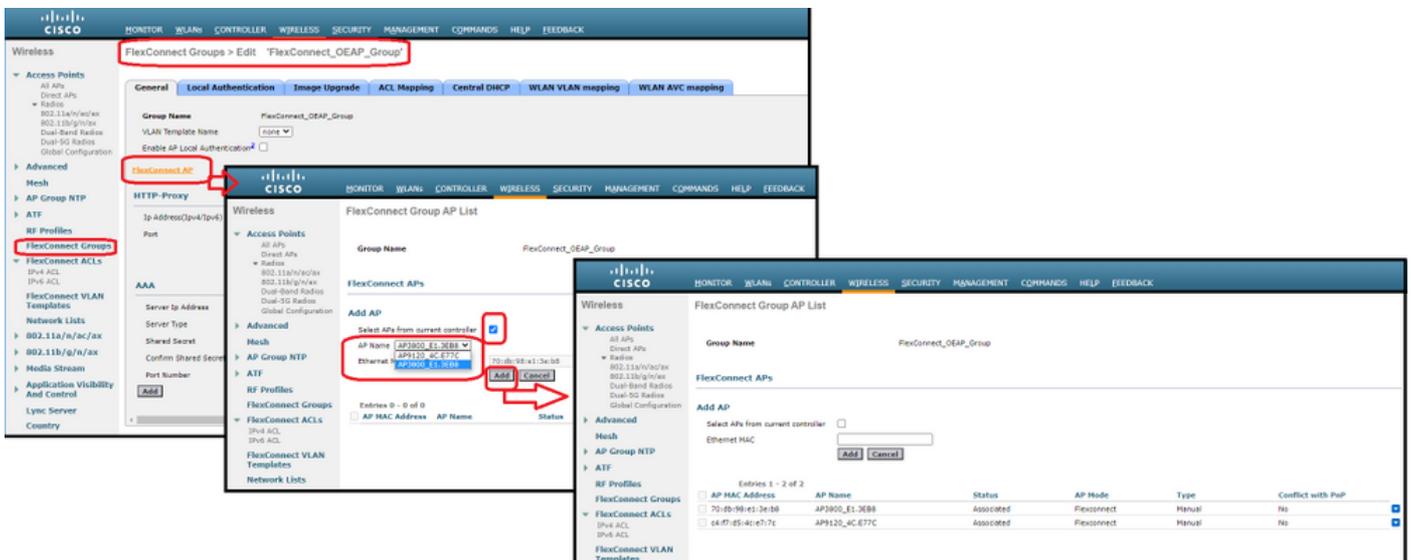
URL Rules

Seq	Action	Destination Url
-----	--------	-----------------

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。



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 0.0.0.0/0.0.0.0 192.168.1.0/255.255.255.0 Any 0-65535 0-65535 Any Permit
2 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 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-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. 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 :
Radius Retransmit Count..... 3 (default)
Active Radius Timeout..... 5 (default)
```

```
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 ID..... 436973636f0000000000000000000000000000
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

icmp

No.	Delta	Source	Destination	Length	Info	Ext Tag Number
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...	
21622	0.000374	192.168.1.254	192.168.1.99	74	Echo (ping) reply id=0x0001, seq=220/563...	

> Frame 20859: 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 Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Delta	Source	Destination	Length	Info	Ext Tag Number
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...	
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：通常のシナリオでは、クライアントサブネットワーク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ワーク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ワークで定義された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。

The image shows a Wireshark packet capture window titled "Capturing from Ethernet_yellowCable". The interface includes a menu bar (File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, Help) and a toolbar. The main display area shows a list of captured packets, with packet 108 selected. The packet list table is as follows:

No.	Delta	Source	Destination	Length	Info	Ext Tag Number	Payload Type	C
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...		MSDU	
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...		MSDU	
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...		MSDU	
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...		MSDU	
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...		MSDU	
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...		MSDU	
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...		MSDU	
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, seq=132/337...		MSDU	

Below the packet list, the details pane for the selected packet (Frame 108) is expanded, showing the following protocol layers:

- > 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