

# VMブリッジクライアントに接続するための9800ワイヤレスLANコントローラの設定

## 内容

---

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[ネットワーク図](#)

[コンフィギュレーション](#)

[VLANの設定](#)

[ポリシープロファイルの設定](#)

[WLANの設定](#)

[ポリシータグの設定](#)

[VMの設定](#)

[確認](#)

[VMの確認](#)

[ホストVMの確認](#)

[WLCの確認](#)

[トラブルシューティング](#)

[WLCクライアントモニタリング](#)

[WLCパケットキャプチャ](#)

[Wiresharkパケットキャプチャ](#)

[関連情報](#)

---

## はじめに

このドキュメントでは、仮想マシン(VM)ブリッジクライアントに接続するために9800ワイヤレスLANコントローラ(WLC)を設定する方法について説明します。

## 前提条件

### 要件

次の項目に関する基本的な知識が推奨されます。

- Cisco 9800シリーズワイヤレスLANコントローラ(WLC)の設定の概念
- Cisco Wave 2アクセスポイント(AP)の設定の概念
- Ciscoアクセスポイントの登録とモード設定の概念

- VirtualBoxネットワーキングと仮想マシンのセットアップの概念

## 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。

- Cisco IOS® 17.15.3を搭載した9800-CL WLC
- Control And Provisioning of Wireless Access Points(CAPWAP)APモデルCW9176I
- VirtualBoxバージョン7.1.10を使用するVM
- オペレーティングシステムUbuntuバージョン24.04.2長期サポート(LTS)
- Windows 11 Home搭載ワイヤレスクライアントラップトップ

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、クリアな(デフォルト)設定で作業を開始しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください

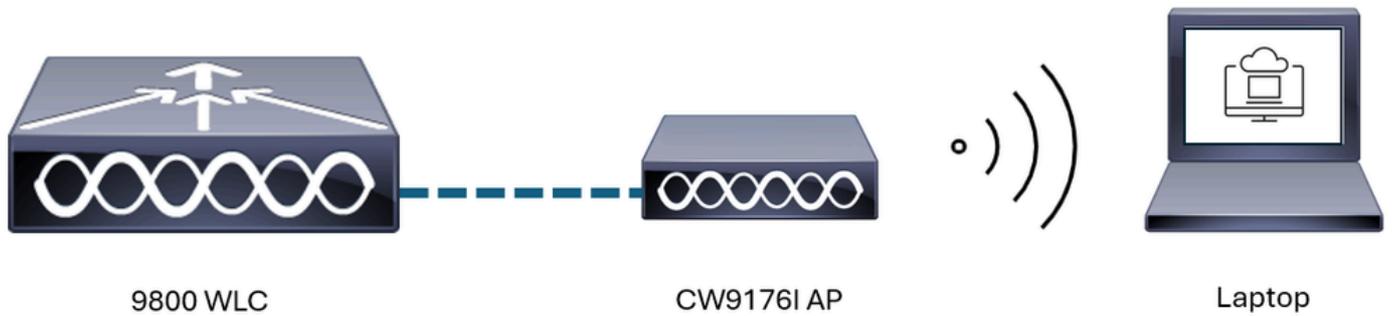
## 背景説明

VMは、ホストラップトップの物理Wi-Fiアダプタを使用してネットワーク接続を確立し、既存のネットワークインフラストラクチャとのシームレスな統合を実現します。DHCPサーバは一意的IPアドレスをVMに割り当て、ネットワーク内での適切な識別と通信を可能にします。

VMはホストのラップトップの物理Wi-Fiアダプタを使用しますが、無線接続を直接管理しません。代わりに、ホストのラップトップはブリッジとして機能し、Wi-Fi接続を管理し、VMへのネットワークアクセスを提供します。その結果、VMはWi-Fiネットワークを直接表示または制御できません。これは、この機能がホストシステムによって処理されるためです。この設定により、ホストの物理リソースを効率的に使用しながら、VMがネットワーク上で堅牢なプレゼンスを維持することが保証されます。

## ネットワーク図

このネットワークダイアグラムには、Cisco Catalyst 9800ワイヤレスLANコントローラ(WLC)と、VirtualBoxでホストされるラップトップや仮想マシン(VM)などのデバイスにワイヤレス接続を提供するCW9176Iアクセスポイント(AP)が含まれています。9800 WLCは中央管理および制御ユニットとして機能し、ワイヤレスネットワークのシームレスな統合と効率的な運用を実現します。CW9176I APは、高度なWi-Fi 7機能を備え、接続デバイスに対して高速で信頼性の高い無線通信を可能にします。ホストVMラップトップはWindows 11 Homeを実行し、Ubuntuソフトウェアを使用してVirtualBox VMを運用します。



ネットワーク図

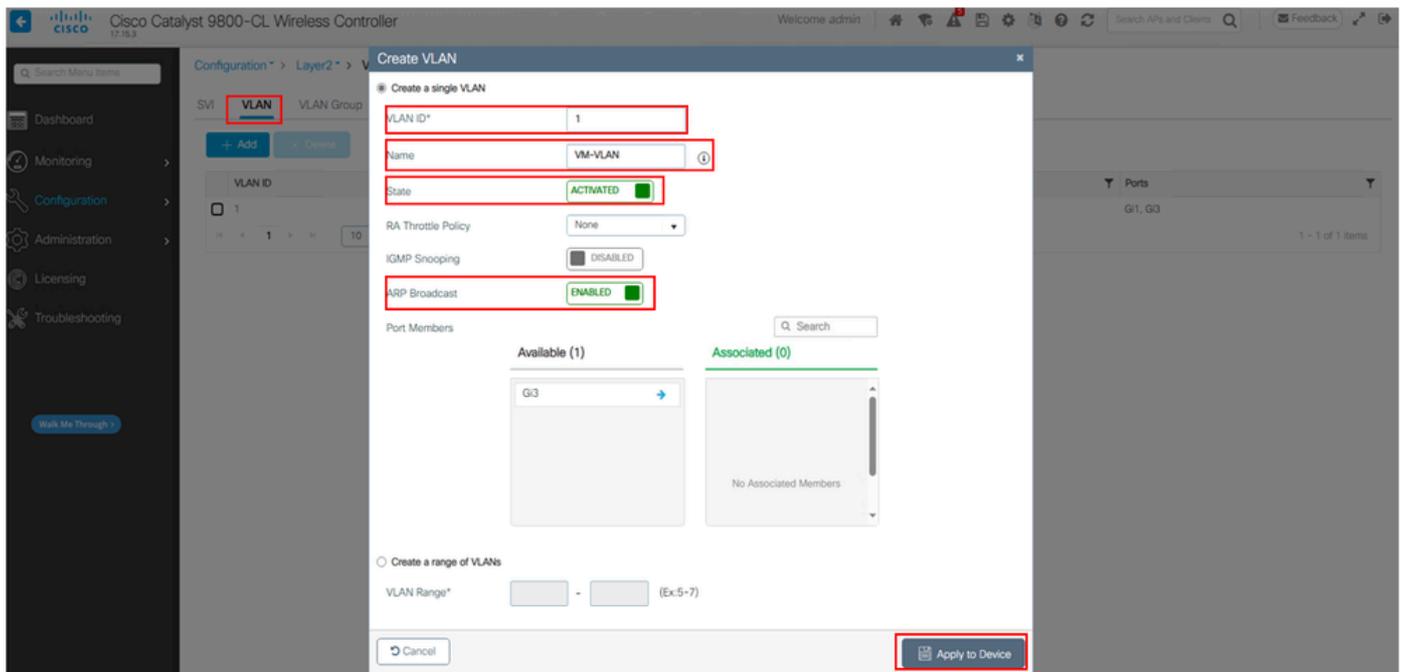
## コンフィギュレーション

### VLANの設定

Cisco Catalyst 9800 Wireless ControllerのARPブロードキャスト機能は、パッシブクライアントを持つネットワークでの通信を可能にするために不可欠です。この機能は、VLAN内のすべてのデバイスにARP要求をブロードキャストします。これは、IP情報をアクティブに送信しないブリッジアダプタモードの仮想マシンなどのパッシブクライアントに特に役立ちます。

### WLC GUI

図に示すように、Configurations > Layer2 > VLAN > Click + Add > VLAN ID "Custom VLAN ID" > Name "Custom Name" > State ACTIVATED > ARP Broadcast ENABLED の順に移動します。



VLANの設定

### WLCのCLI

WLC#

```
WLC#config t
WLC(config)#vlan [VLAN ID]
WLC(config-vlan)#name [WORD]
WLC(config-vlan)#exit
```

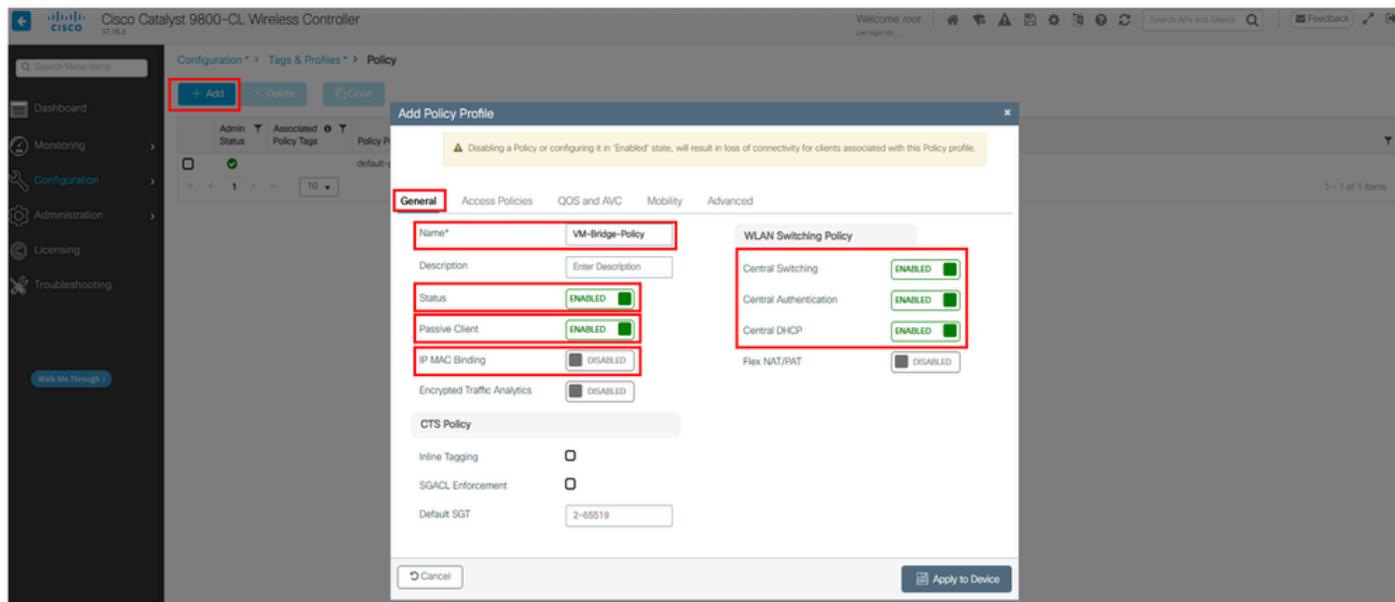
```
WLC(config)#vlan configuration [VLAN ID]
WLC(config-vlan-config)#arp broadcast
WLC(config-vlan-config)#end
WLC#
```

## ポリシープロファイルの設定

Cisco Catalyst 9800でブリッジアダプタを使用して設定されたVMのシームレスな接続を保証するには、パッシブクライアント機能を有効にし、IP MACバインディングを無効にすることが不可欠です。この設定により、ワイヤレスコントローラは1つのMACアドレスに関連付けられた複数のIPアドレスを処理できます。これは仮想化環境で一般的です。パッシブクライアントを有効にすると、VMマシンへのトラフィックフローが確保されます。IP-MACバインディングを無効にすると、コントローラはトラフィックをIP盗用として識別せずに、トラフィックをVMマシンに転送できます。

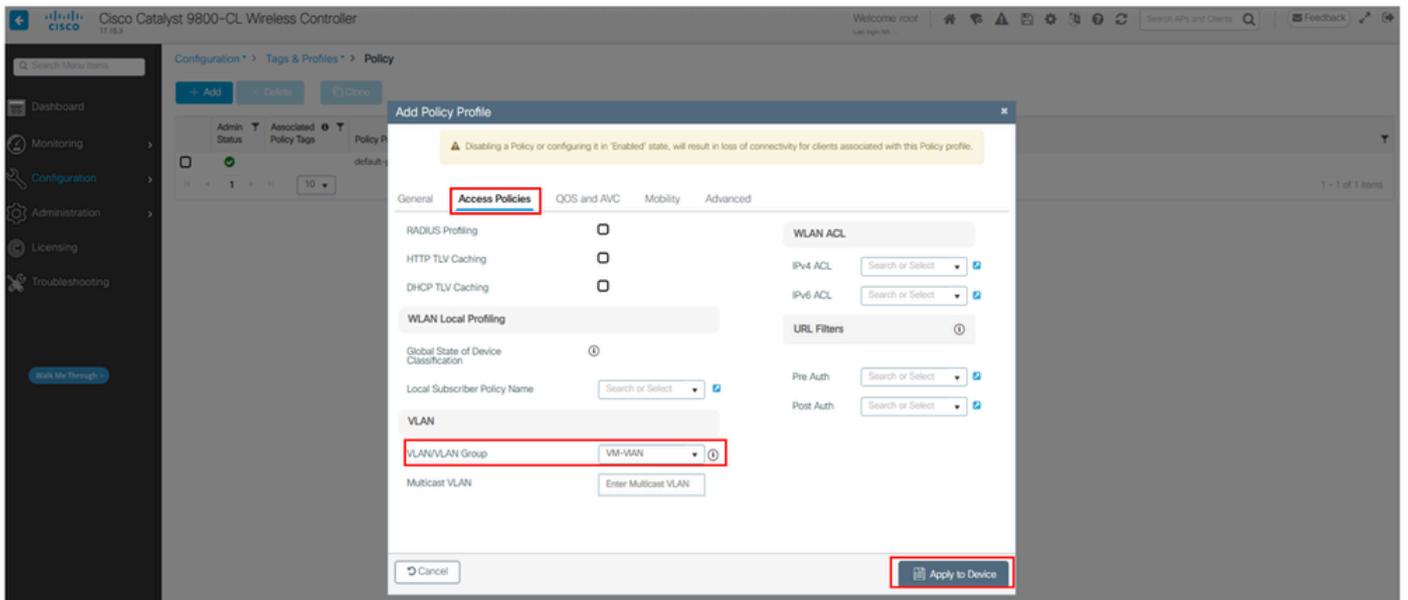
## WLC GUI

図に示すように、Configurations > Tags & Profile > Policy > Click + Add > General > WLAN Switching Policy > Central Switching ENABLED > Central Authentication ENABLED > Central DHCP ENABLEDの順に移動します。



## ポリシー設定

図に示すように、Access Policies > VLAN > VLAN/VLAN Group > Configure VLANの順に選択し、Apply to Deviceをクリックします。



ポリシー設定

## WLCのCLI

```
WLC#  
WLC#config t  
WLC(config)#wireless profile policy [WORD]  
WLC(config-wireless-policy)#shutdown  
WLC(config-wireless-policy)#passive-client  
WLC(config-wireless-policy)#no ip mac-binding  
WLC(config-wireless-policy)#central switching  
WLC(config-wireless-policy)#central dhcp  
WLC(config-wireless-policy)#central authentication  
WLC(config-wireless-policy)#vlan [WORD | VLAN ID]  
WLC(config-wireless-policy)#no shutdown  
WLC(config-wireless-policy)#end  
WLC#
```



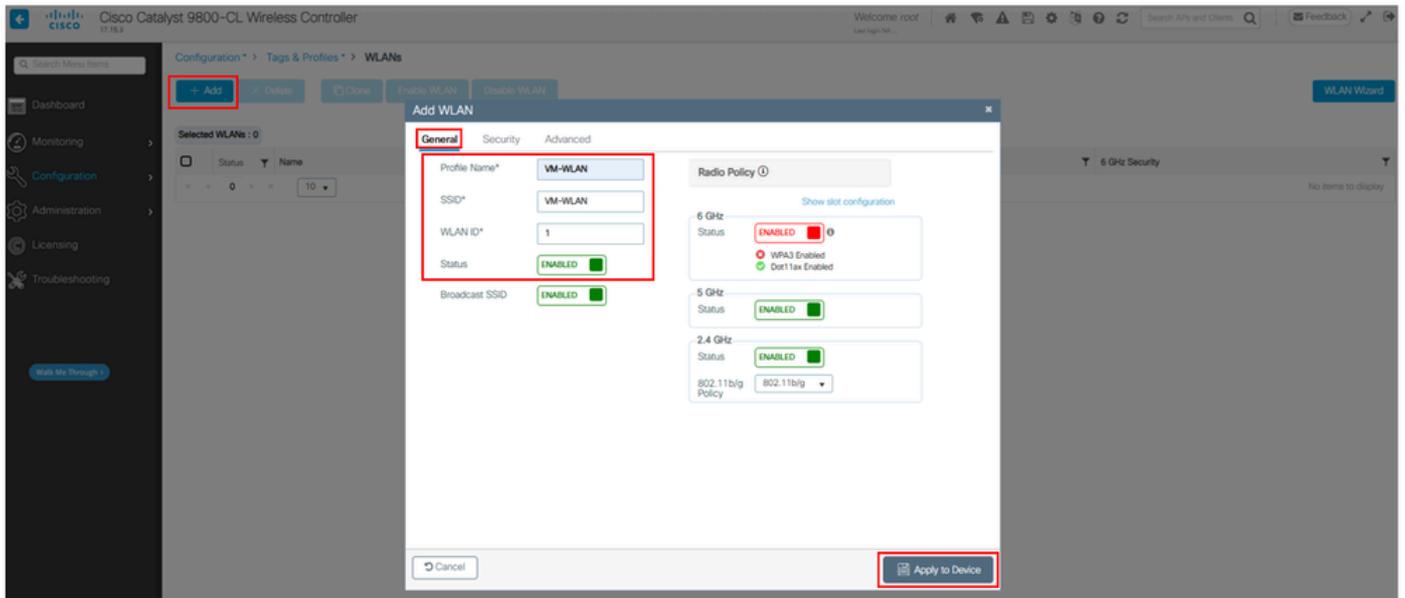
警告：ポリシーを無効にするか、有効な状態で設定すると、このポリシープロファイルに関連付けられているクライアントの接続が失われます。

---

## WLANの設定

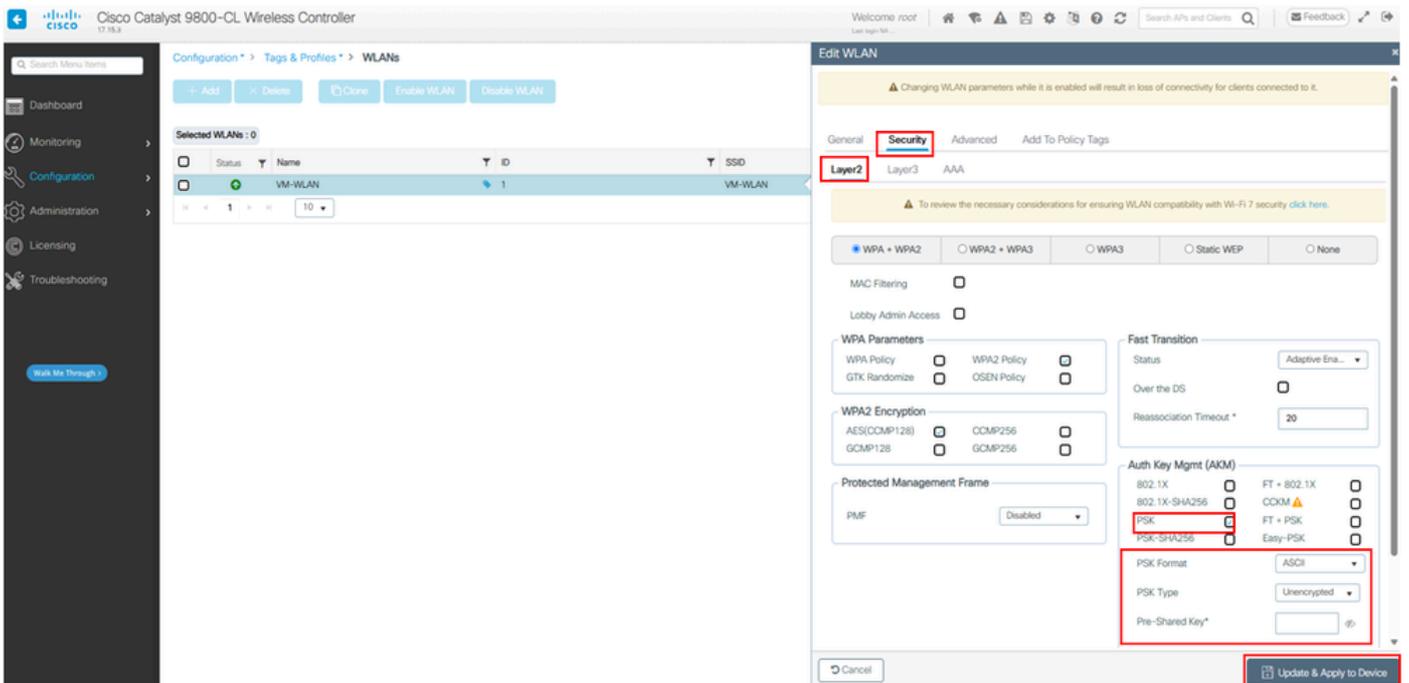
この例では、事前共有キー(PSK)認証用に設定されたWLANを示しています。ただし、ブリッジアダプタを使用して、WLANをVMの802.1X認証用に設定できます。

図に示すように、Configurations > Tags & Profile > WLAN > Click + Add > General > Profile Name "Custom Name" > SSID "Custom Name" > WLAN ID\* "Custom Name" > Status ENABLED > Apply to Deviceの順に移動します。



WLANの設定

図に示すように、Security > Layer2 > PSK "checkbox" > PSK Format ASCII > PSK Type Unencrypted > Pre-Shared Key\* "Custom Key" > Update & Apply to Deviceの順に選択します。



WLANの設定

## WLCのCLI

```

WLC#
WLC#config t
WLC(config)#wlan [WORD] [WLAN Identifier]
WLC(config-wlan)#shutdown
WLC(config-wlan)#security wpa akm psk
WLC(config-wlan)#no security wpa akm dot1x
WLC(config-wlan)#security wpa psk set-key ascii [WORD]

```

```
WLC(config-wlan)#no shutdown
WLC(config-wlan)#end
WLC#
```

---



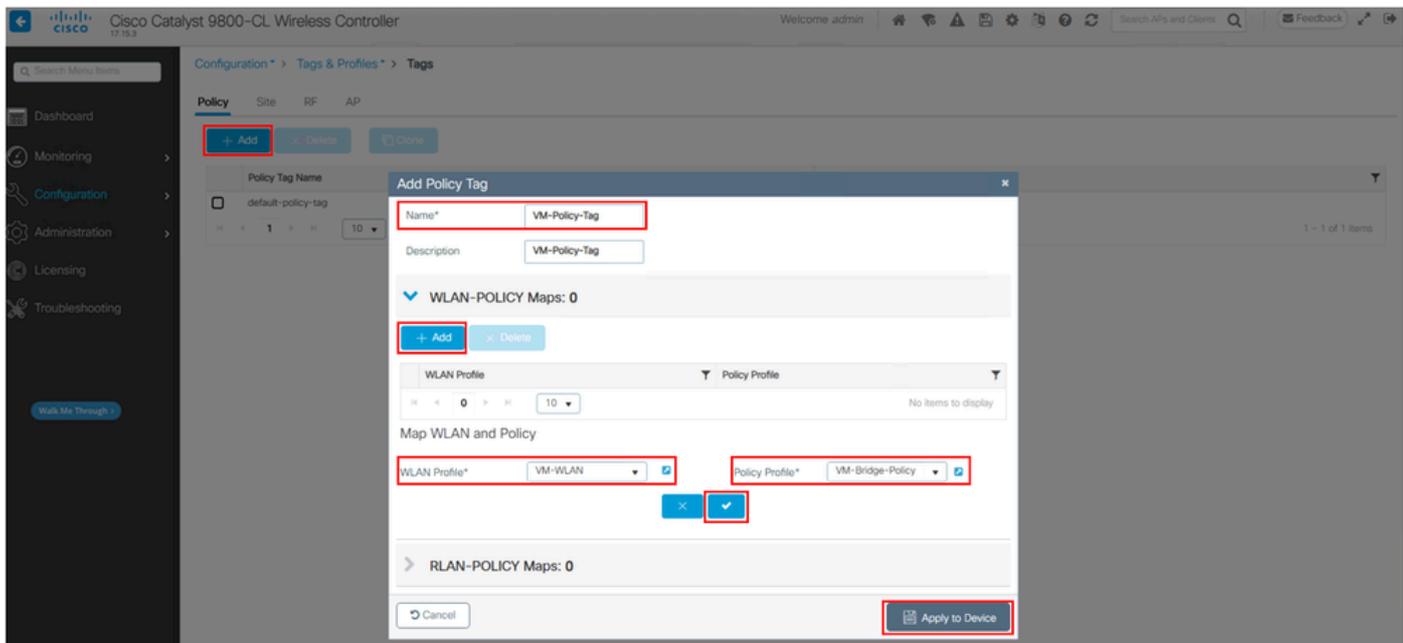
警告：有効な状態でWLANパラメータを変更すると、接続されているクライアントの接続が失われます。

---

## ポリシータグの設定

この例では、特定のWLANプロファイルを特定のポリシープロファイルにバインドするためのポリシータグ設定を示しています。

図に示すように、Configurations > Tags & Profile > TAG > Click + Add > Name “Custom Name” > WLAN-POLICY Maps: > Click + Add > WLAN Profile\* “Select Custom WLAN” > Policy Profile\* “Select Custom Policy” > “青いチェックボックス” > Apply to Deviceの順にクリックします。



ポリシータグの設定

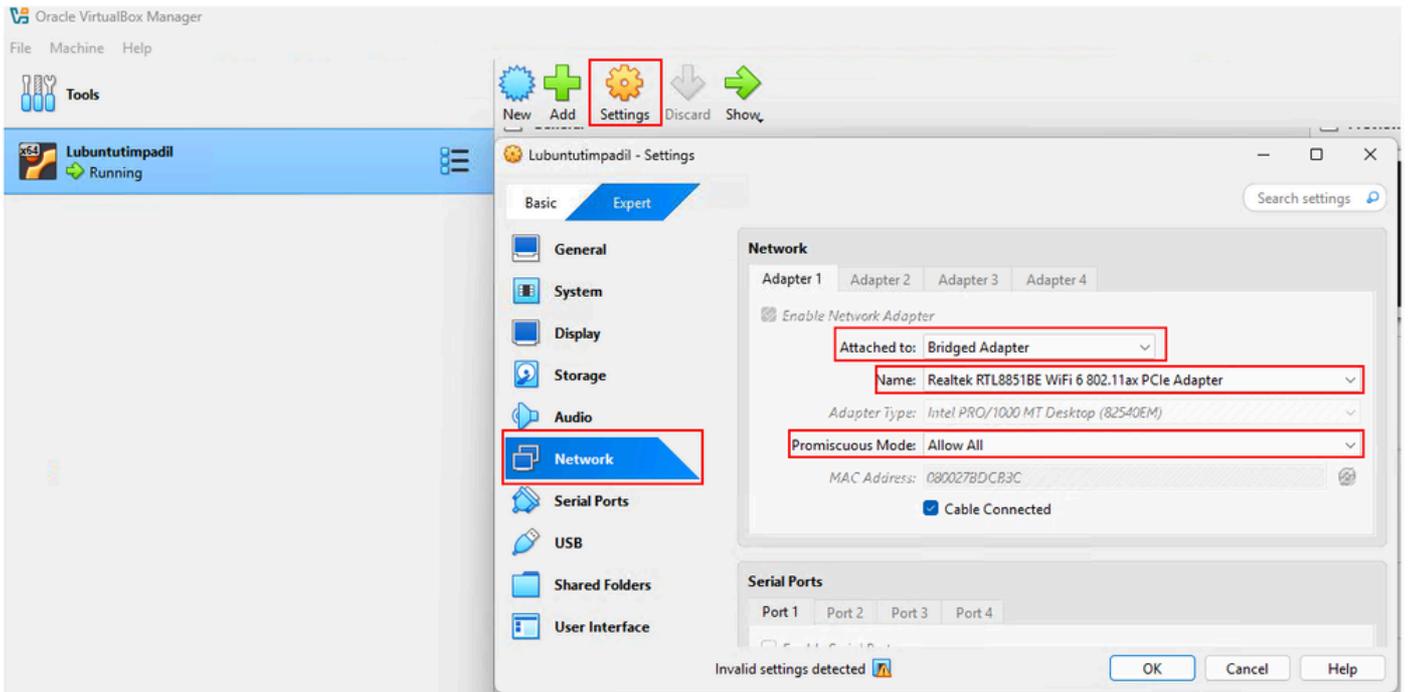
## WLCのCLI

```
WLC#  
WLC#config t  
WLC(config)#wireless tag policy [WORD]  
WLC(config-policy-tag)#wlan [WORD] policy [WORD]  
WLC(config-policy-tag)#end  
WLC#
```

## VMの設定

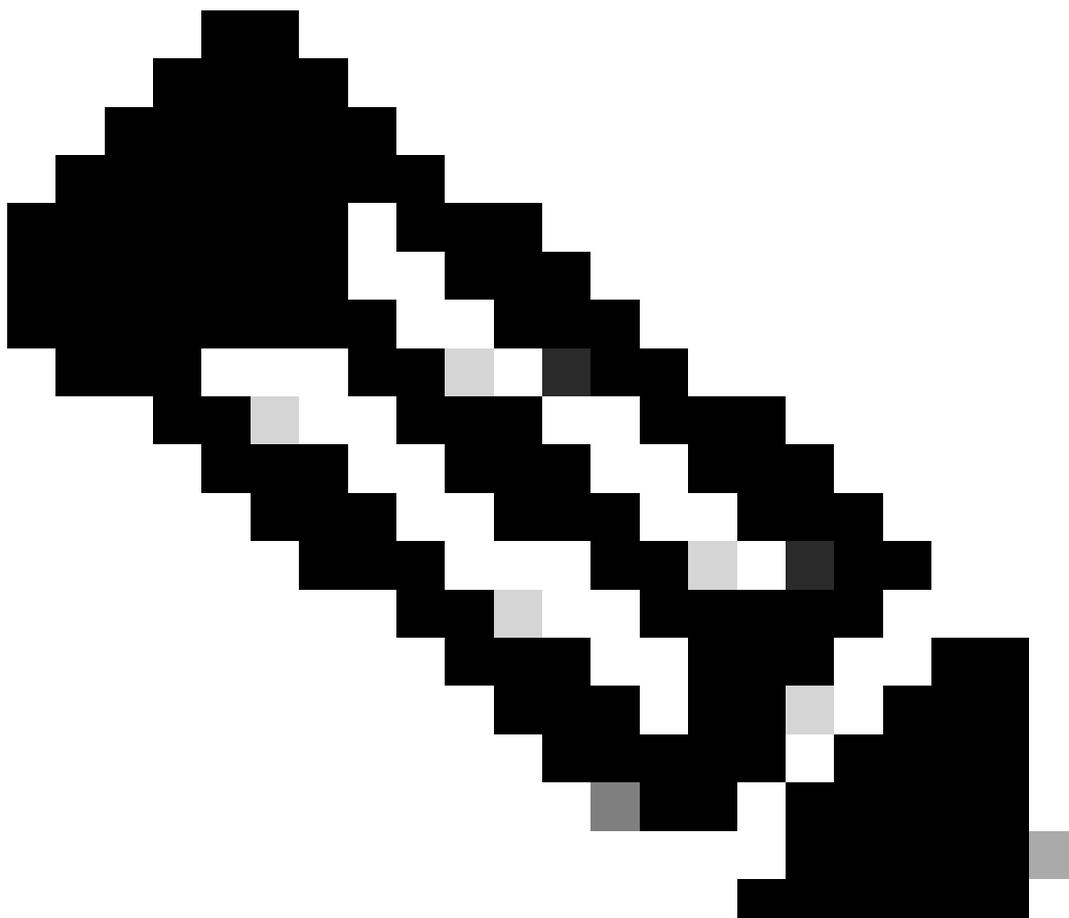
ブリッジアダプタ機能を使用すると、VMからホストマシンの物理ネットワークに直接アクセスできます。

図に示すように、Setting > Network > Attached to: Select Bridged Adapter > Name: "Select Laptop Physical WiFi Adapter" > Promiscuous Mode: Allow Allの順に選択します。



VMの設定

---



注：このセットアップではUbuntu OS搭載のVirtualBoxを使用しますが、使用する仮想化プラットフォームによって、特定のVM設定の場所と命名規則が異なる場合があります。

---

## 確認

VMおよび9800 WLCから、次のコマンドと方法を使用して設定を確認できます。

### VMの確認

VMがDHCPサーバからIPアドレスを正常に取得したことを確認するには、VMのコマンドラインインターフェイスでifconfigコマンドを実行します。出力には、割り当てられたIPアドレス（DHCP経由で取得された場合）を含むネットワーク設定が表示されます。

```
File Actions Edit View Help
admin@timpadillubuntu: ~ x
admin@timpadillubuntu:~$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.166.111 netmask 255.255.255.0 broadcast 192.168.1
66.255
    inet6 fe80::a00:27ff:febd:cb3c prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:bd:cb:3c txqueuelen 1000 (Ethernet)
    RX packets 7880 bytes 573918 (573.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 398 bytes 32329 (32.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 166 bytes 15376 (15.3 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 166 bytes 15376 (15.3 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

VMコマンドラインインターフェイス

次に、VMのコマンドラインインターフェイス(CLI)でpingを実行して、ゲートウェイの到達可能性を確認します。

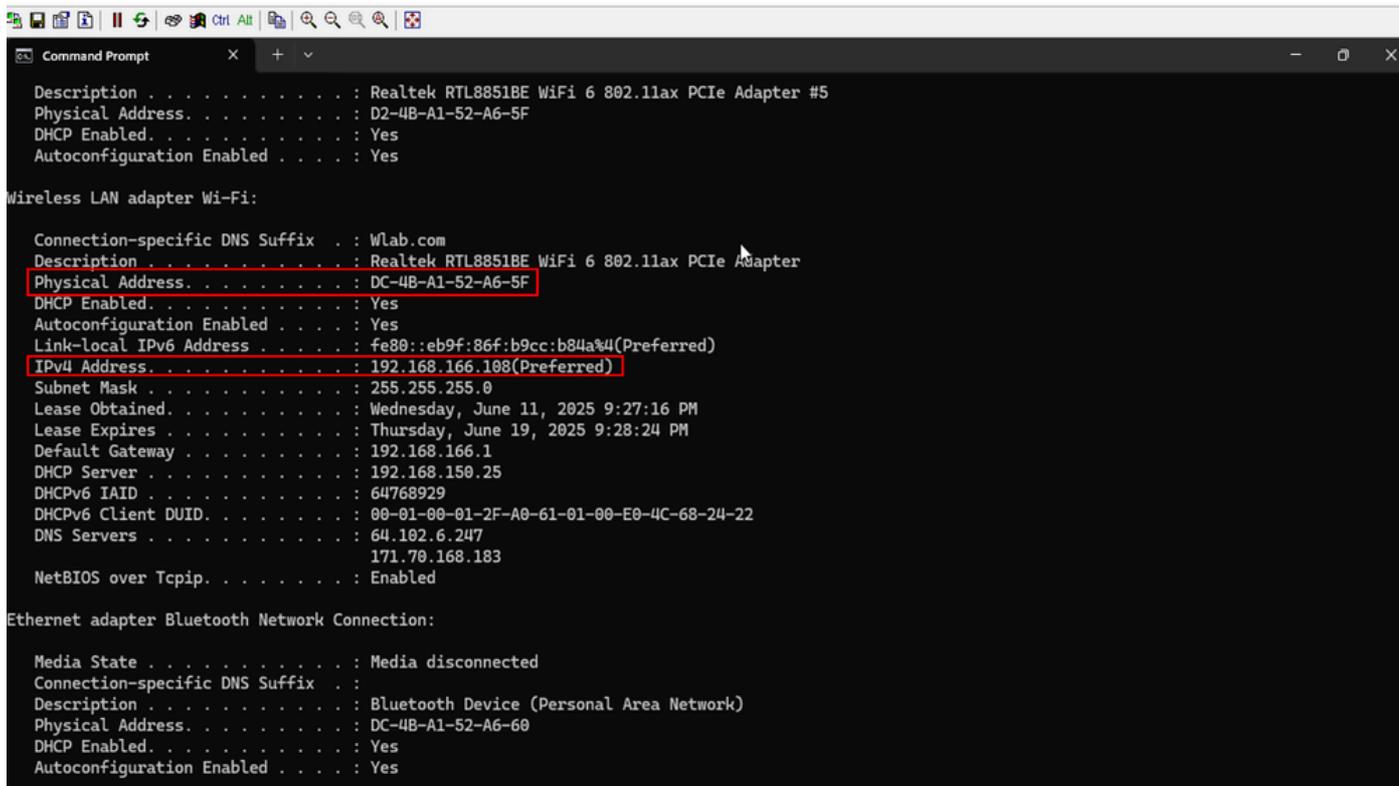
```
admin@timpadillubuntu: ~
File Actions Edit View Help
admin@timpadillubuntu: ~ x
admin@timpadillubuntu:~$ ping 192.168.166.1
PING 192.168.166.1 (192.168.166.1) 56(84) bytes of data.
64 bytes from 192.168.166.1: icmp_seq=1 ttl=64 time=175 ms
64 bytes from 192.168.166.1: icmp_seq=2 ttl=64 time=3.32 ms
64 bytes from 192.168.166.1: icmp_seq=3 ttl=64 time=28.6 ms
64 bytes from 192.168.166.1: icmp_seq=4 ttl=64 time=29.8 ms
64 bytes from 192.168.166.1: icmp_seq=5 ttl=64 time=67.7 ms
64 bytes from 192.168.166.1: icmp_seq=6 ttl=64 time=21.3 ms
64 bytes from 192.168.166.1: icmp_seq=7 ttl=64 time=17.3 ms
64 bytes from 192.168.166.1: icmp_seq=8 ttl=64 time=4.52 ms
```

VMコマンドラインインターフェイス

## ホストVMの確認

ホストVMラップトップのIPアドレスとMACアドレスを確認します。

ホストVMラップトップCLIに移動し、コマンドifconfig /allを実行します。



```
Command Prompt
Description . . . . . : Realtek RTL8851BE WiFi 6 802.11ax PCIe Adapter #5
Physical Address. . . . . : D2-4B-A1-52-A6-5F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes

Wireless LAN adapter Wi-Fi:

Connection-specific DNS Suffix . . : Wlab.com
Description . . . . . : Realtek RTL8851BE WiFi 6 802.11ax PCIe Adapter
Physical Address. . . . . : DC-4B-A1-52-A6-5F
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-Local IPv6 Address . . . . . : fe80::eb9f:86f:b9cc:b84a%4(Preferred)
IPv4 Address. . . . . : 192.168.166.108(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Wednesday, June 11, 2025 9:27:16 PM
Lease Expires . . . . . : Thursday, June 19, 2025 9:28:24 PM
Default Gateway . . . . . : 192.168.166.1
DHCP Server . . . . . : 192.168.150.25
DHCPv6 IAID . . . . . : 64768929
DHCPv6 Client DUID. . . . . : 00-01-00-01-2F-A0-61-01-00-E0-4C-68-24-22
DNS Servers . . . . . : 64.102.6.247
                          171.70.168.183
NetBIOS over Tcpi. . . . . : Enabled

Ethernet adapter Bluetooth Network Connection:

Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . . :
Description . . . . . : Bluetooth Device (Personal Area Network)
Physical Address. . . . . : DC-4B-A1-52-A6-60
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
```

ホストVMラップトップ

## WLCの確認

### WLCのCLI

```
WLC#
WLC#show wireless profile policy detailed [WORD]
WLC#show wireless tag policy detailed [WORD]
WLC#show wlan name [WORD]
WLC#show vlan
WLC#show platform software arp broadcast
WLC#
```

## トラブルシュート

WLCは、ホストVMラップトップの物理WiFiアダプタの関連付けの詳細 ( IPアドレスとMACアドレスなど ) のみを表示します。VMを関連付けられたクライアントとして認識せず、VMのIPアドレスまたはMACアドレスを表示しません。

## WLCクライアントモニタリング

IPアドレス192.168.166.108とMACアドレスdc4b.a152.a65fがホストVMラップトップに割り当てられます。VM自体のIPアドレスとMACアドレスは、9800 WLCでは直接表示されないことに注意してください。ただし、ワイヤレスLANコントローラ(WLC)でパケットキャプチャを実行すると、ICMP要求の送信元アドレスとしてVMのIPアドレス192.168.166.111が使用されていることがわかります。同様に、ICMP応答は宛先アドレスとしてVMのIPアドレスを利用します。

図に示すように、Monitoring > Wireless > Clientsの順に選択します。この図は、ホストVMラップトップのIPアドレスとMACアドレスがCisco 9800 WLCのGUIに明確に表示されることを示しています。

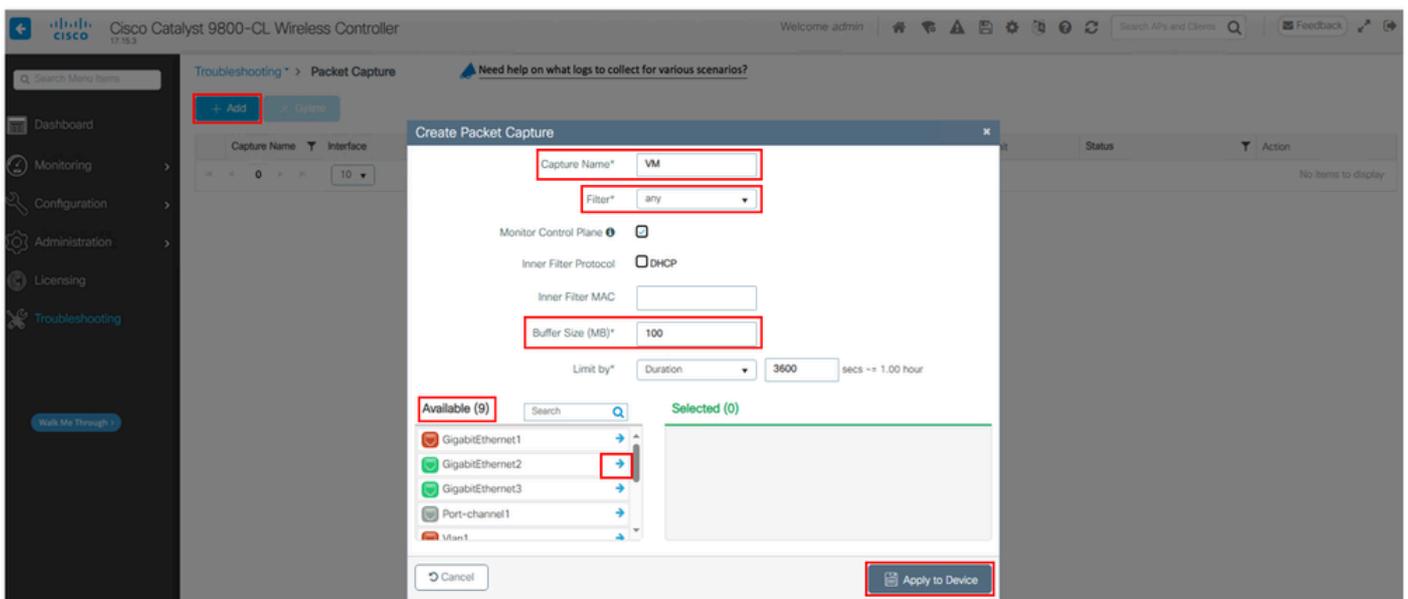


WLCクライアントモニタリング

## WLCパケットキャプチャ

この例では、9800 WLCでのパケットキャプチャの設定を示しています。

図に示すように、Troubleshooting > Packet Capture > Click + Add > Capture Name\* "Create Custom Name" > Filter\* "any" > Buffer Size\* "100" > Available "Select Interface" > Apply to Deviceの順に移動します。



WLCパケットキャプチャの設定

## WLCのCLI

```

WLC#
WLC#monitor capture [WORD] interface [Interface] [Interface Number] both
WLC#monitor capture [WORD] buffer size 100
WLC#monitor capture [WORD] match any
WLC#monitor capture [WORD] start
WLC#monitor capture [WORD] stop
WLC#monitor capture [WORD] export flash:[Name.pcap]
WLC#no monitor capture [WORD]
WLC# copy flash:<Name.pcap> tftp://<IP ADD>/<Name.pcap>
WLC#

```

## Wiresharkパケットキャプチャ

Wiresharkパケットキャプチャでは、VMのIPアドレス192.168.166.111がICMP要求の送信元アドレスとして示されています。また、ICMP応答は宛先アドレスと同じIPアドレスを使用します。

- Receiver addressはAPのMACアドレス
- 送信元アドレスは、ホストVMラップトップのMACアドレスです
- 宛先アドレスは、ゲートウェイMACアドレスです
- 送信元アドレスは、ホストVMラップトップのMACアドレスです

次の図は、ゲートウェイIPアドレス(192.168.166.1)に対するVM ICMP要求のWiresharkパケットキャプチャの例です。

No.	Time	Source Address	Destination Address	Protocol	Source Port	Dest Port	Length	MAC.SRC	MAC.DST	802.11 Info	802.11 TX Rate	Network	MAC	Signal
68	2025/162 21:35:25.702951	192.168.166.111	192.168.166.1	ICMP	5248	5247	176	WistronNeweb_52:a6:5f	Wmware_84:5e:ce	Echo (ping) request	id=0x0000	192.168.166.1	dc:4b:a1:52:a6:5f	
69	2025/162 21:35:25.702951	192.168.166.1	192.168.166.111	ICMP	5247	5248	168	Wmware_84:5e:ce	WistronNeweb_52:a6:5f	Echo (ping) reply	id=0x0000	192.168.166.111	00:50:56:04:5e:ce	

Receiver address: Cisco\_6a:11:80 (f0:d8:05:6a:11:80)  
 Transmitter address: WistronNeweb\_52:a6:5f (dc:4b:a1:52:a6:5f)  
 Destination address: Vmware\_84:5e:ce (00:50:56:04:5e:ce)  
 Source address: WistronNeweb\_52:a6:5f (dc:4b:a1:52:a6:5f)

Receiver address: Cisco\_6a:11:80 (f0:d8:05:6a:11:80)  
 Transmitter address: WistronNeweb\_52:a6:5f (dc:4b:a1:52:a6:5f)  
 Destination address: Vmware\_84:5e:ce (00:50:56:04:5e:ce)  
 Source address: WistronNeweb\_52:a6:5f (dc:4b:a1:52:a6:5f)

Wiresharkパケットキャプチャ

## 関連情報

- [Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーションガイド、Cisco IOS XE 17.15.x](#)
- [Cisco Catalyst 9800シリーズワイヤレスコントローラ、Cisco IOS XE 17.15.xのリリースノート](#)
- [シスコワイヤレスCW9176アクセスポイント導入ガイド](#)

## 翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。