

配置9800无线LAN控制器以连接VM网桥客户端

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[网络图](#)

[配置](#)

[VLAN 配置](#)

[策略配置文件配置](#)

[WLAN配置](#)

[策略标记配置](#)

[VM配置](#)

[验证](#)

[VM确认](#)

[主机VM确认](#)

[WLC确认](#)

[故障排除](#)

[WLC客户端监控](#)

[WLC数据包捕获](#)

[Wireshark数据包捕获](#)

[相关信息](#)

简介

本文档介绍如何配置9800无线局域网控制器(WLC)以连接虚拟机(VM)网桥客户端。

先决条件

要求

Cisco 建议您具有以下主题的基础知识：

- Cisco 9800系列无线局域网控制器(WLC)配置概念
- Cisco Wave 2接入点(AP)配置概念
- 思科接入点注册和模式配置概念
- VirtualBox网络和虚拟机设置概念

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 9800-CL WLC，带Cisco IOS® 17.15.3
- 无线接入点(CAPWAP)AP型号CW9176I的控制和调配
- 具有VirtualBox版本7.1.10的VM
- 操作系统Ubuntu版本24.04.2长期支持(LTS)
- 采用Windows 11 Home的无线客户端笔记本电脑

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，请确保您了解任何命令的潜在影响

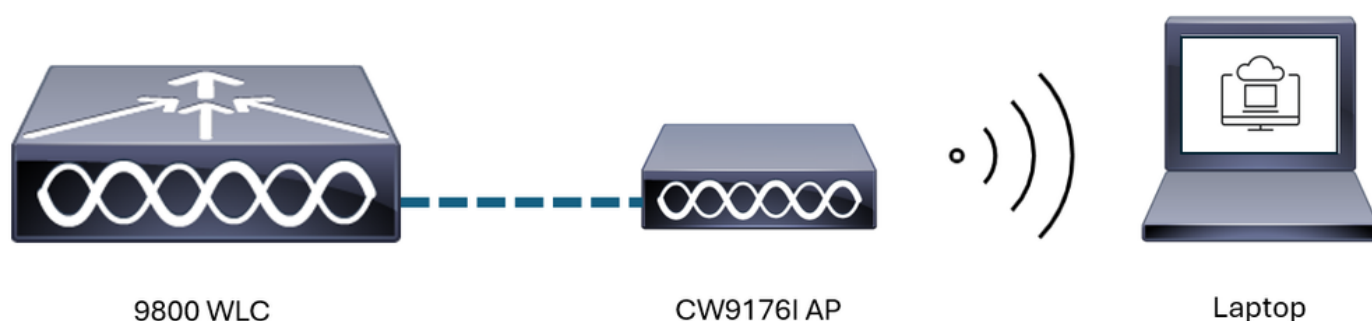
背景信息

VM利用主机笔记本电脑的物理Wi-Fi适配器建立网络连接，确保与现有网络基础设施无缝集成。DHCP服务器为VM分配唯一的IP地址，从而在网络中实现正确的标识和通信。

虽然VM使用主机笔记本电脑物理Wi-Fi适配器，但它不直接管理无线连接。相反，主机笔记本电脑充当网桥，管理Wi-Fi连接并提供对VM的网络访问。因此，虚拟机无法直接查看或控制Wi-Fi网络，因为此功能由主机系统处理。此配置可确保VM在有效利用主机物理资源的同时，在网络上保持强大的在线状态。

网络图

网络图包含Cisco Catalyst 9800无线LAN控制器(WLC)和CW9176I接入点(AP)，它们提供到设备（例如笔记本电脑和托管在VirtualBox上的虚拟机[VM]）的无线连接。9800 WLC充当中央管理和控制单元，确保无线网络的无缝集成和高效运行。CW9176I AP配备高级Wi-Fi 7功能，可支持相连设备的高速可靠无线通信。主机虚拟机笔记本电脑运行Windows 11 Home并运行带Ubuntu软件的VirtualBox虚拟机。



网络图

配置

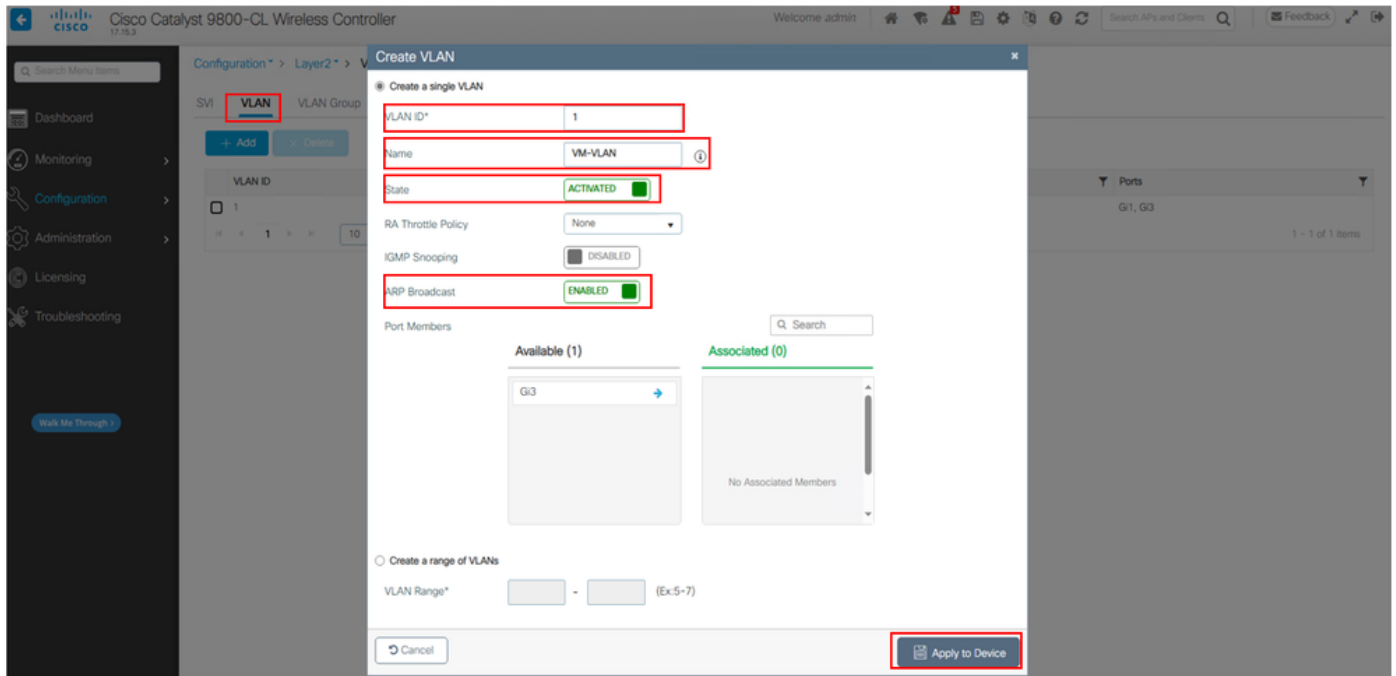
VLAN 配置

Cisco Catalyst 9800无线控制器上的ARP广播功能对于在拥有被动客户端的网络中实现通信至关重要。此功能在VLAN内的所有设备上广播ARP请求，这对于被动客户端（例如桥接适配器模式下的

虚拟机) 特别有用, 因为它们不会主动发送其IP信息。

WLC GUI

导航至配置>第2层> VLAN > 点击+ Add > VLAN ID "Custom VLAN ID" > Name "Custom Name" > State ACTIVATED > ARP Broadcast ENABLED, 如图所示。



VLAN 配置

WLC CLI

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

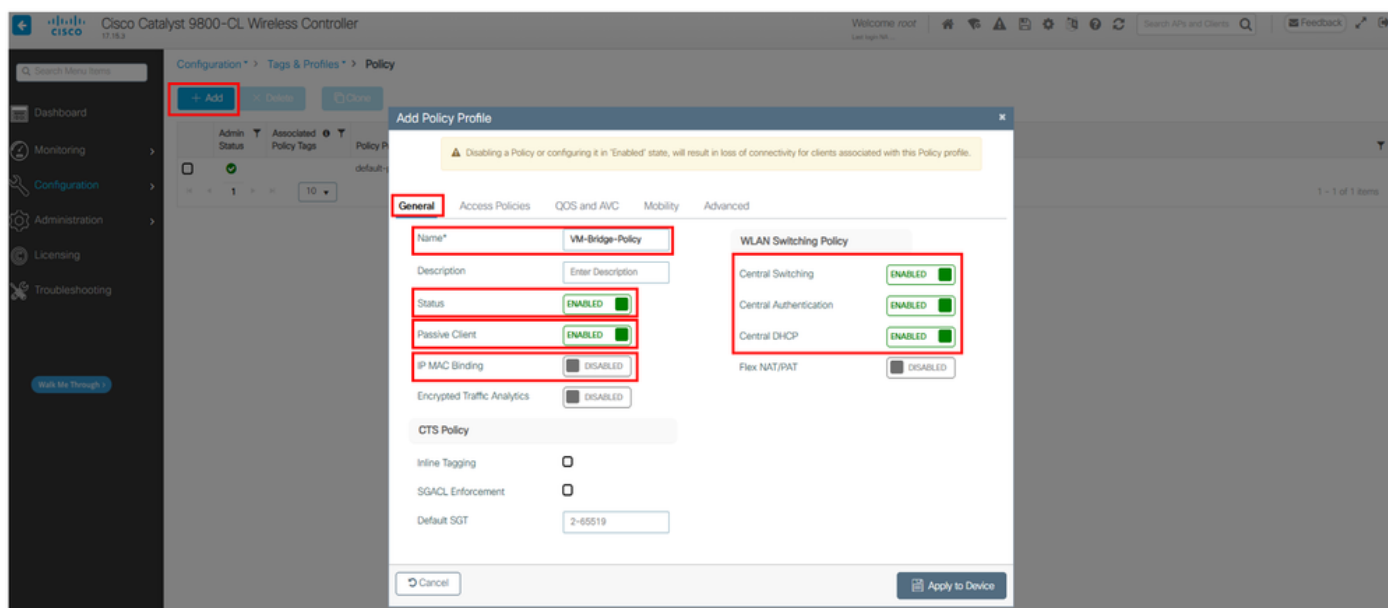
```
WLC(config)#vlan configuration [VLAN ID]  
WLC(config-vlan-config)#arp broadcast  
WLC(config-vlan-config)#end  
WLC#
```

策略配置文件配置

要确保在Cisco Catalyst 9800上使用网桥适配器配置的VM无缝连接, 必须启用被动客户端功能并禁用IP MAC绑定。此设置允许无线控制器处理与单个MAC地址关联的多个IP地址, 这在虚拟化环境中很常见。启用被动客户端可确保流量流向VM计算机。禁用IP-MAC绑定允许控制器将流量转发到VM计算机, 而不将其标识为IP Theft。

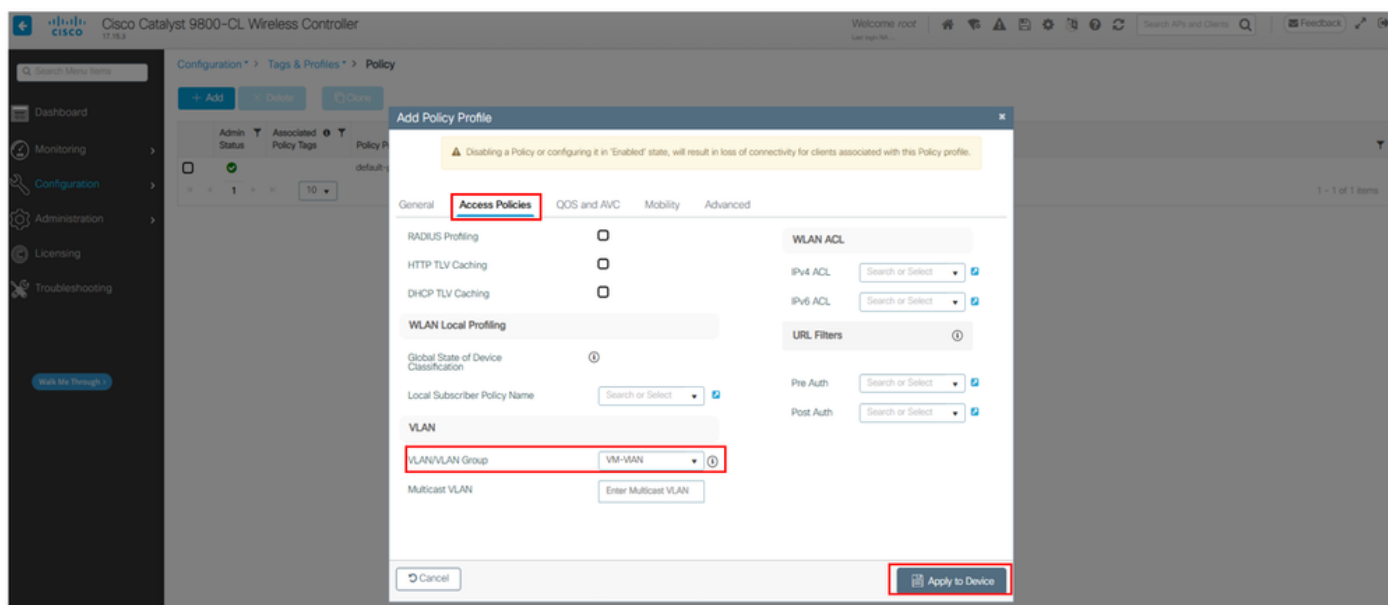
WLC GUI

导航到配置>标记和配置文件>策略>点击+添加>常规> WLAN交换策略>已启用中央交换>已启用中央身份验证>已启用中央DHCP，如图所示。



策略配置

导航到访问策略> VLAN > VLAN/VLAN组>配置VLAN >点击应用到设备，如图所示。



策略配置

WLC 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#
```

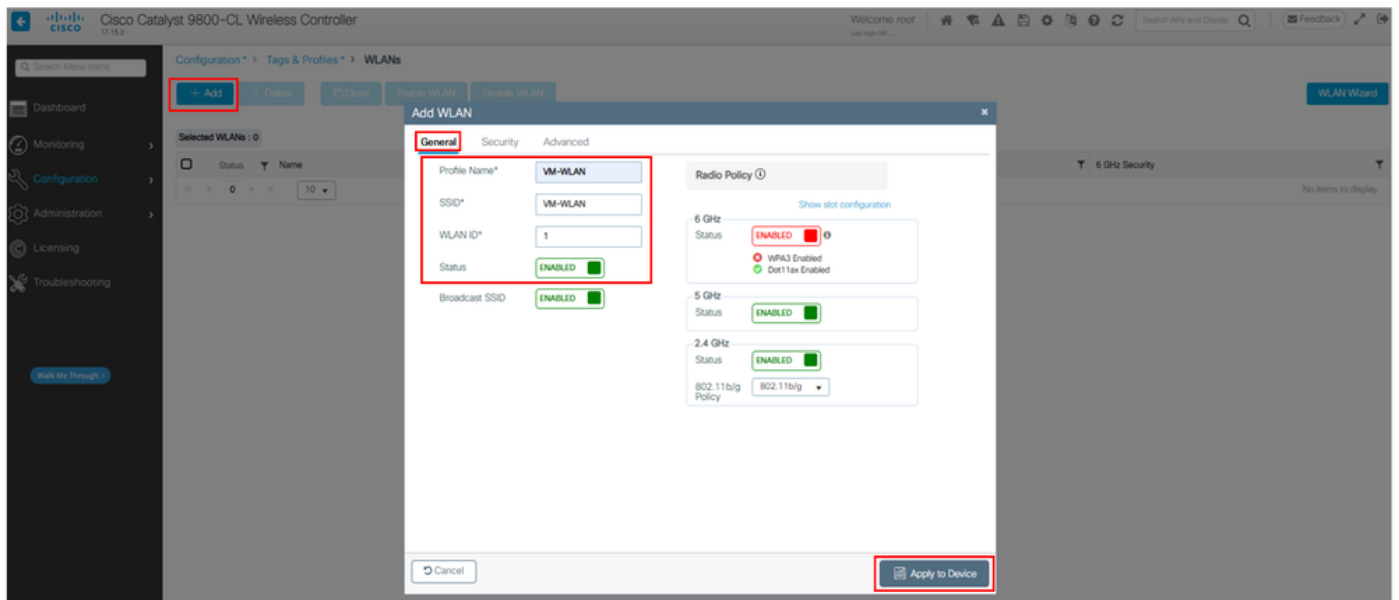


警告：禁用策略或将其配置为启用状态，会导致与此策略配置文件关联的客户端失去连接。

WLAN配置

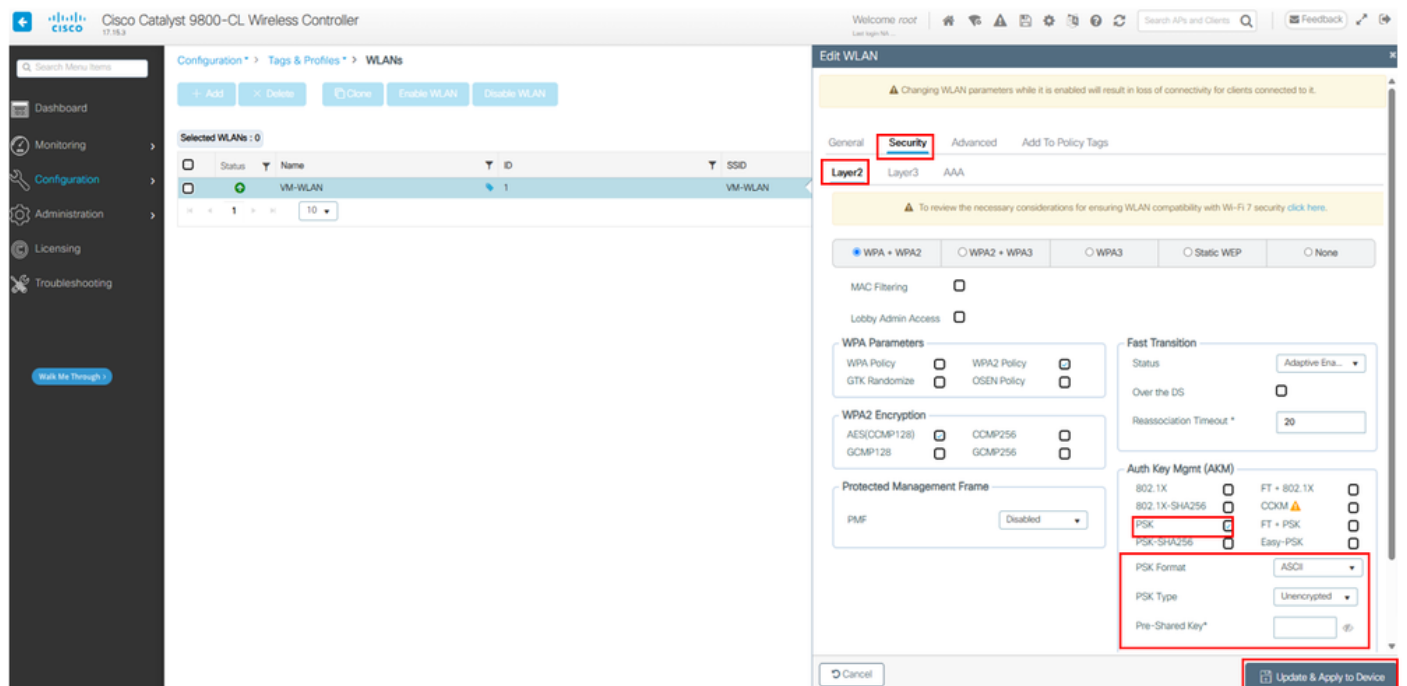
本示例说明为预共享密钥(PSK)身份验证配置的WLAN。但是，可以使用网桥适配器为VM配置WLAN以进行802.1X身份验证。

导航至配置>标记和配置文件> WLAN > 点击+添加>常规>配置文件名称“自定义名称”> SSID“自定义名称”> WLAN ID*“自定义名称”>状态ENABLED > 点击应用到设备，如图所示。



WLAN配置

导航到安全>Layer2 > PSK "复选框" > PSK Format ASCII > PSK Type Unencrypted > Pre-Shared Key* "Custom Key" > Click Update & Apply to Device，如图所示。



WLAN配置

WLC 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#
```

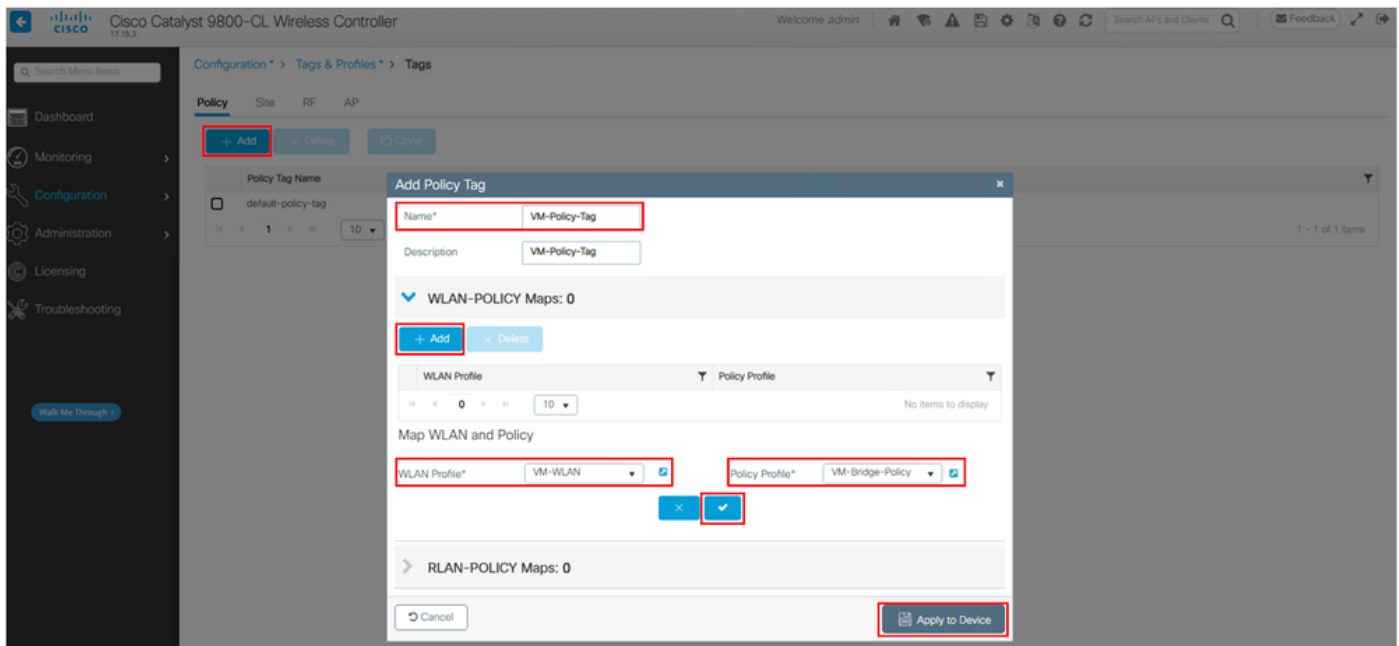


警告：启用WLAN时更改WLAN参数会导致与其连接的客户端失去连接。

策略标记配置

本示例说明将特定WLAN配置文件与特定策略配置文件绑定的策略标记配置。

导航到配置>标记和配置文件>标记>点击+添加>名称“自定义名称”> WLAN-POLICY映射：>点击+添加> WLAN配置文件* "选择自定义WLAN" >策略配置文件* "选择自定义策略" >点击"蓝色复选框">点击应用到设备，如图所示。



策略标记配置

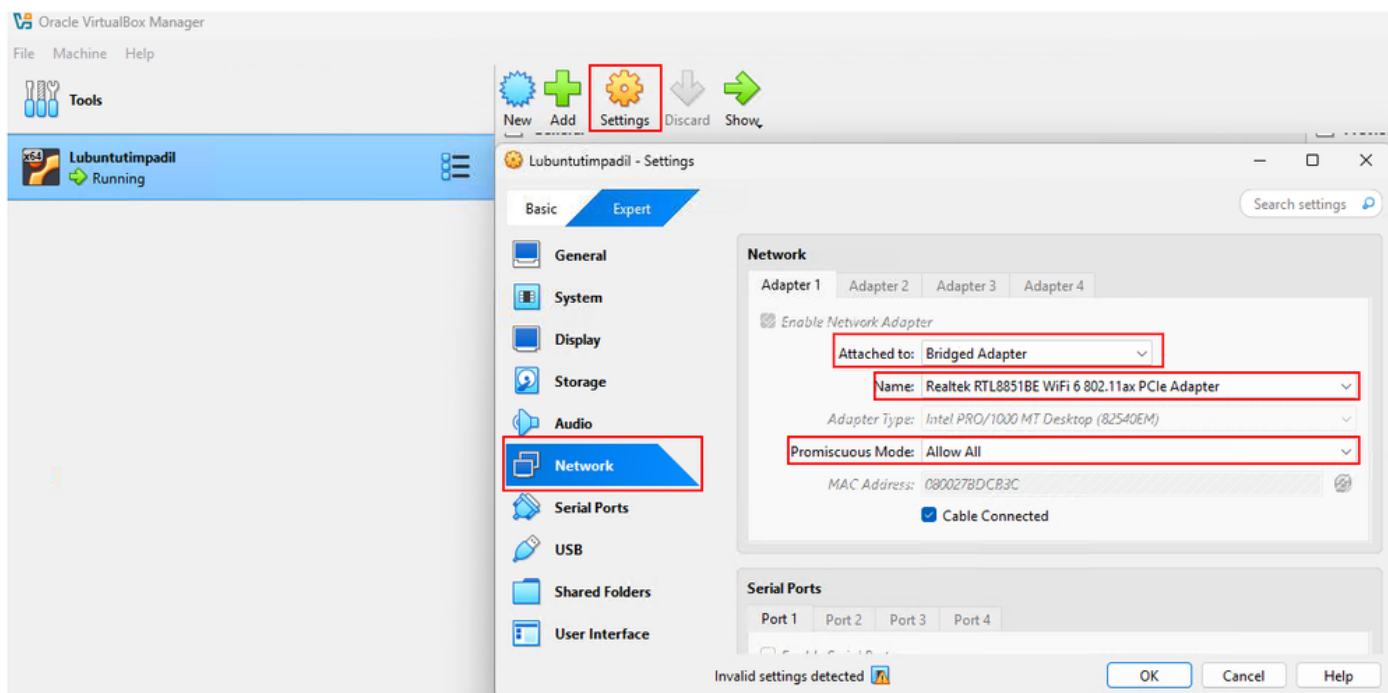
WLC CLI

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

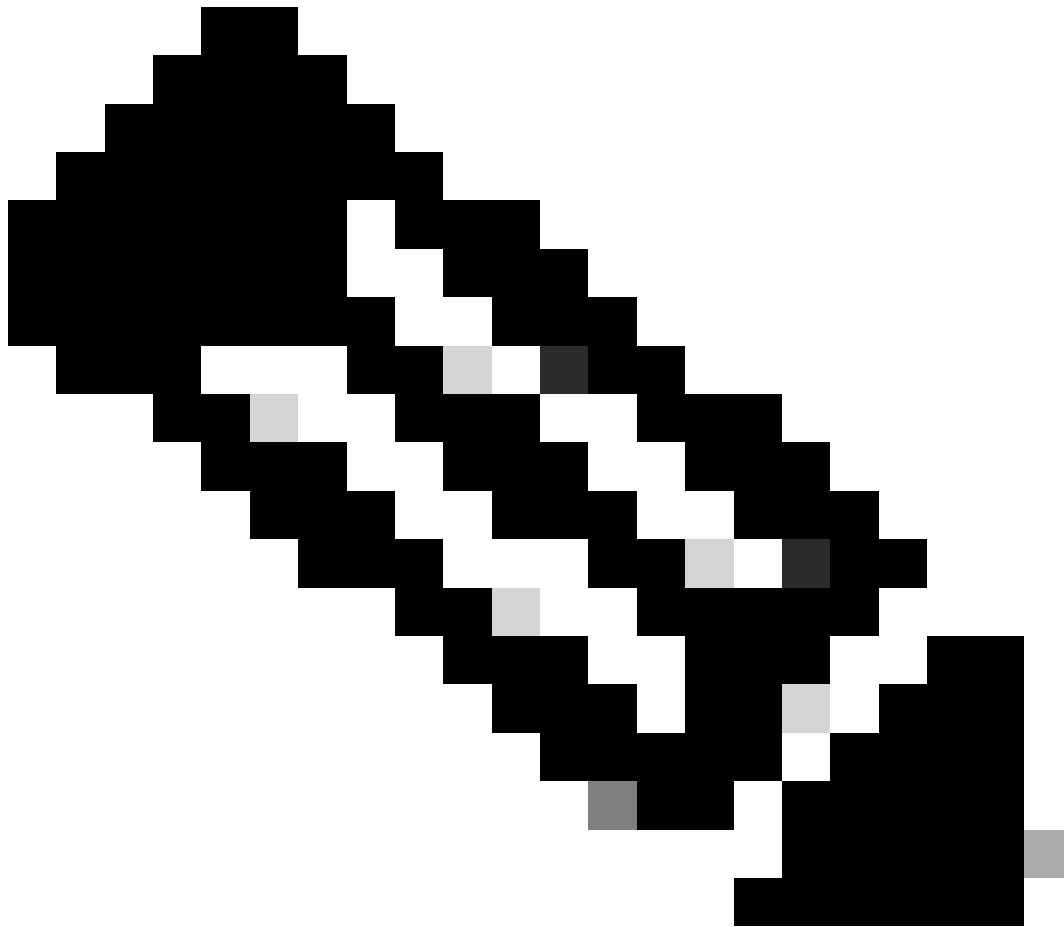
VM配置

桥接适配器功能使VM能够直接访问主机物理网络。

导航到设置>网络>连接到：选择Bridged Adapter > Name:“Select Laptop Physical WiFi Adapter” > Promiscuous Mode:选择Allow All（全部允许），如图所示。



VM配置



注意：虽然此设置使用带有Ubuntu操作系统的VirtualBox，但具体虚拟机设置的位置和命名规则可能因使用的虚拟化平台而异。

验证

从VM和9800 WLC中，可以使用这些命令和方法检查配置。

VM确认

要确认VM已成功从DHCP服务器获取IP地址，请在VM命令行界面中执行ifconfig命令。输出显示网络配置，包括分配的IP地址（如果通过DHCP获取）。

```
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命令行界面

现在在VM的命令行界面中执行ping以验证网关的可达性。

```
admin@timpadilLubuntu: ~
File Actions Edit View Help
admin@timpadilLubuntu: ~ x

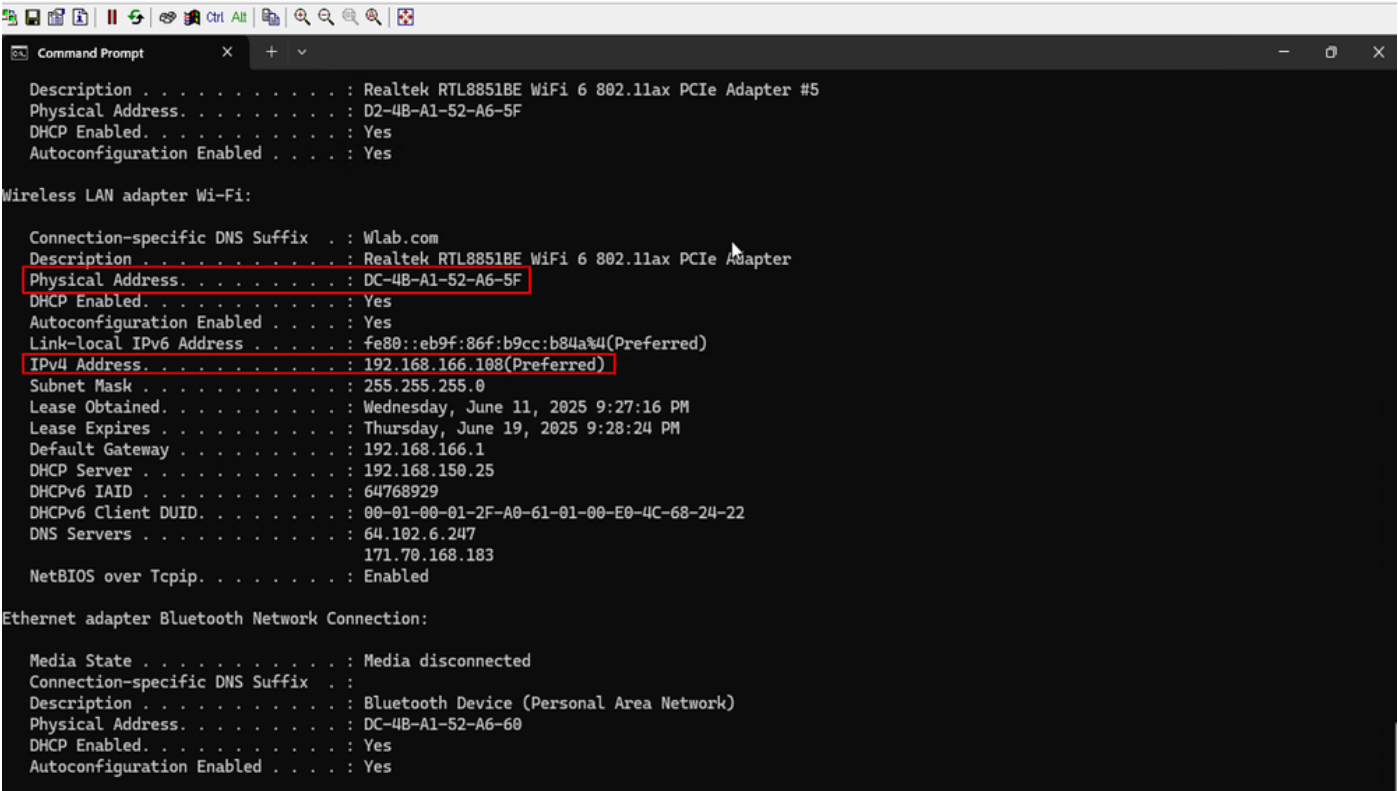
admin@timpadilLubuntu:~$ ping 192.168.166.1
PING 192.168.166.1 (192.168.166.1) 56(84) bytes of data.
64 bytes from 192.168.166.1: icmp_seq=1 ttl=64 time=175 ms
64 bytes from 192.168.166.1: icmp_seq=2 ttl=64 time=3.32 ms
64 bytes from 192.168.166.1: icmp_seq=3 ttl=64 time=28.6 ms
64 bytes from 192.168.166.1: 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命令行界面

主机VM确认

验证主机VM笔记本电脑的IP和MAC地址。

导航到Host VM laptop CLI (主机VM笔记本电脑CLI) ，然后执行ifconfig/all命令。



主机VM笔记本电脑

WLC确认

WLC 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#
```

故障排除

WLC仅显示主机VM笔记本电脑物理WiFi适配器的关联详细信息，包括其IP地址和MAC地址。它不会将VM识别为关联的客户端，并且不会显示VM的IP地址或MAC地址。

WLC客户端监控

IP地址192.168.166.108和MAC地址dc4b.a152.a65f已分配给主机VM笔记本电脑。请注意，虚拟机本身的IP和MAC地址在9800 WLC上不直接可见。但是，通过在无线LAN控制器上执行数据包捕获，您可以观察用作ICMP请求的源地址的VM IP地址192.168.166.111。同样，ICMP应答使用VM的IP地址作为目的地址。

导航到Monitoring > Wireless > Clients，如图所示。该图显示主机VM笔记本电脑的IP和MAC地址在Cisco 9800 WLCs GUI中清晰可见。

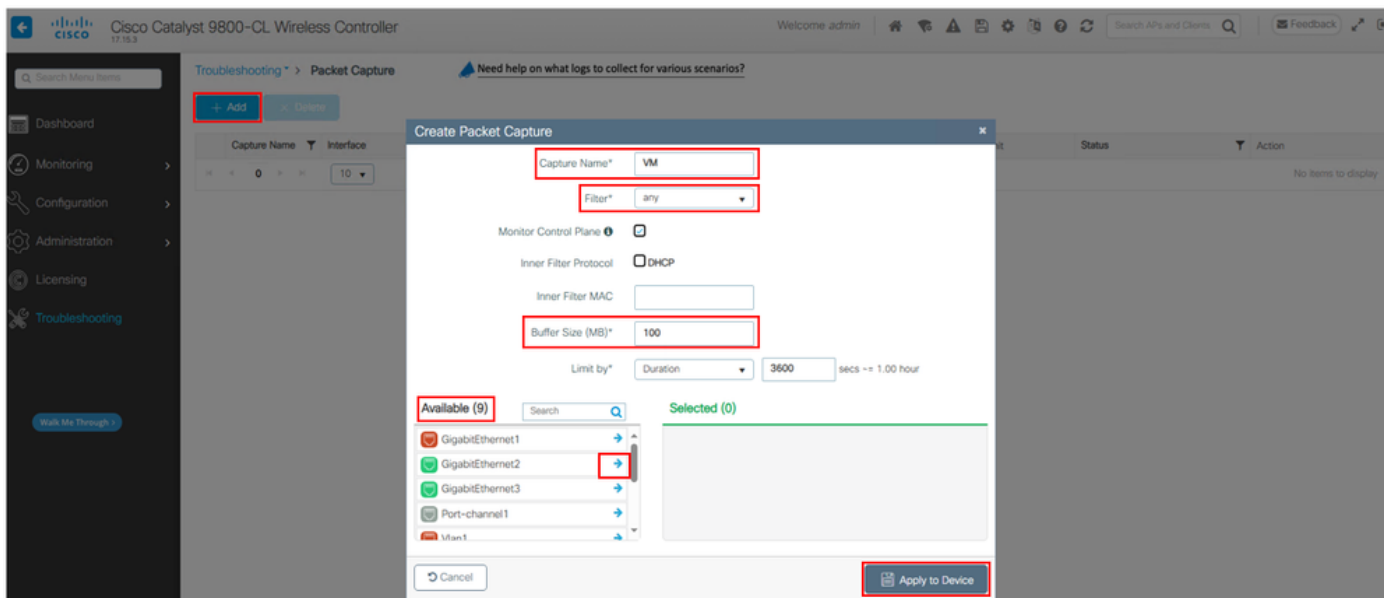


WLC客户端监控

WLC数据包捕获

本示例演示了9800 WLC上的数据包捕获配置。

导航到故障排除>数据包捕获>单击+添加>捕获名称* "创建自定义名称" > Filter* "any" > Buffer Size* "100" > Available "Select Interface" > Click Apply to Device，如图所示。



WLC数据包捕获配置

WLC CLI

WLC#

WLC#monitor capture [WORD] interface [Interface] [Interface Number] both

WLC#monitor capture [WORD] buffer size 100

WLC#monitor capture [WORD] match any

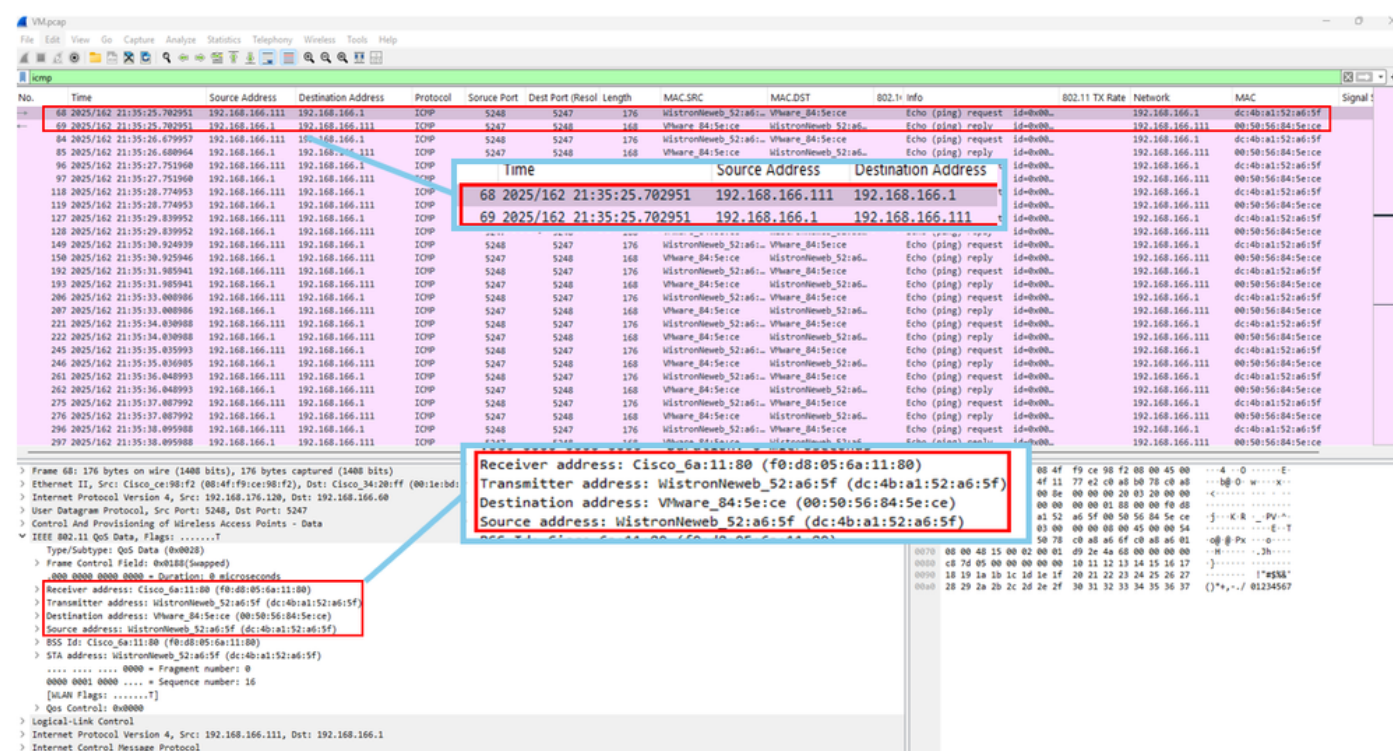
```
WLC#monitor capture [WORD] start
WLC#monitor capture [WORD] stop
WLC#monitor capture [WORD] export flash:[Name.pcap]
WLC#no monitor capture [WORD]
WLC# copy flash:<Name.pcap> tftp://<IP ADD>/<Name.pcap>
WLC#
```

Wireshark数据包捕获

在Wireshark数据包捕获中，观察到VM的IP地址192.168.166.111作为ICMP请求的源地址。此外，ICMP应答使用与目的地址相同的IP地址。

- 接收方地址是AP MAC地址
- 发射器地址是主机VM笔记本电脑MAC地址
- 目的地址是网关MAC地址
- 源地址是主机VM笔记本电脑MAC地址

图中所示的图片是Wireshark数据包捕获虚拟机ICMP请求到网关IP地址(192.168.166.1)的示例。



Wireshark数据包捕获

相关信息

- [Cisco Catalyst 9800系列无线控制器软件配置指南, Cisco IOS XE 17.15.x](#)
- [Cisco Catalyst 9800系列无线控制器、Cisco IOS XE 17.15.x版本说明](#)
- [思科无线CW9176接入点部署指南](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。