配置使用NAT的9800无线局域网控制器移动隧道

目录

简介

本文档介绍如何使用网络地址转换(NAT)移动隧道配置9800无线局域网控制器(WLC)。

先决条件

要求

Cisco 建议您了解以下主题：

- 静态网络地址转换(NAT)配置和概念。
- 9800无线局域网控制器移动隧道配置和概念。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 9800无线控制器系列(Catalyst 9800-L)、Cisco IOS® XE Gibralto 17.9.4
- 集成多业务路由器(ISR)、Cisco IOS® XE Gibraltar 17.6.5
- Catalyst 3560系列交换机，Cisco IOS® XE Gibraltar 15.2.4E10

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。

背景信息

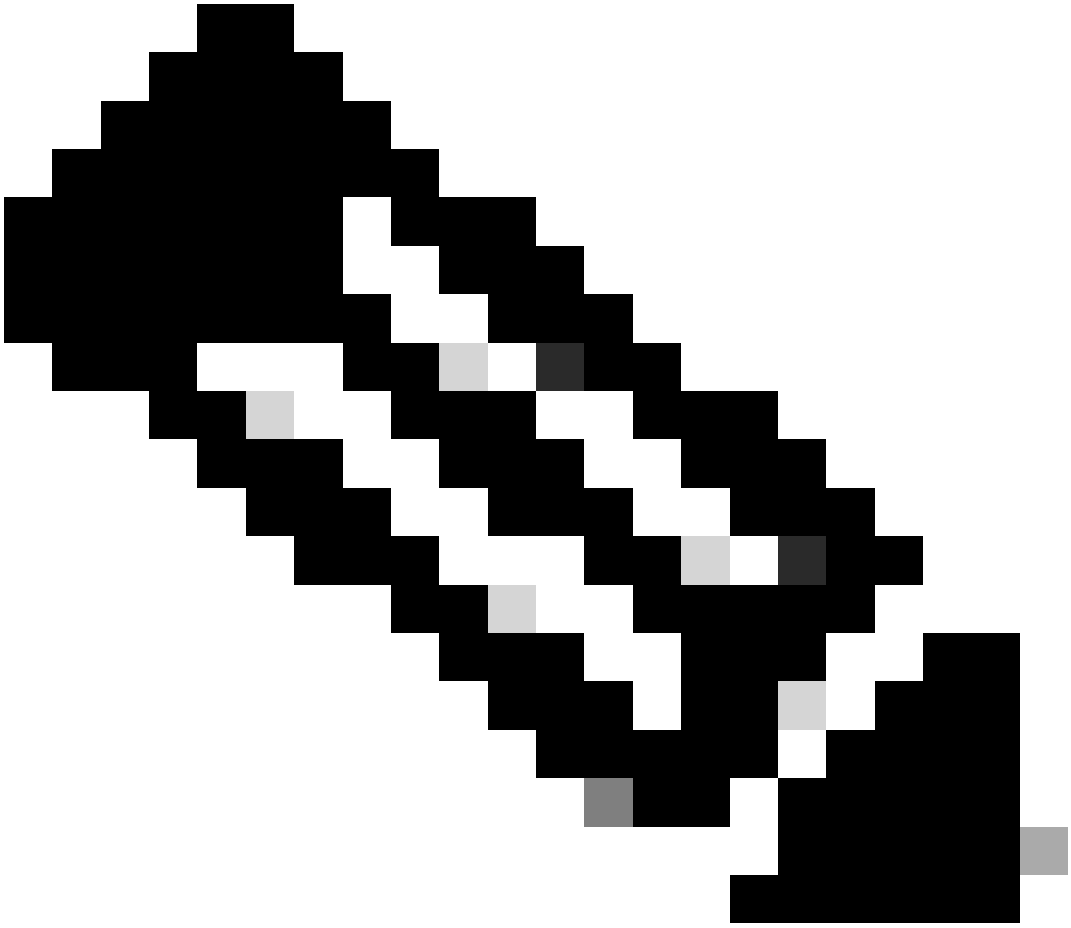
在两个或多个无线局域网控制器(WLC)之间创建移动隧道，意图在它们之间共享信息，例如接入点信息、无线客户端信息、RRM信息等。

它还可以用作基于锚点-外部设计的配置。本文档介绍如何使用网络地址控制(NAT)在无线局域网控制器(WLC)之间配置移动隧道。

WLC移动隧道可以有以下四种状态之一：

- 控制和数据路径关闭
- 控制路径关闭（这意味着数据路径处于打开状态）
- 数据路径关闭（这意味着控制打开）
- Up

移动隧道的最终和正确状态是：启用，任何其他状态都需要进一步调查。移动隧道在CAPWAP udp端口16666和16667上运行，udp端口16666用于控制路径，而16667用于数据路径，因此，必须确保这些端口在WLC之间处于打开状态。

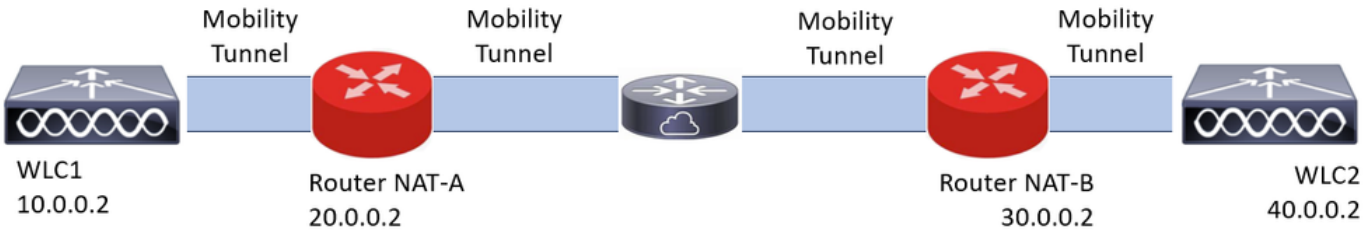


注意：有关不使用NAT的WLC移动隧道配置，请参阅在Catalyst 9800无线LAN控制器上配置移动拓扑

对移动组的NAT支持的限制

- 只能配置静态NAT (1:1)。
- 不支持具有相同公共IP地址的多个移动隧道对等体。
- 每个成员都必须具有唯一的私有IP地址。
- 不支持端口地址转换(PAT)。
- 不支持无线客户端漫游的版本间控制器移动(IRCM)。
- 不支持IPv6地址转换。
- WLC代码版本17.7.1及更高版本支持具有移动隧道的网络访问控制(NAT)。

网络图



配置

在路由器上配置NAT

在此配置中使用路由器来提供网络访问控制(NAT)功能，但是，可以使用任何能够执行静态NAT的设备。静态NAT是WLC移动隧道支持的NAT方法，这是路由器配置示例中使用的配置。出于配置目的，使用以下路由器：NAT-A和NAT-B。WLC1位于路由器NAT-A之后，WLC2位于路由器NAT-B之后。

路由器NAT-A配置：

CLI：

<#root>

```
RouterNAT-A#config t
RouterNAT-A(config)#interface GigabitEthernet0/1/
```

0

```
RouterNAT-A(config-if)#ip add 10.0.0.1 255.255.255.0
RouterNAT-A(config-if)#ip nat
```

inside

```
RouterNAT-A(config-if)#end
RouterNAT-A#

RouterNAT-A#config t
RouterNAT-A(config)#interface GigabitEthernet0/1/
```

1

```
RouterNAT-A(config-if)#ip add 20.0.0.1 255.255.255.0
RouterNAT-A(config-if)#ip nat
```

outside

```
RouterNAT-A(config-if)#end
RouterNAT-A#

RouterNAT-A#config t
RouterNAT-A(config)#ip nat inside source static 10.0.0.2 20.0.0.2
RouterNAT-A(config)#end
RouterNAT-A#
```

路由器NAT-B配置：

CLI：

<#root>

```
RouterNAT-B#config t
RouterNAT-B(config)#interface GigabitEthernet0/1/
```

2

```
RouterNAT-B(config-if)#ip add 40.0.0.1 255.255.255.0
RouterNAT-B(config-if)#ip nat
```

inside

```
RouterNAT-B(config-if)#end
RouterNAT-A#

RouterNAT-B#config t
RouterNAT-B(config)#interface GigabitEthernet0/1/
```

3

```
RouterNAT-B(config-if)#ip add 30.0.0.1 255.255.255.0
RouterNAT-B(config-if)#ip nat
```

outside

```
RouterNAT-B(config-if)#end
RouterNAT-A#

RouterNAT-A#config t
RouterNAT-A(config)#ip nat inside source static 40.0.0.2 30.0.0.2
RouterNAT-A(config)#end
RouterNAT-A#
```

在无线局域网控制器上配置使用NAT的移动性

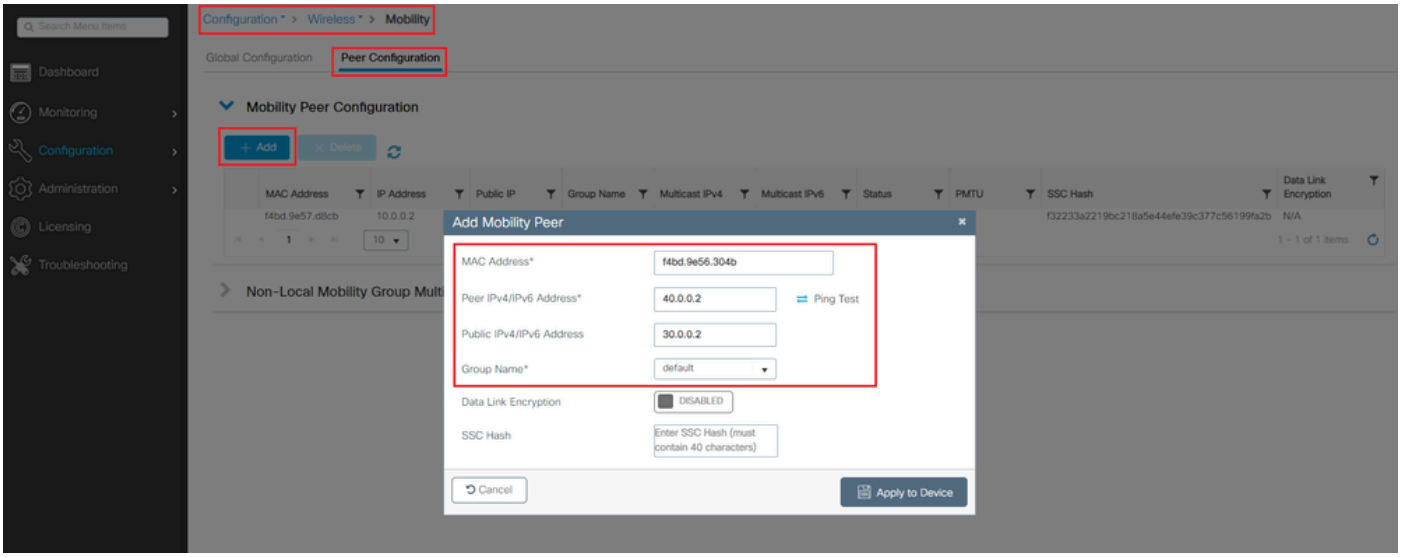
以下是要在WLC之间共享的配置，以使用NAT创建移动隧道：

- 专用移动IP地址
- 公共移动IP地址
- 移动组Mac地址
- 移动组名称

WLC1的配置会添加到WLC2，反之亦然，这可以通过WLC中的CLI或GUI完成，因为此配置的最终目标是使用NAT的移动隧道，所以两个WLC的公共移动IP地址是每个路由器静态NAT配置中配置的NAT IP地址。

WLC1配置：

GUI:

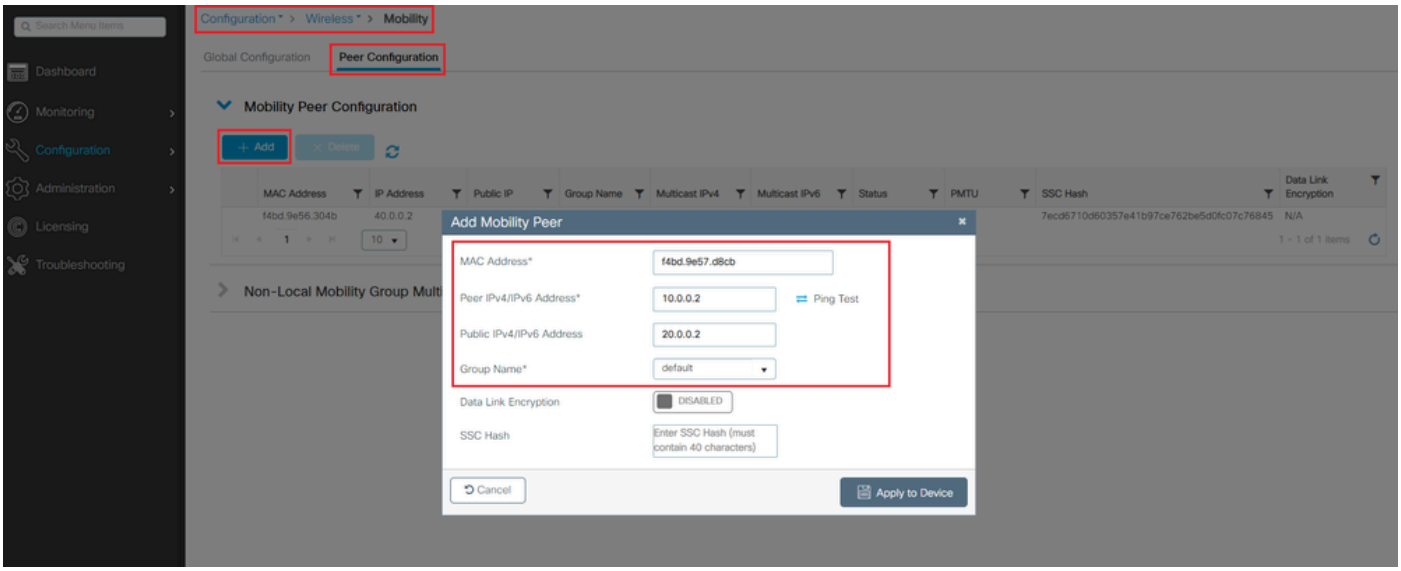


CLI：

```
WLC1#config t
WLC1(config)#wireless mobility group member mac-address f4bd.9e56.304b ip 40.0.0.2 public-ip 30.0.0.2 g
WLC1(config)#end
WLC1#
```

WLC2配置：

GUI:



CLI：

```
WLC2#config t
WLC2(config)#wireless mobility group member mac-address f4bd.9e57.d8cb ip 10.0.0.2 public-ip 20.0.0.2 g
WLC2(config)#end
WLC2#
```

验证

路由器配置验证

从路由器端这些命令可验证NAT配置。NAT配置必须是静态的（如本文档前面所述），因此存在NAT的内部和外部配置。

路由器NAT-A

```
RouterNAT-A#show run interface GigabitEthernet0/1/0
interface GigabitEthernet0/1/0
ip add 10.0.0.1 255.255.255.0
ip nat inside
!
RouterNAT-A#show run interface GigabitEthernet0/1/1
interface GigabitEthernet0/1/1
ip add 20.0.0.1 255.255.255.0
ip nat outside
!
RouterNAT-A#show run | in ip nat inside
ip nat inside source static 10.0.0.2 20.0.0.2
```

路由器NAT-B

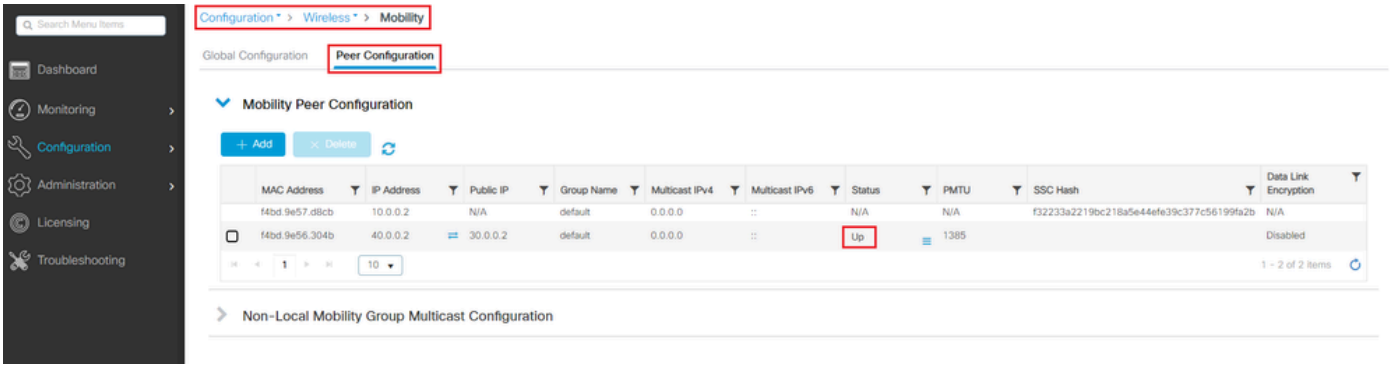
```
RouterNAT-B#show run interface GigabitEthernet0/1/2
interface GigabitEthernet0/1/2
ip add 40.0.0.1 255.255.255.0
ip nat inside
!
RouterNAT-B#show run interface GigabitEthernet0/1/3
interface GigabitEthernet0/1/3
ip add 30.0.0.1 255.255.255.0
ip nat outside
!
RouterNAT-B#show run | in ip nat inside
ip nat inside source static 40.0.0.2 30.0.0.2
```

无线LAN控制器配置验证

从WLC GUI和CLI检查移动隧道的状态，如本文档前面所述，用于确认通过移动隧道在WLC之间正确通信的正确状态是：Up，任何其他状态都需要调查。

WLC1

GUI:



CLI :

<#root>

```
WLC1#
```

show wireless mobility summary

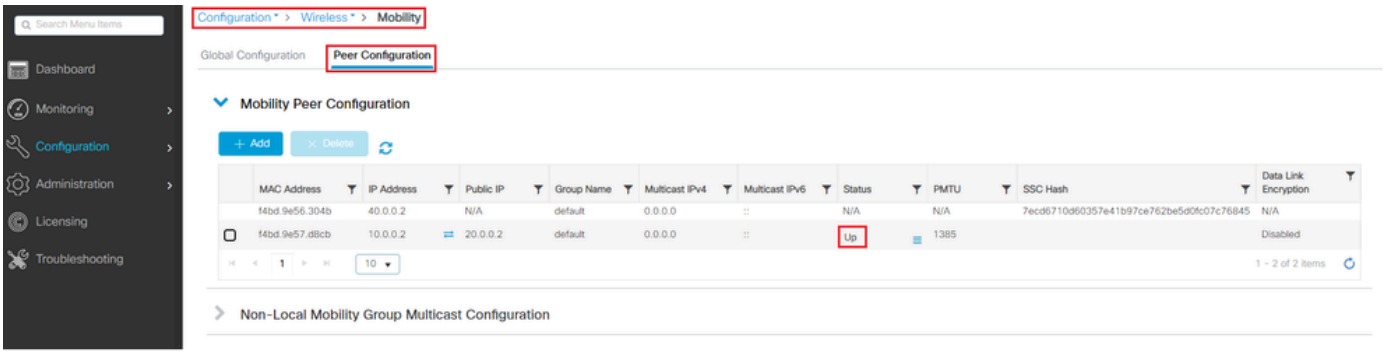
```
Mobility Summary

Wireless Management VLAN: 10
Wireless Management IP Address: 10.0.0.2
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 0
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384, TLS_RSA_AE
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: f4bd.9e57.d8cb
Mobility Domain Identifier: 0x34ac

Controllers configured in the Mobility Domain:

 IP          Public Ip     MAC Address         Group Name     Multicast IPv4     Multicast IPv6   Statu
-----------------------------------------------------------------------------------------------------
10.0.0.2    N/A           f4bd.9e57.d8cb      default        0.0.0.0            ::                N/A
40.0.0.2    30.0.0.2      f4bd.9e56.304b      default        0.0.0.0            ::
```

Up

```
         1385
```

WLC2

GUI:



CLI：

<#root>

WLC2#

show wireless mobility summary

```
Mobility Summary

Wireless Management VLAN: 40
Wireless Management IP Address: 40.0.0.2
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 0
Mobility High Cipher : False
Mobility DTLS Supported Ciphers: TLS_ECDHE_RSA_AES128_GCM_SHA256, TLS_RSA_AES256_GCM_SHA384, TLS_RSA_AE
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: default
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: f4bd.9e56.304b
Mobility Domain Identifier: 0x34ac

Controllers configured in the Mobility Domain:

 IP          Public Ip     MAC Address         Group Name     Multicast IPv4     Multicast IPv6    Statu
-------------------------------------------------------------------------------------------------------
40.0.0.2    N/A           f4bd.9e56.304b     default        0.0.0.0            ::                N/A
10.0.0.2    20.0.0.2      f4bd.9e57.d8cb     default        0.0.0.0            ::
```

Up

```
         1385
```

故障排除

路由器故障排除

从路由器端验证IP NAT转换是否正确进行。

IP NAT转换和统计信息

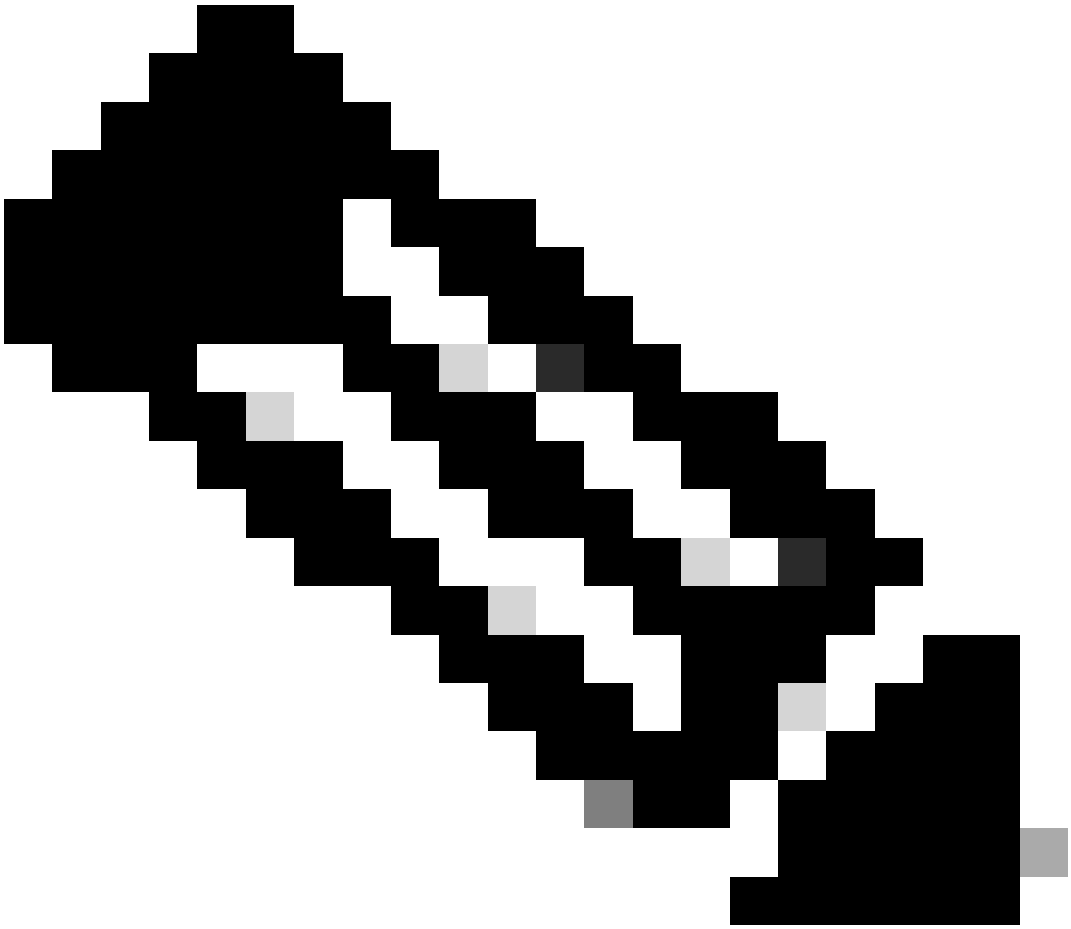
使用这些命令查看在路由器中执行的内部和外部转换，以及检查NAT统计信息。

```
#show ip nat translations
#show ip nat statistics
```

IP NAT debug

此命令从路由器的角度调试NAT转换，以了解NAT是如何发生的，或路由器执行NAT转换时是否存在任何问题。

```
#debug ip nat
#show debug
```



注意：路由器上的任何debug命令都可能导致过载，从而导致路由器无法运行。使用路由器中的调试时必须极其小心，如果可能，在生产期间不要在关键的生产路由器上运行任何调试，则需要维护窗口。

无线局域网控制器故障排除

如果移动隧道显示的任何状态不正确（处于Up状态），可以从WLC收集此处的信息。

移动进程日志

此命令生成过去和现在的移动日志

```
#show logging process mobilityd start last 1 days to-file bootflash:mobilitytunnel.txt
```

使用命令，可以在WLC自身中读取收集到的信息

```
#more bootflash:mobilitytunnel.txt
```

还可以使用命令从WLC导出收集到的信息，以便在外部源中读取这些信息

```
#copy bootflash:mobilitytunnel.txt tftp://<TFTP IP ADD>/mobilitytunnel.txt
```

移动调试和跟踪

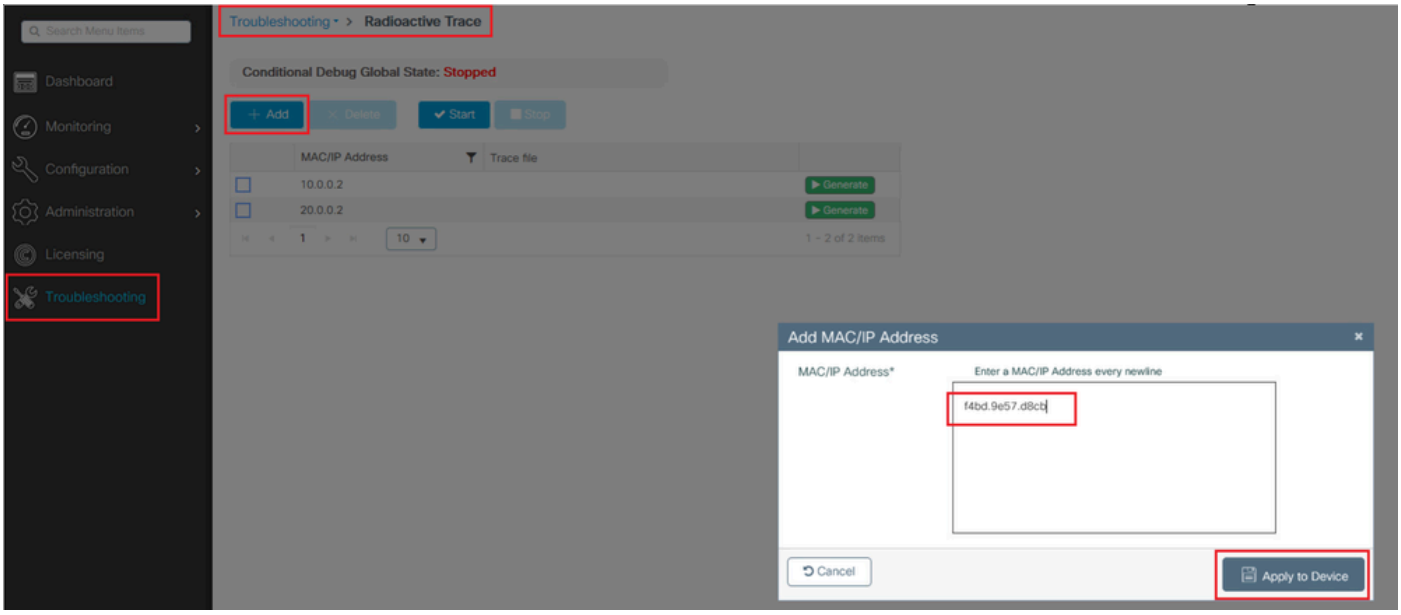
调试和跟踪可以提供更详细的信息，以防移动进程日志无法生成足够的信息来查找问题。

当使用NAT为移动隧道收集调试和跟踪信息时，在trace部分输入以下信息以同时获取信息来更好地了解行为非常重要：

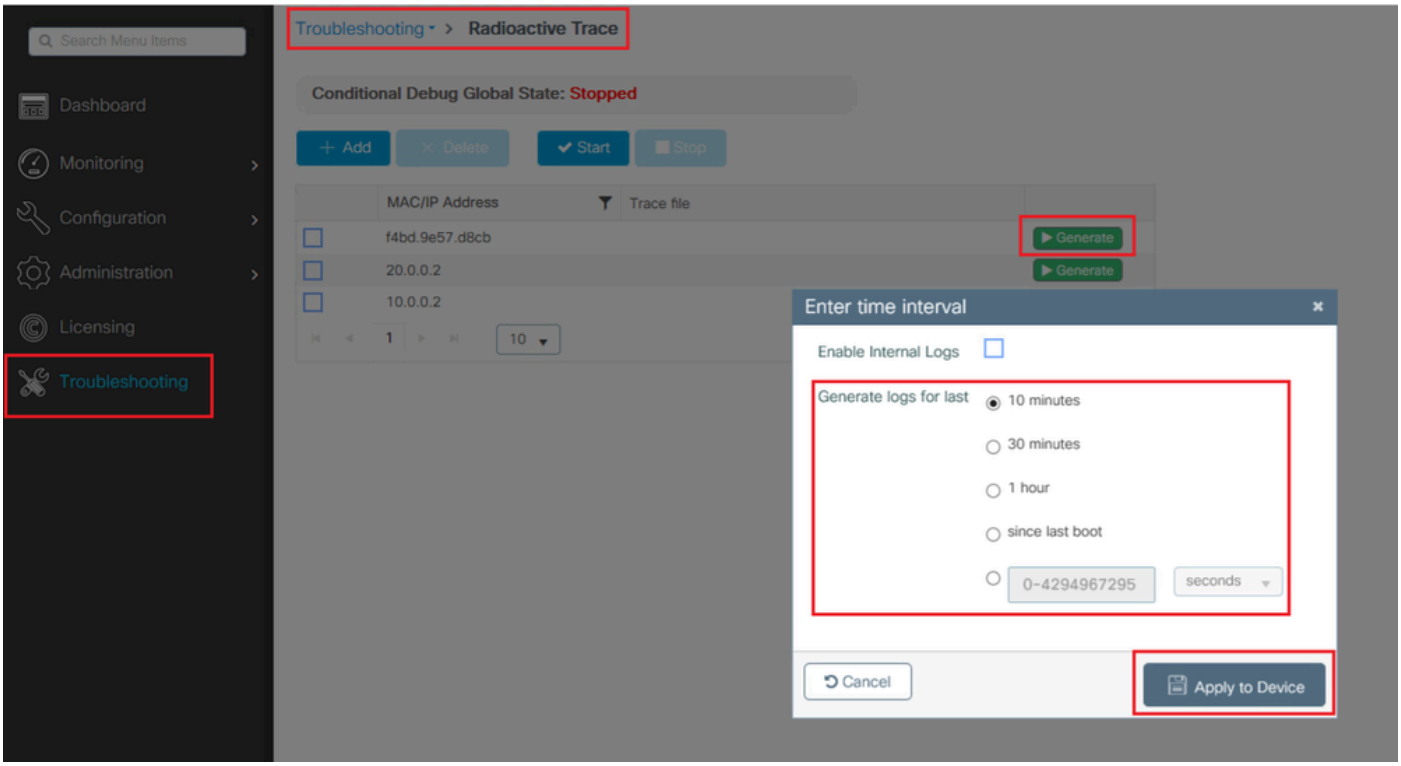
- 对等体公共移动IP地址
- 对等专用移动IP地址
- 对等移动Mac地址

在本示例中，在WLC2中输入WLC1的公有IP地址和私有IP地址以及移动MAC地址，同样必须向后执行，在WLC1的RA跟踪部分中，输入WLC2的私有IP地址和公有IP地址。

WLC GUI



调试和跟踪可以从GUI中收集，如下所示。



WLC CLI

```
debug platform condition feature wireless ip 10.0.0.2
debug platform condition feature wireless ip 20.0.0.2
debug platform condition feature wireless mac f4bd.9e57.d8cb
```

要收集调试信息，可以使用此命令。根据需要更改调试收集的时间。

```
#show logging profile wireless last 30 minutes filter mac f4bd.9e57.d8cb to-file bootflash:mobilityf4bd
#show logging profile wireless last 30 minutes filter ip 10.0.0.2 to-file bootflash:mobility10002.txt
#show logging profile wireless last 30 minutes filter ip 20.0.0.2 to-file bootflash:mobility20002.txt
```

使用传输协议将文件复制到外部源。

```
#copy bootflash:mobilityf4bd9e57d8cb.txt tftp://<TFTP IP ADD>/mobilityf4bd9e57d8cb.txt
#copy bootflash:mobility10002.txt tftp://<TFTP IP ADD>/mobility10002.txt
#copy bootflash:mobility20002.txt tftp://<TFTP IP ADD>/mobility20002.txt
```

数据包捕获

9800 WLC能够捕获嵌入式数据包，使用此功能可检查对于使用NAT的移动隧道，WLC之间交换了哪些数据包。

在本示例中，在WLC2中使用WLC1的专用IP地址设置数据包捕获，同样必须向后执行，其中必须使用WLC1中WLC2的专用IP地址设置数据包捕获。

为了捕获数据包，可以创建ACL来过滤数据包，并只显示我们通过NAT查找的移动隧道的数据包，创建ACL后，ACL将作为过滤器附加到数据包捕获中。由于该ACL是数据包报头中的地址，因此可以使用移动专用IP地址创建ACL。

```
#config t
(config)#ip access-list extended Mobility
(config-ext-nacl)#permit ip host 10.0.0.2 any
(config-ext-nacl)#permit ip any host 10.0.0.2
(config-ext-nacl)#end

#monitor capture MobilityNAT interface <Physical Interface/Port-Channel number> both access-list Mobili
```

在捕获开始之前，此命令可用于检查监控器捕获配置。

```
#show monitor capture MobilityNAT
```

一旦显示器捕获准备就绪并选中，即可启动该捕获。

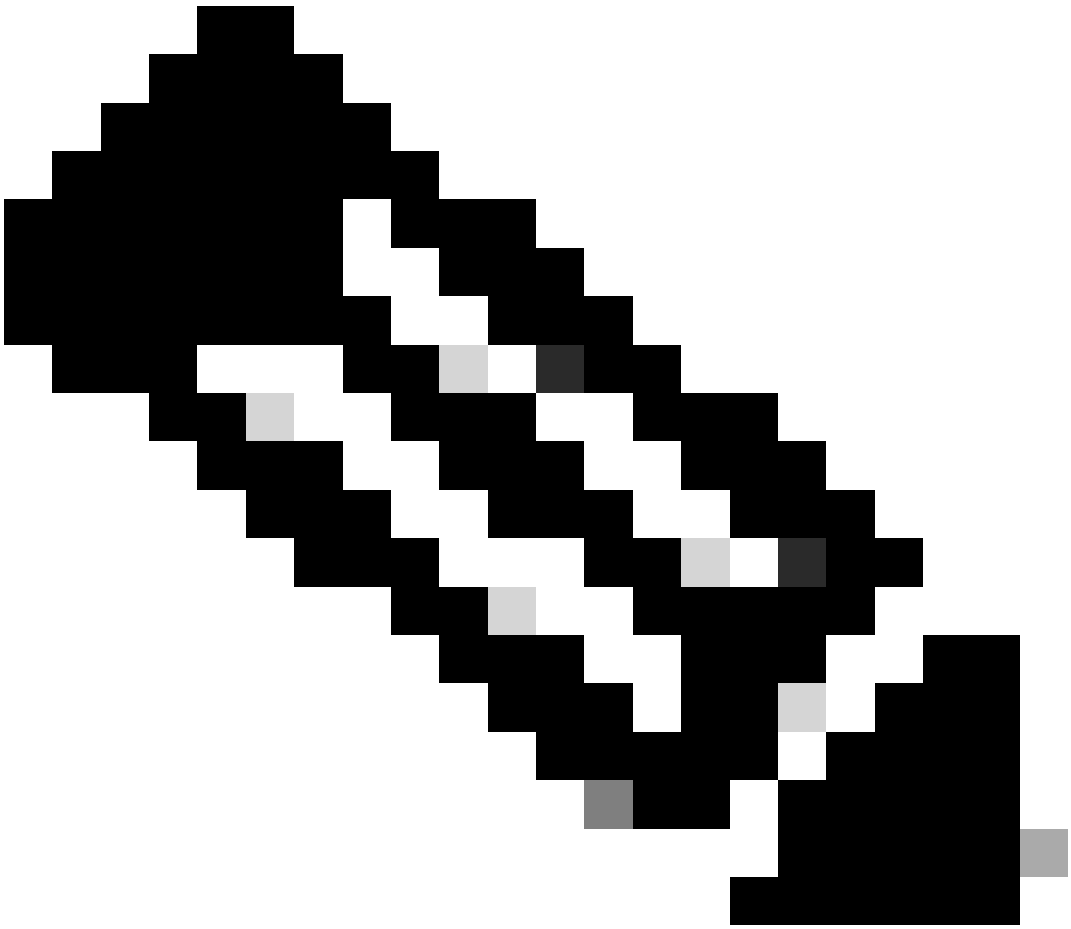
```
#monitor capture MobilityNAT start
```

要停止此命令，可以使用此命令。

```
#monitor capture MobilityNAT stop
```

一旦监控器捕获停止，就可以使用传输协议将其导出到外部源。

```
#monitor capture MobilityNAT export tftp://<TFTP IP ADD>/MobilityNat.pcap
```



注意：具有NAT的移动隧道是一种需要WLC之间双向会话的功能，由于该功能的性质，强烈建议同时从两个WLC收集日志、调试和跟踪或数据包捕获，以更好地了解具有NAT数据包交换的移动隧道。

清除调试、跟踪和数据包捕获

获取所需信息后，可以按照此处所述从WLC中删除调试、跟踪和嵌入式数据包捕获配置。

调试和跟踪

```
#clear platform condition all
```

数据包捕获

```
#config t
(config)# no ip access-list extended Mobility
(config)#end
#no monitor capture MobilityNAT
```

强烈建议在收集所需信息后清除WLC中执行的故障排除配置。

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）。