

設定使用NAT的9800無線LAN控制器行動通道

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[對移動組的NAT支援的限制](#)

[網路圖表](#)

[設定](#)

[在路由器上配置NAT](#)

[在無線區域網控制器上配置使用NAT的移動性](#)

[驗證](#)

[路由器配置驗證](#)

[無線LAN控制器組態驗證](#)

[疑難排解](#)

[路由器故障排除](#)

[IP NAT轉換和統計資訊](#)

[IP NAT調試](#)

[無線區域網控制器故障排除](#)

[移動進程日誌](#)

[移動調試和跟蹤](#)

[封包擷取](#)

[清除調試、跟蹤和資料包捕獲](#)

簡介

本文說明如何使用透過網路位址翻譯(NAT)的行動通道設定9800無線Lan控制器(WLC)。

必要條件

需求

思科建議您瞭解以下主題：

- 靜態網路位址翻譯(NAT)組態和概念。
- 9800無線Lan控制器行動通道組態和概念。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- Catalyst 9800無線控制器系列(Catalyst 9800-L)、Cisco IOS® XE直布羅陀版17.9.4
- 整合多業務路由器(ISR) , Cisco IOS® XE直布羅陀版17.6.5
- Catalyst 3560系列交換器 , Cisco IOS® XE直布羅陀版15.2.4E10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除 (預設) 的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

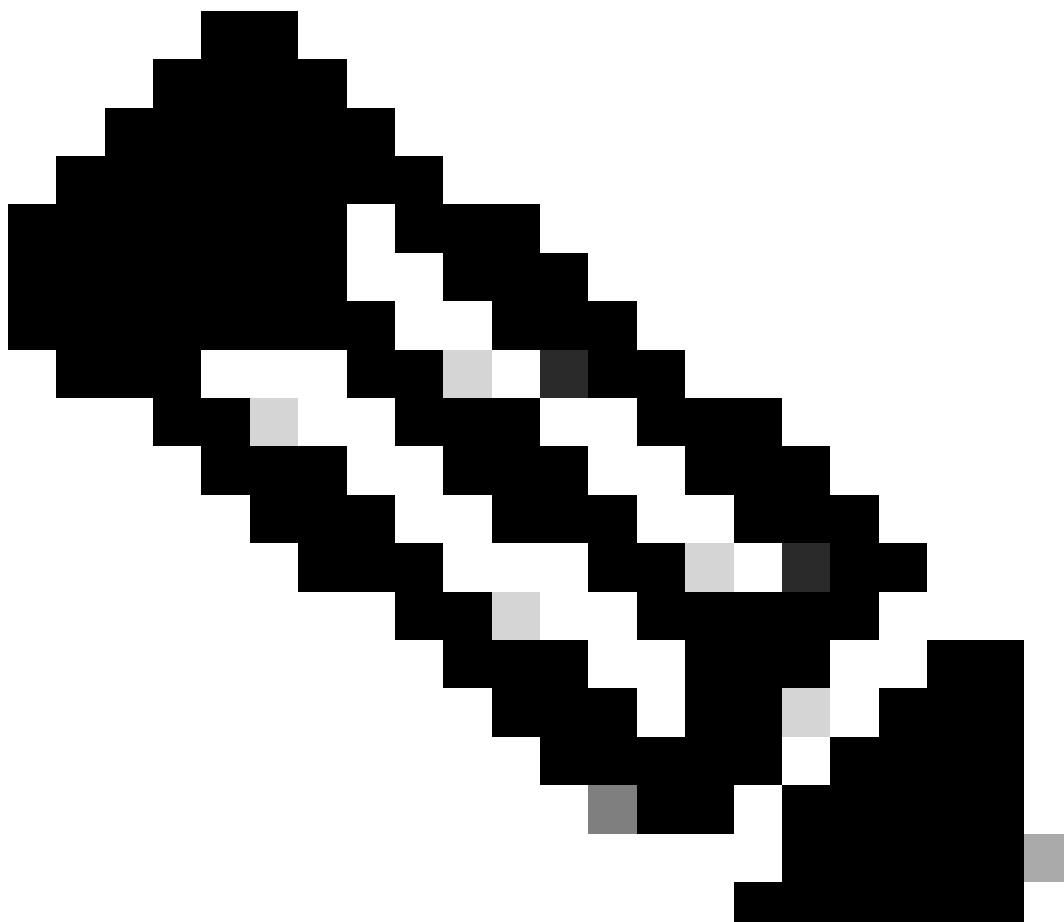
在兩個或多個無線LAN控制器(WLC)之間建立移動隧道，意圖在其中共用資訊，例如存取點資訊、無線客戶端資訊、RRM資訊等。

它還可以用作基於錨點-外部設計的配置。本檔案介紹如何使用網路位址控制(NAT)在無線LAN控制器(WLC)之間設定行動通道。

WLC行動通道可以有以下四種狀態之一：

- 控制和資料路徑向下
- 控制路徑向下 (這表示資料路徑向上)
- 資料路徑關閉 (表示控制功能啟動)
- UP

移動隧道的最終和正確狀態是：啟用，任何其他狀態都需要進一步調查。移動隧道在CAPWAP UDP埠16666和16667上運行，而UDP埠16666用於控制路徑，而16667用於資料路徑，因此，有必要確保在WLC之間打開這些埠。

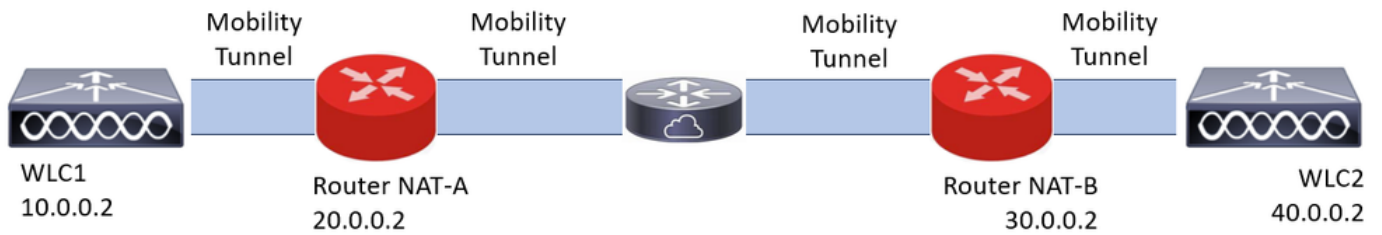


注意：有關不帶NAT的WLC移動隧道配置，請參閱[在Catalyst 9800無線LAN控制器上配置移動拓撲](#)

對移動組的NAT支援的限制

- 只能配置靜態NAT (1:1)。
- 不支援具有相同公共IP地址的多個移動隧道對等體。
- 每個成員都必須具有唯一的私有IP地址。
- 不支援埠地址轉換(PAT)。
- 不支援無線使用者端漫遊的版本間控制器行動性(IRCM)。
- 不支援IPv6地址轉換。
- WLC代碼版本17.7.1及更高版本支援使用移動隧道的網路訪問控制(NAT)。

網路圖表



設定

在路由器上配置NAT

在此配置中使用路由器來提供網路訪問控制(NAT)功能，但是，可以使用任何能夠執行靜態NAT的裝置。靜態NAT是WLC移動隧道支援的NAT方法，這是路由器配置示例中使用的配置。出於配置目的，使用以下路由器：NAT-A和NAT-B。WLC1在路由器NAT-A之後，WLC2在路由器NAT-B之後。

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#
```

在無線區域網控制器上配置使用NAT的移動性

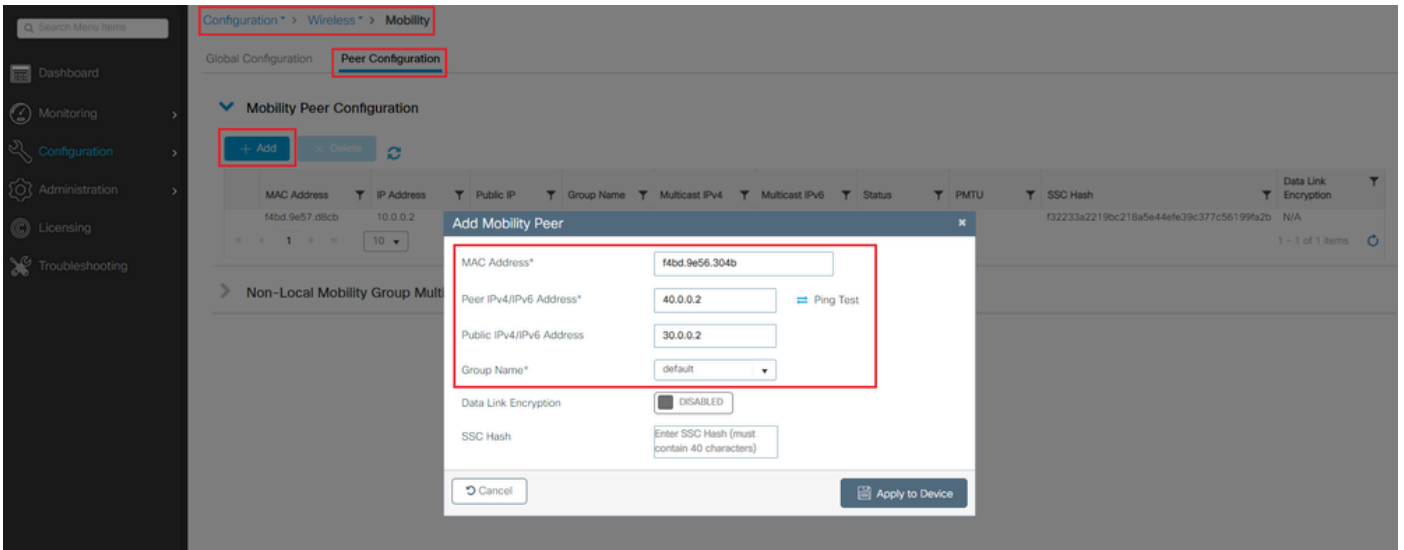
這是要在WLC之間共用的配置，用於透過NAT建立移動隧道：

- 專用移動IP地址
- 公共移動IP地址
- 移動組Mac地址
- 移動組名稱

WLC1的配置增加到WLC2，反之亦然，這可以透過WLC中的CLI或GUI完成，因為使用NAT的移動隧道是此配置的最終目標，兩個WLC的公共移動IP地址是每個路由器靜態NAT配置中配置的NAT IP地址。

WLC1配置：

GUI :

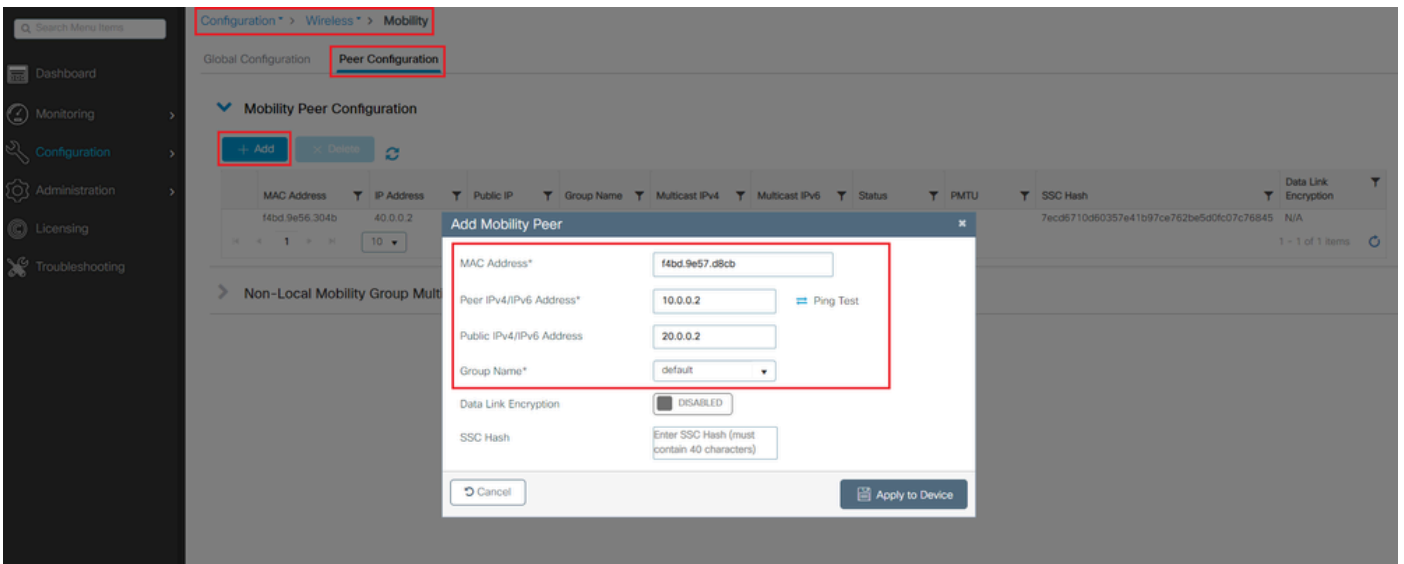


CLI :

```
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#
```

驗證

路由器配置驗證

從路由器端，這些命令檢驗NAT配置。NAT配置必須為靜態（如文檔前面所述），因此NAT的內部和外部配置均存在。

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

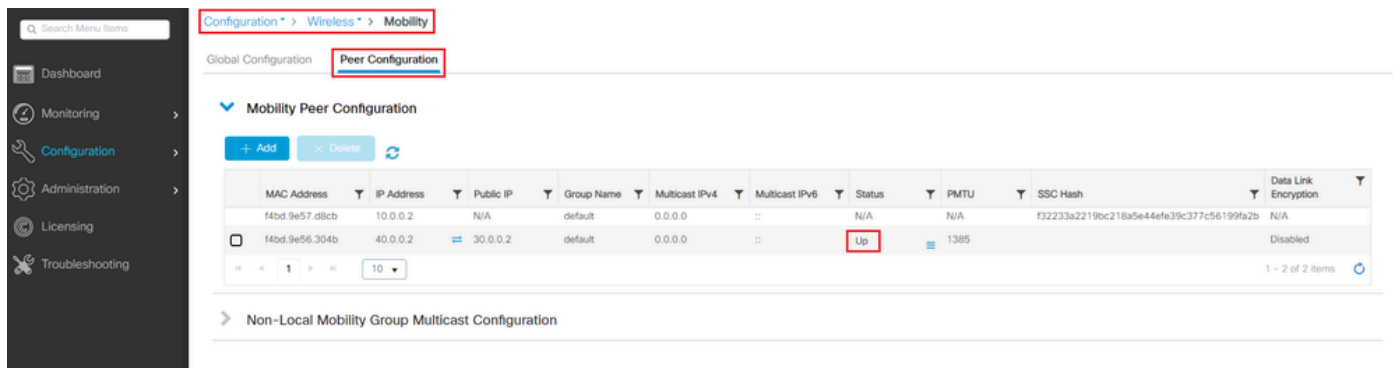
```
RouterNAT-B#show run interface GigabitEthernet0/1/2
interface GigabitEthernet0/1/2
ip add 40.0.0.1 255.255.255.0
ip nat inside
!
RouterNAT-B#show run interface GigabitEthernet0/1/3
interface GigabitEthernet0/1/3
ip add 30.0.0.1 255.255.255.0
ip nat outside
!
RouterNAT-B#show run | in ip nat inside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

無線LAN控制器組態驗證

從WLC GUI和CLI檢查移動隧道的狀態，如本文檔前面所述，用於確認WLC之間透過移動隧道進行正確通訊的正確狀態為：Up，任何其他狀態都需要進行調查。

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_AES128_GCM_SHA256
 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:

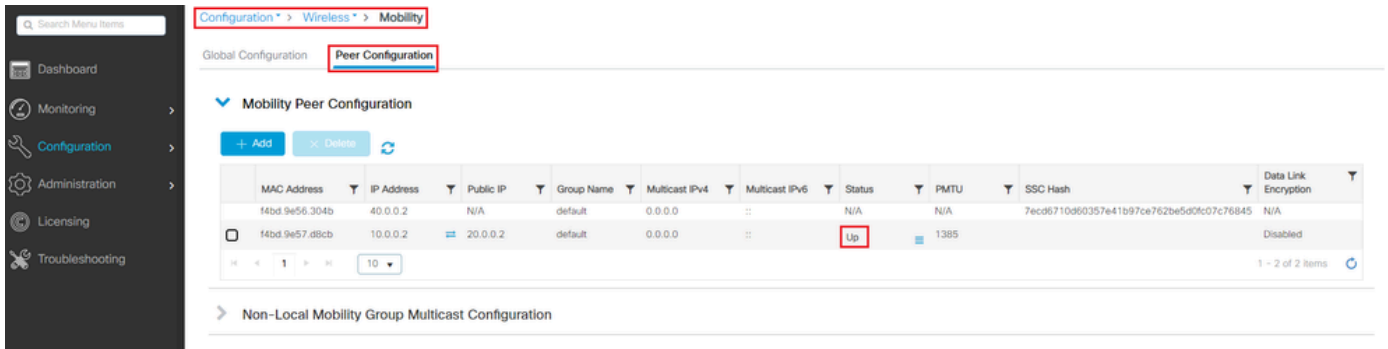
IP	Public Ip	MAC Address	Group Name	Multicast IPv4	Multicast IPv6	Status
10.0.0.2	N/A	f4bd.9e57.d8cb	default	0.0.0.0	::	N/A
40.0.0.2	30.0.0.2	f4bd.9e56.304b	default	0.0.0.0	::	

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_AES

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	Status
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

UP

1385

疑難排解

路由器故障排除

從路由器端驗證IP NAT轉換是否正確進行。

IP NAT轉換和統計資訊

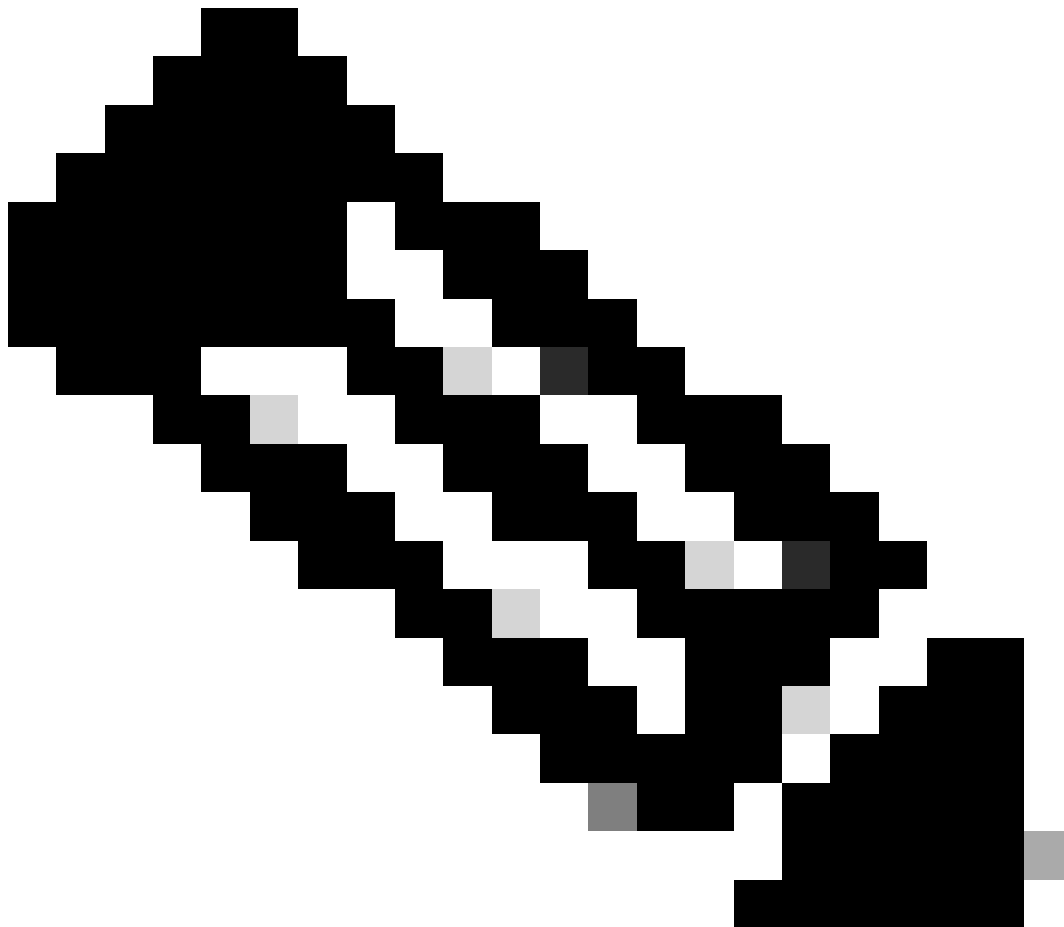
使用這些命令檢視在路由器中執行的內部和外部轉換，以及檢查NAT統計資料。

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

IP NAT調試

此命令從路由器的角度調試NAT轉換，以瞭解NAT如何進行，或者路由器執行NAT轉換時是否存在任何問題。

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



注意：路由器上的任何debug命令都可能導致過載，從而導致路由器無法運行。使用路由器調試時必須特別小心，如果可能，在生產期間不要對重要的生產路由器運行任何調試，則需要維護窗口。

無線區域網控制器故障排除

如果移動隧道顯示的任何狀態都不正確（即處於Up狀態），可以從WLC收集此資訊。

移動進程日誌

此命令生成過去和現在的移動日誌

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

可使用命令在WLC自身中讀取收集的資訊

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

使用命令，還可以從WLC導出收集的資訊，以便在外部源中讀取它

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

移動調試和跟蹤

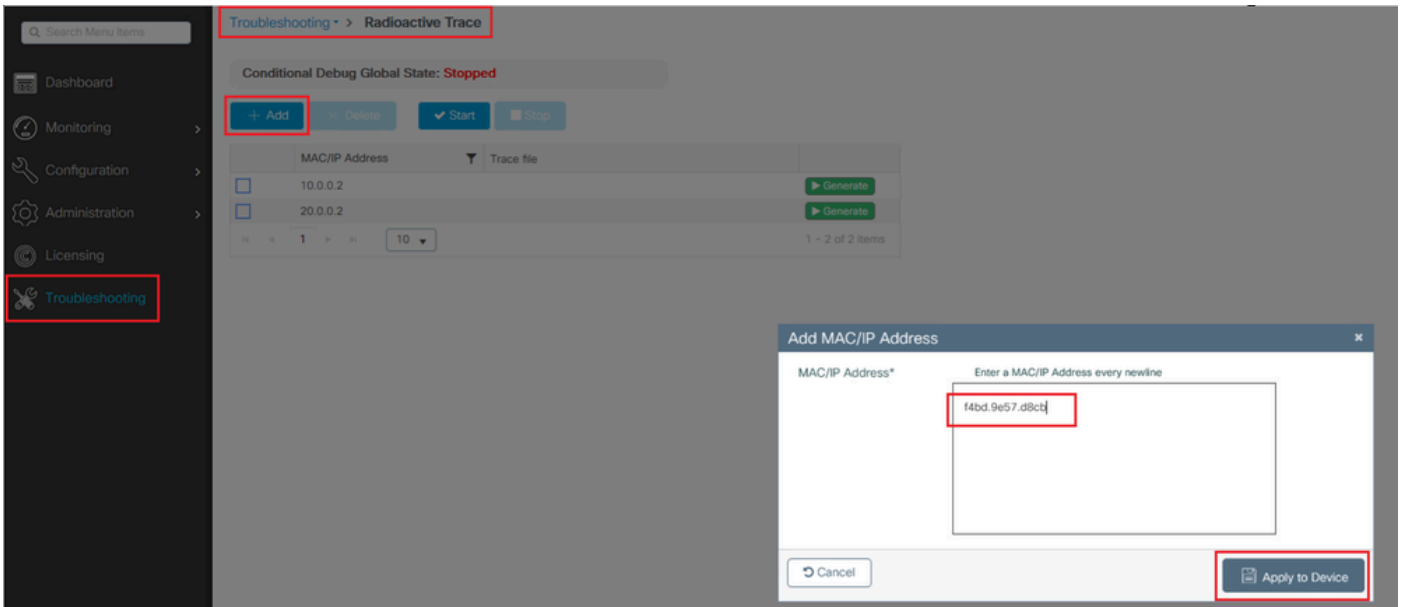
調試和跟蹤可以提供更詳細的資訊，以防移動進程日誌無法生成足夠的資訊來查詢問題。

當透過NAT為移動隧道收集調試和跟蹤資訊時，在跟蹤部分輸入這些資訊以同時獲取資訊以更好地瞭解行為非常重要：

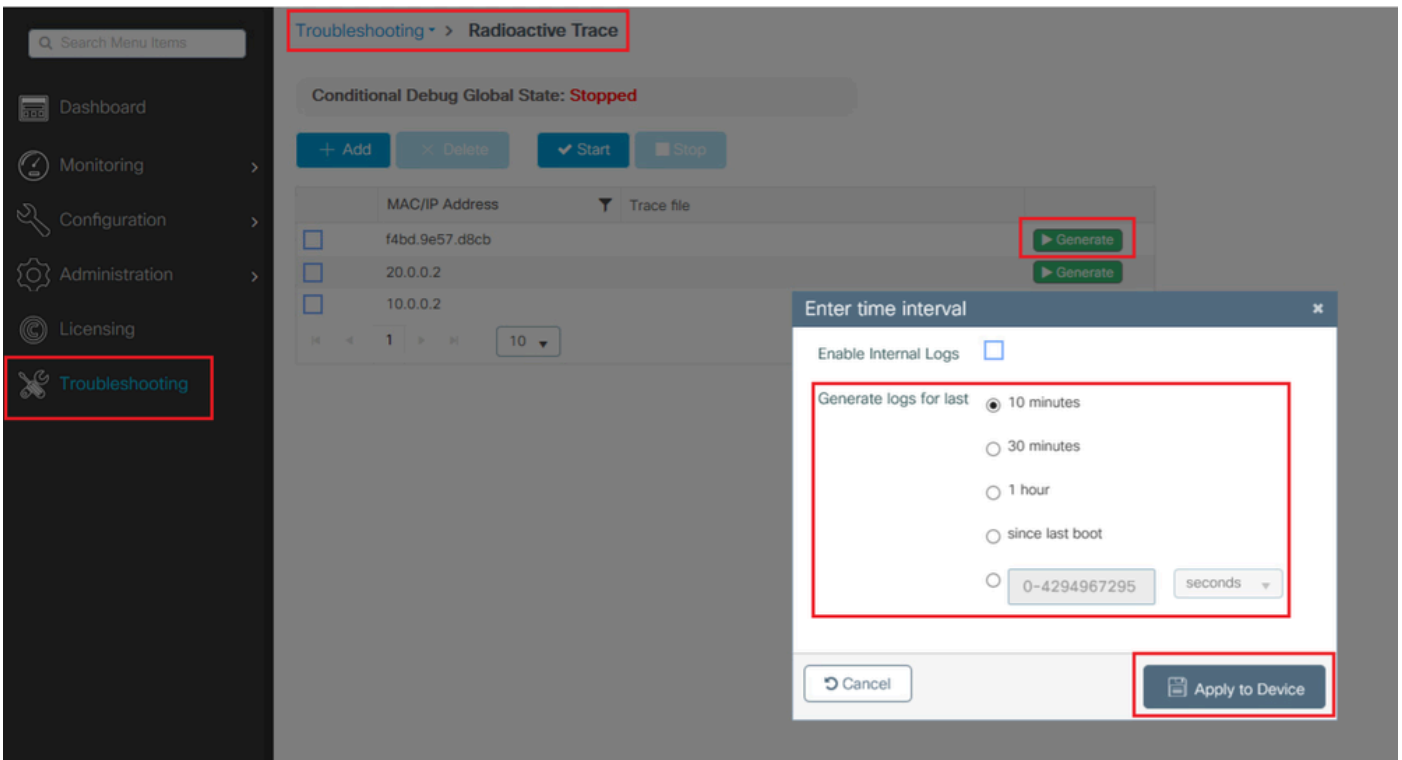
- 對等公共移動IP地址
- 對等體專用移動IP地址
- 對等移動Mac地址

在本例中，在WLC2中輸入了公有和私有IP地址以及WLC1的移動性MAC地址，同樣也必須向後執行，其中在WLC1的RA跟蹤部分輸入了私有和公有IP地址以及WLC2的移動性Mac地址。

WLC GUI



可以從GUI收集調試和跟蹤，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
```

要收集調試資訊，可以使用此命令。視需要變更偵錯收集的時間。

```
#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
```

使用傳輸通訊協定將檔案複製到外部來源。

```
#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
```

封包擷取

9800 WLC能夠擷取嵌入式封包，並使用此功能檢查使用NAT在行動通道的WLC之間交換哪些封包。

。

在本例中，WLC1的專用IP地址在WLC2中用於設定資料包捕獲，同樣的工作必須向後進行，其中必須使用WLC1中WLC2的專用IP地址設定資料包捕獲。

要捕獲資料包，可以建立ACL來過濾資料包，並僅顯示我們使用NAT查詢的移動隧道的資料包，建立ACL後，ACL將作為過濾器附加到資料包捕獲中。ACL可以使用移動專用IP地址建立，因為這些地址位於資料包報頭中。

```
#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 MobilityNAT
```

在捕獲開始之前，此命令可用於檢查監控捕獲配置。

```
#show monitor capture MobilityNAT
```

一旦準備好並檢查監控器捕獲，即可啟動監控器捕獲。

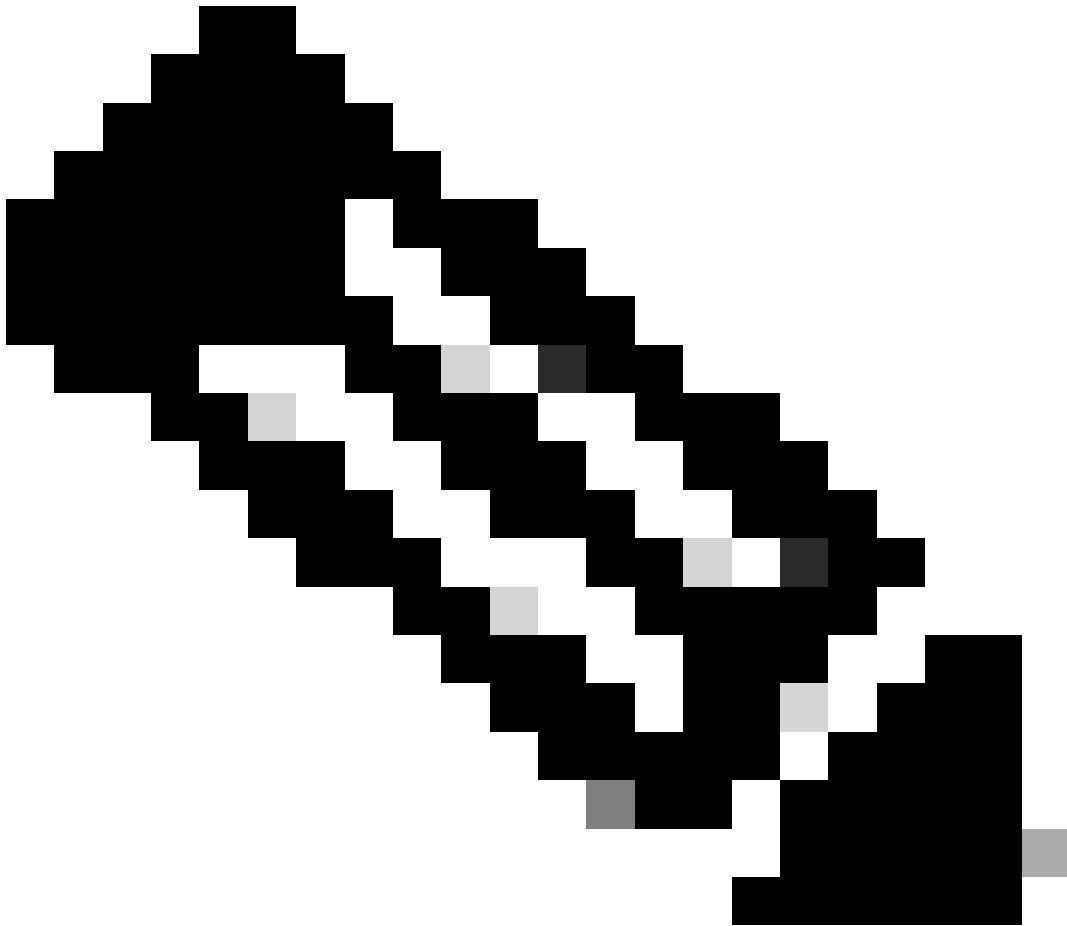
```
#monitor capture MobilityNAT start
```

若要停止它，可以使用這個指令。

```
#monitor capture MobilityNAT stop
```

一旦監控器捕獲停止，就可以使用傳輸協定將其導出到外部源。

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



注意：使用NAT的移動隧道是一種需要WLC之間雙向會話的功能，由於該功能的性質，強烈建議同時從兩個WLC收集日誌、調試和跟蹤或資料包捕獲，以便更好地瞭解使用NAT資料包交換的移動隧道。

清除調試、跟蹤和資料包捕獲

獲取所需資訊後，可以按照此處所述從WLC中刪除調試、跟蹤和嵌入式資料包捕獲配置。

調試和跟蹤

```
#clear platform condition all
```

資料包捕獲

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

強烈建議您在收集到所需資訊後，清除WLC中執行的疑難排解組態。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。