

NATを使用した9800ワイヤレスLANコントローラモビリティトンネルの設定

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](#)

[モビリティグループでのNATサポートに関する制限事項](#)

[ネットワーク図](#)

[設定](#)

[ルータでのNATの設定](#)

[ワイヤレスLANコントローラでのNATによるモビリティの設定](#)

[確認](#)

[ルータ設定の確認](#)

[ワイヤレスLANコントローラ\(WLC\)設定の確認](#)

[トラブルシューティング](#)

[ルータのトラブルシューティング](#)

[IP NAT変換と統計情報](#)

[IP NATのデバッグ](#)

[ワイヤレスLanコントローラのトラブルシューティング](#)

[モビリティプロセスログ](#)

[モビリティのデバッグとトレース](#)

[パケットキャプチャ](#)

[明確なデバッグ、トレース、およびパケットキャプチャ](#)

はじめに

このドキュメントでは、ネットワークアドレス変換(NAT)を介したモビリティトンネルで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

次の項目に関する知識があることを推奨しています。

- スタティックネットワークアドレス変換(NAT)の設定と概念。
- 9800ワイヤレスLANコントローラ(WLC)モビリティトンネルの設定と概念。

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。

- Catalyst 9800ワイヤレスコントローラシリーズ(Catalyst 9800-L)、Cisco IOS® XE Gibraltar 17.9.4
- サービス統合型ルータ(ISR)、Cisco IOS® XE Gibraltar 17.6.5
- Catalyst 3560シリーズスイッチ、Cisco IOS® XE Gibraltar 15.2.4E10

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。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。

背景説明

モビリティトンネルは、アクセスポイント情報、ワイヤレスクライアント情報、RRM情報などの情報をコントローラ間で共有するために、2つ以上のワイヤレスLANコントローラ(WLC)間で作成されます。

また、アンカーと外部の設計に基づく設定としても使用できます。このドキュメントでは、ネットワークアドレス制御(NAT)を使用してワイヤレスLANコントローラ(WLC)間にモビリティトンネルを設定する方法について説明します。

WLCモビリティトンネルは、次の4つの状態のいずれかになります。

- 制御およびデータパスダウン
- Control Path Down (これはData path is upを意味します)
- データパスの停止 (制御が稼働していることを意味します)
- 2013年以降

モビリティトンネルの最終的で正確な状態は、アップ状態です。その他の状態ではさらに調査が必要です。モビリティトンネルは、CAPWAP UDPポート16666および16667を介して動作します。UDPポート16666は制御パス用で、16667はデータパス用です。このため、これらのポートがWLC間で開いていることを確認する必要があります。

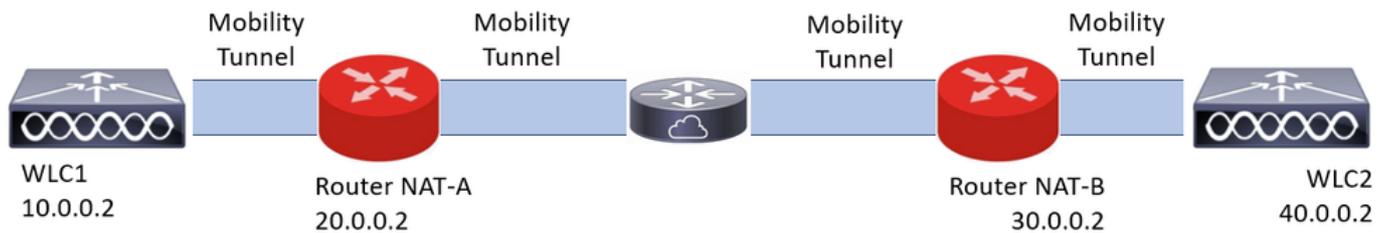


注:NATを使用しないWLCモビリティトンネル設定については、『[Catalyst 9800ワイヤレスLANコントローラでのモビリティポロジの設定](#)』を参照してください。

モビリティグループでのNATサポートに関する制限事項

- スタティックNAT(1:1)だけを設定できます。
- 同じパブリックIPアドレスを持つ複数のモビリティトンネルピアはサポートされていません。
- 各メンバーには一意のプライベートIPアドレスが必要です。
- ポートアドレス変換(PAT)はサポートされていません。
- ワイヤレスクライアントローミング用のリリース間コントローラモビリティ(IRCM)はサポートされていません。
- IPv6アドレス変換はサポートされていません。
- モビリティトンネルを使用したネットワークアクセスコントロール(NAT)は、WLCコードバージョン17.7.1以降でサポートされています。

ネットワーク図



設定

ルータでのNATの設定

この設定では、ネットワークアクセスコントロール(NAT)機能を提供するためにルータが使用されますが、スタティックNATを実行できる任意のデバイスを使用できます。スタティックNATはWLCモビリティトンネル用にサポートされているNAT方式であり、これはルータの設定例で使用されている設定です。設定目的で、NAT-AおよびNAT-Bのルータが使用されます。WLC1はルータNAT-Aの背後にあり、WLC2はルータNAT-Bの背後にあります。

ルータのNAT-A設定：

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#
```

ルータのNAT-B設定：

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#
```

ワイヤレスLANコントローラでのNATによるモビリティの設定

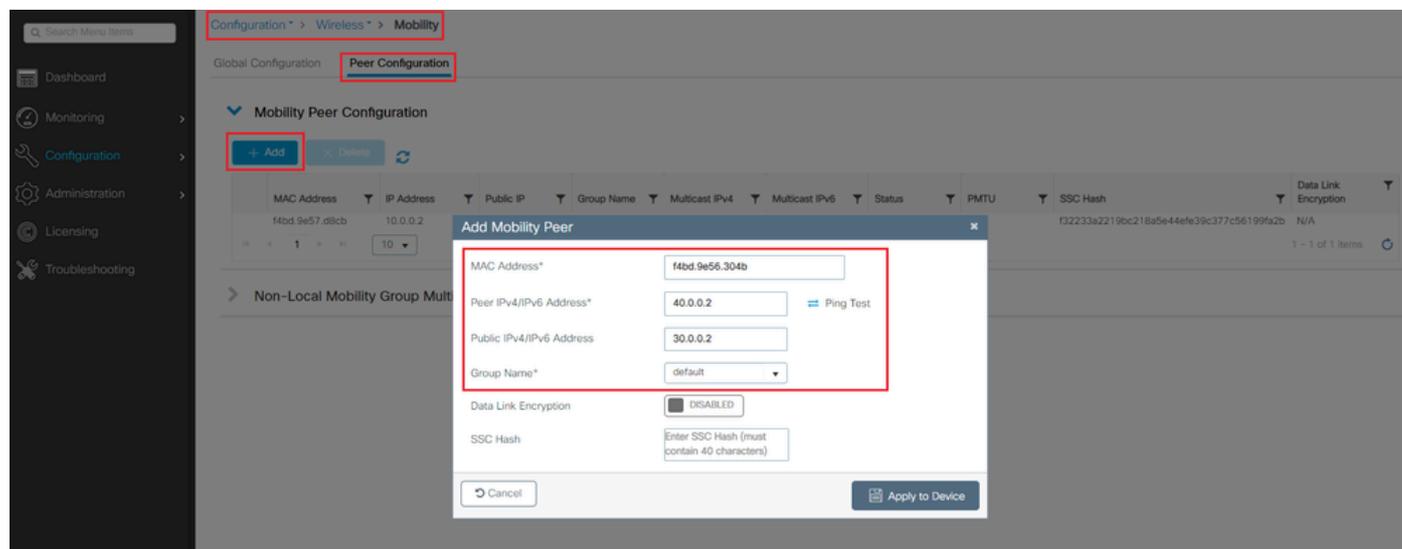
NATを使用してモビリティトンネルを作成するためにWLC間で共有する設定を次に示します。

- プライベートモビリティIPアドレス
- パブリックモビリティIPアドレス
- モビリティグループのMACアドレス
- モビリティグループの名前

WLC1の設定をWLC2に追加する方法と、WLC2の設定をWLCでCLIまたはGUIを使用して追加する方法です。NATを使用したモビリティトンネルはこの設定の最終目標であるため、両方のWLCのパブリックモビリティIPアドレスは、各ルータのスタティックNAT設定で設定されたNAT IPアドレスになります。

WLC1の設定：

GUI：

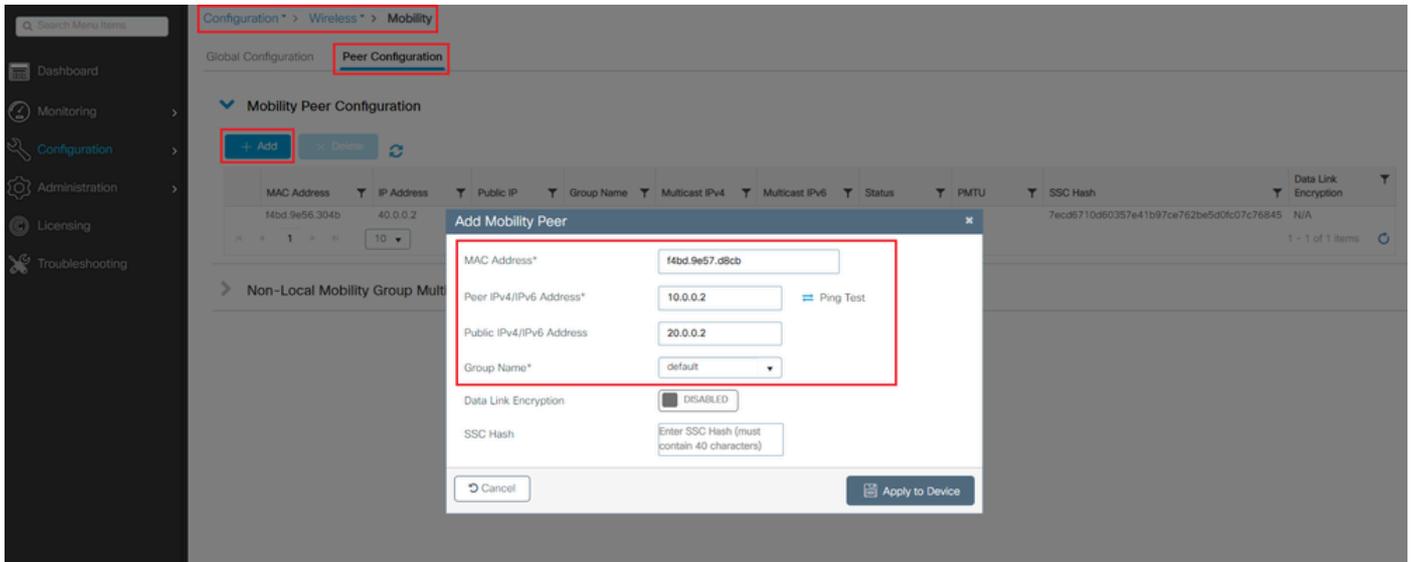


CLI：

```
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の設定：

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#
```

確認

ルータ設定の確認

ルータ側からこれらのコマンドを使用してNAT設定を確認します。NATの内部と外部の設定が存在するため、NAT設定は (ドキュメントで前述したように) スタティックである必要があります。

ルータ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
```

ルータNAT B

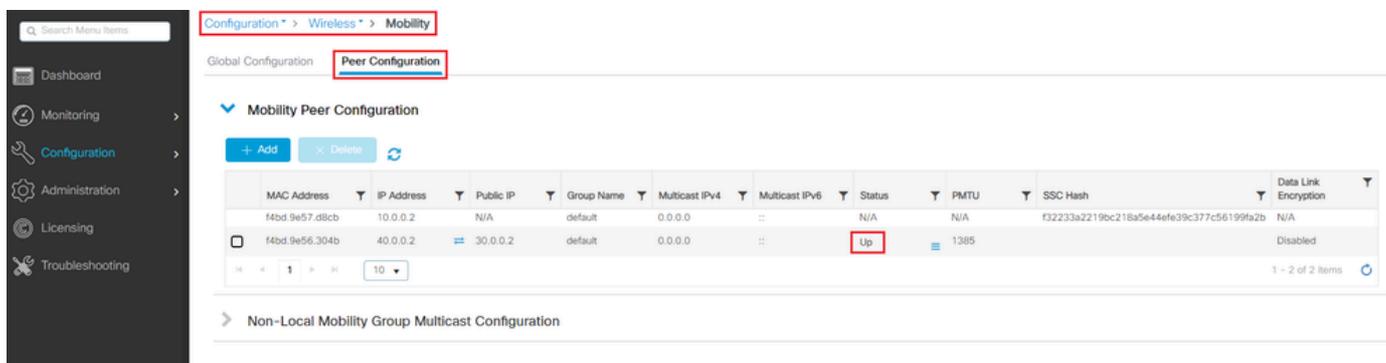
```
RouterNAT-B#show run interface GigabitEthernet0/1/2
interface GigabitEthernet0/1/2
ip add 40.0.0.1 255.255.255.0
ip nat inside
!
RouterNAT-B#show run interface GigabitEthernet0/1/3
interface GigabitEthernet0/1/3
ip add 30.0.0.1 255.255.255.0
ip nat outside
!
RouterNAT-B#show run | in ip nat inside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

ワイヤレスLANコントローラ(WLC)設定の確認

このドキュメントで前述したように、モビリティトンネルのステータスをWLC GUIおよびCLIで確認します。モビリティトンネルを介したWLC間の正しい通信を確認するための正しいステータスは、「Up, any other status needs investigation」です。

WLC1

GUI :



The screenshot shows the Cisco WLC GUI navigation path: Configuration > Wireless > Mobility. Under Peer Configuration, a table lists mobility peers. The peer with IP 40.0.0.2 is highlighted with a red box around the 'Up' status.

MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
f4bd.9e57.d8cb	10.0.0.2	N/A	default	0.0.0.0	::	N/A	N/A	f32233a2219bc218a5e44efe39c377c56199fa2b	N/A
<input type="checkbox"/>	f4bd.9e56.304b	40.0.0.2	= 30.0.0.2	default	0.0.0.0	::	Up	1385	Disabled

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	::	N/A

Up

1385

WLC2

GUI :

Configuration > Wireless > Mobility

Global Configuration Peer Configuration

Mobility Peer Configuration

MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash	Data Link Encryption
f4bd.9e56.304b	40.0.0.2	N/A	default	0.0.0.0	::	N/A	N/A	7ecd6710d60357e41b97ce762be5d0c07c76845	N/A
f4bd.9e57.d8cb	10.0.0.2	20.0.0.2	default	0.0.0.0	::	Up	1385		Disabled

Non-Local Mobility Group Multicast Configuration

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_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.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

1385

トラブルシューティング

ルータのトラブルシューティング

ルータ側から、IP NAT変換が正しく行われていることを確認します。

IP NAT変換と統計情報

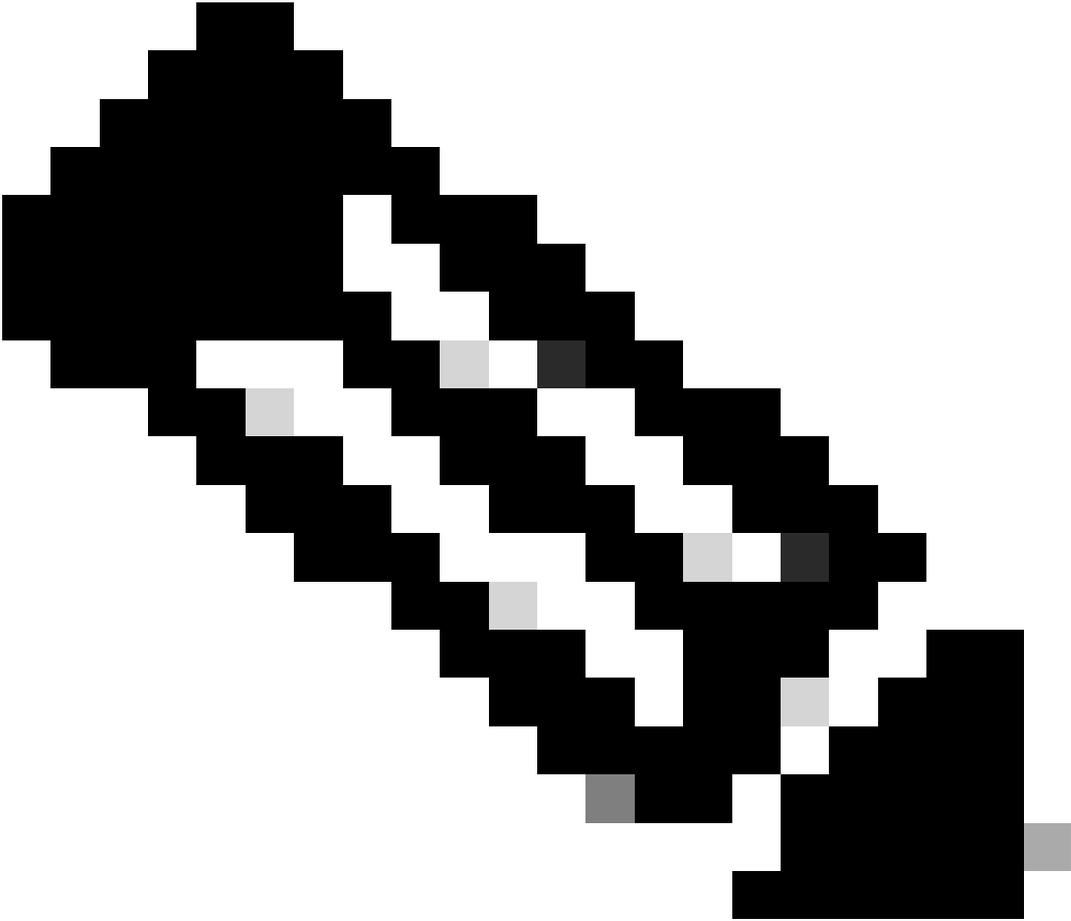
次のコマンドを使用して、ルータで実行されている内部および外部の変換を確認し、NAT統計情報をチェックします。

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

IP NATのデバッグ

このコマンドは、ルータの観点からNAT変換をデバッグして、NATの仕組みを理解したり、ルータによるNAT変換の実行中に問題が発生したかどうかを理解します。

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



注:ルータでdebugコマンドを実行すると過負荷が発生し、ルータが動作不能になる可能性があります。ルータのデバッグは細心の注意を払って使用する必要があります。可能であれば、実稼働時に重要な実稼働ルータでデバッグを実行しないでください。メンテナンスウィンドウが必要です。

ワイヤレスLanコントローラのトラブルシューティング

ここに示す情報は、正しい状態ではない状態 (アップ状態) がモビリティトンネルで表示される場合に、WLCから収集できます。

モビリティプロセスログ

このコマンドは、過去と現在の時刻からモビリティログを生成します

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

収集した情報は、コマンドを使用してWLC自体で読み取ることができます

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

収集した情報は、WLCからエクスポートして、コマンドを使用して外部ソースに読み込むこともできます

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

モビリティのデバッグとトレース

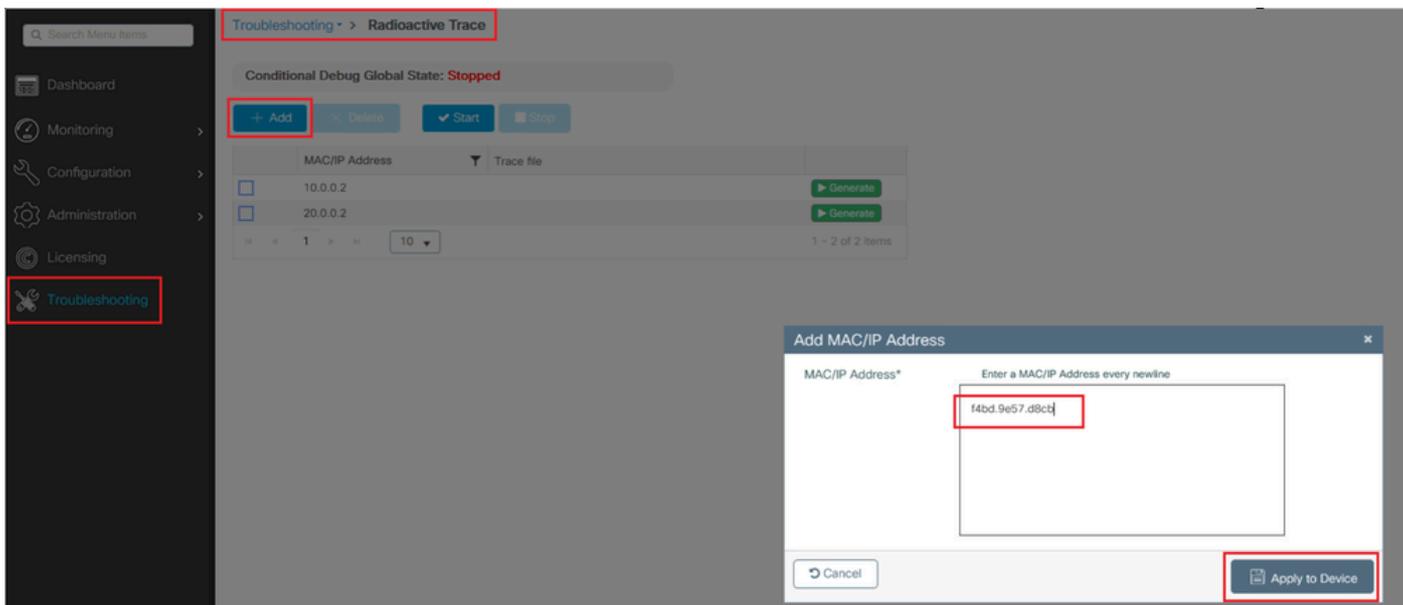
デバッグとトレースは、モビリティプロセスログが問題を見つけるのに十分な情報を生成できない場合に備えて、より詳細な情報を提供できます。

NATを使用したモビリティトンネル用にデバッグとトレースを収集する場合、動作をよりよく理解するために、次の情報をトレースセクションに入力して情報を同時に取得することが重要です。

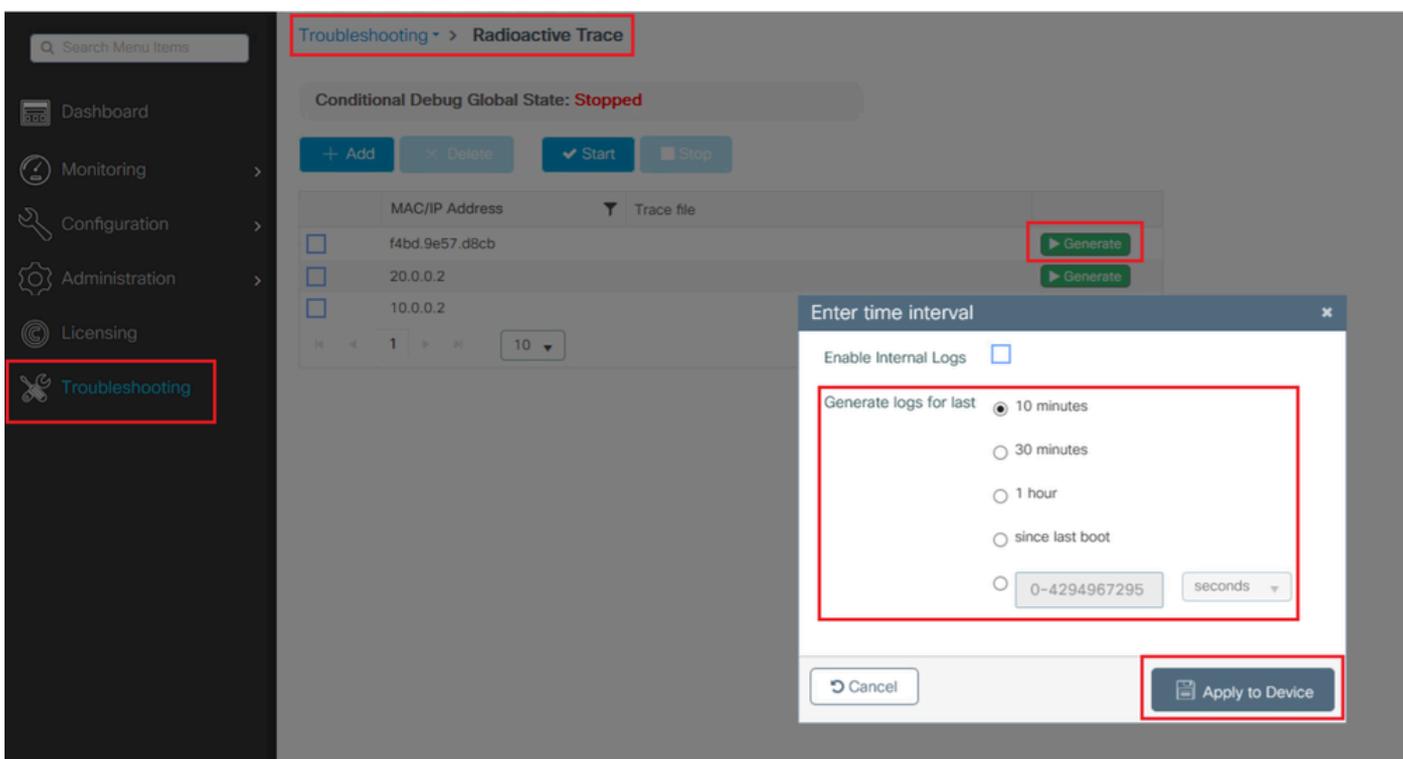
- ピアパブリックモビリティIPアドレス
- ピアプライベートモビリティIPアドレス
- ピアモビリティMacアドレス

この例では、パブリックおよびプライベートのIPアドレスとWLC1のモビリティMACアドレスをWLC2に入力します。同じことを逆に行う必要があります。ここでは、WLC1のRAトレースセクションで、プライベートおよびパブリックのIPアドレスとWLC2のモビリティMACアドレスを入力します。

WLC GUI



デバッグとトレースは、次に示すようにGUIから収集できます。



WLCの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
```

デバッグ情報を収集するには、このコマンドを使用できます。必要に応じて、デバッグコレクションの時刻を変更します。

```
#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
```

転送プロトコルを使用してファイルを外部ソースにコピーします。

```
#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
```

パケット キャプチャ

9800 WLCには、組み込みパケットキャプチャを取得する機能があります。この機能を使用して、NATを使用したモビリティトンネルのためにWLC間で交換されるパケットを確認します。

この例では、WLC1のプライベートIPアドレスは、パケットキャプチャをセットアップするためにWLC2で使用されます。逆方向で行う必要があり、パケットキャプチャのセットアップのためにWLC1のWLC2のプライベートIPアドレスを使用する必要があります。

パケットキャプチャを取得するために、パケットをフィルタリングしてNATを使用したモビリティトンネルを検索するパケットのみを表示するACLを作成できます。作成されたACLは、フィルタとしてパケットキャプチャに添付されます。モビリティプライベートIPアドレスはパケットヘッダー内のアドレスであるため、このACLを作成するには、このモビリティプライベートIPアドレスを使用します。

```
#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 Mobility
```

キャプチャを開始する前に、このコマンドを使用してモニタのキャプチャ設定を確認できます。

```
#show monitor capture MobilityNAT
```

モニタキャプチャの準備が整い、チェックされると、開始できます。

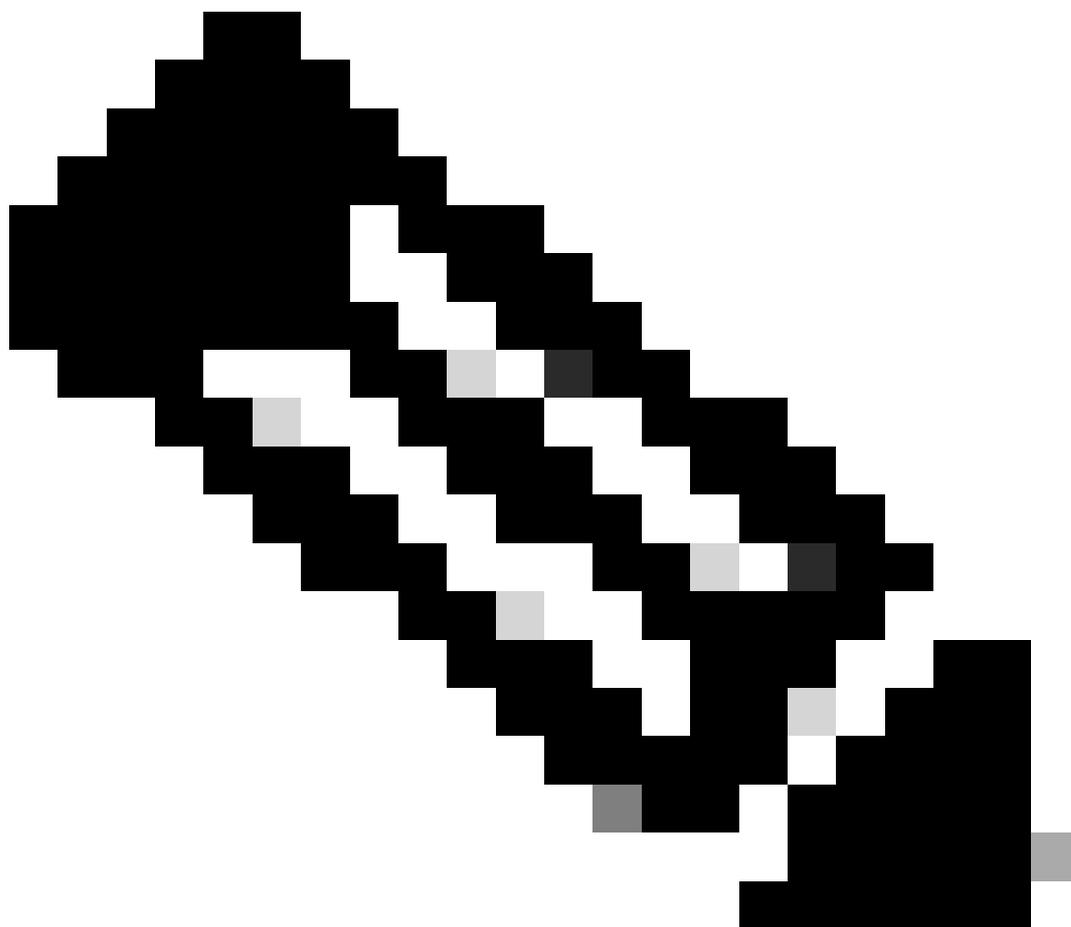
```
#monitor capture MobilityNAT start
```

これを停止するには、このコマンドを使用できます。

```
#monitor capture MobilityNAT stop
```

モニタキャプチャが停止すると、転送プロトコルを使用して外部ソースにエクスポートできます。

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



注：NATを使用したモビリティトンネルはWLC間で双方向の通信を必要とする機能です。この機能の性質上、両方のWLCからログ、デバッグ、トレース、またはパケットキャ

プチャを同時に収集して、NATパケット交換を使用したモビリティトンネルについて詳しく理解しておくことを強くお勧めします。

明確なデバッグ、トレース、およびパケットキャプチャ

必要な情報を取得したら、次に説明するように、デバッグ、トレース、および組み込みパケットキャプチャ(EPC)設定をWLCから削除できます。

デバッグとトレース

```
#clear platform condition all
```

パケット キャプチャ

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

必要な情報を収集したら、WLCで実行したトラブルシューティング設定をクリアすることを強く推奨します。

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。