Configure 9800 Wireless LAN Controller Mobility Tunnel with NAT

Contents

Introduction

This document describes how to configure 9800 Wireless Lan Controllers (WLC) with a mobility tunnel over Network Address Translation (NAT).

Prerequisites

Requirements

Cisco recommends you have knowledge of these topics:

- Static Network Address translation (NAT) configuration and concepts.
- 9800 Wireless Lan Controller mobility tunnel configuration and concepts.

Components Used

The information in this document is based on these software and hardware versions:

- Catalyst 9800 Wireless Controller Series (Catalyst 9800-L), Cisco IOS® XE Gibraltar 17.9.4
- Integrated Services Routers (ISR), Cisco IOS® XE Gibraltar 17.6.5
- Catalyst 3560 Series Switch, Cisco IOS® XE Gibraltar 15.2.4E10

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Mobility tunnels are created between two or more Wireless Lan Controllers (WLC) with the intention to share information among them such as Access Point information, Wireless Client information, RRM information and more.

It can also be used as a configuration based for Anchor - Foreign designs. This document describes how to configure a mobility tunnel between Wireless Lan Controllers (WLC) with Network Address Control (NAT).

WLC mobility tunnel can have one of this four states:

- Control and Data Path Down
- Control Path Down (this implies Data path is up)
- Data Path Down (this implies Control is up)
- Up

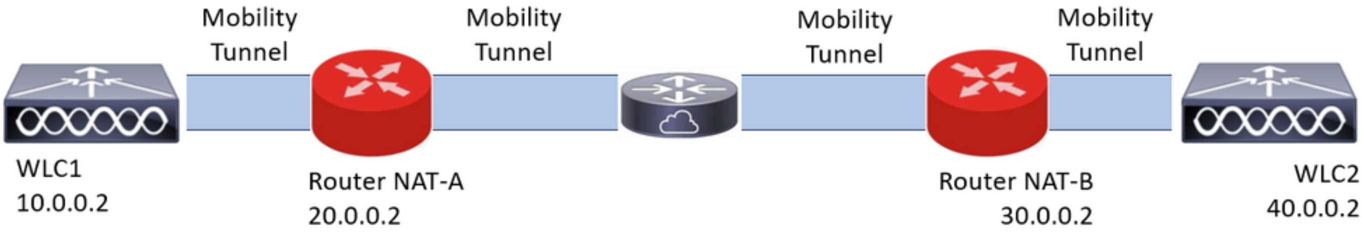
The final and correct state for a mobility tunnel is: Up, any other state requires further investigation. Mobility tunnels work over CAPWAP udp ports 16666 and 16667 from which udp port 16666 is for Control Path and 16667 for Data Path, due to this it is necessary to ensure these ports are open between the WLCs.

Note: For WLC mobility tunnel configuration **without** NAT refer to Configure Mobility Topologies on Catalyst 9800 Wireless LAN Controllers

Restrictions for NAT support on Mobility Groups

- Only Static NAT (1:1) can be configured.
- Multiple Mobility Tunnel peers with the same public IP Address is not supported.
- Every member must have an unique private IP Address.
- Port Address translation (PAT) is not supported.
- Inter-Release Controller Mobility (IRCM) for wireless client roam is not supported.
- IPv6 Address translation is not supported.
- Network Access Control (NAT) with Mobility Tunnel is supported from WLC code version 17.7.1 and above.

Network Diagram



Configure

Configure NAT on Router

Routers are used in this configuration to provide Network Access Control (NAT) capabilities, however, any device capable to do static NAT can be used. Static NAT is the NAT method supported for WLC mobility tunnels, this is the configuration used in the Routers configuration example. For configuration purposes these routers are used: NAT-A and NAT-B. The WLC1 is behind router NAT-A and WLC2 is behind router NAT-B.

Router **NAT-A** configuration:

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#
```

Router **NAT-B** configuration:

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#
```

Configure Mobility with NAT on Wireless Lan Controller

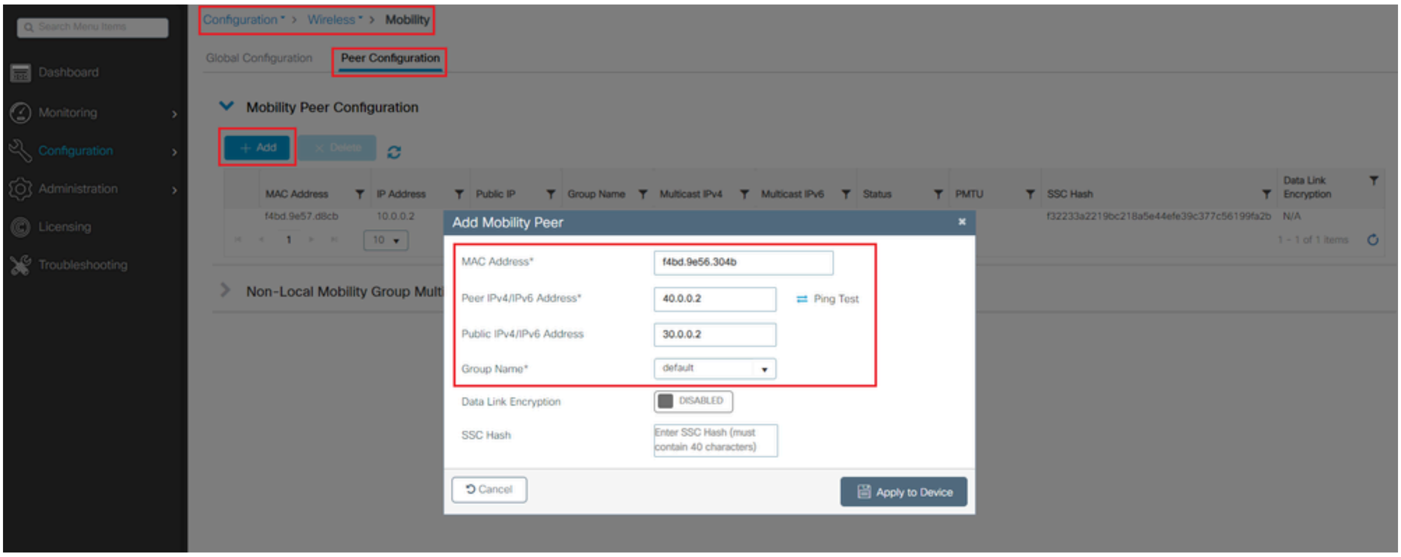
This is the configuration to share between WLCs to create the mobility tunnel with NAT:

- Private mobility IP Address
- Public mobility IP Address
- Mobility group Mac Address
- Mobility group name

The configuration of WLC1 is added to WLC2 and vice-versa, this can be done via CLI or GUI in the WLCs, since mobility tunnel with NAT is the final goal of this configuration the Public mobility IP Address of both WLCs is the NAT IP Address configured in the static NAT configuration in each router.

WLC1 configuration:

GUI:



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							f32233a2219bc218a5e44efe39c377c56199fa2b	N/A

1 - 1 of 1 items

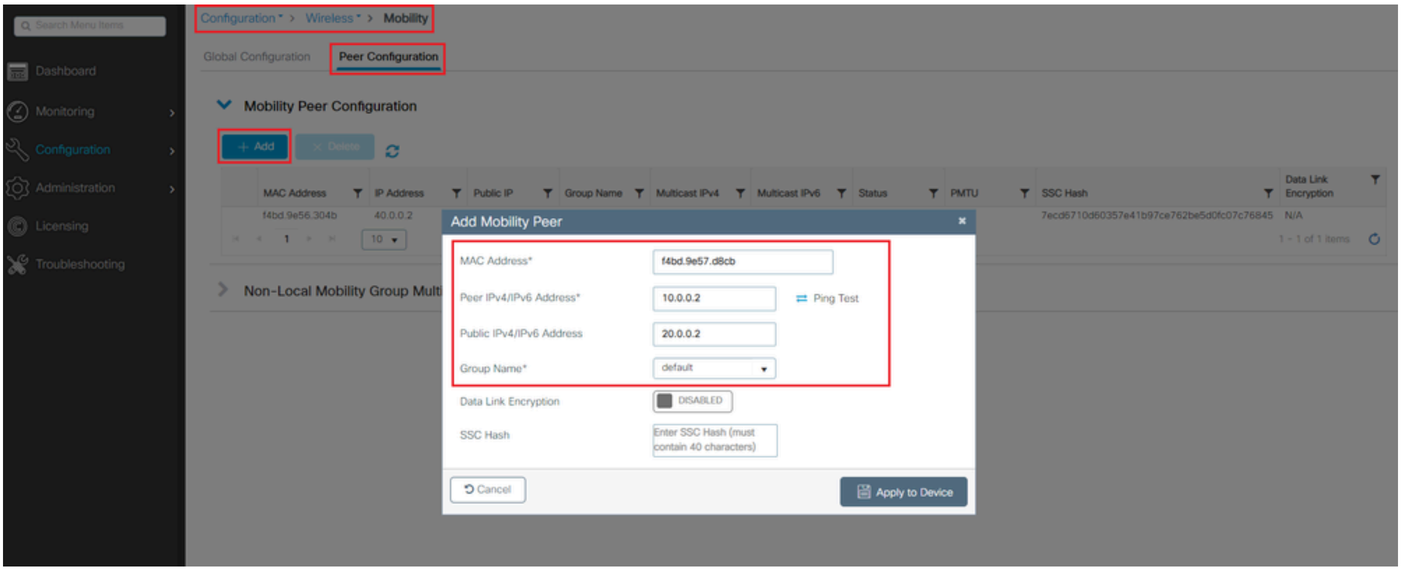
MAC Address*	f4bd.9e56.304b
Peer IPv4/IPv6 Address*	40.0.0.2
Public IPv4/IPv6 Address	30.0.0.2
Group Name*	default
Data Link Encryption	DISABLED
SSC Hash	Enter SSC Hash (must contain 40 characters)

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 configuration:

GUI:



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							7ecd6710d60357e41b97ce762be5d0fc07c76845	N/A

1 - 1 of 1 items

MAC Address*	f4bd.9e57.d8cb
Peer IPv4/IPv6 Address*	10.0.0.2
Public IPv4/IPv6 Address	20.0.0.2
Group Name*	default
Data Link Encryption	DISABLED
SSC Hash	Enter SSC Hash (must contain 40 characters)

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#
```

Verify

Router Configuration Verification

From the Router side these commands verify the NAT configuration. NAT configuration must be static (as mentioned earlier in the document) due to which the inside and outside configuration for NAT are present.

RouterNAT-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
```

RouterNAT-B

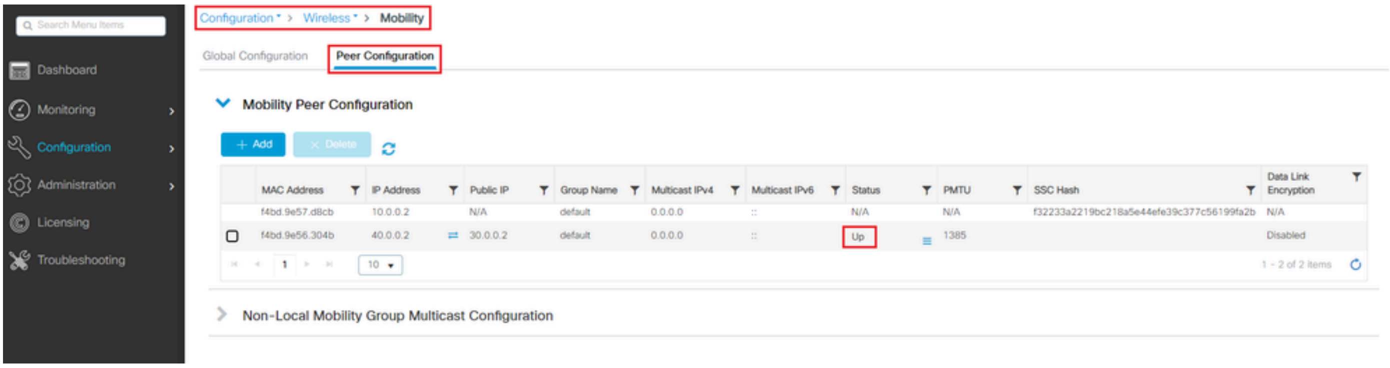
```
RouterNAT-B#show run interface GigabitEthernet0/1/2
interface GigabitEthernet0/1/2
ip add 40.0.0.1 255.255.255.0
ip nat inside
!
RouterNAT-B#show run interface GigabitEthernet0/1/3
interface GigabitEthernet0/1/3
ip add 30.0.0.1 255.255.255.0
ip nat outside
!
RouterNAT-B#show run | in ip nat inside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

Wireless LAN Controller Configuration Verification

Check from the WLC GUI and CLI the status of the mobility tunnel, as mentioned earlier in this document the correct status to confirm a correct communication between the WLCs over mobility tunnel is: Up, any other status needs investigation.

WLC1

GUI:



	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
□	f4bd.9e56.304b	40.0.0.2	⇄	30.0.0.2	default	0.0.0.0	::	Up	≡	1385		Disabled

1 10 1 - 2 of 2 items

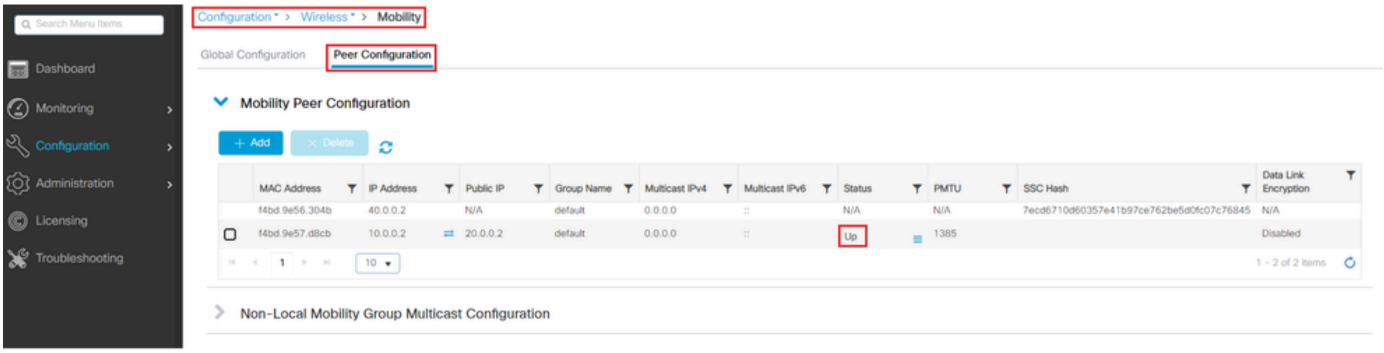
CLI:

<#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:



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	7ecd6710d60357e41b97ce762be5d0fc07c76845	N/A
□	f4bd.9e57.d8cb	10.0.0.2	⇄	20.0.0.2	default	0.0.0.0	::	Up	≡	1385		Disabled

1 10 1 - 2 of 2 items

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_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
```

Troubleshoot

Router Troubleshoot

Verify from the Router side the IP NAT translations are taking place correctly.

IP NAT translations and statistics

Use these commands to review the inside and outside translations are being performed in the router, as well as checking the NAT statistics.

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

IP NAT debug

This command debugs the NAT translation from the router perspective to understand how the NAT is taking place or if there is any issue while the router does the NAT translation.

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

Note: Any **debug** command on a router could cause overload which causes the router to become inoperable. Debugs in routers must be used with extreme caution, if possible do not run any debug on a critical production router during production time, a maintenance window is desired.

Wireless Lan Controller Troubleshoot

The information here can be gathered from the WLC in case the mobility tunnel shows any state that is not the correct state which is Up.

Mobility process logs

This command generates mobility logs from the past and present time

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

The information gathered can be read in the WLC itself with the command

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

The information gathered can also be exported from the WLC to read it in an external source with the command

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

Mobility debugs and traces

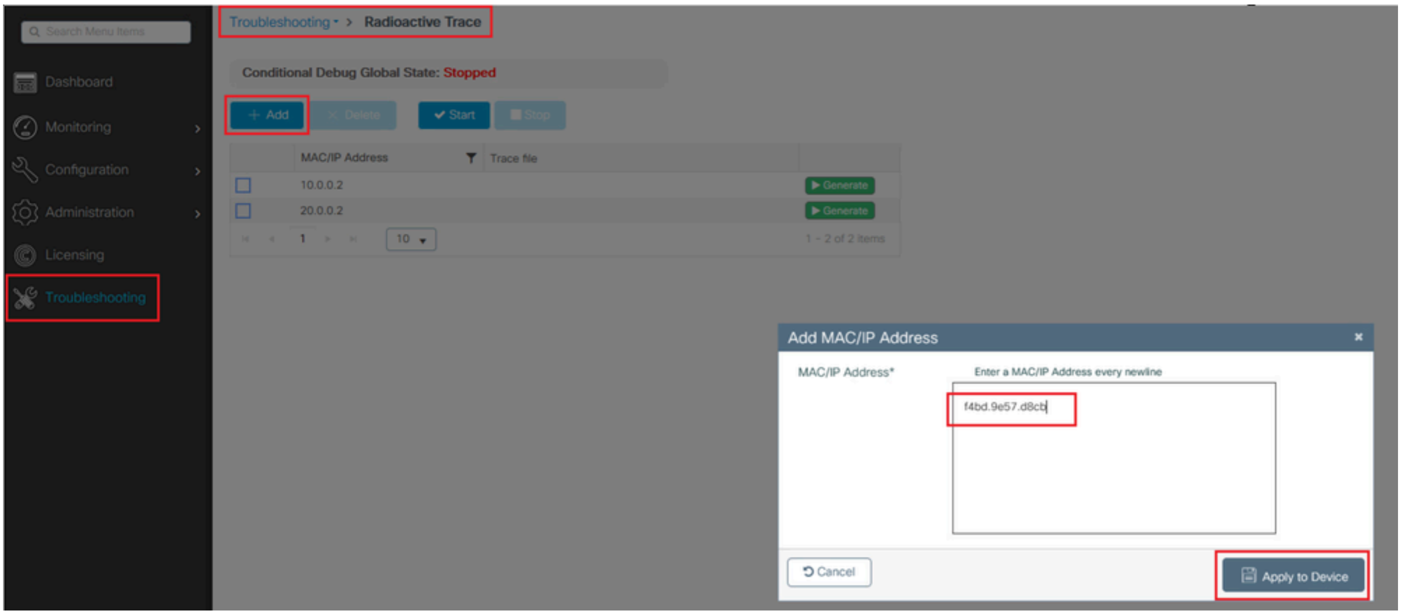
Debugs and traces can provide more detailed information in case the mobility process logs are not able to generate information enough to find the issue.

When debugs and traces are gathered for mobility tunnel with NAT it is important to enter these information in the trace section to get the information simultaneously to better understand the behavior:

- Peer public Mobility IP Address
- Peer private Mobility IP Address
- Peer mobility Mac Address

In this example the public and private IP Address along with the mobility MAC Address of WLC1 is entered in WLC2, the same has to be done backwards, where we enter the private and public IP Address along with the mobility Mac Address of WLC2 in the RA Trace section of WLC1.

WLC GUI



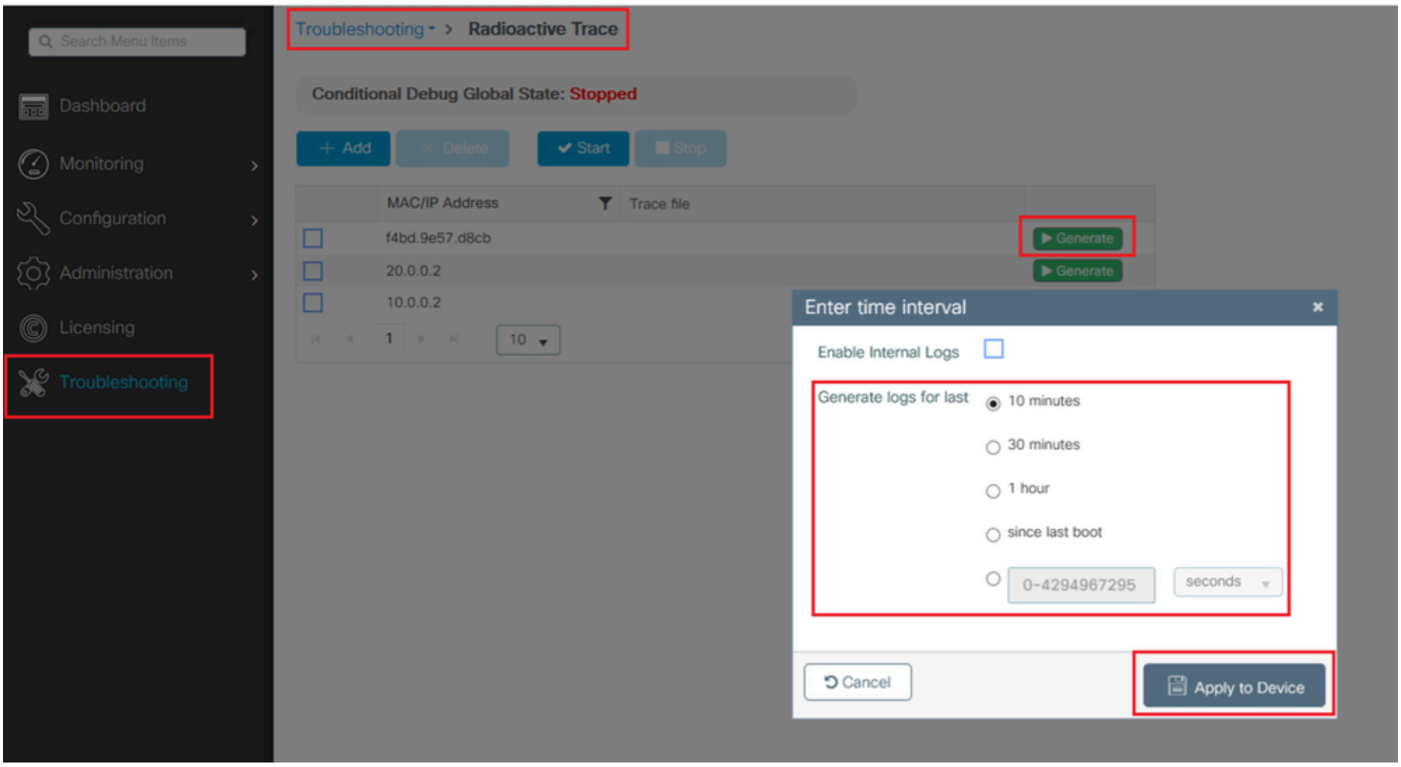
Conditional Debug Global State: Stopped

MAC/IP Address	Trace file
10.0.0.2	
20.0.0.2	

1 - 2 of 2 items

MAC/IP Address* f4bd.9e57.d8cb

Debugs and Traces can be collected from the GUI as shown.



Conditional Debug Global State: Stopped

MAC/IP Address	Trace file
f4bd.9e57.d8cb	
20.0.0.2	
10.0.0.2	

Enable Internal Logs □

Generate logs for last ● 10 minutes ○ 30 minutes ○ 1 hour ○ since last boot ○ 0-4294967295 seconds

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
```

To collect the debugs this command can be used. Change the time of the debugs collection as needed.

```
#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
```

Copy the files to an external source with a transfer protocol.

```
#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
```

Packet captures

The 9800 WLC has the capability to take embedded packet captures, use this feature to check what packets are exchanged between WLCs for the mobility tunnel with NAT.

In this example the private IP Address of WLC1 is used in WLC2 to set up the packet capture, the same has to be done backwards, where it has to be used the private IP Address of WLC2 in the WLC1 for the packet capture set up.

To take the packet capture an ACL can be created to filter the packets and show only the packets we look for mobility tunnel with NAT, once the ACL is created it is attached to the packet capture as a filter. The ACL can be created with the mobility private IP Address since those are the ones in the packet header.

```
#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
```

Before the capture starts this command can be used to check the monitor capture configuration.

```
#show monitor capture MobilityNAT
```

Once the monitor capture is ready and checked it can be started.

```
#monitor capture MobilityNAT start
```

To stop it this command can be used.

```
#monitor capture MobilityNAT stop
```

Once the monitor capture stops it can exported to an external source with a transfer protocol.

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

Note: Mobility tunnel with NAT is a feature that requires a two way conversation between WLCs, due to the nature of the feature it is highly recommended to gather the logs, debugs and traces or packet captures from both WLCs at the same time to better understand the mobility tunnel with NAT packet exchange.

Clear debugs, traces and packet captures

Once the needed information is taken the debugs, traces and embedded packet capture configuration can be deleted from the WLC as described here.

Debugs and traces

```
#clear platform condition all
```

Packet capture

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

It is highly recommended to clear the troubleshoot configuration that was performed in the WLC once the needed information was gathered.