

NAT로 9800 무선 LAN 컨트롤러 모빌리티 터널 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[모빌리티 그룹에 대한 NAT 지원 제한](#)

[네트워크 다이어그램](#)

[구성](#)

[라우터에서 NAT 구성](#)

[NAT on Wireless Lan Controller로 모빌리티 구성](#)

[다음을 확인합니다.](#)

[라우터 컨피그레이션 확인](#)

[무선 LAN 컨트롤러 컨피그레이션 확인](#)

[문제 해결](#)

[라우터 문제 해결](#)

[IP NAT 변환 및 통계](#)

[IP NAT 디버그](#)

[무선 LAN 컨트롤러 문제 해결](#)

[모빌리티 프로세스 로그](#)

[모빌리티 디버그 및 추적](#)

[패킷 캡처](#)

[디버그, 추적 및 패킷 캡처 지우기](#)

소개

이 문서에서는 NAT(Network Address Translation)를 통한 모빌리티 터널로 9800 WLC(Wireless Lan Controller)를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 주제에 대해 숙지할 것을 권장합니다.

- 고정 NAT(Network Address Translation) 구성 및 개념
- 9800 Wireless Lan Controller 모빌리티 터널 구성 및 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

모빌리티 터널은 액세스 포인트 정보, 무선 클라이언트 정보, RRM 정보 등과 같은 정보를 공유하기 위해 둘 이상의 WLC(Wireless Lan Controller) 간에 생성됩니다.

또한 Anchor - Foreign 디자인을 기반으로 한 구성으로 사용할 수 있습니다. 이 문서에서는 NAT(Network Address Control)를 사용하여 WLC(Wireless Lan Controller) 간 모빌리티 터널을 구성하는 방법에 대해 설명합니다.

WLC 모빌리티 터널은 다음 4가지 상태 중 하나를 가질 수 있습니다.

- 제어 및 데이터 경로 아래로
- 제어 경로 작동 중지(데이터 경로가 작동 중임을 의미)
- 데이터 경로 아래로(컨트롤이 작동함을 의미함)
- 위로

모빌리티 터널의 최종 및 올바른 상태는 Up입니다. 다른 모든 상태에는 추가 조사가 필요합니다. 모빌리티 터널은 CAPWAP udp 포트 16666 및 16667을 통해 작동하며, 여기서 udp 포트 16666은 제어 경로에, 16667은 데이터 경로에 사용됩니다. 따라서 WLC 간에 이러한 포트가 열려 있는지 확인해야 합니다.

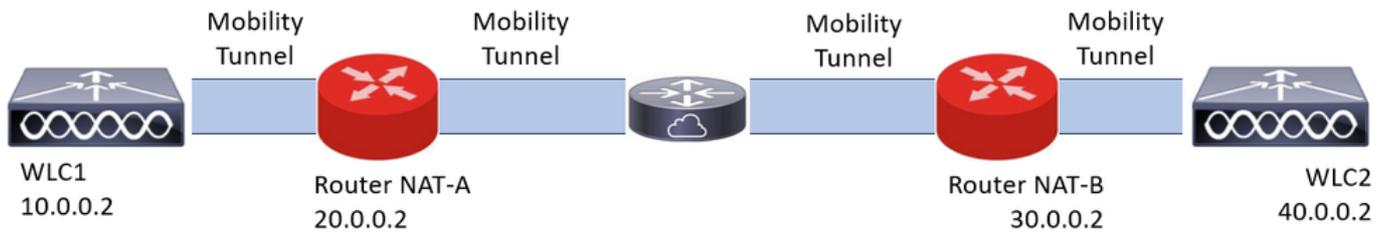


참고: NAT가 없는 WLC 모빌리티 터널 컨피그레이션의 경우 [Catalyst 9800 Wireless LAN Controller에서 모빌리티 토폴로지 구성을 참조하십시오](#)

모빌리티 그룹에 대한 NAT 지원 제한

- 고정 NAT(1:1)만 구성할 수 있습니다.
- 동일한 공용 IP 주소를 사용하는 여러 모빌리티 터널 피어는 지원되지 않습니다.
- 모든 구성원은 고유한 개인 IP 주소를 가져야 합니다.
- PAT(Port Address Translation)는 지원되지 않습니다.
- 무선 클라이언트 로밍용 IRCM(Inter-Release Controller Mobility)은 지원되지 않습니다.
- IPv6 주소 변환은 지원되지 않습니다.
- 모빌리티 터널이 있는 NAT(Network Access Control)는 WLC 코드 버전 17.7.1 이상에서 지원됩니다.

네트워크 다이어그램



구성

라우터에서 NAT 구성

이 컨피그레이션에서는 라우터를 사용하여 NAT(Network Access Control) 기능을 제공하지만, 고정 NAT를 수행할 수 있는 모든 디바이스를 사용할 수 있습니다. 고정 NAT는 WLC 모빌리티 터널에서 지원되는 NAT 방법입니다. 라우터 컨피그레이션 예에서 사용되는 컨피그레이션입니다. 컨피그레이션을 위해 NAT-A 및 NAT-B 라우터가 사용됩니다. WLC1은 라우터 NAT-A 뒤에 있고 WLC2는 라우터 NAT-B 뒤에 있습니다.

라우터 NAT-A 구성:

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#

라우터 NAT-B 구성:

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#
```

NAT on Wireless Lan Controller로 모빌리티 구성

NAT를 사용하여 모빌리티 터널을 생성하기 위해 WLC 간에 공유하기 위한 컨피그레이션입니다.

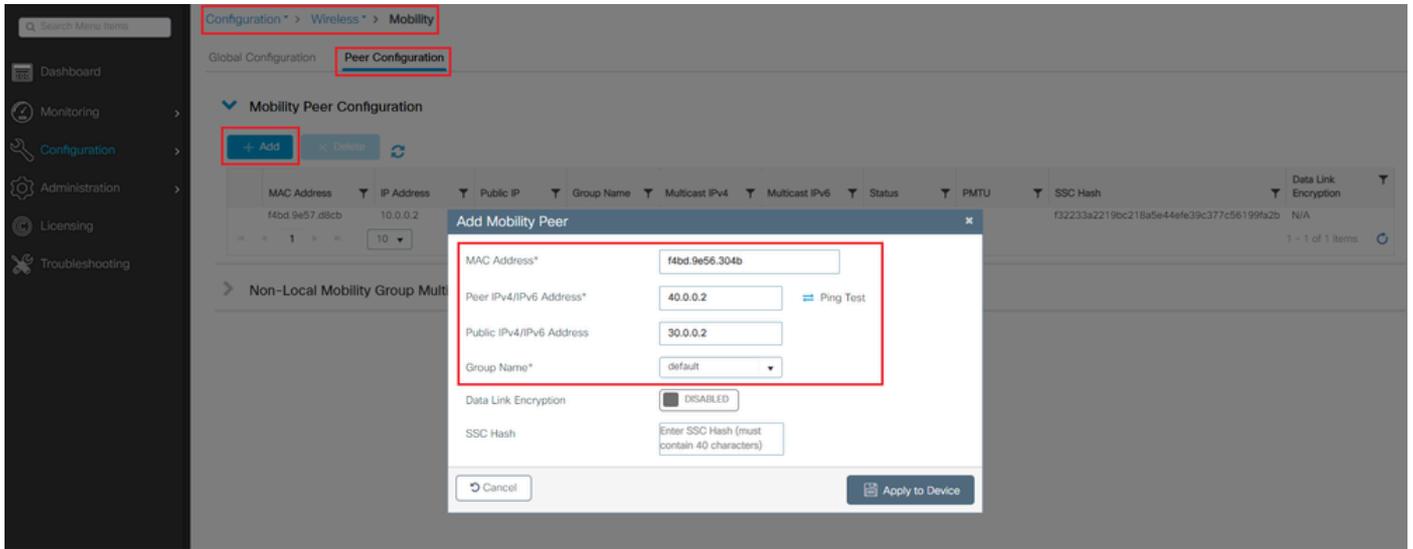
- 프라이빗 모빌리티 IP 주소
- 퍼블릭 모빌리티 IP 주소
- 모빌리티 그룹 Mac 주소
- 모빌리티 그룹 이름

WLC1의 컨피그레이션이 WLC2에 추가되고 그 반대의 경우도 마찬가지입니다. NAT를 통한 모빌리티 터널이 이 컨피그레이션의 최종 목표이므로 두 WLC의 퍼블릭 모빌리티 IP 주소는 각 라우터

의 고정 NAT 컨피그레이션에 구성된 NAT IP 주소입니다.

WLC1 구성:

GUI:

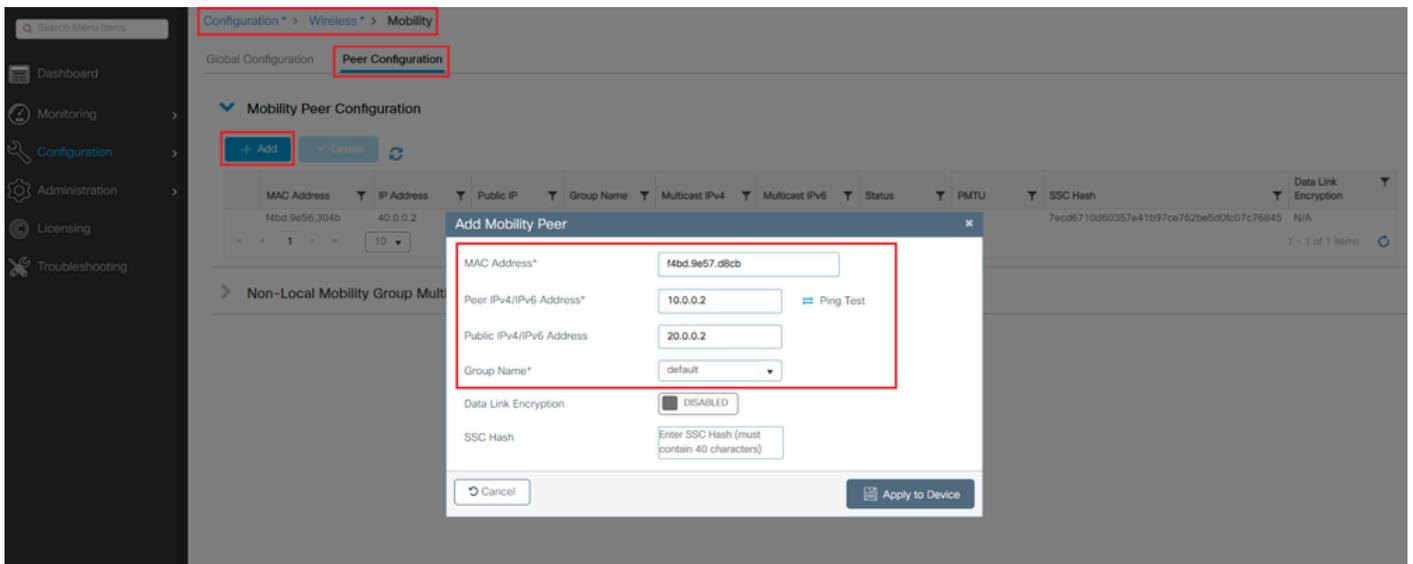


CLI:

```
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
WLC1(config)#end
WLC1#
```

WLC2 구성:

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#
```

다음을 확인합니다.

라우터 컨피그레이션 확인

라우터 측에서 이 명령은 NAT 컨피그레이션을 확인합니다. NAT 컨피그레이션은 NAT의 내부 및 외부 컨피그레이션이 존재하기 때문에(앞서 설명했듯이) 고정적이어야 합니다.

라우터NAT-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
```

라우터NAT-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
```

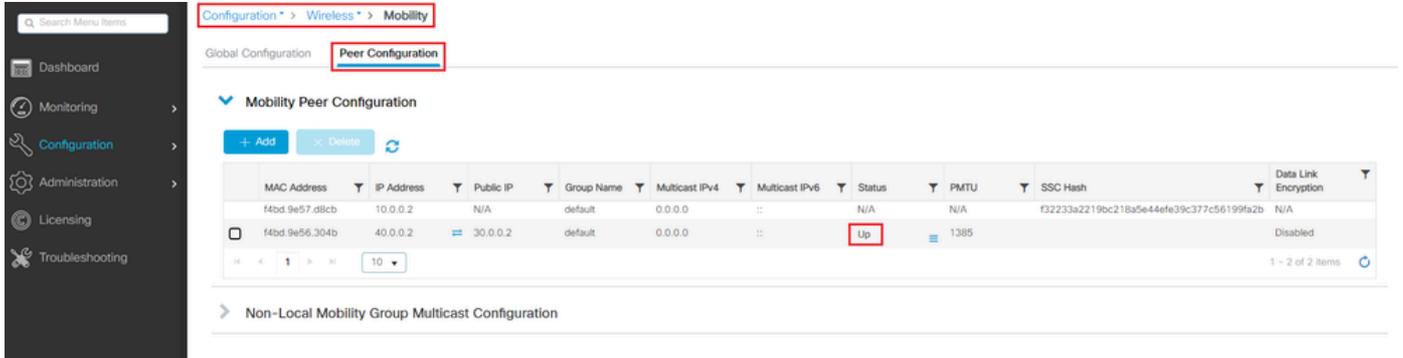
무선 LAN 컨트롤러 컨피그레이션 확인

WLC GUI 및 CLI에서 모빌리티 터널의 상태를 확인합니다. 이 문서의 앞부분에서 설명한 것처럼 모

빌리티 터널을 통한 WLC 간의 올바른 통신을 확인하기 위한 올바른 상태는 다음과 같습니다. 작동, 다른 모든 상태에 대한 조사가 필요합니다.

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:

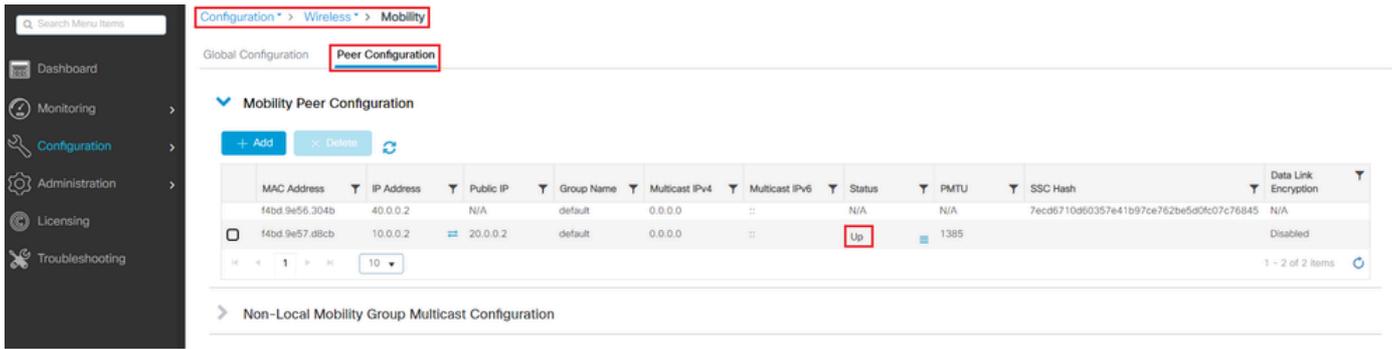
IP	Public Ip	MAC Address	Group Name	Multicast IPv4	Multicast IPv6	Status
10.0.0.2	N/A	f4bd.9e57.d8cb	default	0.0.0.0	::	N/A
40.0.0.2	30.0.0.2	f4bd.9e56.304b	default	0.0.0.0	::	

```
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_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
```

문제 해결

라우터 문제 해결

라우터 측에서 IP NAT 변환이 올바르게 수행되는지 확인합니다.

IP NAT 변환 및 통계

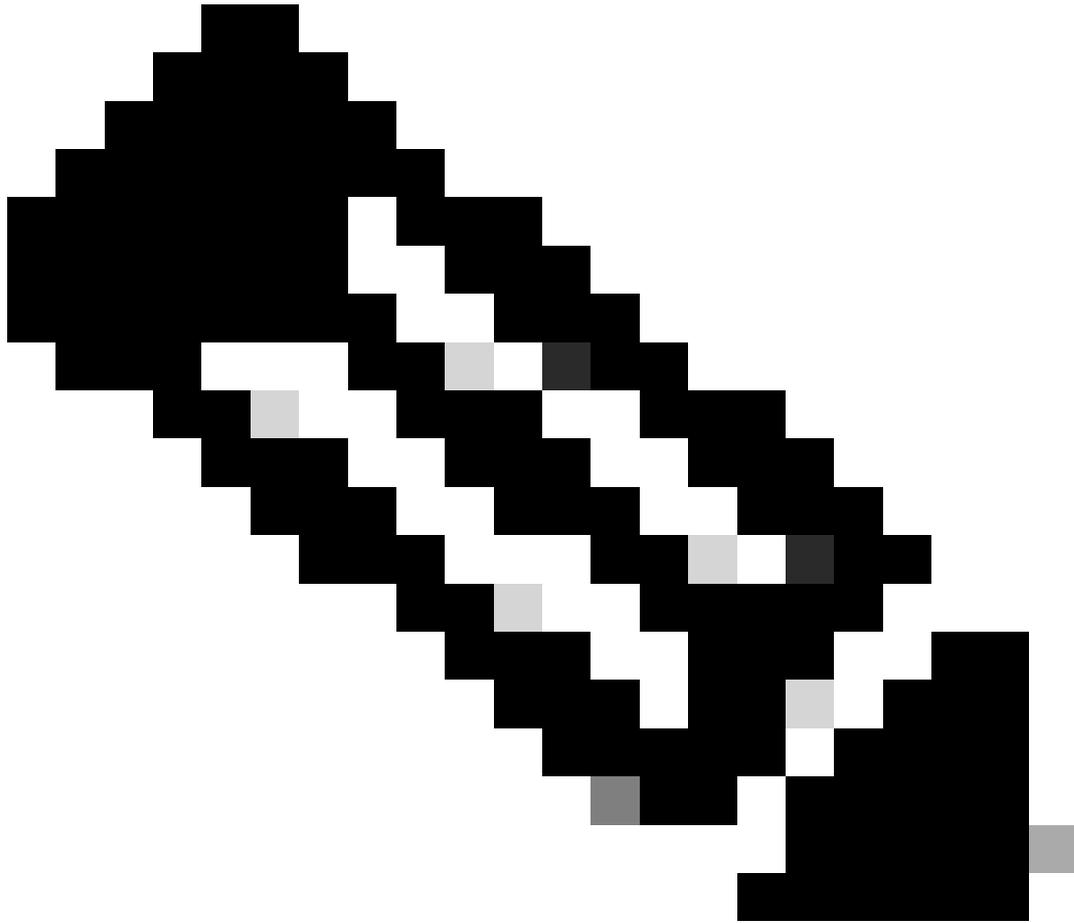
이 명령을 사용하여 라우터에서 수행되는 내부 및 외부 변환을 검토하고 NAT 통계를 확인할 수 있습니다.

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

IP NAT 디버그

이 명령은 라우터 관점에서 NAT 변환을 디버깅하여 NAT가 발생하는 방식 또는 라우터가 NAT 변환을 수행하는 동안 문제가 발생한 경우를 파악합니다.

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



참고: 라우터의 debug 명령을 실행하면 오버로드가 발생하여 라우터를 사용할 수 없게 될 수 있습니다. 라우터의 디버그는 극도로 주의해서 사용해야 합니다. 프로덕션 시간 중에 중요한 프로덕션 라우터에서 디버그를 실행하지 않는 경우 유지 관리 기간이 필요합니다.

무선 LAN 컨트롤러 문제 해결

모빌리티 터널이 올바른 상태가 아닌 Up 상태를 표시하는 경우 WLC에서 정보를 수집할 수 있습니다.

모빌리티 프로세스 로그

이 명령은 과거 및 현재 시간의 모빌리티 로그를 생성합니다

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

수집된 정보는 명령을 사용하여 WLC 자체에서 읽을 수 있습니다

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

수집된 정보를 WLC에서 내보내 명령을 사용하여 외부 소스에서 읽을 수도 있습니다

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

모빌리티 디버그 및 추적

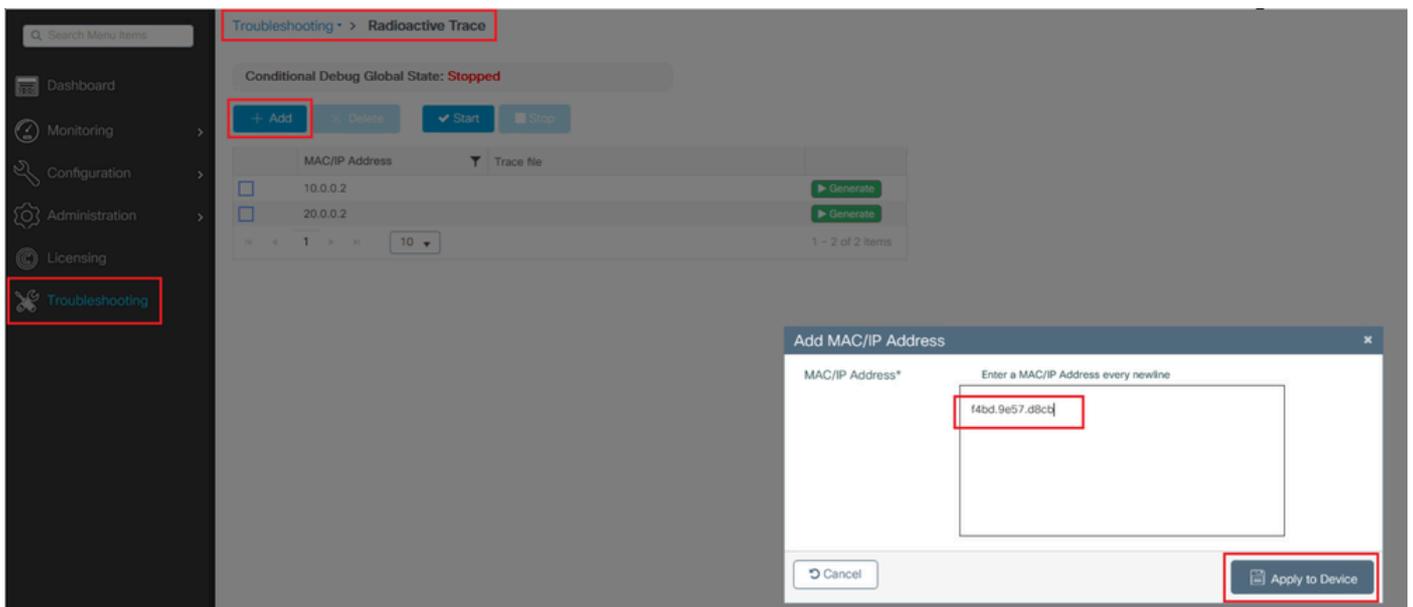
디버깅 및 추적은 모빌리티 프로세스 로그가 문제를 찾을 수 있을 만큼 정보를 생성하지 못할 경우 더 자세한 정보를 제공할 수 있습니다.

NAT를 사용하는 모빌리티 터널에 대해 디버그 및 추적이 수집되면 동작을 더 잘 이해하기 위해 정보를 동시에 가져오려면 추적 섹션에 이러한 정보를 입력해야 합니다.

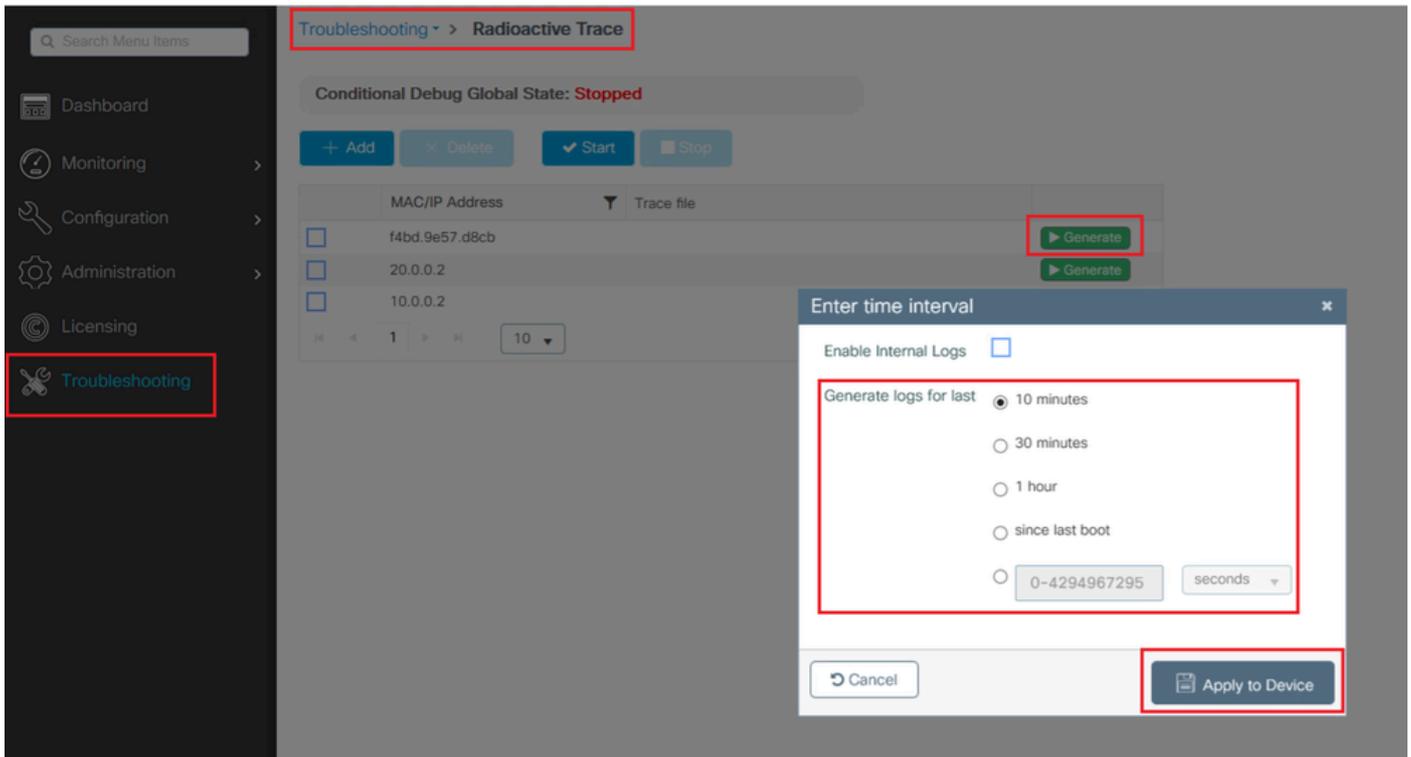
- 피어 공용 모빌리티 IP 주소
- 피어 개인 모빌리티 IP 주소
- 피어 모빌리티 Mac 주소

이 예에서는 WLC1의 모빌리티 MAC 주소와 함께 공용 및 사설 IP 주소가 WLC2에 입력됩니다. 이 경우 WLC1의 RA 추적 섹션에서 WLC2의 모빌리티 MAC 주소와 함께 사설 및 공용 IP 주소를 입력해야 합니다.

WLC GUI



그림과 같이 GUI에서 디버그 및 추적을 수집할 수 있습니다.



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
```

디버그를 수집하려면 이 명령을 사용할 수 있습니다. 필요에 따라 디버그 컬렉션의 시간을 변경합니다.

```
#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
```

전송 프로토콜을 사용하여 파일을 외부 소스에 복사합니다.

```
#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
```

패킷 캡처

9800 WLC는 내장된 패킷 캡처를 이용할 수 있으며, 이 기능을 사용하여 NAT를 통해 모빌리티 터

널의 WLC 간에 어떤 패킷이 교환되는지 확인할 수 있습니다.

이 예에서는 WLC1의 개인 IP 주소가 WLC2에서 패킷 캡처를 설정하는 데 사용되는데, 이 경우 패킷 캡처 설정을 위해 WLC1에서 WLC2의 개인 IP 주소를 사용해야 합니다.

패킷 캡처를 수행하려면 ACL을 생성하여 패킷을 필터링하고 NAT를 통해 모빌리티 터널에서 찾는 패킷만 표시할 수 있습니다. ACL이 생성되면 패킷 캡처에 필터로 연결됩니다. ACL은 패킷 헤더의 IP 주소이므로 모빌리티 프라이빗 IP 주소로 생성할 수 있습니다.

```
#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
```

캡처가 시작되기 전에 이 명령을 사용하여 모니터 캡처 컨피그레이션을 확인할 수 있습니다.

```
#show monitor capture MobilityNAT
```

모니터 캡처가 준비되고 선택되면 시작할 수 있습니다.

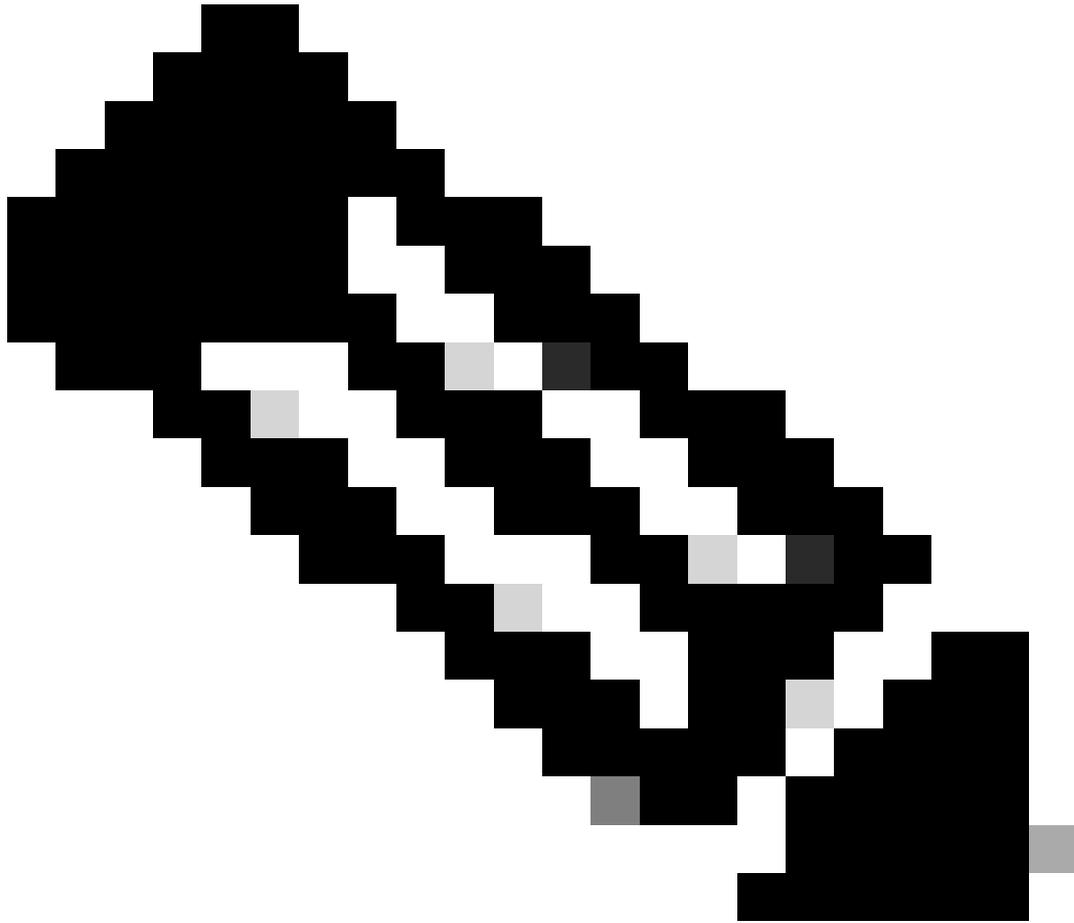
```
#monitor capture MobilityNAT start
```

이를 중지하려면 이 명령을 사용할 수 있습니다.

```
#monitor capture MobilityNAT stop
```

모니터 캡처가 중지되면 전송 프로토콜을 사용하여 외부 소스로 내보낼 수 있습니다.

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



참고: NAT를 사용하는 모빌리티 터널은 WLC 간의 양방향 대화가 필요한 기능입니다. 이 기능의 특성상 NAT 패킷 교환을 사용하는 모빌리티 터널을 더 잘 이해하기 위해 두 WLC의 로그, 디버그 및 추적 또는 패킷 캡처를 동시에 수집하는 것이 좋습니다.

디버그, 추적 및 패킷 캡처 지우기

필요한 정보를 가져오면 여기에 설명된 대로 추적 및 포함된 패킷 캡처 컨피그레이션을 WLC에서 삭제할 수 있습니다.

디버그 및 추적

```
#clear platform condition all
```

패킷 캡처

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

필요한 정보가 수집되면 WLC에서 수행된 트러블슈팅 컨피그레이션을 지우는 것이 좋습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.