

# Konfigurieren des 9800 Wireless LAN Controller Mobility Tunnel mit NAT

## Inhalt

---

### [Einleitung](#)

### [Voraussetzungen](#)

#### [Anforderungen](#)

#### [Verwendete Komponenten](#)

### [Hintergrundinformationen](#)

#### [Einschränkungen für NAT-Unterstützung für Mobilitätsgruppen](#)

### [Netzwerkdiagramm](#)

### [Konfigurieren](#)

#### [Konfigurieren von NAT auf dem Router](#)

#### [Konfigurieren von Mobilität mit NAT auf dem Wireless LAN-Controller](#)

### [Überprüfung](#)

#### [Überprüfung der Router-Konfiguration](#)

#### [Konfigurationsverifizierung des Wireless LAN-Controllers](#)

### [Fehlerbehebung](#)

#### [Router-Fehlerbehebung](#)

##### [IP NAT-Übersetzungen und -Statistiken](#)

##### [IP NAT-Debugging](#)

#### [Wireless LAN Controller-Fehlerbehebung](#)

##### [Mobility-Prozessprotokolle](#)

##### [Mobilitätsdebugs und -nachverfolgung](#)

##### [Paketerfassung](#)

##### [Klare Fehlersuche, Nachverfolgung und Paketerfassung](#)

---

## Einleitung

In diesem Dokument wird die Konfiguration der 9800 Wireless LAN Controller (WLC) mit einem Mobility Tunnel über Network Address Translation (NAT) beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in den folgenden Bereichen verfügen:

- Statische Network Address Translation (NAT)-Konfiguration und -Konzepte
- Konfiguration und Konzepte des Wireless LAN Controller 9800 Mobility Tunnels.

## Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Hintergrundinformationen

Mobility-Tunnel werden zwischen zwei oder mehr Wireless LAN Controllern (WLC) erstellt, um Informationen wie Access Point-Informationen, Wireless Client-Informationen, RRM-Informationen und mehr untereinander auszutauschen.

Es kann auch als eine Konfiguration für Anchor - Fremde Designs verwendet werden. Dieses Dokument beschreibt die Konfiguration eines Mobility-Tunnels zwischen Wireless LAN Controllern (WLC) mit Network Address Control (NAT).

Der WLC-Mobility-Tunnel kann einen der folgenden vier Status haben:

- Steuerungs- und Datenpfad nach unten
- Control Path Down (dies impliziert, dass der Datenpfad aktiv ist)
- Datenpfad nach unten (dies impliziert, dass die Steuerung aktiviert ist)
- Up

Der endgültige und korrekte Status für einen Mobilitätstunnel lautet: "Auf". Für jeden anderen Status ist eine weitere Untersuchung erforderlich. Mobility-Tunnel arbeiten über die CAPWAP-UDP-Ports 16666 und 16667, von denen der UDP-Port 16666 für Control Path und 16667 für Data Path steht. Aus diesem Grund muss sichergestellt werden, dass diese Ports zwischen den WLCs offen sind.



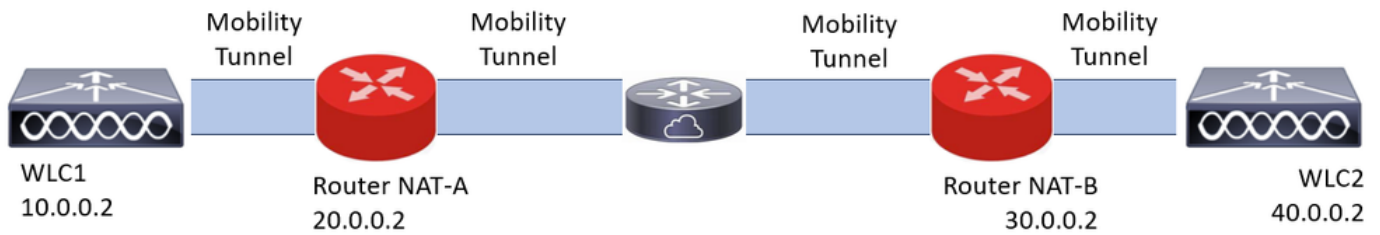
Hinweis: Informationen zur Konfiguration des WLC-Mobilitätstunnels ohne NAT finden Sie unter [Konfigurieren von Mobilitätstopologien auf Catalyst 9800 Wireless LAN-Controllern](#).

---

## Einschränkungen für NAT-Unterstützung für Mobilitätsgruppen

- Nur statische NAT (1:1) kann konfiguriert werden.
- Mehrere Mobility Tunnel-Peers mit derselben öffentlichen IP-Adresse werden nicht unterstützt.
- Jedes Mitglied muss über eine eindeutige private IP-Adresse verfügen.
- Port Address Translation (PAT) wird nicht unterstützt.
- Inter-Release Controller Mobility (IRCM) für Wireless-Client-Roaming wird nicht unterstützt.
- IPv6-Adressumwandlung wird nicht unterstützt.
- Network Access Control (NAC) mit Mobility Tunnel wird ab WLC Code Version 17.7.1 unterstützt.

## Netzwerkdiagramm



## Konfigurieren

### Konfigurieren von NAT auf dem Router

In dieser Konfiguration werden Router verwendet, um Funktionen für die Netzwerkzugriffskontrolle (NAT) bereitzustellen. Es kann jedoch jedes Gerät verwendet werden, das statische NAT ausführen kann. Static NAT ist die für WLC-Mobility-Tunnel unterstützte NAT-Methode. Dies ist die im Konfigurationsbeispiel "Router" verwendete Konfiguration. Zu Konfigurationszwecken werden diese Router verwendet: NAT-A und NAT-B. Der WLC1 befindet sich hinter Router NAT-A und der WLC2 hinter Router NAT-B.

Router NAT-A-Konfiguration:

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-Konfiguration:

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#
```

## Konfigurieren von Mobilität mit NAT auf dem Wireless LAN-Controller

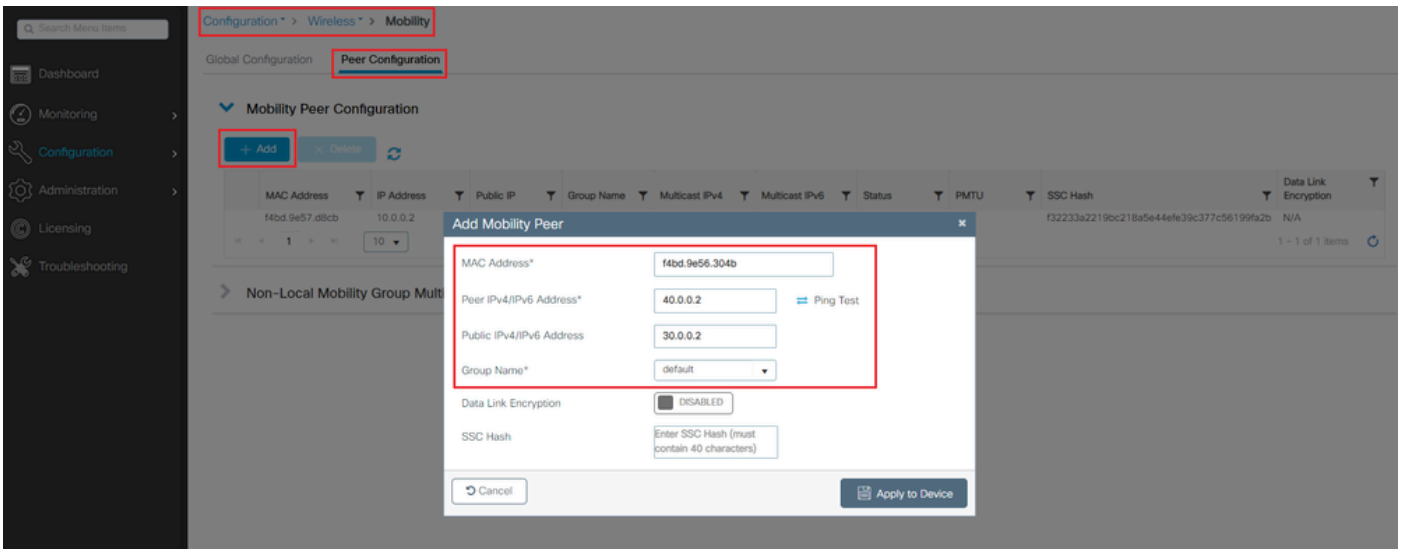
Dies ist die Konfiguration, die von WLCs gemeinsam genutzt werden muss, um den Mobility Tunnel mit NAT zu erstellen:

- Private Mobility-IP-Adresse
- IP-Adresse für öffentliche Mobilität
- Mobilitätsgruppe MAC-Adresse
- Name der Mobilitätsgruppe

Die Konfiguration von WLC1 wird zu WLC2 hinzugefügt und umgekehrt. Dies kann über CLI oder GUI in den WLCs erfolgen, da der Mobilitätstunnel mit NAT das letzte Ziel dieser Konfiguration ist. Die öffentliche Mobilitäts-IP-Adresse beider WLCs ist die NAT-IP-Adresse, die in der statischen NAT-Konfiguration in jedem Router konfiguriert ist.

WLC1-Konfiguration:

GUI:

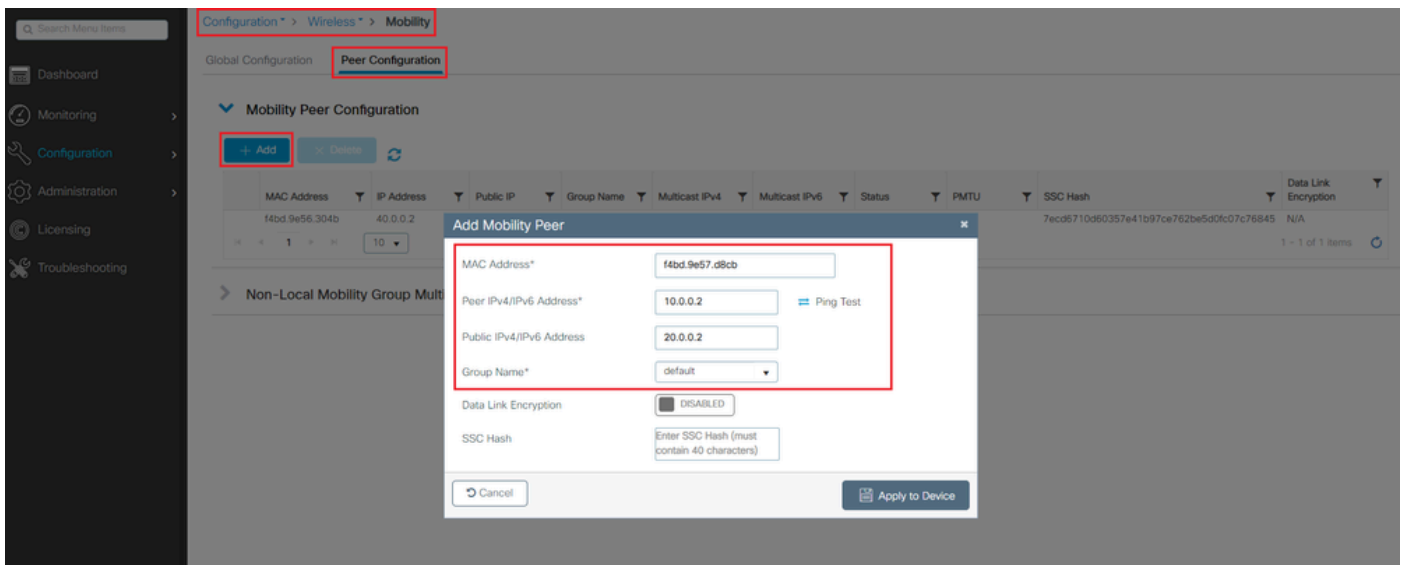


CLI:

```
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-Konfiguration:

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#
```

## Überprüfung

### Überprüfung der Router-Konfiguration

Von der Routerseite aus überprüfen diese Befehle die NAT-Konfiguration. Die NAT-Konfiguration muss statisch sein (wie in diesem Dokument bereits erwähnt), da sowohl die interne als auch die externe NAT-Konfiguration vorhanden ist.

### 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

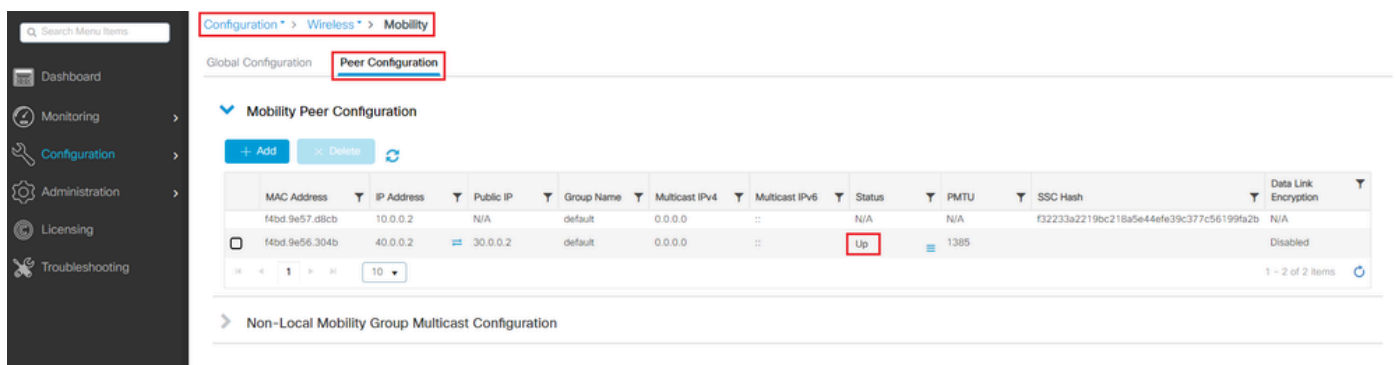
```
RouterNAT-B#show run interface GigabitEthernet0/1/2
interface GigabitEthernet0/1/2
ip add 40.0.0.1 255.255.255.0
ip nat inside
!
RouterNAT-B#show run interface GigabitEthernet0/1/3
interface GigabitEthernet0/1/3
ip add 30.0.0.1 255.255.255.0
ip nat outside
!
RouterNAT-B#show run | in ip nat inside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

## Konfigurationsverifizierung des Wireless LAN-Controllers

Prüfen Sie anhand der WLC-GUI und der CLI den Status des Mobilitätstunnels. Wie bereits in diesem Dokument erwähnt, lautet der richtige Status, um eine korrekte Kommunikation zwischen den WLCs über den Mobilitätstunnel zu bestätigen: "Up" (aktiv). Alle anderen Statusüberprüfungen sind erforderlich.

### WLC1

#### GUI:



The screenshot shows the Cisco WLC GUI navigation path: Configuration > Wireless > Mobility. Under Peer Configuration, there is a table for Mobility Peer Configuration. The table has columns for MAC Address, IP Address, Public IP, Group Name, Multicast IPv4, Multicast IPv6, Status, PMTU, SSC Hash, and Data Link Encryption. The row for MAC Address f4bd.9e56.304b shows a status of 'Up', which is highlighted with a red box. Below the table, there is a section for Non-Local Mobility Group Multicast Configuration.

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

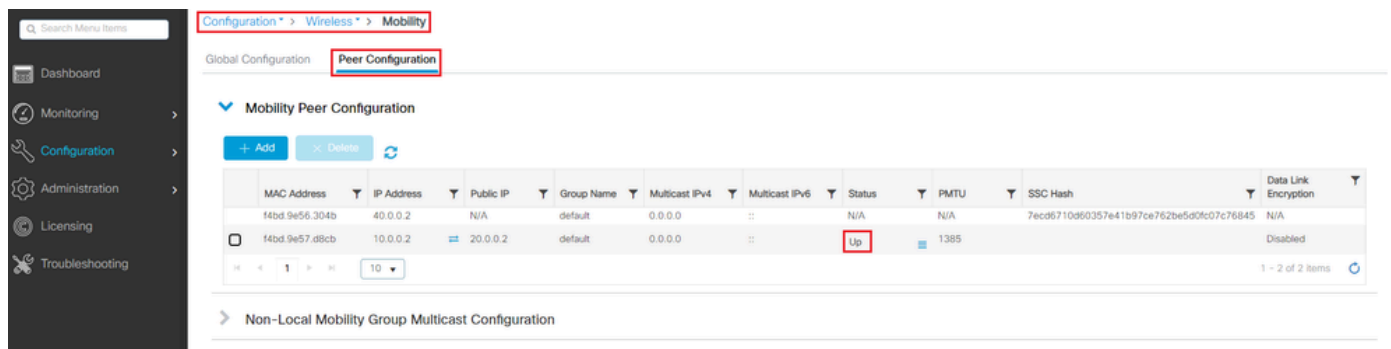
Controllers configured in the Mobility Domain:

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	::	Up

Up  
 1385

## WLC 2

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

## Fehlerbehebung

### Router-Fehlerbehebung

Vergewissern Sie sich, dass die IP NAT-Übersetzungen auf der Routerseite korrekt vorgenommen wurden.

#### IP NAT-Übersetzungen und -Statistiken

Verwenden Sie diese Befehle, um zu überprüfen, welche internen und externen Übersetzungen im Router durchgeführt werden, und um die NAT-Statistiken zu überprüfen.

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

#### IP NAT-Debugging

Mit diesem Befehl wird die NAT-Übersetzung aus der Router-Perspektive gedebuggt, um zu ermitteln, wie die NAT erfolgt, oder ob während der NAT-Übersetzung ein Problem auftritt.

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



Hinweis: Jeder Debug-Befehl auf einem Router kann zu Überlastung führen, wodurch der Router funktionsuntüchtig wird. Bei der Verwendung von Routerdebugs ist äußerste Vorsicht geboten. Wenn Sie während der Produktionszeit möglichst kein Debugging auf einem kritischen Produktionsrouter durchführen, ist ein Wartungsfenster wünschenswert.

---

## Wireless LAN Controller-Fehlerbehebung

Die Informationen hierzu können vom WLC abgerufen werden, falls der Mobilitätstunnel einen Status anzeigt, der nicht der richtige ist, nämlich "Up" (aktiv).

### Mobility-Prozessprotokolle

Mit diesem Befehl werden Mobilitätsprotokolle aus der Vergangenheit und der Gegenwart erstellt.

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

Die erfassten Informationen können mit dem Befehl

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

Die gesammelten Informationen können auch vom WLC exportiert werden, um sie mithilfe des Befehls in einer externen Quelle zu lesen.

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

### Mobilitätsdebugs und -nachverfolgung

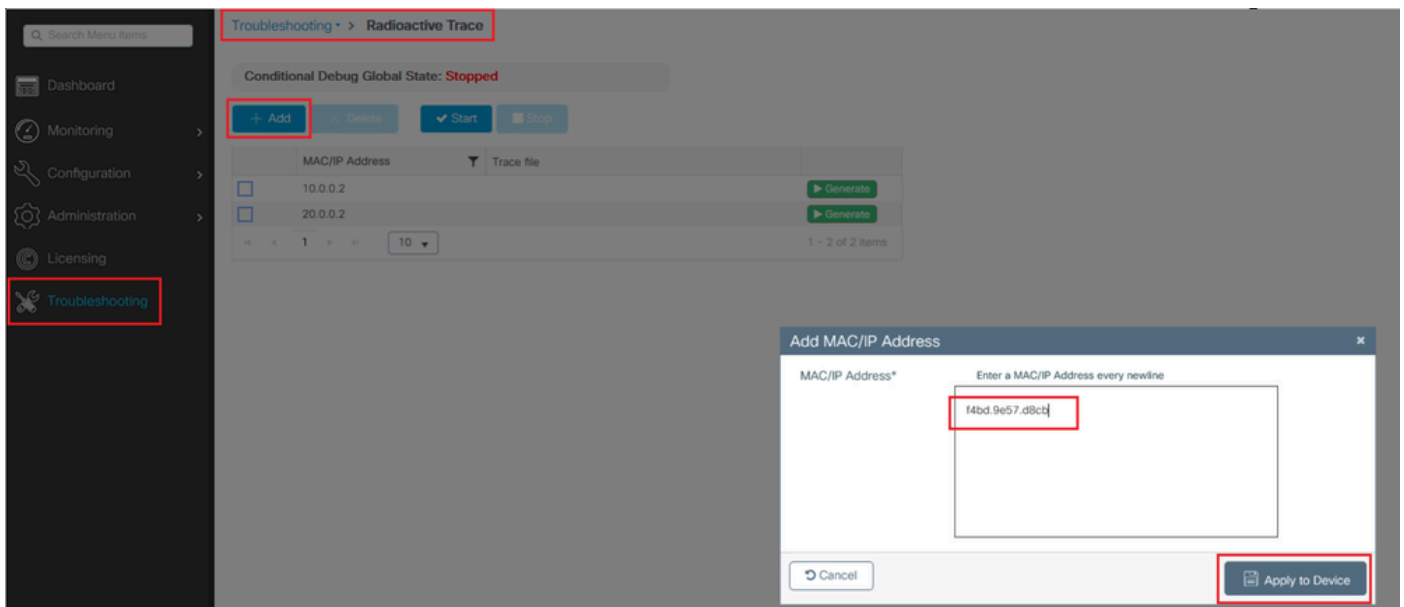
Debugs und Traces können detailliertere Informationen bereitstellen, falls die Mobilitätsprozessprotokolle nicht in der Lage sind, ausreichend Informationen zu generieren, um das Problem zu finden.

Wenn Debugs und Traces für einen Mobility Tunnel mit NAT erfasst werden, ist es wichtig, diese Informationen in den Trace-Abschnitt einzugeben, um die Informationen gleichzeitig abzurufen und das Verhalten besser zu verstehen:

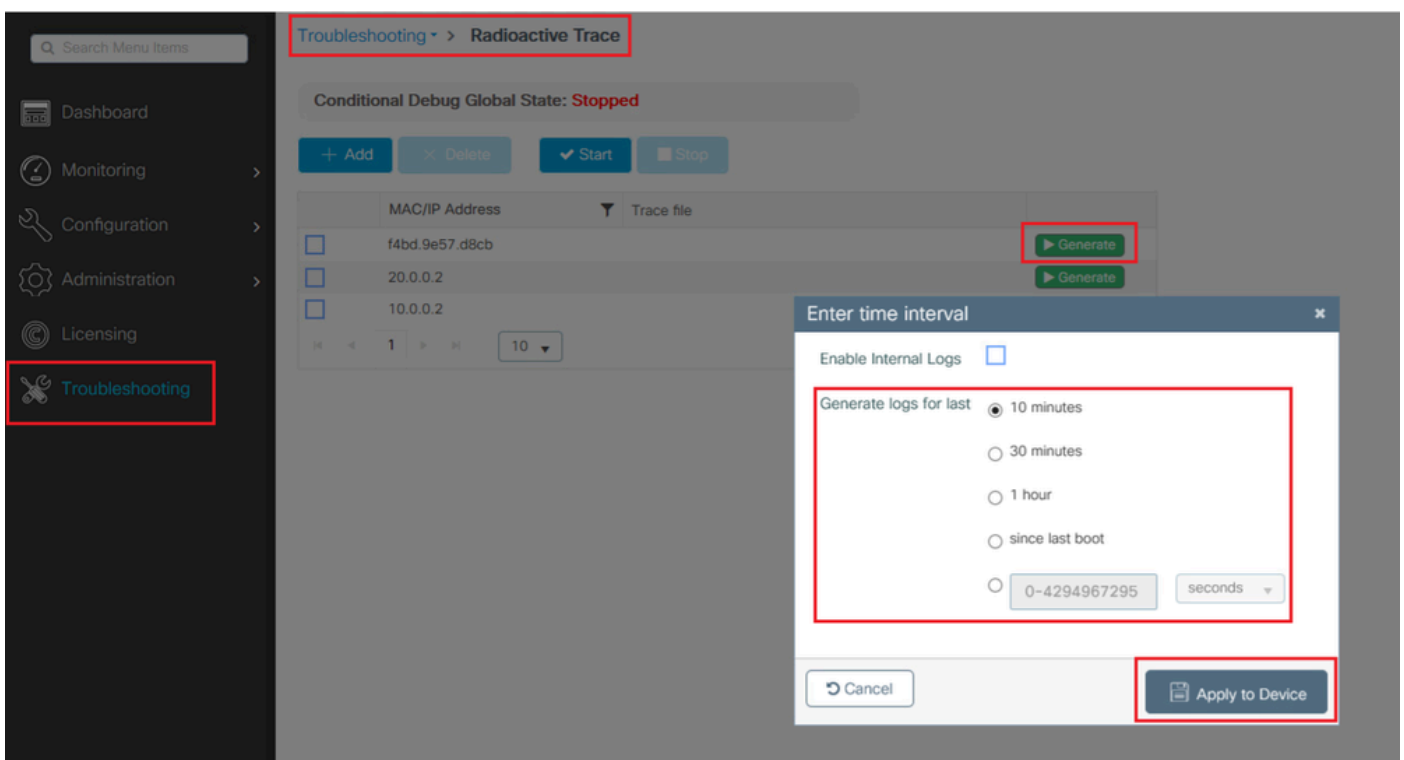
- Öffentliche Peer-Mobility-IP-Adresse
- Private Mobility-IP-Adresse des Peers
- Mac-Adresse für Peer-Mobilität

In diesem Beispiel wird die öffentliche und die private IP-Adresse zusammen mit der Mobility-MAC-Adresse von WLC1 in WLC2 eingegeben. Dies muss rückwärts erfolgen, wobei die private und die öffentliche IP-Adresse zusammen mit der Mobility-MAC-Adresse von WLC2 im Abschnitt RA Trace von WLC1 eingegeben werden.

WLC-Benutzeroberfläche



Debugs und Traces können wie dargestellt über die GUI gesammelt werden.



## 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
```

Zum Sammeln der Debugs kann dieser Befehl verwendet werden. Ändern Sie den Zeitpunkt der debugs-Auflistung nach Bedarf.

```
#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
```

Kopieren Sie die Dateien mithilfe eines Übertragungsprotokolls in eine externe Quelle.

```
#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
```

## Paketerfassung

Der 9800 WLC kann eingebettete Paketerfassungen übernehmen. Verwenden Sie diese Funktion, um zu überprüfen, welche Pakete zwischen WLCs für den Mobility-Tunnel mit NAT ausgetauscht werden.

In diesem Beispiel wird die private IP-Adresse von WLC1 in WLC2 verwendet, um die Paketerfassung einzurichten. Dies muss rückwärts erfolgen, wobei sie für die Einrichtung der Paketerfassung die private IP-Adresse von WLC2 in WLC1 verwendet.

Um die Paketerfassung vorzunehmen, kann eine ACL erstellt werden, um die Pakete zu filtern und nur die Pakete anzuzeigen, nach denen wir mit NAT nach einem Mobility Tunnel suchen. Sobald die ACL erstellt wurde, wird sie als Filter an die Paketerfassung angehängt. Die ACL kann mit der privaten Mobility-IP-Adresse erstellt werden, da diese im Paket-Header enthalten ist.

```
#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
```

Vor Beginn der Erfassung kann dieser Befehl verwendet werden, um die Überwachungserfassungskonfiguration zu überprüfen.

```
#show monitor capture MobilityNAT
```

Sobald die Monitorerfassung bereit und aktiviert ist, kann sie gestartet werden.

```
#monitor capture MobilityNAT start
```

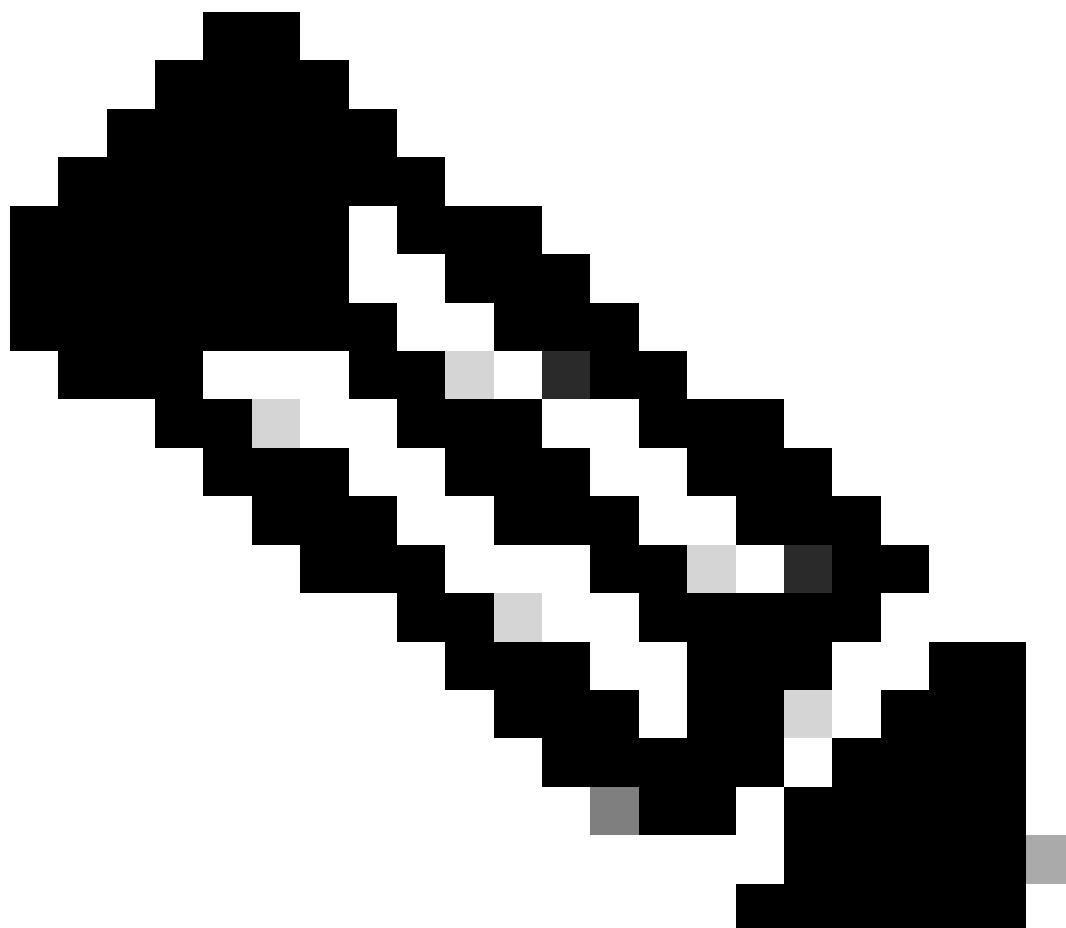
Um es zu stoppen, kann dieser Befehl verwendet werden.

```
#monitor capture MobilityNAT stop
```

Sobald die Monitorerfassung beendet wird, kann sie mithilfe eines Übertragungsprotokolls in eine externe Quelle exportiert werden.

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

---



Hinweis: Mobility Tunnel mit NAT ist eine Funktion, für die ein bidirektionales Gespräch

---

---

zwischen WLCs erforderlich ist. Aufgrund der Art der Funktion wird dringend empfohlen, Protokolle, Debugging- und Traces- bzw. Paketerfassungen von beiden WLCs gleichzeitig zu sammeln, um den Mobility Tunnel mit NAT-Paketaustausch besser zu verstehen.

---

## Klare Fehlersuche, Nachverfolgung und Paketerfassung

Nachdem die erforderlichen Informationen abgerufen wurden, können die Debug-Meldungen, Ablaufverfolgungen und die Konfiguration der integrierten Paketerfassung wie hier beschrieben aus dem WLC gelöscht werden.

## Debugs und Ablaufverfolgungen

```
#clear platform condition all
```

## Paketerfassung

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

Es wird dringend empfohlen, die im WLC durchgeführte Fehlerbehebungs-konfiguration zu löschen, nachdem die erforderlichen Informationen gesammelt wurden.



## Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.