

Configuration du tunnel de mobilité du contrôleur LAN sans fil 9800 avec NAT

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Restrictions pour la prise en charge NAT sur les groupes de mobilité](#)

[Diagramme du réseau](#)

[Configurer](#)

[Configuration de la NAT sur le routeur](#)

[Configuration de la mobilité avec NAT sur le contrôleur LAN sans fil](#)

[Vérifier](#)

[Vérification de la configuration du routeur](#)

[Vérification de la configuration du contrôleur LAN sans fil](#)

[Dépannage](#)

[Dépannage du routeur](#)

[Traductions et statistiques IP NAT](#)

[Débogage NAT IP](#)

[Dépannage du contrôleur LAN sans fil](#)

[Journaux des processus de mobilité](#)

[Débogages et suivis de mobilité](#)

[Captures de paquets](#)

[Effacer les débogages, les suivis et les captures de paquets](#)

Introduction

Ce document décrit comment configurer les contrôleurs de réseau local sans fil (WLC) 9800 avec un tunnel de mobilité sur la traduction d'adresses de réseau (NAT).

Conditions préalables

Exigences

Cisco recommande de posséder des connaissances sur ces sujets :

- Configuration et concepts de la traduction d'adresses de réseau (NAT) statique.
- Configuration et concepts du tunnel de mobilité du contrôleur LAN sans fil 9800.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Gamme de contrôleurs sans fil Catalyst 9800 (Catalyst 9800-L), Cisco IOS® XE Gibraltar 17.9.4
- Routeurs à services intégrés (ISR), Cisco IOS® XE Gibraltar 17.6.5
- Commutateur Catalyst 3560, 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Des tunnels de mobilité sont créés entre deux contrôleurs de réseau local sans fil (WLC) ou plus avec l'intention de partager des informations entre eux telles que des informations de point d'accès, des informations de client sans fil, des informations RRM et plus encore.

Il peut également être utilisé comme configuration basée sur les conceptions Anchor - Foreign. Ce document décrit comment configurer un tunnel de mobilité entre des contrôleurs de réseau local sans fil (WLC) avec le contrôle d'adresse réseau (NAT).

Le tunnel de mobilité WLC peut avoir l'un des quatre états suivants :

- Contrôle et chemin des données inactif
- Chemin de contrôle inactif (cela signifie que le chemin des données est actif)
- Chemin de données inactif (ce qui signifie que le contrôle est actif)
- Haut

L'état final et correct d'un tunnel de mobilité est le suivant : Up (Actif), tout autre état nécessite un examen plus approfondi. Les tunnels de mobilité fonctionnent sur les ports udp CAPWAP 16666 et 16667, à partir desquels le port udp 16666 est pour le chemin de contrôle et 16667 pour le chemin de données. Pour cette raison, il est nécessaire de s'assurer que ces ports sont ouverts entre les WLC.

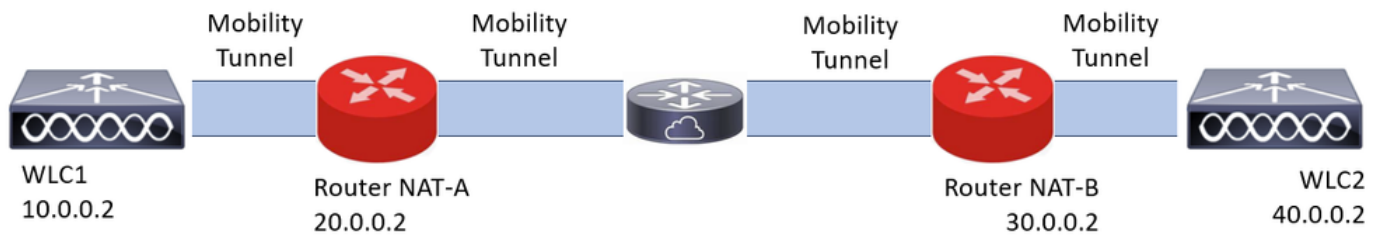


Remarque : pour la configuration du tunnel de mobilité WLC sans NAT, reportez-vous à la section [Configuration des topologies de mobilité sur les contrôleurs LAN sans fil Catalyst 9800](#)

Restrictions pour la prise en charge NAT sur les groupes de mobilité

- Seule la fonction NAT statique (1:1) peut être configurée.
- Plusieurs homologues de tunnel de mobilité avec la même adresse IP publique ne sont pas pris en charge.
- Chaque membre doit avoir une adresse IP privée unique.
- La traduction d'adresses de port (PAT) n'est pas prise en charge.
- La fonction IRCM (Inter-Release Controller Mobility) pour l'itinérance client sans fil n'est pas prise en charge.
- La traduction d'adresses IPv6 n'est pas prise en charge.
- Le contrôle d'accès au réseau (NAT) avec tunnel de mobilité est pris en charge à partir du code WLC version 17.7.1 et ultérieure.

Diagramme du réseau



Configurer

Configuration de la NAT sur le routeur

Les routeurs sont utilisés dans cette configuration pour fournir des fonctionnalités NAT (Network Access Control). Cependant, tout périphérique capable d'effectuer la NAT statique peut être utilisé. La NAT statique est la méthode NAT prise en charge pour les tunnels de mobilité WLC, c'est la configuration utilisée dans l'exemple de configuration des routeurs. À des fins de configuration, ces routeurs sont utilisés : NAT-A et NAT-B. Le WLC1 est derrière le routeur NAT-A et le WLC2 est derrière le routeur NAT-B.

Configuration du routeur NAT-A :

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#
```

Configuration du routeur NAT-B :

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#
```

Configuration de la mobilité avec NAT sur le contrôleur LAN sans fil

Il s'agit de la configuration à partager entre les WLC pour créer le tunnel de mobilité avec NAT :

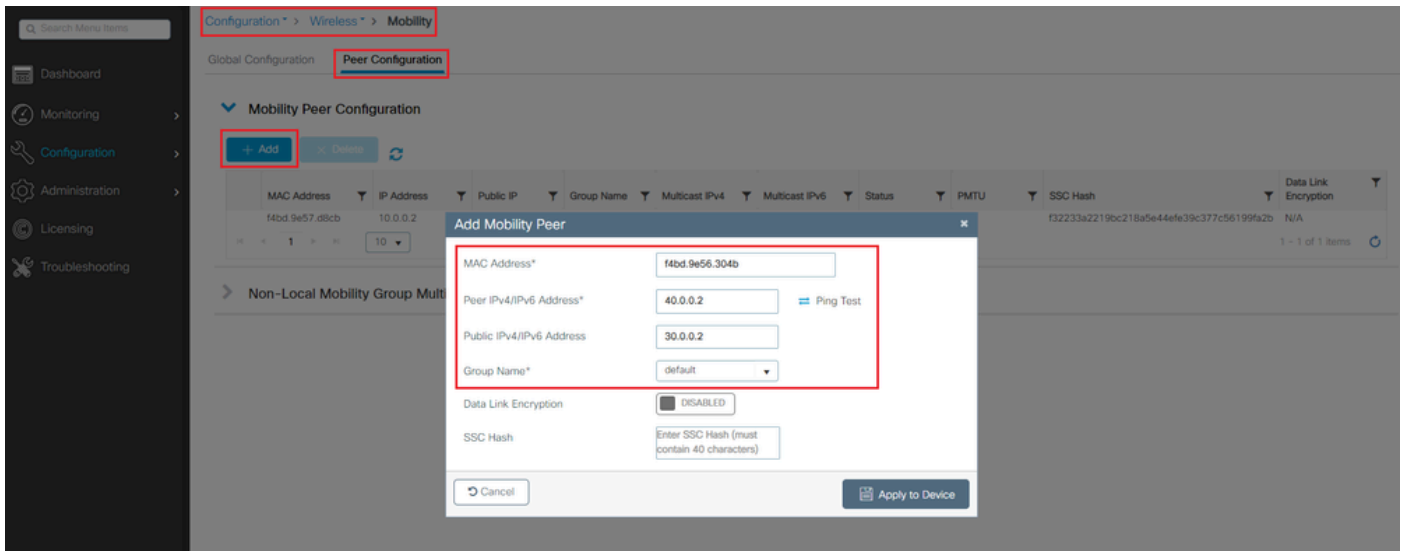
- Adresse IP de mobilité privée
- Adresse IP de mobilité publique
- Groupe de mobilité Adresse Mac

- Nom du groupe de mobilité

La configuration du WLC1 est ajoutée au WLC2 et vice-versa, cela peut être fait via l'interface de ligne de commande ou l'interface graphique dans les WLC, puisque le tunnel de mobilité avec NAT est l'objectif final de cette configuration. L'adresse IP de mobilité publique des deux WLC est l'adresse IP NAT configurée dans la configuration NAT statique dans chaque routeur.

Configuration WLC1 :

IUG:

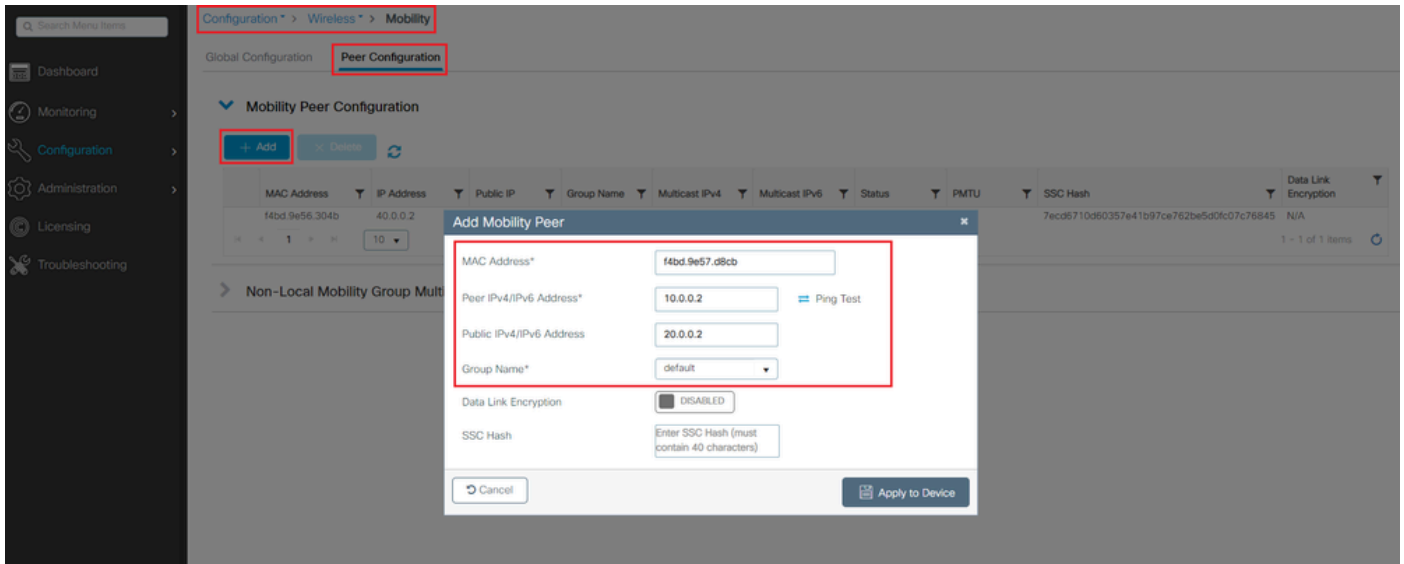


CLI :

```
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#
```

Configuration WLC2 :

IUG:



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#
```

Vérifier

Vérification de la configuration du routeur

Côté routeur, ces commandes permettent de vérifier la configuration NAT. La configuration NAT doit être statique (comme mentionné précédemment dans le document), ce qui explique la présence des configurations interne et externe pour NAT.

Routeur 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
```

RouteurNAT-B

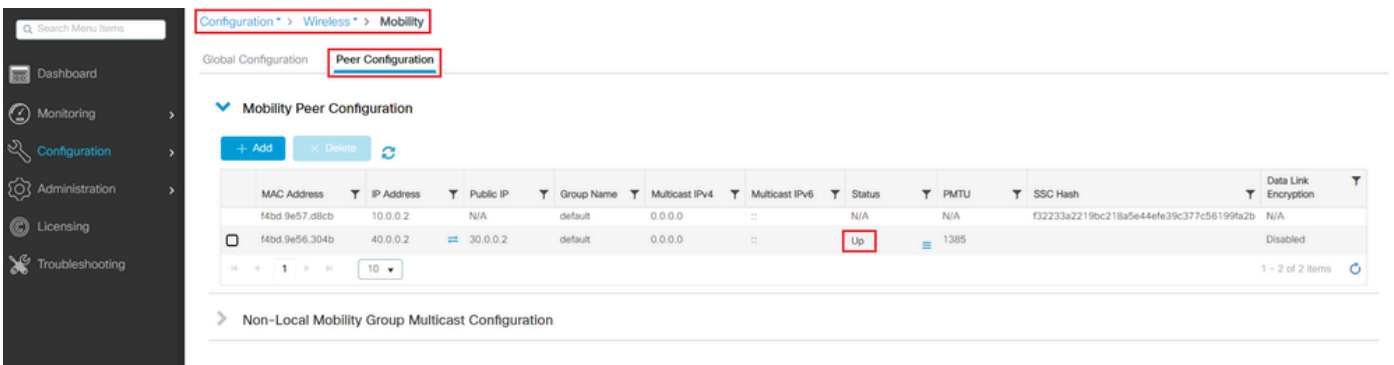
```
RouterNAT-B#show run interface GigabitEthernet0/1/2
interface GigabitEthernet0/1/2
ip add 40.0.0.1 255.255.255.0
ip nat inside
!
RouterNAT-B#show run interface GigabitEthernet0/1/3
interface GigabitEthernet0/1/3
ip add 30.0.0.1 255.255.255.0
ip nat outside
!
RouterNAT-B#show run | in ip nat inside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

Vérification de la configuration du contrôleur LAN sans fil

Vérifiez à partir de l'interface graphique et de la CLI du WLC l'état du tunnel de mobilité, comme mentionné précédemment dans ce document, l'état correct pour confirmer une communication correcte entre les WLC sur le tunnel de mobilité est : Up, any other status need investigation.

WLC1

IUG:



The screenshot shows the Cisco WLC GUI navigation path: Configuration > Wireless > Mobility. Under Peer Configuration, a table lists mobility peers. The second row shows a peer with IP 40.0.0.2 and a status of 'Up', which is highlighted with a red box. The table columns include MAC Address, IP Address, Public IP, Group Name, Multicast IPv4, Multicast IPv6, Status, PMTU, SSC Hash, and Data Link Encryption.

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

IUG:

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
<input checked="" type="checkbox"/>	f4bd.9e57.d8cb	10.0.0.2	20.0.0.2	default	0.0.0.0	::	Up	1385		Disabled

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_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

Dépannage

Dépannage du routeur

Vérifiez du côté du routeur que les traductions IP NAT se déroulent correctement.

Traductions et statistiques IP NAT

Utilisez ces commandes pour examiner les traductions internes et externes effectuées sur le routeur, ainsi que pour vérifier les statistiques NAT.

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

Débogage NAT IP

Cette commande débogue la traduction NAT du point de vue du routeur pour comprendre comment la traduction NAT se déroule ou s'il y a un problème pendant que le routeur effectue la traduction NAT.

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



Remarque : toute commande debug sur un routeur peut provoquer une surcharge qui rend le routeur inutilisable. Les débogages sur les routeurs doivent être utilisés avec une extrême prudence. Si possible, n'exécutez aucun débogage sur un routeur de production critique pendant le temps de production, une fenêtre de maintenance est souhaitée.

Dépannage du contrôleur LAN sans fil

Les informations ici peuvent être collectées à partir du WLC dans le cas où le tunnel de mobilité montre un état qui n'est pas le bon état qui est Up.

Journaux des processus de mobilité

Cette commande génère des journaux de mobilité à partir de l'heure passée et présente

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

Les informations recueillies peuvent être lues dans le WLC lui-même avec la commande

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

Les informations recueillies peuvent également être exportées du WLC pour les lire dans une source externe avec la commande

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

Débogages et suivis de mobilité

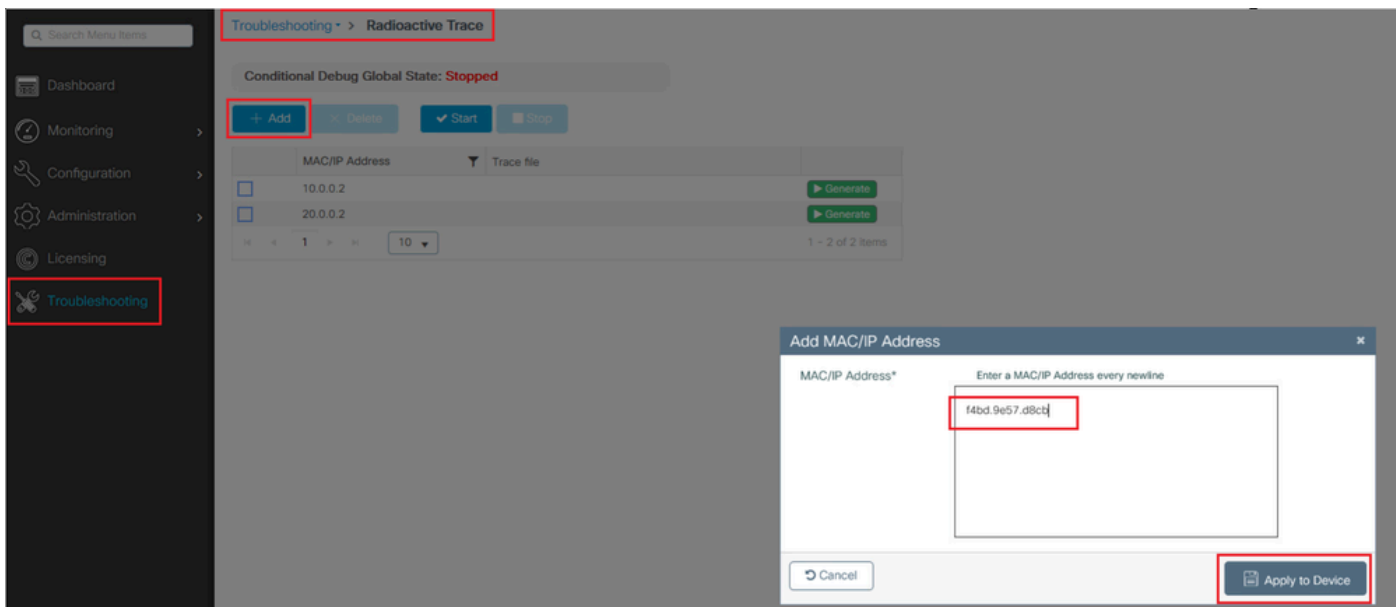
Les débogages et les suivis peuvent fournir des informations plus détaillées au cas où les journaux de processus de mobilité ne seraient pas en mesure de générer suffisamment d'informations pour détecter le problème.

Lorsque des débogages et des traces sont collectés pour le tunnel de mobilité avec NAT, il est important d'entrer ces informations dans la section trace pour obtenir les informations simultanément afin de mieux comprendre le comportement :

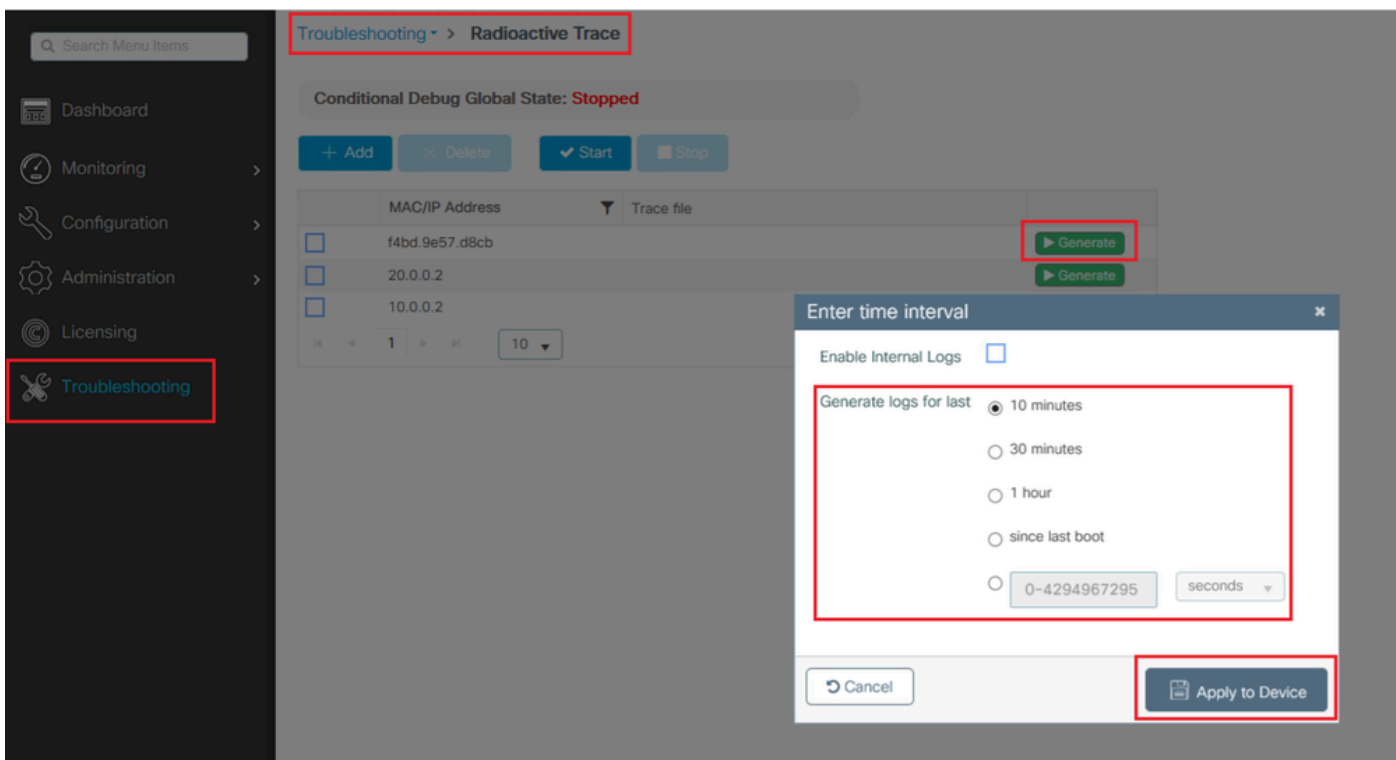
- Adresse IP de mobilité publique homologue
- Adresse IP de mobilité privée homologue
- Adresse Mac de mobilité homologue

Dans cet exemple, l'adresse IP publique et privée avec l'adresse MAC de mobilité de WLC1 est entrée dans WLC2, la même chose doit être faite à l'envers, où nous entrons l'adresse IP privée et publique avec l'adresse MAC de mobilité de WLC2 dans la section RA Trace de WLC1.

GUI WLC



Les débogages et les suivis peuvent être collectés à partir de l'interface utilisateur graphique, comme illustré.



CLI WLC

```
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
```

Pour collecter les débogages, cette commande peut être utilisée. Modifiez l'heure de la collection debugs si nécessaire.

```
#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
```

Copiez les fichiers sur une source externe avec un protocole de transfert.

```
#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
```

Captures de paquets

Le WLC 9800 a la capacité de prendre des captures de paquets intégrées, utilisez cette fonctionnalité pour vérifier quels paquets sont échangés entre les WLC pour le tunnel de mobilité avec NAT.

Dans cet exemple, l'adresse IP privée de WLC1 est utilisée dans WLC2 pour configurer la capture de paquets, la même chose doit être faite à l'envers, où elle doit être utilisée l'adresse IP privée de WLC2 dans le WLC1 pour la configuration de capture de paquets.

Pour prendre la capture de paquets, une ACL peut être créée pour filtrer les paquets et n'afficher que les paquets que nous recherchons pour le tunnel de mobilité avec NAT, une fois que l'ACL est créée, elle est attachée à la capture de paquets en tant que filtre. La liste de contrôle d'accès peut être créée avec l'adresse IP privée de mobilité, car il s'agit des adresses figurant dans l'en-tête du paquet.

```
#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
```

Avant que la capture ne démarre, cette commande peut être utilisée pour vérifier la configuration de la capture du moniteur.

```
#show monitor capture MobilityNAT
```

Une fois la capture du moniteur prête et vérifiée, elle peut être lancée.

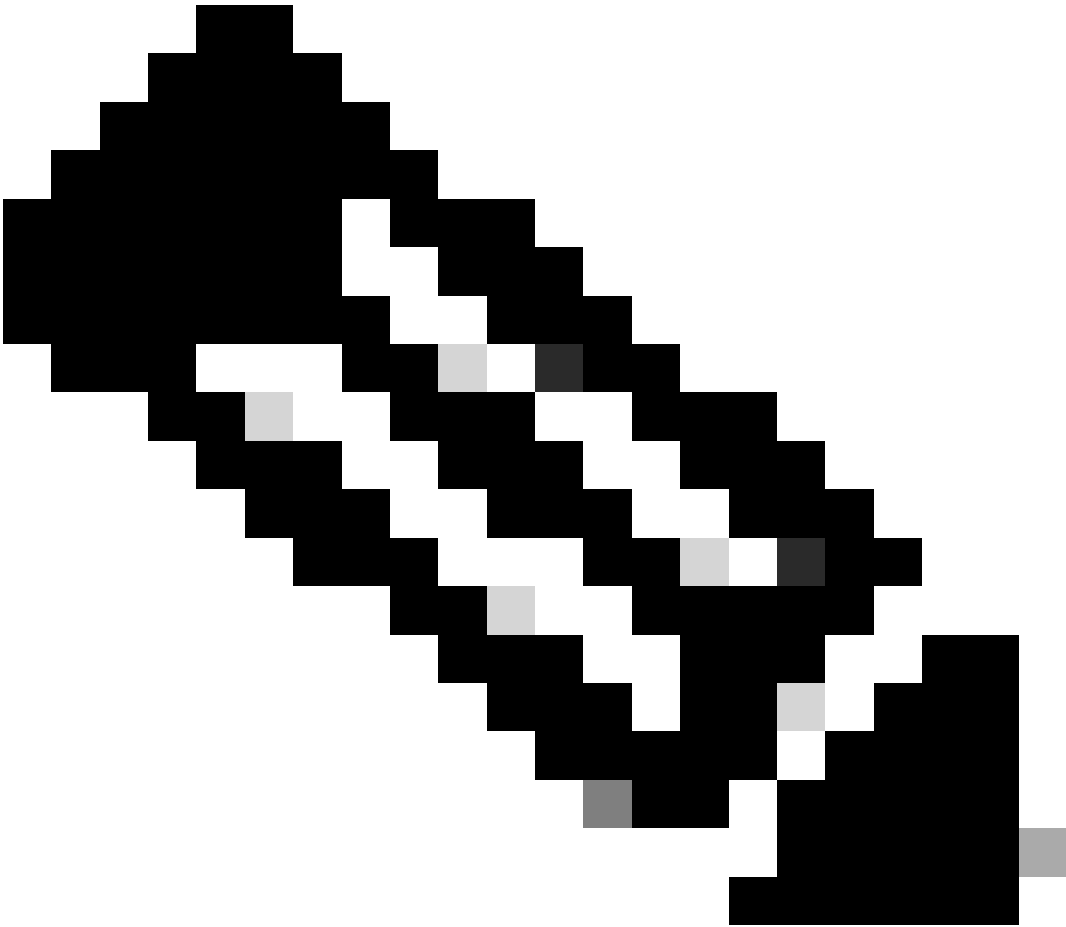
```
#monitor capture MobilityNAT start
```

Pour l'arrêter, cette commande peut être utilisée.

```
#monitor capture MobilityNAT stop
```

Une fois la capture de surveillance arrêtée, elle peut être exportée vers une source externe à l'aide d'un protocole de transfert.

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



Remarque : le tunnel de mobilité avec NAT est une fonctionnalité qui nécessite une conversation bidirectionnelle entre les WLC, en raison de la nature de la fonctionnalité, il est fortement recommandé de collecter les journaux, les débogages et les traces ou les captures de paquets des deux WLC en même temps pour mieux comprendre le tunnel de mobilité avec l'échange de paquets NAT.

Effacer les débogages, les suivis et les captures de paquets

Une fois que les informations nécessaires sont prises, les débogages, les traces et la configuration de capture de paquets intégrée peuvent être supprimés du WLC comme décrit ici.

Débogages et suivis

```
#clear platform condition all
```

Capture de paquets

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

Il est fortement recommandé d'effacer la configuration de dépannage qui a été effectuée dans le WLC une fois que les informations nécessaires ont été recueillies.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.