Configuración de topologías de movilidad en controladores de LAN inalámbrica (WLC) Catalyst 9800

Contenido

Introducción
Prerequisites
Requirements
Componentes Utilizados
Configurar
Diagrama de la red
Directrices y restricciones
Túnel de movilidad entre dos WLC Catalyst 9800
_
Paso 1. Recopile la configuración de movilidad de ambos WLC 9800.
Paso 2. Agregar configuración de peer
Túnel de movilidad entre controladores AireOS WLC y 9800-CL
Diagrama de la red
Configuración de AireOS WLC
Paso 1. Recopile información de movilidad del WLC 9800.
Paso 2. Recopile el valor de Hash del WLC 9800
Paso 3. Agregue la información del 9800 WLC al WLC de AireOS.
Configuración de 9800 WLC
Paso 1. Recopile información sobre la movilidad de AireOS.
Paso 2. Agregue la información de AireOS WLC al 9800 WLC
Verificación
Verificación de AireOS WLC
Verificación del WLC de Catalyst 9800
Troubleshoot
WLC de AireOS
WLC Catalyst 9800
Rastreo activo de radio
Captura de paquetes integrada
Escenarios comunes de Troubleshooting
Ruta de datos y control inactiva por problemas de conectividad
Discordancia de configuración entre WLC
Problemas de intercambio de señales DTLS
La situación de HA SSO
Información Relacionada

Introducción

Este documento describe escenarios de configuración de movilidad que cubren topologías entre los controladores de LAN inalámbrica (WLC) Catalyst 9800 y los WLC de AireOS.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- Acceso CLI o GUI a los controladores inalámbricos.

Componentes Utilizados

- **AireOS WLC** versión 8.10 MR1 o posterior. También puede utilizar **Inter Release Controller Mobility (IRCM)** imágenes especiales 8.5
- 9800 WLC, Cisco IOS® XE v17.3.4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

Directrices y restricciones

1. **Mobility Group** el nombre en el 9800 fuera de la caja es "predeterminado".

Nota:
1) En los casos en que los WLC estén en subredes diferentes, asegúrese de que el puerto UDP 16666 y 16667 esté abierto entre ellos.
2) Se recomienda que ambos WLC 9800 ejecuten la misma versión para que los clientes que se desplazan tengan una experiencia uniforme en los escenarios de itinerancia de capa 3 y de anclaje de invitado.

Túnel de movilidad entre dos WLC Catalyst 9800

Este ejemplo básico describe cómo configurar la movilidad entre dos controladores 9800. Esto se utiliza normalmente para el acceso de invitado (delimitador) o para permitir que los clientes se desplacen por los controladores y preserven la identidad del cliente.

Al configurar la movilidad en C9800, lo primero que debe elegir es el nombre del grupo de movilidad. El nombre del grupo de movilidad rellenado previamente es un valor predeterminado, pero se puede personalizar con el valor deseado.

Debe configurar el mismo nombre de grupo de movilidad entre los controladores cuando un grupo rápido de capa 2 se desplaza como **Fast Transition (FT)** or **Cisco Centralized Key Management (CCKM)** está en uso.

De forma predeterminada, la dirección MAC de Ethernet base del chasis, como se muestra en **show version** se refleja en la GUI de la dirección MAC de movilidad.

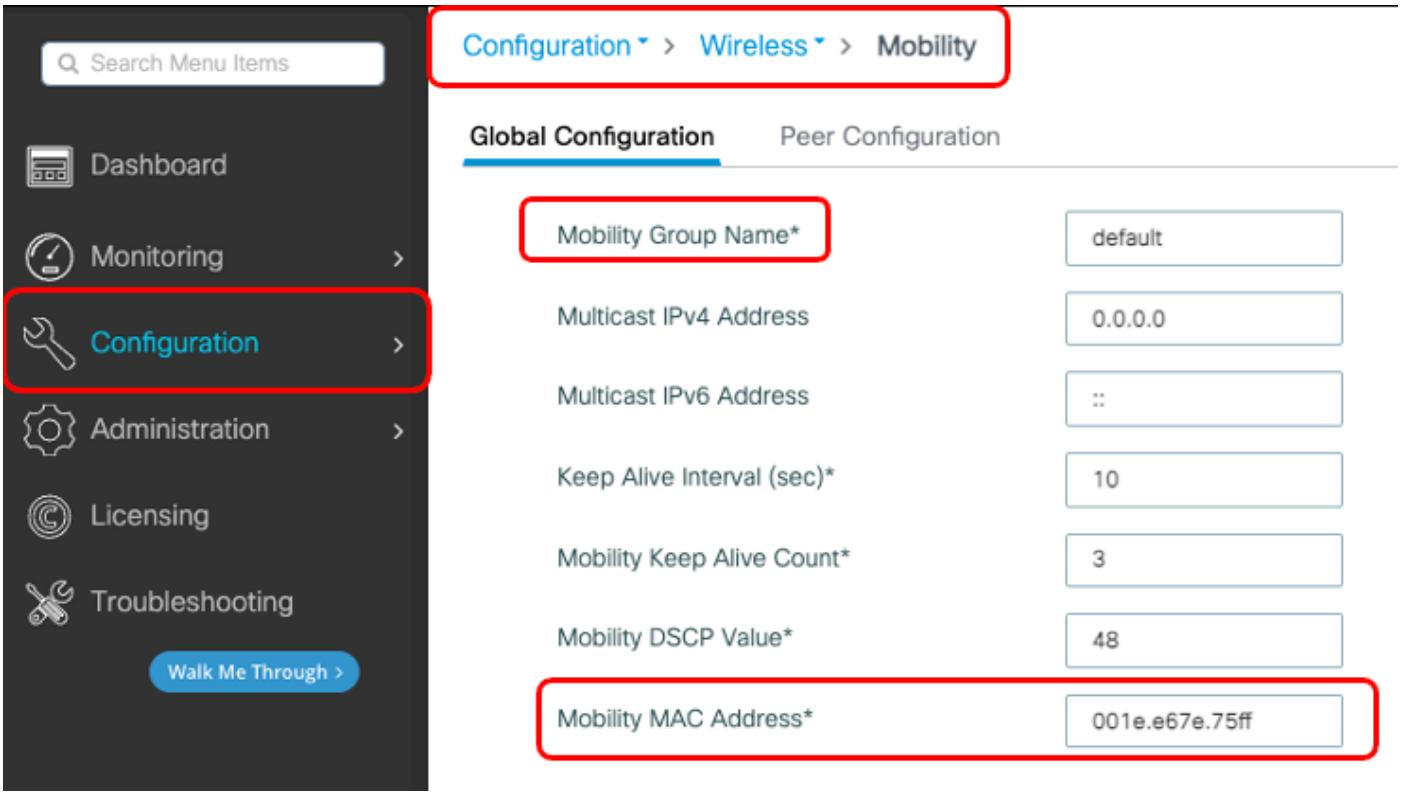
En CLI, de forma predeterminada, la mac de movilidad es 0000.0000.000, como se ve en **show run all | inc mobility mac-address**

En los casos en los que se emparejan los 9800 para **High Availability (HA) Stateful Switchover (SSO):**

Si la configuración se deja en el valor predeterminado y la dirección MAC del chasis se utiliza para formar un túnel de movilidad, el chasis activo y el túnel de movilidad fallan cuando ocurre el failover.

Por lo tanto, es obligatorio que se configure una dirección MAC de movilidad para el par C9800 HA.

Paso 1: En la interfaz gráfica de usuario, vaya a **Configuration > Wireless > Mobility > Global Configuration.**



A través de CLI:

```
# config t
# wireless mobility mac-address  <AAAA.BBBB.CCCC>
# wireless mobility group name <mobility-group-name>
```

Paso 1. Recopile la configuración de movilidad de ambos WLC 9800.

Para ambos WLC 9800, navegue hasta **Configuration > Wireless > Mobility > Global Configuration** y tomar nota de su **Mobility Group Name** y **Mobility MAC Address**.

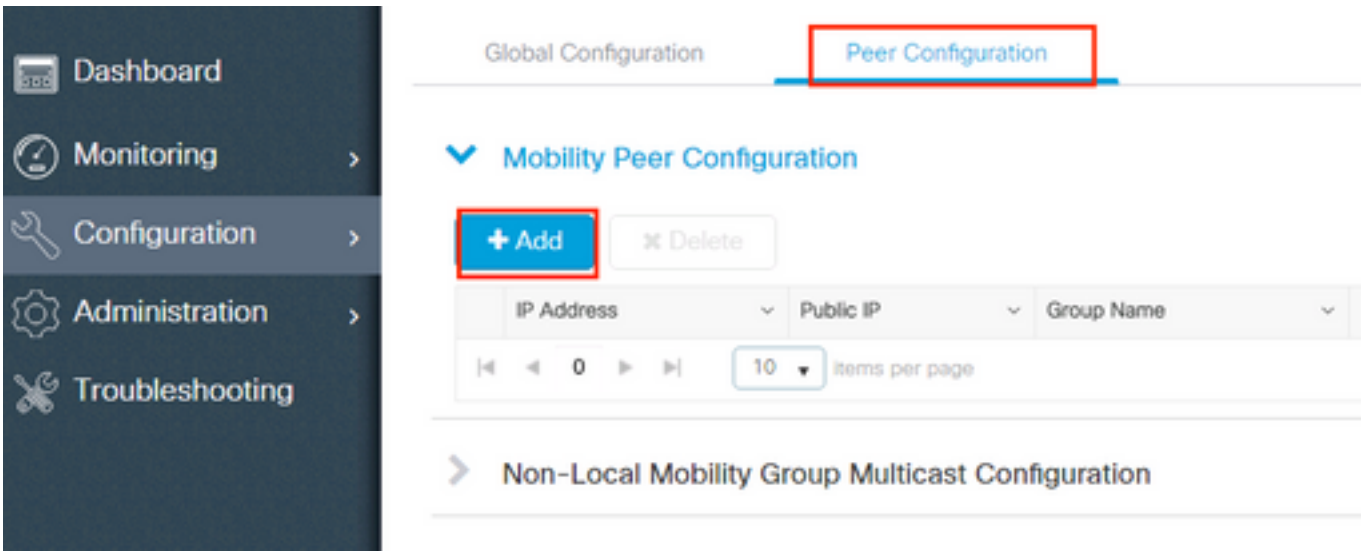
A través de CLI:

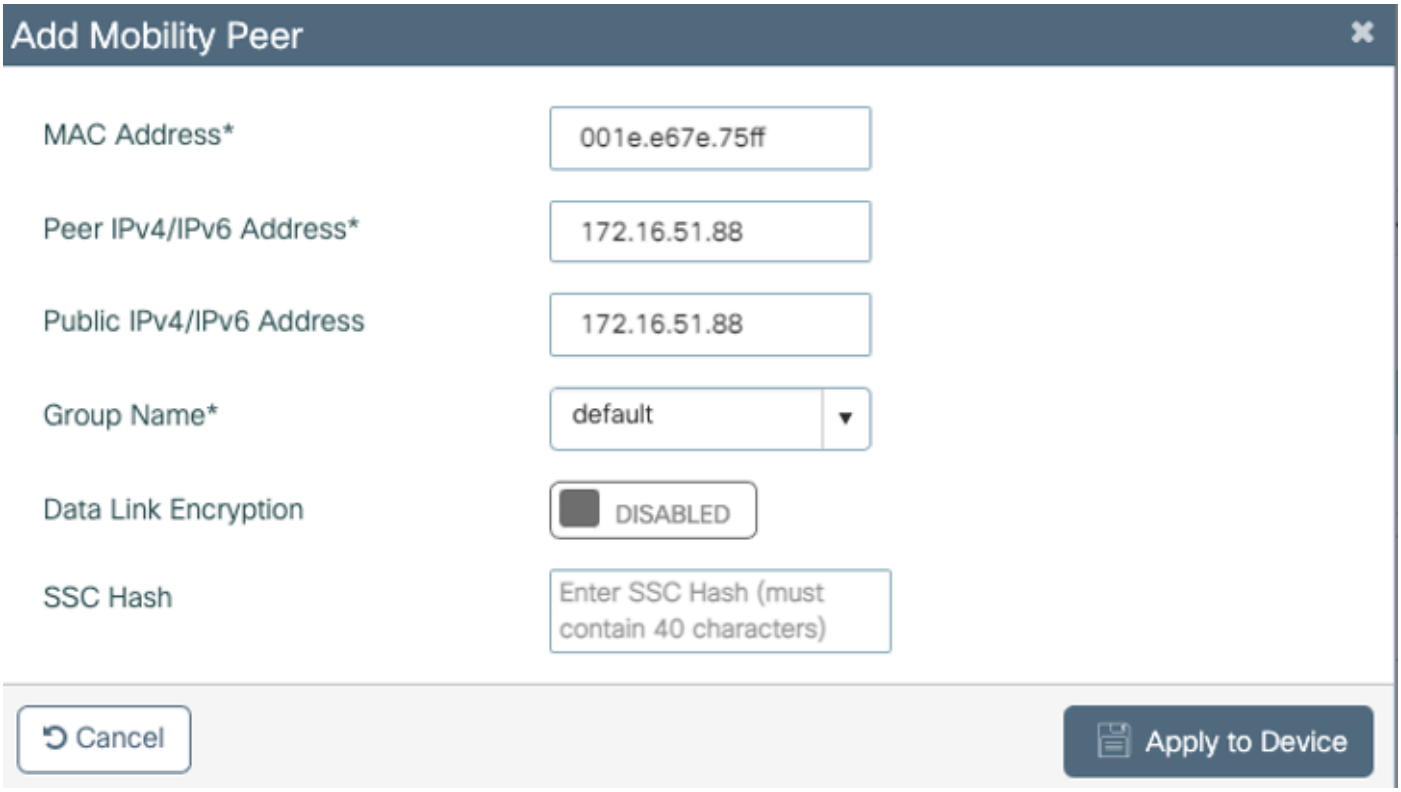
```
#show wireless mobility summary

Mobility Summary

Wireless Management VLAN: 2652
Wireless Management IP Address: 172.16.51.88
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
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: 001e.e67e.75ff
Mobility Domain Identifier: 0x34ac
```

Paso 2. Agregar configuración de peer

Desplácese hasta **Configuration > Wireless > Mobility > Peer Configuration** e introduzca la información del controlador de peer. Haga lo mismo para ambos 9800 WLC.

A través de la GUI:





A través de CLI:

```
# config t
# wireless mobility group member mac-address <peer-mac-address> ip <peer-ip-address> group
<group-name> [ data-link-encryption ]
```

Nota: Opcionalmente, puede activar el cifrado de enlace de datos.

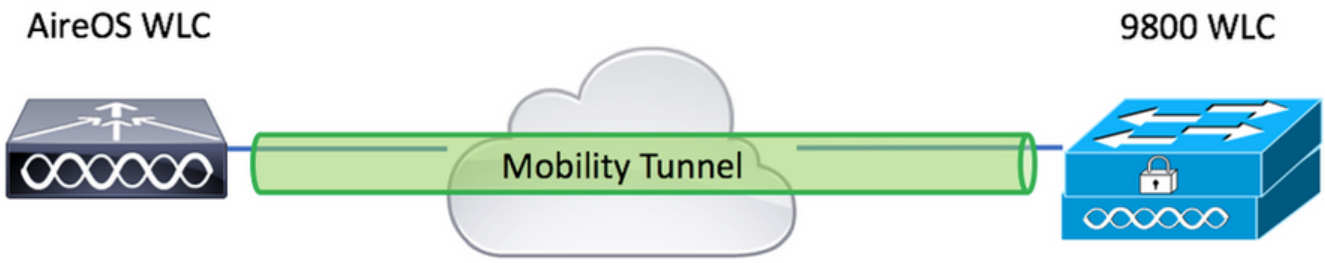
Túnel de movilidad entre controladores AireOS WLC y 9800-CL

Este escenario es normal para **brownfield** o durante la migración del controlador, donde dividimos la red en un área de puntos de acceso (AP) controlada por un controlador AireOS y otra por un 9800.

Es recomendable que los AP se distribuyan entre los controladores por áreas físicas o de RF, de modo que los clientes solamente se muevan entre los controladores cuando se muevan.

Evitar **salt and pepper** implementación. Opcionalmente, esta topología de movilidad también se podría utilizar para **guest anchor** donde 9800 actúa como externo y un AireOS como controlador de anclaje.

Diagrama de la red



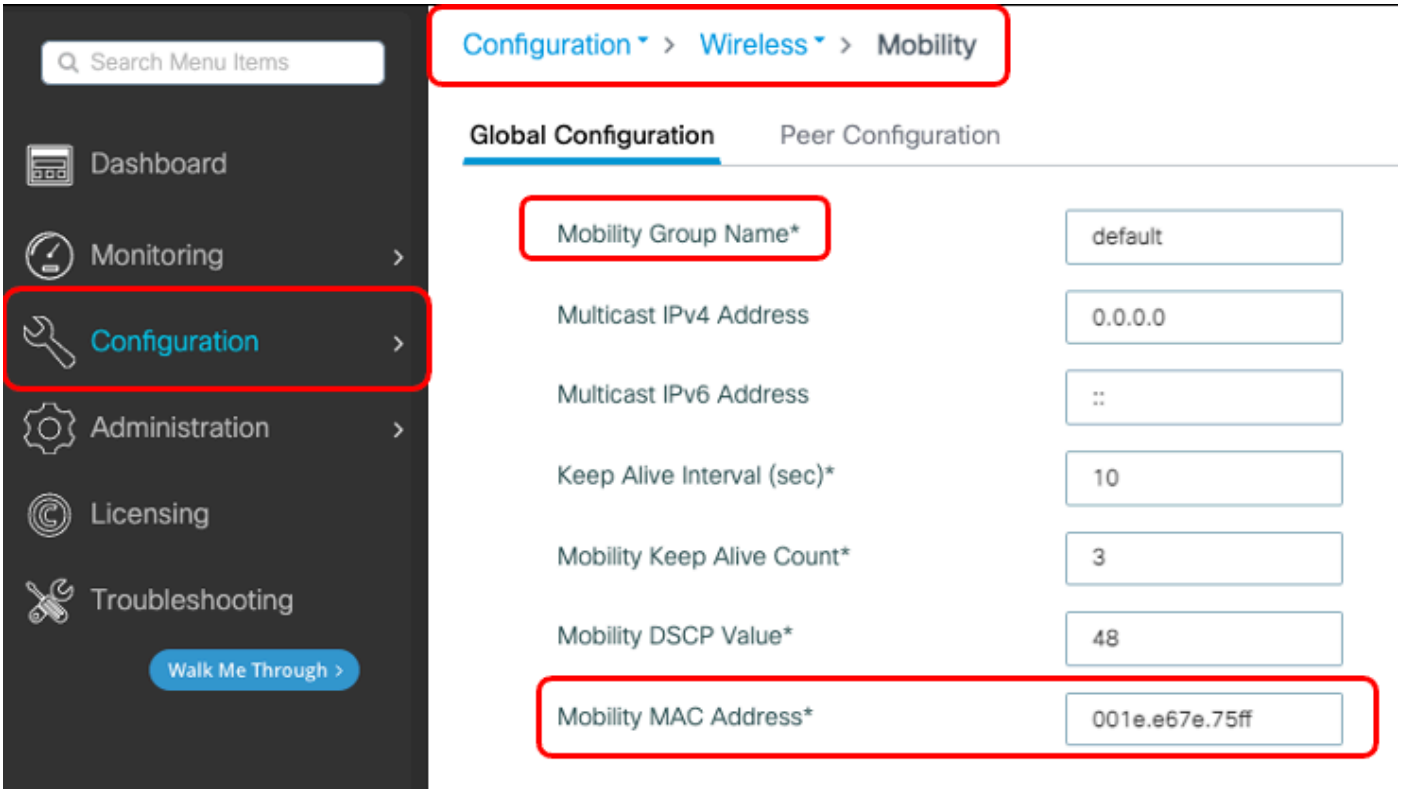
Configuración de AireOS WLC

Si los controladores 9800 están en **High Availability**, asegúrese de haber configurado la dirección MAC de movilidad.

Paso 1. Recopile información de movilidad del WLC 9800.

A través de la GUI:

Desplácese hasta **Configuration > Wireless > Mobility > Global Configuration** y tomar nota de su **Mobility Group Name** y **Mobility MAC Address**.



A través de CLI:

```
#show wireless mobility summary

Mobility Summary

Wireless Management VLAN: 2652
Wireless Management IP Address: 172.16.51.88
Wireless Management IPv6 Address:
Mobility Control Message DSCP Value: 48
```

```
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: 001e.e67e.75ff
Mobility Domain Identifier: 0x34ac
```

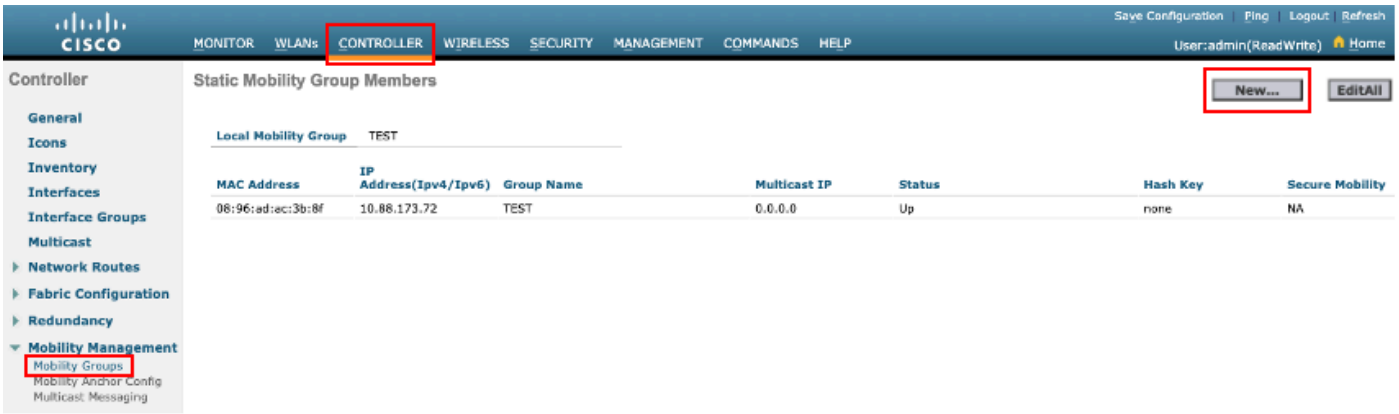
Paso 2. Recopile el valor Hash del WLC 9800

```
# show wireless management trustpoint
Trustpoint Name : Jay-9800_WLC_TP
Certificate Info : Available
Certificate Type : SSC
Certificate Hash : d7bde0898799dbfeffd4859108727d3372d3a63d
Private key Info : Available
FIPS suitability : Not Applicable
```

Paso 3. Agregue la información del 9800 WLC al WLC de AireOS.

A través de la GUI:

Desplácese hasta **CONTROLLER > Mobility Management > Mobility Groups > New.**



Introduzca los valores y haga clic en **Apply.**

> **Nota**: Hash solo se requiere en los casos en los que el 9800 utiliza un certificado autofirmado como el C9800-CL. Los dispositivos de hardware tienen un certificado SUDI y no necesitan un hash (por ejemplo, un 9800-40, 9800-L, etc.).

A través de CLI:

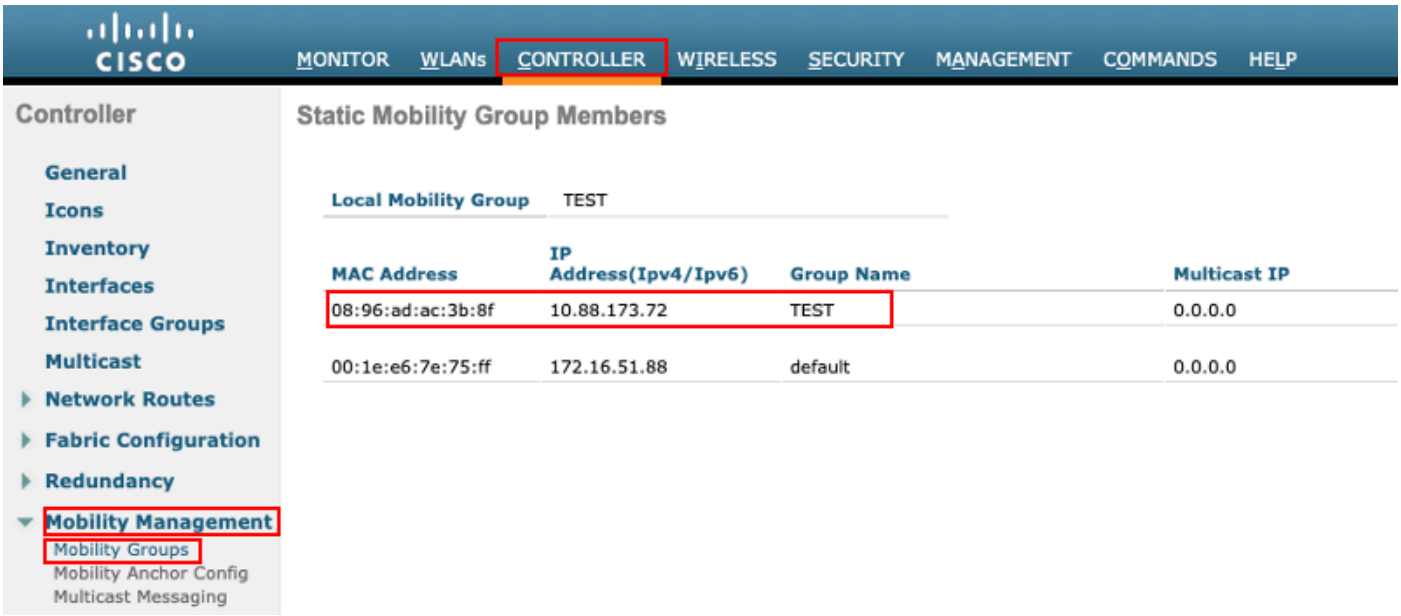
```
>config mobility group member add <9800 mac-address> <9800 WLC-IP> <group-name> encrypt enable
>config mobility group member hash <9800 WLC-IP> <9800 WLC-Hash>
>config mobility group member data-dtls <9800 mac-address> disable
```

Configuración de 9800 WLC

Paso 1. Recopile información sobre la movilidad de AireOS.

A través de la GUI:

Inicie sesión en la GUI de AireOS y navegue hasta **CONTROLLER > Mobility Management > Mobility Groups** y tome nota de la dirección MAC, la dirección IP y el nombre de grupo.



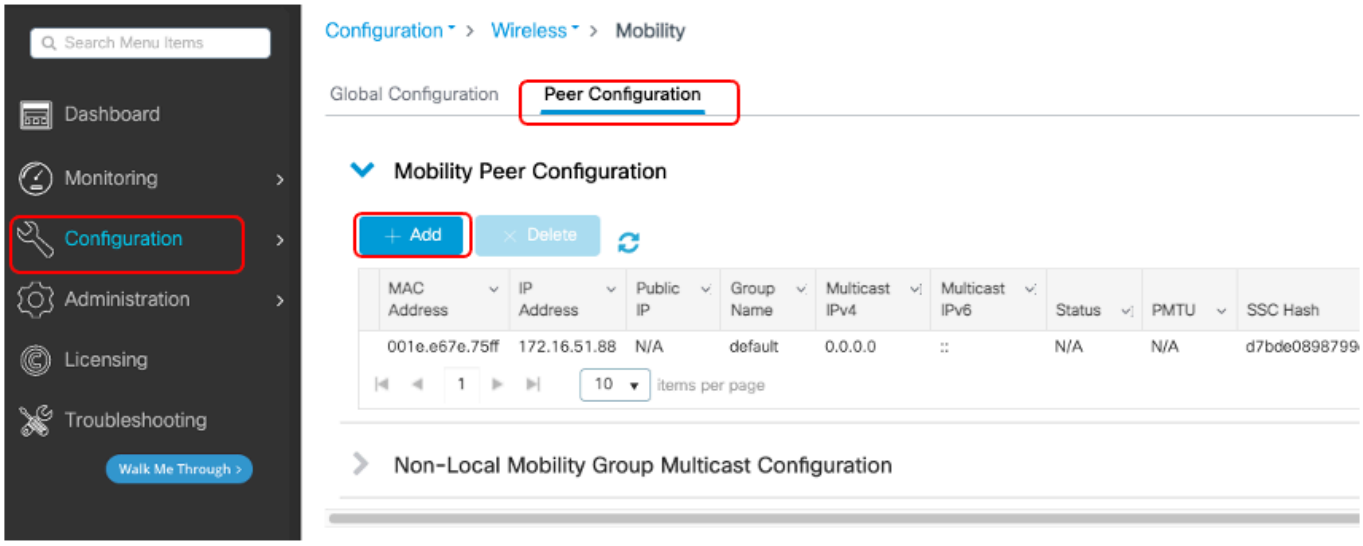
A través de CLI:

```
>show mobility summary

Mobility Protocol Port.......................... 16666
Default Mobility Domain......................... TEST
Multicast Mode ................................. Disabled
Mobility Domain ID for 802.11r.................. 0x6ef9
Mobility Keepalive Interval..................... 10
Mobility Keepalive Count........................ 3
Mobility Group Members Configured............... 2
Mobility Control Message DSCP Value............. 48

Controllers configured in the Mobility Group

 MAC Address        IP Address         Group Name                  Multicast IP
Status
08:96:ad:ac:3b:8f   10.88.173.72         TEST                        0.0.0.0
Up
```

Paso 2. Agregue la información de AireOS WLC al 9800 WLC

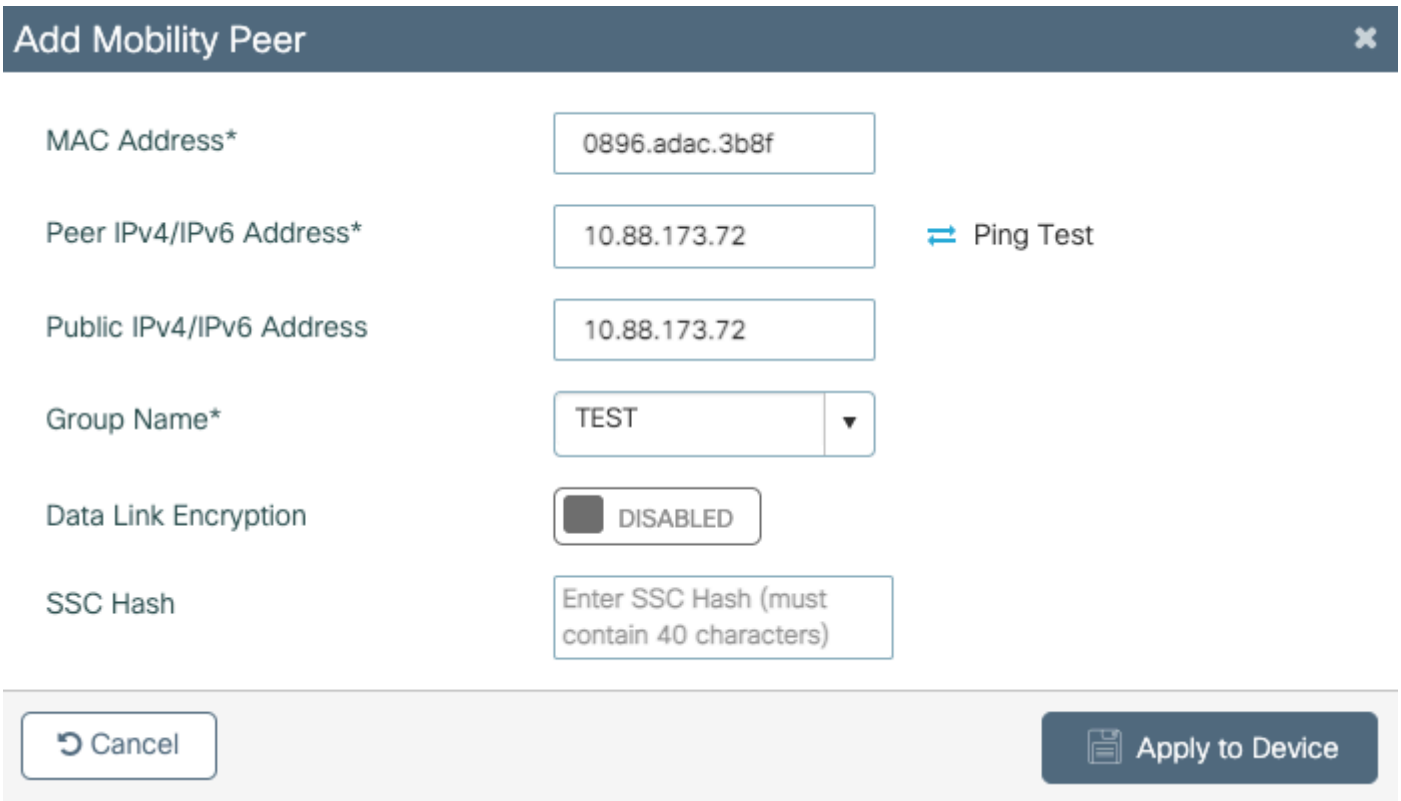
A través de la GUI:

Desplácese hasta **Configuration > Wireless > Mobility > Peer Configuration > Add**



Introduzca la información de AireOS WLC.

> **Nota**: En el WLC 9800, el cifrado del plano de control siempre está habilitado, lo que significa que debe tener la movilidad segura habilitada en el lado de AireOS. Sin embargo, el cifrado de vínculos de datos es opcional. Si lo habilita en el lado 9800, hágalo en AireOS con: **config mobility group member data-dtls enable**



A través de CLI:

```
# config t
# wireless mobility group member mac-address <peer-mac-address> ip <ip-address> group <group-name>
```

Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Verificación de AireOS WLC

```
>show mobility summary

Mobility Protocol Port.......................... 16666
Default Mobility Domain......................... TEST
Multicast Mode ................................. Disabled
Mobility Domain ID for 802.11r.................. 0x6ef9
Mobility Keepalive Interval..................... 10
Mobility Keepalive Count........................ 3
Mobility Group Members Configured............... 2
Mobility Control Message DSCP Value.............. 48

Controllers configured in the Mobility Group
 MAC Address        IP Address                                    Group Name
Multicast IP                                  Status
 00:1e:e6:7e:75:ff  172.16.51.88                                   default
0.0.0.0                                       Up
 08:96:ad:ac:3b:8f  10.88.173.72                                    TEST
0.0.0.0                                       Up
```

Verificación del WLC de Catalyst 9800

```
#show wireless mobility summary
Mobility Summary

Wireless Management VLAN: 2652
Wireless Management IP Address: 172.16.51.88
Mobility Control Message DSCP Value: 48
Mobility Keepalive Interval/Count: 10/3
Mobility Group Name: mb-kcg
Mobility Multicast Ipv4 address: 0.0.0.0
Mobility Multicast Ipv6 address: ::
Mobility MAC Address: 001e.e67e.75ff

Controllers configured in the Mobility Domain:

 IP               Public Ip         Group Name                      Multicast IPv4    Multicast
IPv6                               Status                       PMTU
-------------------------------------------------------------------------------------------------
-----------------------------------------------------------------------
172.16.51.88       N/A               default                         0.0.0.0           ::
N/A                          N/A
10.88.173.72      10.88.173.72        TEST                           0.0.0.0           ::
Up                           1385
```

Troubleshoot

Esta sección proporciona información utilizada para resolver problemas de su configuración.

Para resolver problemas de implementación del túnel de movilidad, utilice estos comandos para depurar el proceso:

WLC de AireOS

Paso 1. Habilite las depuraciones de movilidad.

```
debug mobility handoff enable
debug mobility error enable
debug mobility dtls error enable
debug mobility dtls event enable
debug mobility pmtu-discovery enable
debug mobility config enable
debug mobility directory enable
```

Paso 2. Reproduzca la configuración y verifique el resultado

Ejemplo de creación exitosa de un túnel de movilidad en un WLC de AirOS.

```
*capwapPingSocketTask: Feb 07 09:53:38.507: Client initiating connection on 172.16.0.5:16667 <->
172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.507: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.508: Received DTLS packet from mobility peer 172.16.0.21
bytes: 48
*capwapPingSocketTask: Feb 07 09:53:38.508: mm_dtls2_process_data_rcv_msg:1207 rcvBufLen 48
clr_pkt_len 2048 peer ac100015
*capwapPingSocketTask: Feb 07 09:53:38.508: Record    : type=22, epoch=0, seq=0
*capwapPingSocketTask: Feb 07 09:53:38.508:    Hndshk : type=3, len=23 seq=0, frag_off=0,
frag_len=23
*capwapPingSocketTask: Feb 07 09:53:38.508: Handshake in progress for link 172.16.0.5:16667 <->
172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.508: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.508: DTLS consumed packet from mobility peer 172.16.0.21
bytes: 48
!
!<--output-omited-->
!
*capwapPingSocketTask: Feb 07 09:53:38.511: dtls2_cert_verify_callback: Forcing Certificate
validation as success
*capwapPingSocketTask: Feb 07 09:53:38.511: Peer certificate verified.
*capwapPingSocketTask: Feb 07 09:53:38.511: Handshake in progress for link 172.16.0.5:16667 <->
172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.511: Nothing to send on link 172.16.0.5:16667 <->
172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.511: DTLS consumed packet from mobility peer 172.16.0.21
bytes: 503
*capwapPingSocketTask: Feb 07 09:53:38.511: Received DTLS packet from mobility peer 172.16.0.21
bytes: 56
*capwapPingSocketTask: Feb 07 09:53:38.511: mm_dtls2_process_data_rcv_msg:1207 rcvBufLen 56
clr_pkt_len 2048 peer ac100015
*capwapPingSocketTask: Feb 07 09:53:38.511: Record    : type=22, epoch=0, seq=6
*capwapPingSocketTask: Feb 07 09:53:38.511:    Hndshk : type=13, len=6 seq=3, frag_off=0,
frag_len=6
*capwapPingSocketTask: Feb 07 09:53:38.523: Handshake in progress for link 172.16.0.5:16667 <->
172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.523: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.524: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.524: Sending packet to 172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.524: DTLS consumed packet from mobility peer 172.16.0.21
bytes: 56
*capwapPingSocketTask: Feb 07 09:53:38.527: Received DTLS packet from mobility peer 172.16.0.21
```

```
bytes: 91
*capwapPingSocketTask: Feb 07 09:53:38.527: mm_dtls2_process_data_rcv_msg:1207 rcvBufLen 91
clr_pkt_len 2048 peer ac100015
*capwapPingSocketTask: Feb 07 09:53:38.527: Record    : type=20, epoch=0, seq=8
*capwapPingSocketTask: Feb 07 09:53:38.527: Connection established for link 172.16.0.5:16667 <->
172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.527: ciperspec 1
*capwapPingSocketTask: Feb 07 09:53:38.527: Nothing to send on link 172.16.0.5:16667 <->
172.16.0.21:16667
*capwapPingSocketTask: Feb 07 09:53:38.527: DTLS consumed packet from mobility peer 172.16.0.21
bytes: 91
*mmMobility: Feb 07 09:53:38.527: DTLS Action Result message received
*mmMobility: Feb 07 09:53:38.527:  Key plumb succeeded
*mmMobility: Feb 07 09:53:38.527: mm_dtls2_callback: Connection established with
172.16.0.21:16667
*mmMobility: Feb 07 09:53:38.527: mm_dtls2_db_status_up:895 Connections status up for entry
172.16.0.21:16667
*mmMobility: Feb 07 09:53:38.527: mm_dtls2_callback: DTLS Connection established with
172.16.0.21:16667, Sending update msg to mobility HB
```

WLC Catalyst 9800

De forma predeterminada, los controladores 9800 registran continuamente la información del proceso sin necesidad de ningún procedimiento de depuración especial.

Sólo tiene que conectarse al controlador y recuperar los registros asociados a cualquier componente inalámbrico para solucionar los problemas.

Los registros pueden durar días; eso depende de cuán ocupado esté el controlador.

Para simplificar el análisis, extraiga los registros con un rango de tiempo o para el último número de minutos (el tiempo predeterminado está configurado en 10 minutos) y puede filtrar por direcciones IP o MAC.

Paso 1. Verifique la hora actual en el controlador para que pueda rastrear los registros en el tiempo hasta cuando ocurrió el problema.

```
# show clock
```

Paso 2. Recopile los registros del controlador, en caso de que haya alguna información a nivel del IOS de Cisco que pueda estar relacionada con el problema.

```
# show logging
```

Paso 3. Recopile los seguimientos del nivel de aviso siempre activo para una dirección específica. Puede utilizar la IP o MAC del par de movilidad para filtrar.

```
# show logging profile wireless filter ipv4 to-file bootflash:ra-AAAA.BBBB.CCCC.txt
```

Este comando genera registros de los últimos 10 minutos, es posible ajustar este tiempo con el comando **show logging profile wireless last 1 hour filter mac AAAA.BBBB.CCCC to-file bootflash:ra-AAAA.BBBB.CCCC.txt**.

Puede mostrar el contenido en la sesión o copiar el archivo en un servidor TFTP externo.

```
# more bootflash:always-on-<FILENAME.txt>

or

# copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>
```

Rastreo activo de radio

Si los registros siempre activos no proporcionan suficiente información para saber qué problemas desencadenados durante la configuración del túnel, puede habilitar las depuraciones condicionales y capturar **Radio Active (RA)** , que proporcionan una actividad de proceso más detallada.

Paso 1. Verifique que no haya condiciones de depuración ya habilitadas.

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop


IOSXE Packet Tracing Configs:



Packet Infra debugs:

Ip Address                                              Port
------------------------------------------------------|----------
```

Si ve alguna condición que no esté relacionada con la dirección que desea supervisar, inhabilítela.

Para eliminar una dirección específica:

```
# no debug platform condition feature wireless { mac <aaaa.bbbb.cccc> | ip <a.b.c.d> }
```

Para eliminar todas las condiciones (forma recomendada):

```
# clear platform condition all
```

Paso 2. Agregue la condición de depuración para una dirección que desee supervisar.

```
# debug platform condition feature wireless ip <a.b.c.d>
```

> **Nota**: Si desea supervisar más de un par de movilidad al mismo tiempo, utilice un **debug platform condition feature wireless mac** por dirección MAC.

Paso 3. Haga que el 9800 WLC comience a monitorear la actividad de dirección especificada.

```
# debug platform condition start
```

Nota: La salida de la actividad de movilidad no se muestra, ya que todo se almacena en el búfer interno para su recopilación posterior.

Paso 4. Reproduzca el problema o el comportamiento que desea supervisar.

Paso 5. Detenga las depuraciones.

```
# debug platform condition stop
```

Paso 6. Recopile el resultado de la actividad de dirección.

```
# show logging profile wireless filter ipv4 to-file bootflash:ra-AAAA.BBBB.CCCC.txt
```

Este comando genera registros de los últimos 10 minutos. Es posible ajustar este tiempo con el comando **show logging profile wireless last 1 hour filter mac AAAA.BBBB.CCCC to-file bootflash:ra-AAAA.BBBB.CCCC.txt**.

Puede copiar el archivo **FILENAME.txt** a un servidor externo o muestre el resultado directamente en la pantalla.

Copie el archivo en un servidor externo:

```
# copy bootflash:FILENAME.txt tftp://a.b.c.d/ra-FILENAME.txt
```

Muestre el contenido:

```
# more bootflash:ra-FILENAME.txt
```

Paso 7. Si sigue sin poder encontrar el motivo de un error, recopile el nivel interno de registros.

(No es necesario depurar el cliente de nuevo. Utilice los registros que ya estaban almacenados internamente, pero recopile una gama más amplia de ellos).

```
# show logging profile wireless internal filter ipv4 to-file bootflash:raInternal-
AAAA.BBBB.CCCC.txt
```

Puede copiar el archivo **FILENAME.txt** a un servidor externo o muestre el resultado directamente en la pantalla.

Copie el archivo en un servidor externo:

```
# copy bootflash:FILENAME.txt tftp://a.b.c.d/ra-FILENAME.txt
```

Muestre el contenido:

```
# more bootflash:ra-FILENAME.txt
```

Paso 8. Elimine las condiciones de depuración.

```
# clear platform condition all
```

> **Nota**: Elimine siempre las condiciones de depuración después de una sesión de solución de problemas.

Ejemplo de creación exitosa de un túnel de movilidad en un WLC 9800.

```
2021/09/28 10:20:50.497612 {mobilityd_R0-0}{1}: [errmsg] [26516]: (info): %MM_NODE_LOG-6-
MEMBER_ADDED: Adding Mobility member (IP: IP: 172.16.55.28: default)
2021/09/28 10:20:52.595483 {mobilityd_R0-0}{1}: [mm-client] [26516]: (debug): MAC:
0000.0000.0000 Sending keepalive_data of XID (0) to (ipv4: 172.16.55.28 )
2021/09/28 10:20:52.595610 {mobilityd_R0-0}{1}: [mm-pmtu] [26516]: (debug): Peer IP:
172.16.55.28 PMTU size is 1385 and calculated additional header length is 148
2021/09/28 10:20:52.595628 {mobilityd_R0-0}{1}: [mm-client] [26516]: (debug): MAC:
0000.0000.0000 Sending keepalive_ctrl_req of XID (80578) to (ipv4: 172.16.55.28 )
2021/09/28 10:20:52.595686 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 keepalive data packet misssed, total missed packet = 1
2021/09/28 10:20:52.595694 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 keepalive ctrl packet misssed, total missed packet = 1
2021/09/28 10:21:02.596500 {mobilityd_R0-0}{1}: [mm-client] [26516]: (debug): MAC:
0000.0000.0000 Sending keepalive_data of XID (0) to (ipv4: 172.16.55.28 )
2021/09/28 10:21:02.596598 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 keepalive data packet misssed, total missed packet = 2
2021/09/28 10:21:02.598898 {mobilityd_R0-0}{1}: [mm-client] [26516]: (debug): MAC:
001e.e68c.5dff Received keepalive_data, sub type: 0 of XID (0) from (ipv4: 172.16.55.28 )
2021/09/28 10:21:12.597912 {mobilityd_R0-0}{1}: [mm-client] [26516]: (debug): MAC:
0000.0000.0000 Sending keepalive_data of XID (0) to (ipv4: 172.16.55.28 )
2021/09/28 10:21:12.598009 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 Data link set state to UP (was DOWN)
2021/09/28 10:21:12.598361 {mobilityd_R0-0}{1}: [errmsg] [26516]: (note): %MM_NODE_LOG-5-
KEEP_ALIVE: Mobility Data tunnel to peer IP: 172.16.55.28 changed state to UP

! !<--output-omited--> !

2021/09/28 10:21:22.604098 {mobilityd_R0-0}{1}: [ewlc-infra-evq] [26516]: (debug): DTLS record
type: 22, handshake
2021/09/28 10:21:22.604099 {mobilityd_R0-0}{1}: [ewlc-infra-evq] [26516]: (info): DTLS client
hello
2021/09/28 10:21:22.611477 {mobilityd_R0-0}{1}: [ewlc-infra-evq] [26516]: (debug): DTLS record
type: 22, handshake
2021/09/28 10:21:22.611555 {mobilityd_R0-0}{1}: [ewlc-infra-evq] [26516]: (debug): DTLS record
type: 22, handshake
2021/09/28 10:21:22.611608 {mobilityd_R0-0}{1}: [ewlc-infra-evq] [26516]: (debug): DTLS record
type: 22, handshake
2021/09/28 10:21:22.611679 {mobilityd_R0-0}{1}: [ewlc-infra-evq] [26516]: (debug): DTLS record
type: 22, handshake
2021/09/28 10:21:22.611933 {mobilityd_R0-0}{1}: [mm-dtls] [26516]: (note): Peer IP: 172.16.55.28
Port: 16666, Local IP: 172.16.51.88 Port: 16666 DTLS_SSC_HASH_VERIFY_CB: SSC hash validation
success
2021/09/28 10:21:22.612163 {mobilityd_R0-0}{1}: [ewlc-dtls-sessmgr] [26516]: (info): Remote
Host: 172.16.55.28[16666] Completed cert verification, status:CERT_VALIDATE_SUCCESS

! !<--output-omited--> !

2021/09/28 10:21:52.603200 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 Control link set state to UP (was DOWN)
2021/09/28 10:21:52.604109 {mobilityd_R0-0}{1}: [errmsg] [26516]: (note): %MM_NODE_LOG-5-
KEEP_ALIVE: Mobility Control tunnel to peer IP: 172.16.55.28 changed state to UP
```

Captura de paquetes integrada

La mayoría de las veces, es muy útil para verificar los paquetes intercambiados entre los WLC. Resulta especialmente útil para filtrar capturas con **Access Control Lists (ACLs)** para limitar el tráfico capturado.

Esta es una plantilla de configuración para capturas incrustadas en CLI.

Paso 1. Cree la ACL de filtro:

```
conf t
ip access-list extended <ACL_NAME>
10 permit ip host <WLC_IP_ADDR> host <PEER_WLC_IP_ADDR>
20 permit ip host <PEER_WLC_IP_ADDR>host <WLC_IP_ADDR>
end
```

Paso 2. Defina los parámetros de captura:

```
monitor capture <CAPTURE_NAME> access-list <ACL_NAME> buffer size 10 control-plane both
interface <INTERFACE_NAME> both limit duration 300
```

> **Nota**: Seleccione la interfaz de gestión para el parámetro INTERFACE_NAME

Paso 3. Inicie la captura:

```
monitor capture <CAPTURE_NAME> start
```

Paso 4. Detener la captura:

```
monitor capture <CAPTURE_NAME> stop
```

Paso 5. Vaya a **Troubleshooting > Packet Capture** en la GUI para recopilar el archivo de captura de paquetes.

Escenarios comunes de Troubleshooting

Los siguientes ejemplos consisten en túneles formados entre 9800 WLCs.

Ruta de datos y control inactiva por problemas de conectividad

Habilitar **Always-On-Logs** y **Embedded packet captures** para proporcionar información adicional para solucionar problemas:

```
2021/09/28 09:54:22.490625 {mobilityd_R0-0}{1}: [mm-client] [26516]: (debug): MAC:
0000.0000.0000 Sending keepalive_ctrl_req of XID (80552) to (ipv4: 172.16.55.28 )
2021/09/28 09:54:22.490652 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 keepalive data packet misssed, total missed packet = 29
2021/09/28 09:54:22.490657 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 keepalive ctrl packet misssed, total missed packet = 10
2021/09/28 09:54:32.491952 {mobilityd_R0-0}{1}: [mm-client] [26516]: (debug): MAC:
0000.0000.0000 Sending keepalive_data of XID (0) to (ipv4: 172.16.55.28 )
```

```
2021/09/28 09:54:32.492127 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 keepalive data packet misssed, total missed packet = 30
```

Las capturas de paquetes son útiles para confirmar el comportamiento.

```
 90 2021-09-28 12:33:52.924939 172.16.51.88    172.16.55.28    116 Mobi-Control - PingReq[Malformed Packet]
 91 2021-09-28 12:34:02.925946 172.16.51.88    172.16.55.28    172 Mobi-Data Keep-Alive - Mobility CAPWAP Ping Request
 92 2021-09-28 12:34:12.925946 172.16.51.88    172.16.55.28    172 Mobi-Data Keep-Alive - Mobility CAPWAP Ping Request
 93 2021-09-28 12:34:22.927945 172.16.51.88    172.16.55.28    172 Mobi-Data Keep-Alive - Mobility CAPWAP Ping Request
 94 2021-09-28 12:34:22.927945 172.16.51.88    172.16.55.28    116 Mobi-Control - PingReq[Malformed Packet]
 95 2021-09-28 12:34:32.927945 172.16.51.88    172.16.55.28    172 Mobi-Data Keep-Alive - Mobility CAPWAP Ping Request
 96 2021-09-28 12:34:42.929944 172.16.51.88    172.16.55.28    172 Mobi-Data Keep-Alive - Mobility CAPWAP Ping Request
 97 2021-09-28 12:34:52.930951 172.16.51.88    172.16.55.28    172 Mobi-Data Keep-Alive - Mobility CAPWAP Ping Request
```

Observe que tanto debug como WLC muestran que no hay respuesta a los pings de datos o control. Un escenario común muestra que la conectividad IP está permitida, pero los puertos 16666 o 16667 no están permitidos para comunicarse a través de la red.

Discordancia de configuración entre WLC

En este caso, confirmamos la conectividad para todos los puertos entre los WLC, pero seguimos notando que los keepalives fallan.

Habilitar **Always-On-Logs** y **Embedded packet captures** para proporcionar información adicional para solucionar problemas:

```
2021/09/28 11:34:22.927477 {mobilityd_R0-0}{1}: [mm-client] [26516]: (debug): MAC:
0000.0000.0000 Sending keepalive_data of XID (0) to (ipv4: 172.16.55.28 )
2021/09/28 11:34:22.928025 {mobilityd_R0-0}{1}: [mm-pmtu] [26516]: (debug): Peer IP:
172.16.55.28 PMTU size is 1385 and calculated additional header length is 148
2021/09/28 11:34:22.928043 {mobilityd_R0-0}{1}: [mm-client] [26516]: (debug): MAC:
0000.0000.0000 Sending keepalive_ctrl_req of XID (80704) to (ipv4: 172.16.55.28 )
2021/09/28 11:34:22.928077 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 keepalive data packet misssed, total missed packet = 8
2021/09/28 11:34:22.928083 {mobilityd_R0-0}{1}: [mm-keepalive] [26516]: (note): Peer IP:
172.16.55.28 keepalive ctrl packet misssed, total missed packet = 3
```

Los registros internos en el par 172.16.55.28 nos ayudan a confirmar la discordancia de la configuración

```
2021/09/28 17:33:22.963 {mobilityd_R0-0}{1}: [mm-keepalive] [27081]: (ERR): Peer IP:
172.16.51.88 Failed to validate endpoint: Invalid argument
2021/09/28 17:33:22.963 {mobilityd_R0-0}{1}: [errmsg] [27081]: (ERR): %MM_NODE_LOG-3-
PING_DROPPED: Drop data ping from IP: 172.16.51.88. Failed to validate endpoint
```

La discrepancia de configuración común incluye: nombre de grupo incorrecto, discrepancia en **Data Link Encryption** y la dirección MAC de movilidad incorrecta.

Registro de discordancia de grupo:

```
2021/09/28 17:33:22.963 {mobilityd_R0-0}{1}: [errmsg] [27081]: (ERR): %MM_INFRA_LOG-3-
MSG_PROC_FAILED_GROUP_NAME_HASH: Pkt group name hash: 82FE070E6E9A37A543CEBED96DB0388F Peer
group name hash: 3018E2A00F10176849AC824E0190AC86 Failed to validate endpoint. reason: Group
name hash mismatch.
```

Registro de discordancia de direcciones MAC:

```
2021/09/28 19:09:33.455 {mobilityd_R0-0}{1}: [errmsg] [27081]: (ERR): %MM_INFRA_LOG-3-
```

```
MSG_PROC_FAILED_MAC_ADDR: Pkt MAC: 001e.e67e.75fa Peer MAC: 001e.e67e.75ff Failed to validate endpoint. reason: MAC address mismatch.
```

Problemas de intercambio de señales DTLS

Este tipo de problema está relacionado con los establecimientos de túnel DTLS entre los WLC. Podría ser el caso de que la trayectoria de datos esté ACTIVA pero la trayectoria de control permanezca **DOWN**.

Habilitar **Always-On-Logs** y **Embedded packet captures** para proporcionar información adicional para solucionar problemas:

```
2021/09/28 19:30:23.534 {mobilityd_R0-0}{1}: [mm-msg] [27081]: (ERR): Peer IP: 172.16.51.88 Port: 16666 DTLS_MSG: DTLS message process failed. Error: Invalid argument
2021/09/28 19:30:23.534 {mobilityd_R0-0}{1}: [errmsg] [27081]: (warn): %MM_NODE_LOG-4-DTLS_HANDSHAKE_FAIL: Mobility DTLS Ctrl handshake failed for 172.16.51.88 HB is down, need to re-initiate DTLS handshake
2021/09/28 19:30:23.534 {mobilityd_R0-0}{1}: [ewlc-capwapmsg-sess] [27081]: (ERR): Source IP:172.16.51.88[16666], DTLS message process failed. length:52
```

Uso **show wireless management trustpoint** y **show crypto pki trustpoints commands** para comprobar la información del certificado.

La situación de HA SSO

Si tiene controladores en un par SSO de alta disponibilidad, hay un problema importante que debe conocer. La dirección MAC de movilidad no está configurada de forma predeterminada y puede provocar que el túnel de movilidad se desactive si se produce una conmutación por fallo.

El **resumen show wireless mobility** le brinda el MAC de movilidad actual en uso, pero no necesariamente está configurado. Verifique si la configuración tiene el MAC de movilidad configurado con **show run | i movilidad**

Si el mac de la movilidad no se configura en la configuración en ejecución, cambia al failover al WLC standby y esto hace que los túneles de la movilidad fallen.

La solución sencilla consiste en navegar hasta la página **Configuration > Wireless > Mobility** Web UI (Configuración > Inalámbrico > Movilidad)y pulsar **apply** (**Aplicar**). Esto guarda la MAC de movilidad actual en la configuración. El MAC permanece igual después de la conmutación por fallas y se conservan los túneles de movilidad.

Este problema ocurre principalmente si realiza la configuración de movilidad a través de la línea de comandos y olvida configurar la dirección MAC de movilidad. La interfaz de usuario web guarda automáticamente una dirección MAC de movilidad cuando se aplican los parámetros.

Información Relacionada

- Configuración de la función de movilidad de anclaje WLAN en Catalyst 9800
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).