

# Configurar Topologias de Mobilidade em Catalyst 9800 Wireless LAN Controllers (WLCs)

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Diretrizes e restrições](#)

[Túnel de mobilidade entre dois Catalyst 9800 WLCs](#)

–

[Etapa 1. Colete a configuração de mobilidade de ambas as 9800 WLCs.](#)

[Etapa 2. Adicionar configuração de peer](#)

[Túnel de mobilidade entre controladores AireOS WLC e 9800-CL](#)

[Diagrama de Rede](#)

[Configuração do AireOS WLC](#)

[Etapa 1. Colete informações de mobilidade da WLC 9800.](#)

[Etapa 2. Colete o valor de hash do WLC 9800](#)

[Etapa 3. Adicione as informações da WLC 9800 na WLC AireOS.](#)

[Configuração da WLC 9800](#)

[Etapa 1. Colete informações de mobilidade do AireOS.](#)

[Etapa 2. Adicione as informações do AireOS WLC ao 9800 WLC](#)

[Verificar](#)

[Verificação de WLC AireOS](#)

[Verificação da WLC Catalyst 9800](#)

[Troubleshoot](#)

[WLC AireOS](#)

[WLC Catalyst 9800](#)

[Rastreamento ativo por rádio](#)

[Captura de pacotes incorporada](#)

[Cenários comuns de solução de problemas](#)

[Controle e caminho de dados inativos devido a problemas de conectividade](#)

[Incompatibilidade de configuração entre WLCs](#)

[Problemas de handshake DTLS](#)

[O cenário de HA SSO](#)

[Informações Relacionadas](#)

## Introduction

Este documento descreve os cenários de configuração de mobilidade que cobrem as topologias

entre as controladoras Wireless LAN (WLCs) Catalyst 9800 e as WLCs AireOS.

## Prerequisites

### Requirements

A Cisco recomenda o conhecimento destes tópicos:

- Acesso via CLI ou GUI aos controladores sem fio.

### Componentes Utilizados

- AireOS WLC versão 8.10 MR1 ou posterior. Você também pode usar Inter Release Controller Mobility (IRCM) imagens 8.5 especiais
- WLC 9800, Cisco IOS<sup>®</sup> XE v17.3.4

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

### Diagrama de Rede



### Diretrizes e restrições

1. **Mobility Group** no 9800 fora da caixa é "default".

**Note:**

- 1) Nos casos em que as WLCs estão em sub-redes diferentes, certifique-se de que a porta UDP 16666 e 16667 esteja aberta entre elas.
- 2) Recomenda-se que ambas as 9800 WLCs executem a mesma versão para que os clientes que se movem tenham uma experiência consistente nos cenários de roaming de Camada 3 e âncora de convidado.

### Túnel de mobilidade entre dois Catalyst 9800 WLCs

Este exemplo básico descreve como configurar a mobilidade em dois controladores 9800.

Geralmente, é usado para acesso de convidado (âncora) ou para permitir que os clientes naveguem pelos controladores e preservem a identidade do cliente.

Quando você configura a mobilidade no C9800, a primeira coisa a escolher é o nome do grupo de mobilidade. O nome do grupo de mobilidade pré-preenchido é um padrão, mas você pode personalizá-lo para um valor desejado.

Você deve configurar o mesmo nome de grupo de mobilidade nos controladores quando uma camada 2 rápida se movimenta como **Fast Transition (FT)** Or **Cisco Centralized Key Management (CCKM)** está em uso.

Por padrão, o endereço MAC Ethernet base do chassi conforme visto na `show version` é refletido na GUI para endereço MAC de mobilidade.

Na CLI, por padrão, o mac de mobilidade é 0000.0000.000 como visto na `show run all | inc mobility mac-address`

Nos casos em que os 9800s estão emparelhados para **High Availability (HA) Stateful Switchover (SSO)**:

Se a configuração for deixada como padrão e o endereço MAC do chassi for usado para formar o túnel de mobilidade, o chassi ativo e o túnel de mobilidade falharão quando ocorrer failover.

Portanto, é obrigatório que um endereço MAC de mobilidade seja configurado para o par HA C9800.

Etapa 1: na GUI, navegue até **Configuration > Wireless > Mobility > Global Configuration**.

The screenshot shows the Cisco GUI configuration page for Mobility. The breadcrumb navigation at the top is **Configuration > Wireless > Mobility**. The left sidebar has **Configuration** highlighted. The main content area shows the **Global Configuration** tab with the following fields:

Field	Value
Mobility Group Name*	default
Multicast IPv4 Address	0.0.0.0
Multicast IPv6 Address	::
Keep Alive Interval (sec)*	10
Mobility Keep Alive Count*	3
Mobility DSCP Value*	48
Mobility MAC Address*	001e.e67e.75ff

Através do CLI:

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

```
# wireless mobility group name <mobility-group-name>
```

## Etapa 1. Colete a configuração de mobilidade de ambas as 9800 WLCs.

Para as WLCs 9800, navegue até **Configuration > Wireless > Mobility > Global Configuration** e tome nota da **SUA Mobility Group Name** e **Mobility MAC Address**.

Através do 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
```

## Etapa 2. Adicionar configuração de peer

Navegue até **Configuration > Wireless > Mobility > Peer Configuration** e insira as informações do controlador par. Faça o mesmo para as duas 9800 WLCs.

Através da GUI:

The screenshot displays the Cisco GUI interface for configuring mobility peers. On the left, a dark sidebar contains navigation icons and labels: Dashboard, Monitoring, Configuration, Administration, and Troubleshooting. The main content area shows two tabs: 'Global Configuration' and 'Peer Configuration', with the latter selected and highlighted by a red box. Below the tabs, the 'Mobility Peer Configuration' section is active. It includes a blue '+ Add' button and a grey 'Delete' button, both highlighted with red boxes. Underneath these buttons is a table with three columns: 'IP Address', 'Public IP', and 'Group Name'. The table currently shows 0 items. Below the table, there is a pagination control showing '10 items per page'. At the bottom of the page, there is a section for 'Non-Local Mobility Group Multicast Configuration'.

### Add Mobility Peer ✕

MAC Address*	<input type="text" value="001e.e67e.75ff"/>
Peer IPv4/IPv6 Address*	<input type="text" value="172.16.51.88"/>
Public IPv4/IPv6 Address	<input type="text" value="172.16.51.88"/>
Group Name*	<input type="text" value="default"/> ▼
Data Link Encryption	<input type="checkbox"/> DISABLED
SSC Hash	<input type="text" value="Enter SSC Hash (must contain 40 characters)"/>

Através do CLI:

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

**Observação:** como opção, você pode ativar a Criptografia de Link de Dados.

## Túnel de mobilidade entre controladores AireOS WLC e 9800-CL

Este cenário é normal para *brownfield* ou durante a migração do controlador, em que dividimos a rede em uma área de pontos de acesso (APs) controlada por um controlador AireOS e outra por um 9800.

É aconselhável que os APs sejam distribuídos entre os controladores por áreas físicas ou de RF, para que os clientes só façam roaming entre os controladores quando eles se moverem.

Evitar *salt and pepper* implantação. Opcionalmente, essa topologia de mobilidade também pode ser usada para *guest anchor* em que 9800 atua como estrangeiro e um AireOS como controlador âncora.

### Diagrama de Rede



## Configuração do AireOS WLC

Se seus controladores 9800 estiverem em High Availability, verifique se você configurou o endereço MAC de mobilidade.

### Etapa 1. Colete informações de mobilidade da WLC 9800.

Através da GUI:

Navegue até **Configuration > Wireless > Mobility > Global Configuration** e tome nota da sua **Mobility Group Name** e **Mobility MAC Address**.

The screenshot shows the GUI for configuring mobility on an AireOS WLC. The breadcrumb navigation path is **Configuration > Wireless > Mobility**. The **Configuration** menu item is highlighted. The **Global Configuration** tab is selected. The following fields are visible:

Field	Value
Mobility Group Name*	default
Multicast IPv4 Address	0.0.0.0
Multicast IPv6 Address	::
Keep Alive Interval (sec)*	10
Mobility Keep Alive Count*	3
Mobility DSCP Value*	48
Mobility MAC Address*	001e.e67e.75ff

Através do 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

## Etapa 2. Colete o valor de Hash da 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
```

## Etapa 3. Adicione as informações da WLC 9800 na WLC AireOS.

Através da GUI:

Navegue até **CONTROLLER > Mobility Management > Mobility Groups > New.**

The screenshot shows the Cisco GUI interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', 'SECURITY', 'MANAGEMENT', 'COMMANDS', and 'HELP'. The 'CONTROLLER' tab is active. The left sidebar shows 'Mobility Management' expanded, with 'Mobility Groups' selected. The main content area displays 'Static Mobility Group Members' with a table containing one entry for a 'TEST' group. A 'New...' button is highlighted in the top right corner.

Local Mobility Group	TEST					
MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP	Status	Hash Key	Secure Mobility
08:96:ad:ec:3b:8f	10.88.173.72	TEST	0.0.0.0	Up	none	NA

Insira os valores e clique em **Apply**.

The screenshot shows the 'Mobility Group Member > New' configuration page. The 'CONTROLLER' tab is active. The page contains several input fields for configuration: Member IP Address (172.16.51.88), Member MAC Address (001e.e67e.75ff), Group Name (default), Secure Mobility (Enabled), Data Tunnel Encryption (Disabled), High Cipher (Disabled), and Hash (d7bde0898799dbfeffd4859108727d3372d3a63d). A 'Back' button and an 'Apply' button are visible at the bottom right.

**Observação:** o hash só é necessário nos casos em que o 9800 usa um certificado autoassinado, como o C9800-CL. Os dispositivos de hardware têm um certificado SUDI e não precisam de um hash (por exemplo, um 9800-40, 9800-L e assim por diante).

Através do 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
```

## Configuração da WLC 9800

### Etapa 1. Colete informações de mobilidade do AireOS.

Através da GUI:

Faça login na GUI do AireOS e navegue até **CONTROLLER > Mobility Management > Mobility Groups** e anote o endereço MAC, o endereço IP e o nome do grupo.

**Static Mobility Group Members**

MAC Address	IP Address(Ipv4/Ipv6)	Group Name	Multicast IP
08:96:ad:ac:3b:8f	10.88.173.72	TEST	0.0.0.0
00:1e:e6:7e:75:ff	172.16.51.88	default	0.0.0.0

Através do 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
```

### Etapa 2. Adicione as informações do AireOS WLC ao 9800 WLC

Através da GUI:

Navegue até **Configuration > Wireless > Mobility > Peer Configuration > Add**

Configuration > Wireless > Mobility

Global Configuration **Peer Configuration**

▼ Mobility Peer Configuration

**+ Add** **× Delete**

MAC Address	IP Address	Public IP	Group Name	Multicast IPv4	Multicast IPv6	Status	PMTU	SSC Hash
001e.e67e.75ff	172.16.51.88	N/A	default	0.0.0.0	::	N/A	N/A	d7bde0898799

1 10 items per page

➤ Non-Local Mobility Group Multicast Configuration

Insira as informações do AireOS WLC.

**Observação:** na WLC 9800, a criptografia do plano de controle está sempre habilitada, o que significa que você precisa ter a mobilidade segura habilitada no lado do AireOS. No entanto, a criptografia de enlace de dados é opcional. Se você habilitá-lo no lado 9800, habilite-o no AireOS com: **config mobility group data-dtls enable**

### Add Mobility Peer ✕

MAC Address\*

Peer IPv4/IPv6 Address\*  ⇄ Ping Test

Public IPv4/IPv6 Address

Group Name\*  ▼

Data Link Encryption  DISABLED

SSC Hash

↶ Cancel 📄 Apply to Device

Através do CLI:

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

**Verificar**

Use esta seção para confirmar se a sua configuração funciona corretamente.

## Verificação de WLC AireOS

```
>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	Status	Group Name
Multicast IP			
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	

## Verificação da WLC 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 IPv6	Public Ip	Group Name Status	Multicast IPv4 PMTU	Multicast
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 seção fornece informações usadas para solucionar problemas da sua configuração.

Para solucionar problemas de implementação do túnel de mobilidade, use estes comandos para depurar o processo:

## WLC AireOS

## Etapa 1. Ative as depurações de mobilidade.

```
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
```

## Etapa 2. Reproduzir a configuração e verificar a saída

### Exemplo de uma criação de túnel de mobilidade bem-sucedida em uma WLC 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 09:53:38.524: 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

Por padrão, os controladores 9800 registram continuamente as informações do processo sem a necessidade de qualquer procedimento especial de depuração.

Basta conectar-se ao controlador e recuperar os registros associados a qualquer componente sem fio para fins de solução de problemas.

Os registros podem se estender por dias; isso depende de quão ocupado o controlador está.

Para simplificar a análise, extraia os registros com um intervalo de tempo ou para o último número de minutos (o tempo padrão é definido como 10 minutos) e você pode filtrar por endereços IP ou MAC.

Etapa 1. Verifique a hora atual na controladora para que você possa rastrear os logs no tempo de volta até quando o problema ocorreu.

```
# show clock
```

Etapa 2. Colete os registros do controlador, caso haja alguma informação no Cisco IOS que possa estar relacionada ao problema.

```
# show logging
```

Etapa 3. Colete os rastreamentos de nível de aviso sempre ativo para um endereço específico. Você pode usar o peer móvel IP ou MAC para filtrar.

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

Esse comando gera logs para os últimos 10 minutos. É possível ajustar esse horário com o comando `show logging profile wireless last 1 hour filter mac AAAA.BBBB.CCCC to-file bootflash:ra-AAAA.BBBB.CCCC.txt`.

Você pode exibir o conteúdo na sessão ou copiar o arquivo para um 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>
```

## Rastreamento ativo por rádio

Se os logs sempre ativos não fornecerem informações suficientes para saber quais problemas acionados durante a configuração do túnel, você poderá ativar depurações condicionais e capturar **Radio Active (RA)** rastreamentos, que fornecem uma atividade de processo mais detalhada.

Etapa 1. Verifique se não há condições de depuração já habilitadas.

```
# show debugging
IOSXE Conditional Debug Configs:

Conditional Debug Global State: Stop
```

```
IOSXE Packet Tracing Configs:
```

```
Packet Infra debugs:
```

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

Se você vir qualquer condição que não esteja relacionada ao endereço que deseja monitorar, desative-a.

Para remover um endereço específico:

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

Para remover todas as condições (maneira recomendada):

```
# clear platform condition all
```

Etapa 2. Adicione a condição de depuração para um endereço que você deseja monitorar.

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

**Observação:** se quiser monitorar mais de um peer de mobilidade ao mesmo tempo, use um **debug platform condition feature wireless mac** por endereço MAC.

Etapa 3. Peça que a WLC 9800 inicie o monitoramento da atividade de endereço especificada.

```
# debug platform condition start
```

**Observação:** a saída da atividade de mobilidade não é exibida, pois tudo é armazenado em buffer internamente para ser coletado posteriormente.

Etapa 4. Reproduza o problema ou o comportamento que você deseja monitorar.

Etapa 5. Pare as depurações.

```
# debug platform condition stop
```

Etapa 6. Colete a saída da atividade de endereço.

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

Esse comando gera logs para os últimos 10 minutos. É possível ajustar esse tempo com o comando **show logging profile wireless last 1 hour filter mac AAAA.BBB.CCCC to-file bootflash:ra-AAAA.BBBB.CCCC.txt**.

Você pode copiar o **FILENAME.txt** a um servidor externo ou exibir a saída diretamente na tela.

Copie o arquivo para um servidor externo:

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

Mostre o conteúdo:

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

Passo 7. Se você ainda não conseguir encontrar o motivo de uma falha, colete o nível interno de logs.

(Não é necessário depurar o cliente novamente. Use os logs que já foram armazenados internamente, mas colete uma faixa maior deles).

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

Você pode copiar o **FILENAME.txt** a um servidor externo ou exibir a saída diretamente na tela.

Copie o arquivo para um servidor externo:

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

Mostre o conteúdo:

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

Etapa 8. Remova as condições de depuração.

```
# clear platform condition all
```

**Observação:** sempre remova as condições de depuração após uma sessão de solução de problemas.

Exemplo de criação bem-sucedida de túnel de mobilidade em uma 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 missed, 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 missed, 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 missed, 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 pacotes incorporada

Na maioria das vezes, é muito útil verificar pacotes trocados entre WLCs. É especialmente útil

filtrar capturas com **Access Control Lists (ACLs)** para limitar o tráfego capturado.

Este é um modelo de configuração para capturas incorporadas no CLI.

Etapa 1. Crie a 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
```

Etapa 2. Defina os parâmetros de captura:

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

**Observação:** selecione a interface de gerenciamento para o parâmetro **INTERFACE\_NAME**

Etapa 3. Inicie a captura:

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

Etapa 4. Pare a captura:

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

Etapa 5. Navegue para **Troubleshooting > Packet Capture** na GUI para coletar o arquivo de captura de pacote.

## Cenários comuns de solução de problemas

Os próximos exemplos consistem em túneis formados entre 9800 WLCs.

### Controle e caminho de dados inativos devido a problemas de conectividade

Enable **Always-On-Logs** e **Embedded packet captures** para fornecer informações adicionais para a solução de 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 missed, 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 missed, 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 missed, total missed packet = 30
```

As capturas de pacotes são úteis para confirmar o comportamento.

```
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 a depuração e a WLC mostram que não há resposta aos pings de Controle ou Dados. Um cenário comum mostra que a conectividade IP é permitida, mas as portas 16666 ou 16667 não têm permissão para se comunicar pela rede.

## Incompatibilidade de configuração entre WLCs

Nesse caso, confirmamos a conectividade para todas as portas entre as WLCs, mas continuamos a notar falhas de keepalives.

Enable **Always-On-Logs** E **Embedded packet captures** para fornecer informações adicionais para a solução de 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 missed, 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 missed, total missed packet = 3
```

Os logs internos no par 172.16.55.28 nos ajudam a confirmar a incompatibilidade de configuração

```
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
```

A incompatibilidade de configuração comum inclui: nome de grupo incorreto, incompatibilidade ativada **Data Link Encryption** e endereço MAC de mobilidade incorreto.

Log de incompatibilidade 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.
```

Log de incompatibilidade de endereços 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 handshake DTLS

Esse tipo de problema está relacionado aos estabelecimentos de túnel DTLS entre WLCs. Pode ser que o caminho de dados esteja UP, mas o caminho de controle permaneça **DOWN**.

Enable **Always-On-Logs** e **Embedded packet captures** para fornecer informações adicionais para a solução de 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
```

Use **show wireless management trustpoint** e **show crypto pki trustpoints** commands para verificar as informações do certificado.

## O cenário de HA SSO

Se você tiver controladores no par SSO de alta disponibilidade, há um problema importante a ser observado. O endereço MAC de mobilidade não é configurado por padrão e pode fazer com que o túnel de mobilidade fique inativo se ocorrer um failover.

O **show wireless mobility summary** fornece o MAC de mobilidade atual em uso, mas não é necessariamente configurado. Verifique se a configuração tem o MAC de mobilidade configurado com **show run | i Mobilidade**

Se o mac de mobilidade não estiver configurado na configuração de execução, ele será alterado no failover para o WLC em standby e isso causará a falha dos túneis de mobilidade.

A solução simples é navegar até a página **Configuration > Wireless > Mobility** da interface do usuário da Web e pressionar **apply**. Isso salva o MAC de mobilidade atual na configuração. O MAC então permanece o mesmo após o failover e os túneis de mobilidade são preservados.

Esse problema ocorre principalmente se você fizer a configuração de mobilidade por meio da linha de comando e esquecer de configurar o endereço MAC de mobilidade. A interface de usuário da Web salva automaticamente um endereço MAC de mobilidade quando você aplica as configurações.

## Informações Relacionadas

- [Configurar o recurso de mobilidade de âncora de WLAN no Catalyst 9800](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.