Configurar SSO de alta disponibilidade no Catalyst 9800 | Guia de início rápido

Contents

Introdução

Este documento descreve como configurar o SSO (Stateful Switchover) de alta disponibilidade em um modo RP+RMI, em um Catalyst 9800 WLC.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento de

- Modelo de configuração sem fio Catalyst 9800.
- Conceitos de alta disponibilidade conforme abordado no guia de HA SSO.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- C9800-CL v17.9.2

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Embora a configuração de HA SSO possa exigir apenas 3 deles, aqui 4 endereços IP da mesma rede que a interface de gerenciamento sem fio (WMI) foram usados para facilitar o acesso à GUI do controlador.

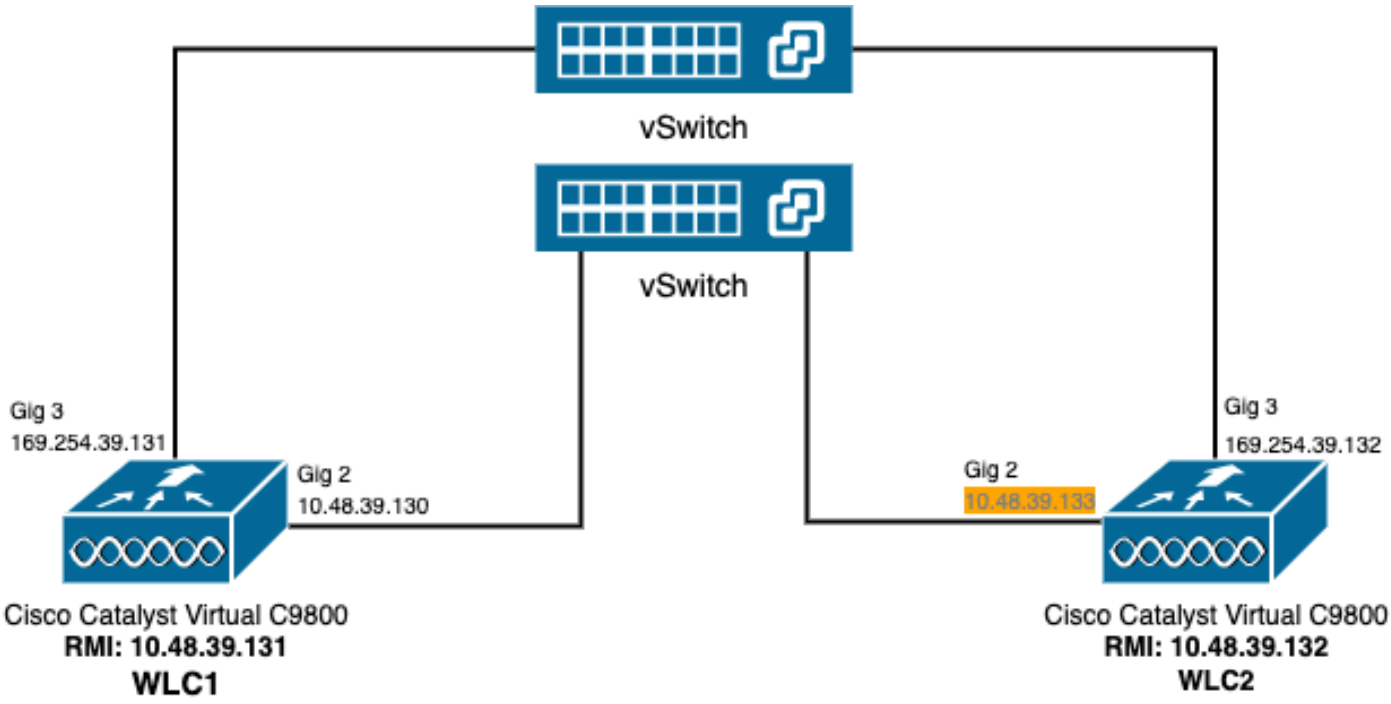
Informações de Apoio

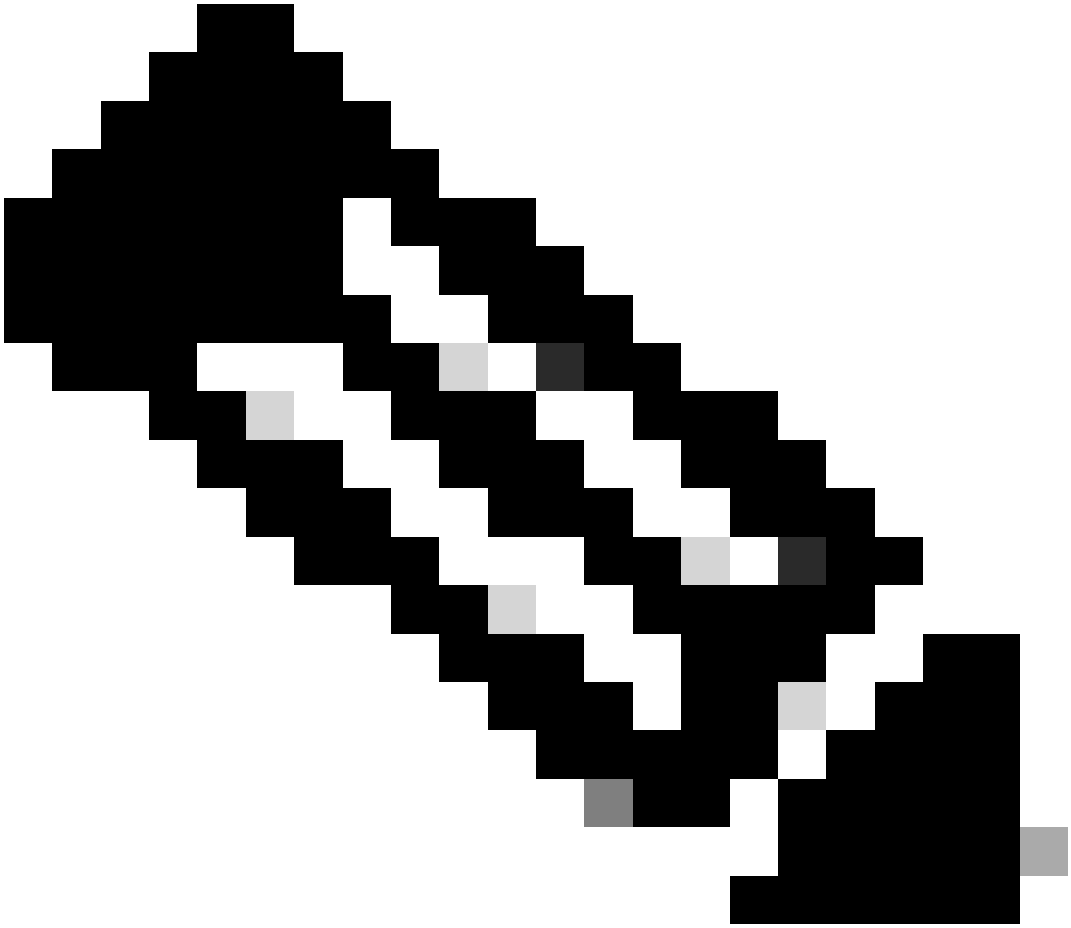
O recurso SSO de alta disponibilidade no controlador sem fio permite que o access point estabeleça um túnel CAPWAP com o controlador sem fio ativo e o controlador sem fio ativo para compartilhar uma cópia espelhada do AP e do banco de dados do cliente com o controlador sem fio em standby. Quando ocorrem switchovers (ou seja, o controlador ativo falha e, portanto, o Standby toma a mão), os APs unidos não entram no estado Discovery e os clientes não se desconectam. Há apenas um túnel CAPWAP mantido de cada vez entre os APs e o controlador sem fio que está em um estado Ativo.

As duas unidades formam uma conexão peer por meio de uma porta RP dedicada (ou uma interface virtual para VMs) e ambos os controladores compartilham o mesmo endereço IP na interface de gerenciamento. A interface RP é usada para sincronizar a configuração em massa e incremental em tempo de execução e garantir o status operacional de ambos os controladores do par HA. Além disso, quando RMI + RP é usado, os controladores em standby e ativo têm uma interface de gerenciamento de redundância (RMI) à qual são atribuídos endereços IP, ou seja, usados para garantir a acessibilidade do gateway. O estado CAPWAP dos pontos de acesso que estão no estado Run também é sincronizado do controlador sem fio ativo para o controlador sem fio Hot-Standby, que permite que os pontos de acesso sejam comutados por completo quando o controlador sem fio ativo falhar. Os APs não entram no estado Discovery quando o controlador sem fio ativo falha e o controlador sem fio em standby assume como o controlador sem fio ativo para atender à rede.

Configurar

Diagrama de Rede


vSwitch
vSwitch
Gig 3
169.254.39.131
Gig 2
10.48.39.130
Gig 3
169.254.39.132
Gig 2
10.48.39.133
Cisco Catalyst Virtual C9800
RMI: 10.48.39.131
WLC1
Cisco Catalyst Virtual C9800
RMI: 10.48.39.132
WLC2



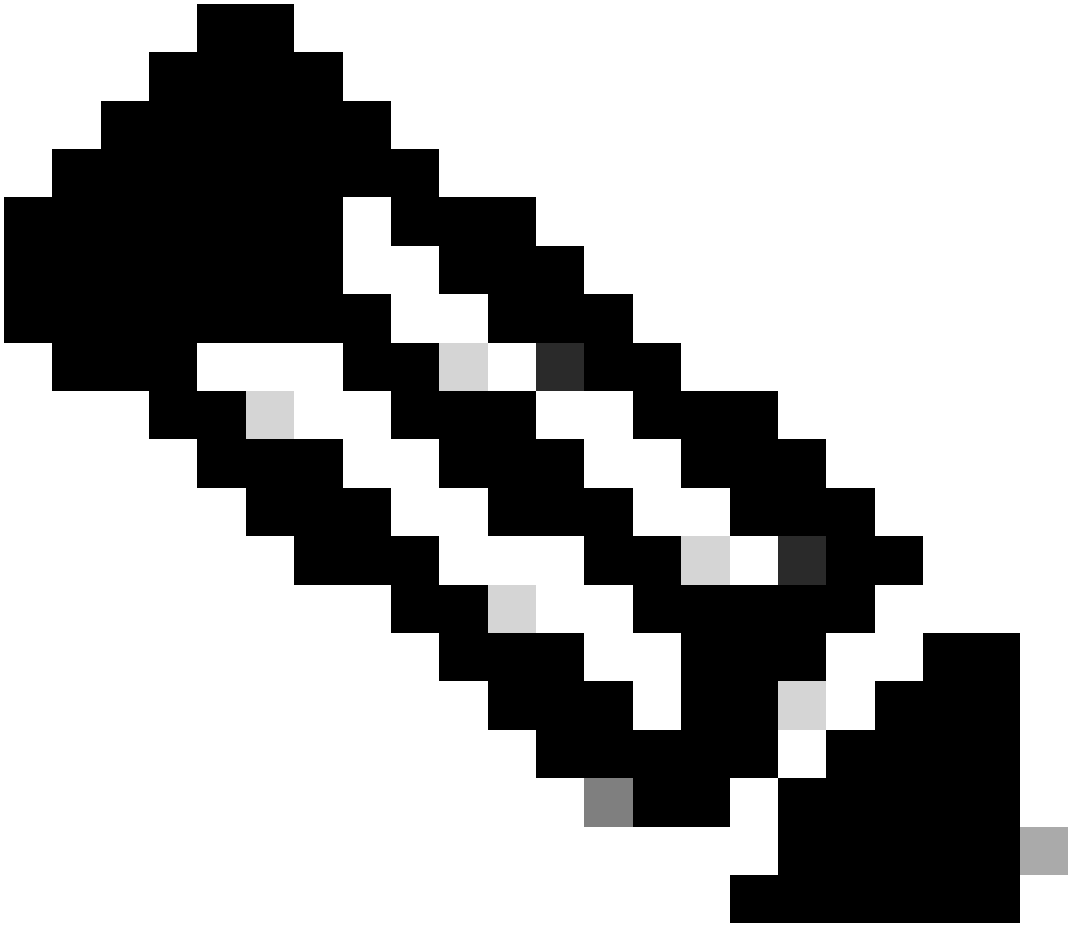
Observação: em laranja, é realçado o endereço IP temporário atribuído à interface virtual GigabitEthernet 2 do controlador 9800-CL designado como WLC2. Esse endereço IP é definido temporariamente como a WMI para a WLC2 e permite acesso à GUI dessa instância para facilitar a configuração de HA SSO. Depois que o SSO HA é configurado, esse endereço é liberado, pois apenas uma única WMI é usada para um par de controladores SSO HA.

Configurações

Neste exemplo, o SSO (stateful switchover) de HA (alta disponibilidade) é configurado entre duas instâncias do 9800-CL, que executam a mesma versão do software Cisco IOS, que foi configurada com WMIs separadas e com GUI acessível em

- O endereço IP 10.48.39.130 para o primeiro, conhecido como WLC1;
- O endereço IP 10.48.39.133 para o segundo, conhecido como WLC2.

Além desses endereços IP, 2 endereços adicionais na mesma sub-rede (e VLAN) foram usados, ou seja, 10.48.39.131 e 10.48.39.132. Esses são os endereços IP da interface de gerenciamento de redundância (RMI) para o chassi 1 (WLC1) e o chassi 2 (WLC2), respectivamente.



Observação: depois que o HA é configurado entre as duas controladoras, 10.48.39.133 é liberado e 10.48.39.130 se torna a única WMI da minha configuração. Portanto, após a configuração, apenas 3 endereços IP estão em uso, o da WMI e o dos RMIs.

A configuração das interfaces para ambos os dispositivos antes mesmo de iniciarem a configuração de HA deve ser semelhante àquelas fornecidas neste exemplo.

```
WLC1#show running-config | s interface
interface GigabitEthernet1
 shutdown
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet2
 switchport trunk allowed vlan 39
 switchport mode trunk
 negotiation auto
 no mop enabled
 no mop sysid
```

```
interface GigabitEthernet3
 negotiation auto
 no mop enabled
 no mop sysid
interface Vlan1
 no ip address
 shutdown
 no mop enabled
 no mop sysid
interface Vlan39
 ip address 10.48.39.130 255.255.255.0
 no mop enabled
 no mop sysid
wireless management interface Vlan39
```

```
WLC2#show running-config | s interface
interface GigabitEthernet1
 shutdown
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet2
 switchport trunk allowed vlan 39
 switchport mode trunk
 negotiation auto
 no mop enabled
 no mop sysid
interface GigabitEthernet3
 negotiation auto
 no mop enabled
 no mop sysid
interface Vlan1
 no ip address
 shutdown
 no mop enabled
 no mop sysid
interface Vlan39
 ip address 10.48.39.133 255.255.255.0
 no mop enabled
 no mop sysid
wireless management interface Vlan39
```

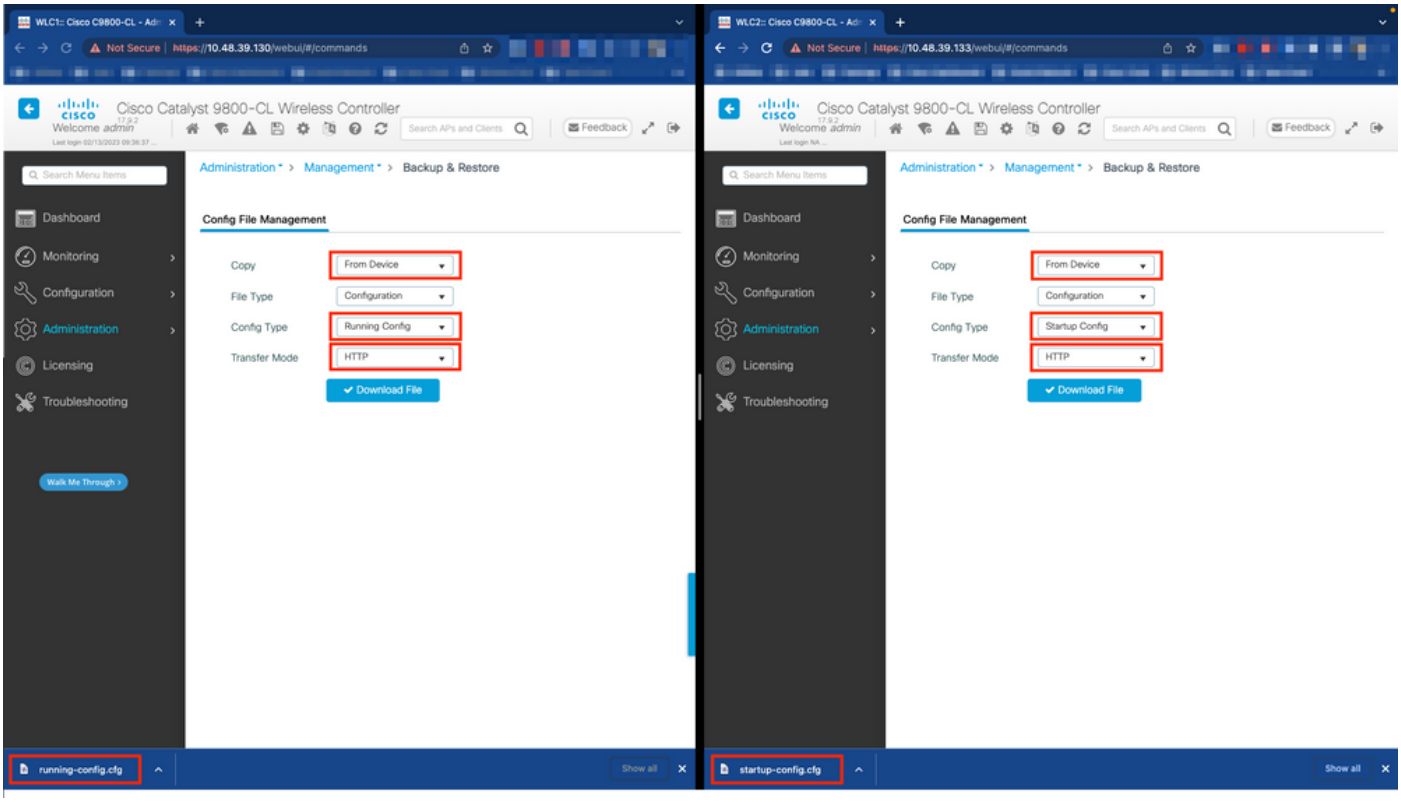
Neste exemplo, a WLC1 é designada como a controladora primária (ou seja, o chassi 1), enquanto a WLC2 é a secundária (ou seja, o chassi 2). Isso significa que o par HA feito dos 2 controladores usa a configuração da WLC1 e que o da WLC2 é perdido após o processo.

Etapa 1. (Opcional) Fazer backup dos arquivos Startup Config e Running Config dos controladores.

Um manuseio incorreto pode ocorrer e resultar em perda de configuração. Para evitar isso, é altamente recomendável fazer backup da configuração de inicialização e de execução de ambos os controladores usados na configuração de HA. Isso pode ser feito facilmente usando a GUI ou a CLI do 9800.

Na GUI:

Na guia *Administração → gerenciamento → backup e restauração* da GUI 9800 (consulte a captura de tela), é possível fazer o download da configuração de inicialização e execução usada atualmente pelo controlador.



Neste exemplo, a inicialização (lado esquerdo) e a configuração (lado direito) são baixadas diretamente, através do HTTP, no dispositivo que hospeda o navegador usado para acessar a GUI do WLC. É possível ajustar facilmente o modo de transferência e o destino do arquivo do qual será feito o backup, com o campo Transfer Mode (Modo de transferência).

Na CLI:

```
WLCx#copy running-config tftp://<SERVER-IP>/run-backup_x.cfg
Address or name of remote host [<SERVER-IP>]?
Destination filename [run-backup_x.cfg]?
!!
19826 bytes copied in 1.585 secs (12509 bytes/sec)
WLCx#copy startup-config tftp://<SERVER-IP>/start-backup_x.cfg
Address or name of remote host [<SERVER-IP>]?
Destination filename [start-backup_x.cfg]?
!!
20482 bytes copied in 0.084 secs (243833 bytes/sec)
```

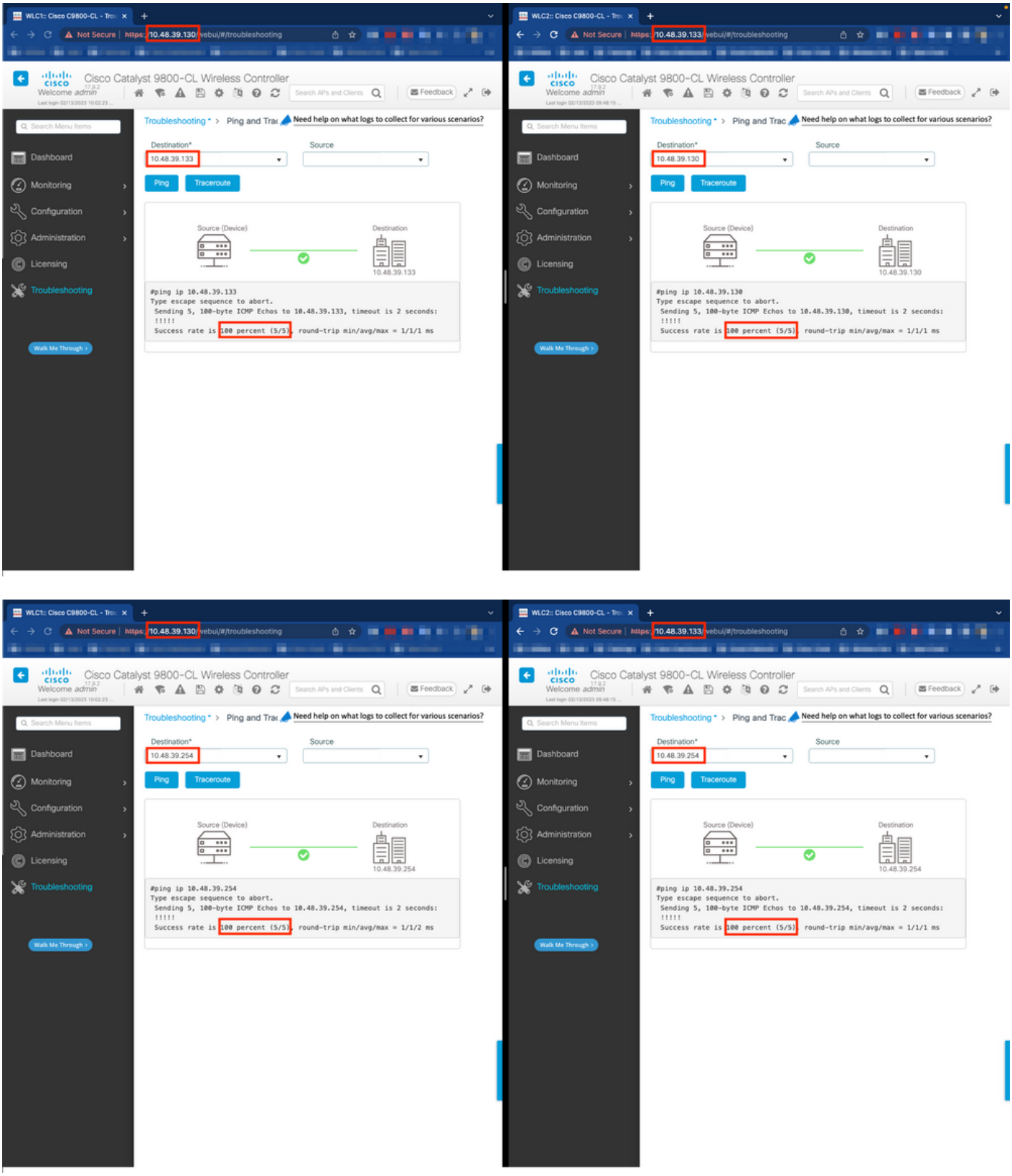
Substitua o <SERVER-IP> pelo IP do servidor TFTP no qual o arquivo de configuração de inicialização/execução é copiado.

Etapa 2. (Opcional) Garanta a conectividade da rede.

Nas GUIs ou CLIs da WLC, é possível executar testes de conectividade simples, ou seja, fazer ping no gateway de ambos os dispositivos e fazer ping nos dispositivos entre eles. Isso garante que ambos os controladores tenham a conectividade necessária para configurar o HA.

Na GUI:

A ferramenta *Ping e Traceroute* da guia *Troubleshooting* da GUI 9800 pode ser usada para testar a conectividade entre os próprios controladores e entre cada WLC e seu gateway de rede, como mostrado nessas figuras.



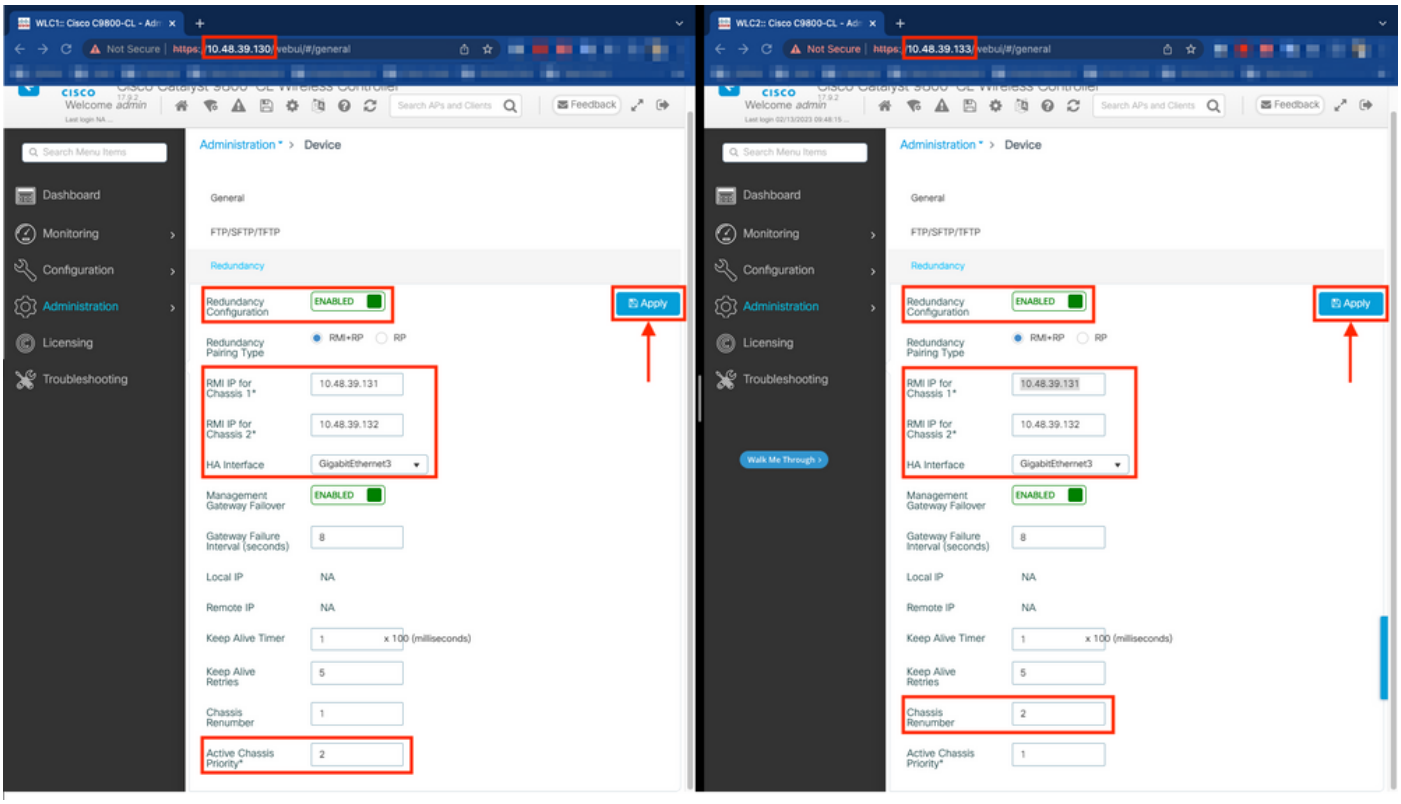
Na CLI:

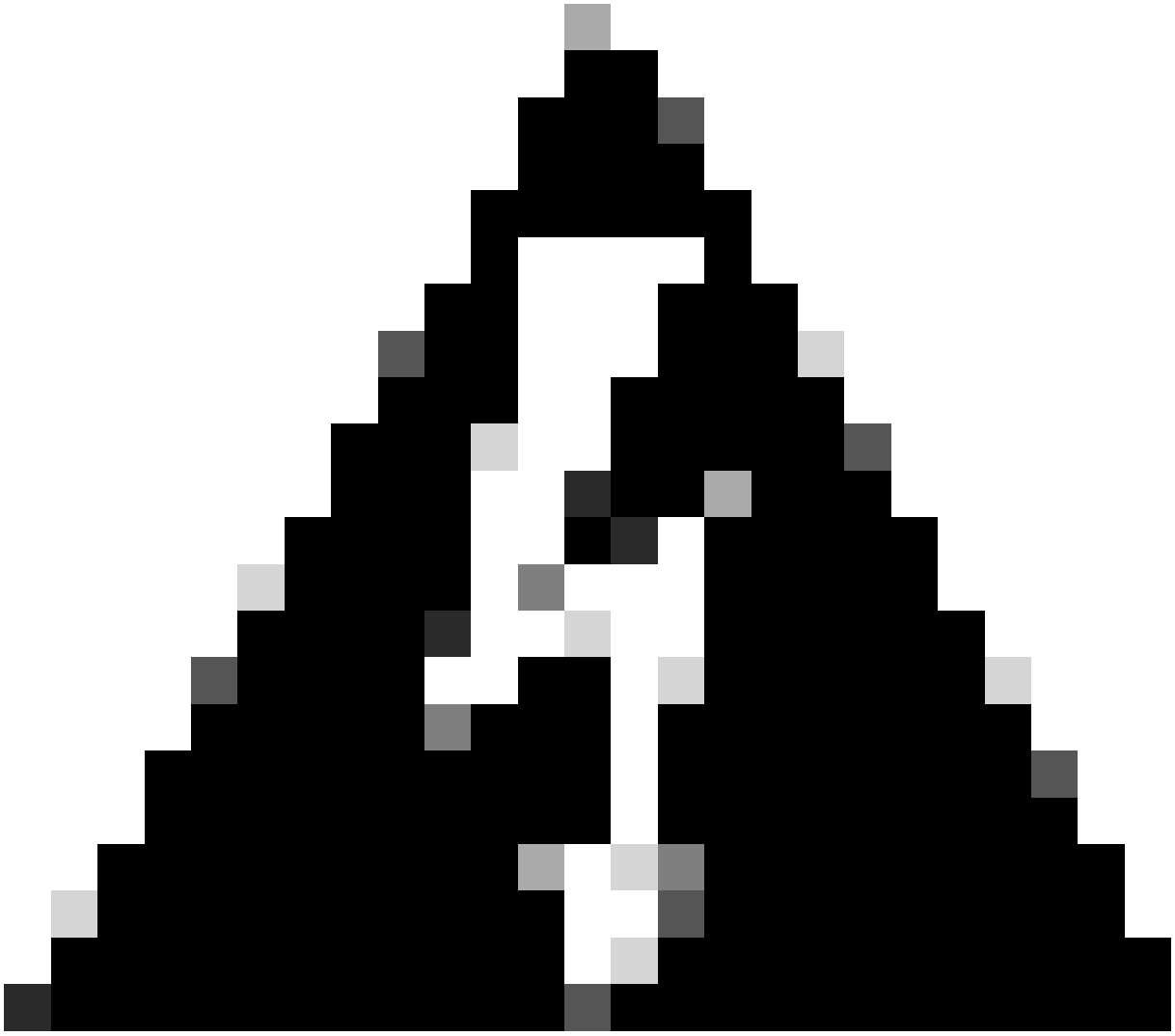
```
WLCx#ping 10.48.39.133 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.48.39.133, t
```

Etapa 3. Configure a redundância com o tipo de emparelhamento RMI + RP.

Com a conectividade entre cada dispositivo garantida, a redundância pode ser configurada entre os controladores. Esta captura de tela mostra

como a configuração é feita na guia *Redundancy* da página *Administration→ Device* da GUI 9800.





Aviso: neste exemplo, a WLC1 foi designada como controladora primária, o que significa que é aquela cuja configuração é replicada para a outra controladora. Certifique-se de aplicar a prioridade/renumeração de chassi apropriada para usar a configuração apropriada com seu par HA e não perder nenhuma parte dele.

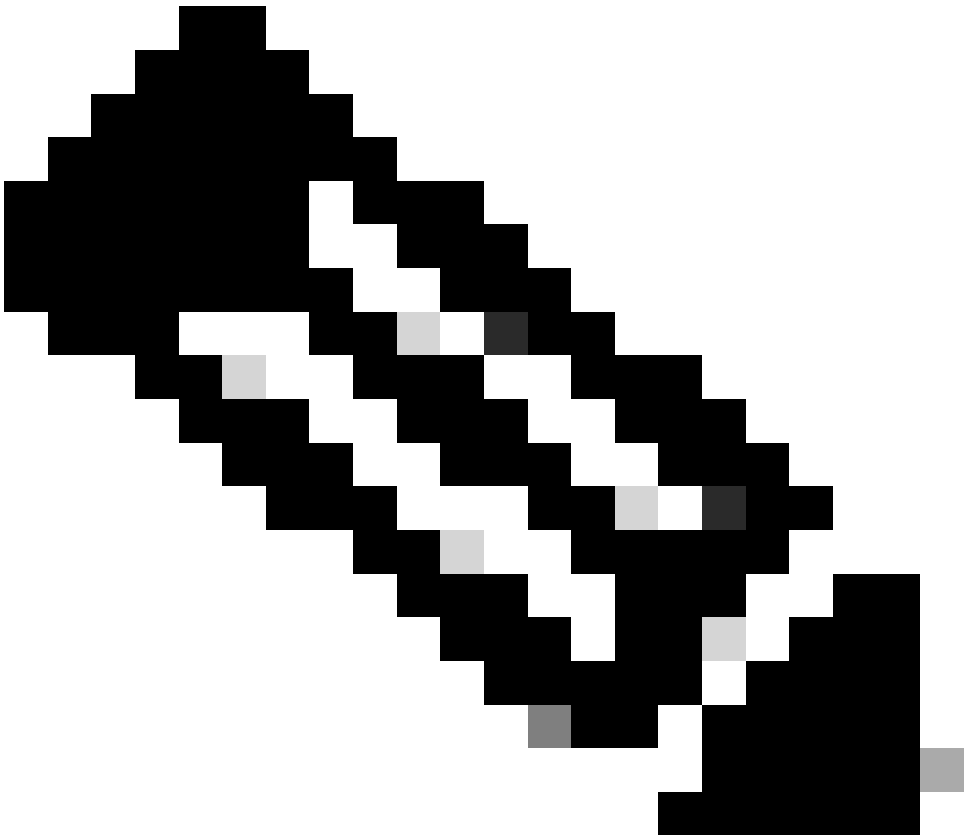
Vamos analisar os campos configurados e sua finalidade

- **Configuração de redundância:** deve ser habilitada para usar redundância entre WLCs.
- **Tipo de emparelhamento de redundância:** como este guia aborda o SSO HA usando a configuração RMI, o tipo de emparelhamento configurado deve ser RMI + RP, usando a interface de gerenciamento de redundância e a porta de redundância.

Também é possível optar por configurar a redundância usando somente a porta de redundância. No entanto, quando RP é escolhido apenas, a acessibilidade do gateway não é verificada, apenas o estado da WLC redundante é

- **IP RMI para o chassi 1/2:** esses campos atribuem os endereços IP fornecidos à interface de redundância designada para ambas as instâncias. Neste exemplo, ambos os IPs RMI para os chassis 1 e 2 foram configurados como sendo respectivamente 10.48.39.131 e 10.48.39.132, como descrito antes e mostrado no diagrama de rede.

- **Interface HA:** ao usar dispositivos virtuais, o mapeamento entre as placas de interface de rede virtual (vNIC) do hipervisor e as interfaces de rede da máquina virtual pode ser configurado de diferentes maneiras. Portanto, a interface usada para redundância é configurável para Cisco Catalyst 9800-CLs. Aqui, o GigabitEthernet 3 foi usado, conforme recomendado pelo guia de implantação do 9800-CL.



Observação: ao usar dispositivos C9800 físicos, as interfaces usadas em HA e RP são as padrão e não são configuráveis. De fato, as WLCs 9800 de hardware têm uma interface de redundância dedicada que é separada das WLCs de rede.

- **Failover do gateway de gerenciamento:** conforme detalhado no guia de configuração de HA SSO, este método de redundância implementa a verificação do gateway padrão, feita pelo envio periódico do ping do Internet Control Message Protocol (ICMP) ao gateway. As controladoras ativa e standby usam o IP RMI como o IP de origem para essas verificações. Essas mensagens são enviadas em um intervalo de 1 segundo.

- **Intervalo de falha do gateway:** representa o tempo durante o qual uma verificação de gateway deve falhar consecutivamente antes de o gateway ser declarado como não alcançável. Por padrão, ele é configurado como 8 segundos. Como as verificações de gateway são enviadas a cada segundo, isso representa 8 falhas consecutivas para acessar o gateway.

- **IP local/remoto:** esses são os IPs RP configurados para os chassis 1 e 2. Esses endereços IP são gerados automaticamente como 169.254.x.x, em que x.x é derivado dos dois últimos octetos da interface de gerenciamento.

- **Temporizador de manutenção de atividade:** conforme detalhado no guia de configuração de HA SSO, os chassis ativo e em espera enviam mensagens de manutenção de atividade entre si para garantir que ambos ainda estejam disponíveis. O temporizador de manutenção de atividade é a quantidade de tempo que separa o envio de 2 mensagens de manutenção de atividade entre cada chassi. Por padrão, as mensagens de keep-alive são enviadas a cada 100 ms. Geralmente, recomenda-se aumentar esse valor com a 9800-CL para evitar switchovers abusivos sempre que a infraestrutura de VM introduz pequenos atrasos (instantâneos, etc.)

- **Tentativas de Keep Alive:** este campo configura o valor de repetição de keepalive do peer antes de declarar que o peer está inativo. Se o temporizador de keep-alive e o valor padrão repetido forem usados, um peer será reivindicado como inativo se as 5 mensagens de keep alive enviadas no intervalo de tempo de 100 ms forem deixadas sem resposta (ou seja, se o link de redundância estiver inativo por 500 ms).

- **Renumeração do chassi:** o número do chassi que o dispositivo deve usar (1 ou 2).

    - Na WLC2 (10.48.39.133), o chassi é renumerado para 2. Por padrão, o número do chassi é 1. Os endereços IP das portas RP são derivados da RMI. Se o número do chassi for o mesmo em ambos os controladores, a derivação IP da porta RP local será a mesma e a detecção falhará. Renumerar o chassi para evitar esse cenário chamado Ativo-Ativo.

- **Prioridade ativa do chassi:** a prioridade usada para definir qual configuração deve ser usada pelo par HA. O dispositivo com a prioridade mais alta é aquele que é replicado para o outro. A configuração do chassi com a prioridade mais baixa é, portanto, perdida.

Na WLC1 (10.48.39.130), a prioridade do chassi ativo foi definida como 2. Isso serve para garantir que esse chassi seja escolhido como o ativo (e, portanto, que sua configuração seja usada) no par HA criado.

Depois que essas configurações forem feitas, use o botão *Apply* para aplicar a configuração às controladoras.

Na CLI

Primeiro, configure um endereço IP secundário na interface virtual usada para configurar o RMI em ambos os dispositivos.

```
WLC1#configure terminal WLC1(config)#interface vlan 39 WLC1(config-if)# ip address 10.48.39.131 255.255
```

```
WLC2#configure terminal WLC2(config)#interface vlan 39 WLC2(config-if)# ip address 10.48.39.132 255.255
```

Em seguida, habilite a redundância em ambos os dispositivos

```
WLC1#configure terminal WLC1(config)#redundancy WLC1(config-red)#mode sso WLC1(config-red)#end
```

```
WLC2#configure terminal WLC2(config)#redundancy WLC2(config-red)#mode sso WLC2(config-red)#end
```

Configurar a prioridade do chassi, como WLC1, torna-se o controlador principal

```
WLC1#show chassis Chassis/Stack Mac Address : 0001.0202.aabb - Local Mac Address Mac persistency wait t
```

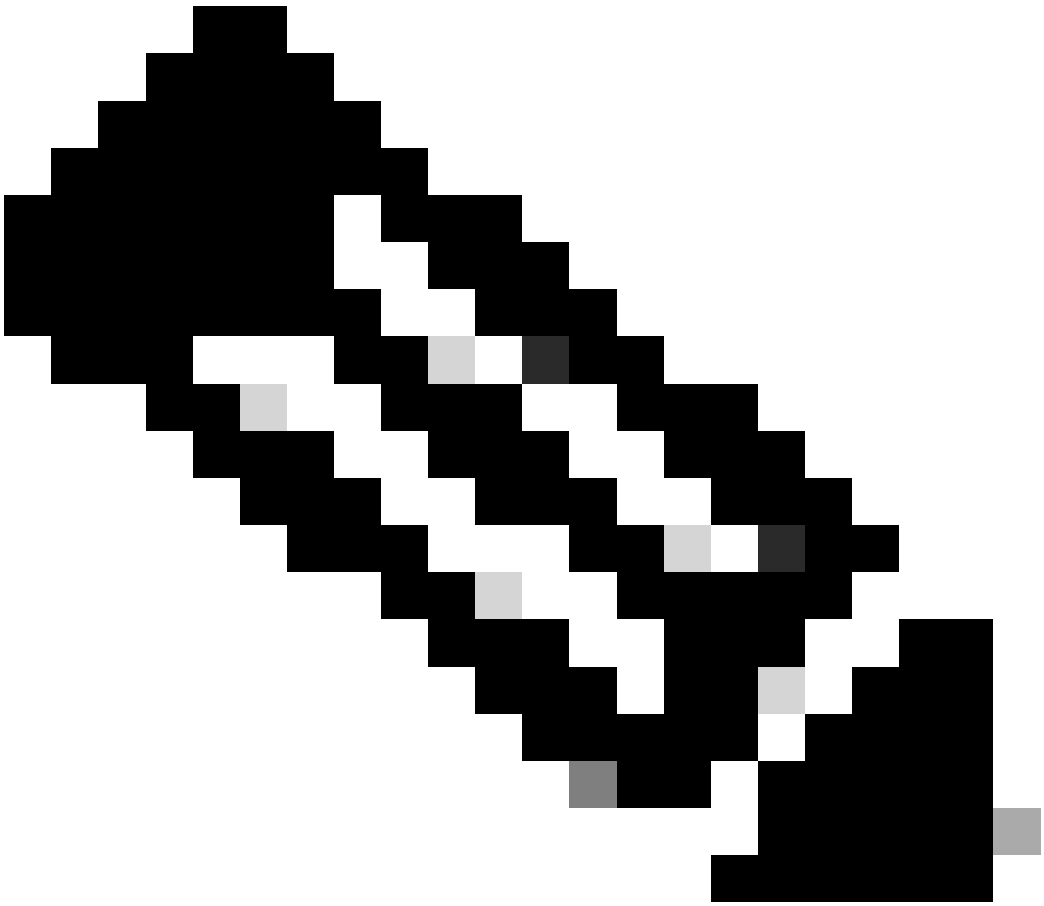
Renumerar o chassi para WLC2 que se torna o controlador secundário

```
WLC2#show chassis Chassis/Stack Mac Address : 0001.0202.aabb - Local Mac Address Mac persistency wait t
```

Por fim, configure o RMI em ambos os dispositivos

```
WLC1#chassis redundancy ha-interface GigabitEthernet 3 WLC1#configure terminal WLC1(config)#redun-manag
```

```
WLC2#chassis redundancy ha-interface GigabitEthernet 3 WLC2#configure terminal WLC2(config)#redun-manag
```



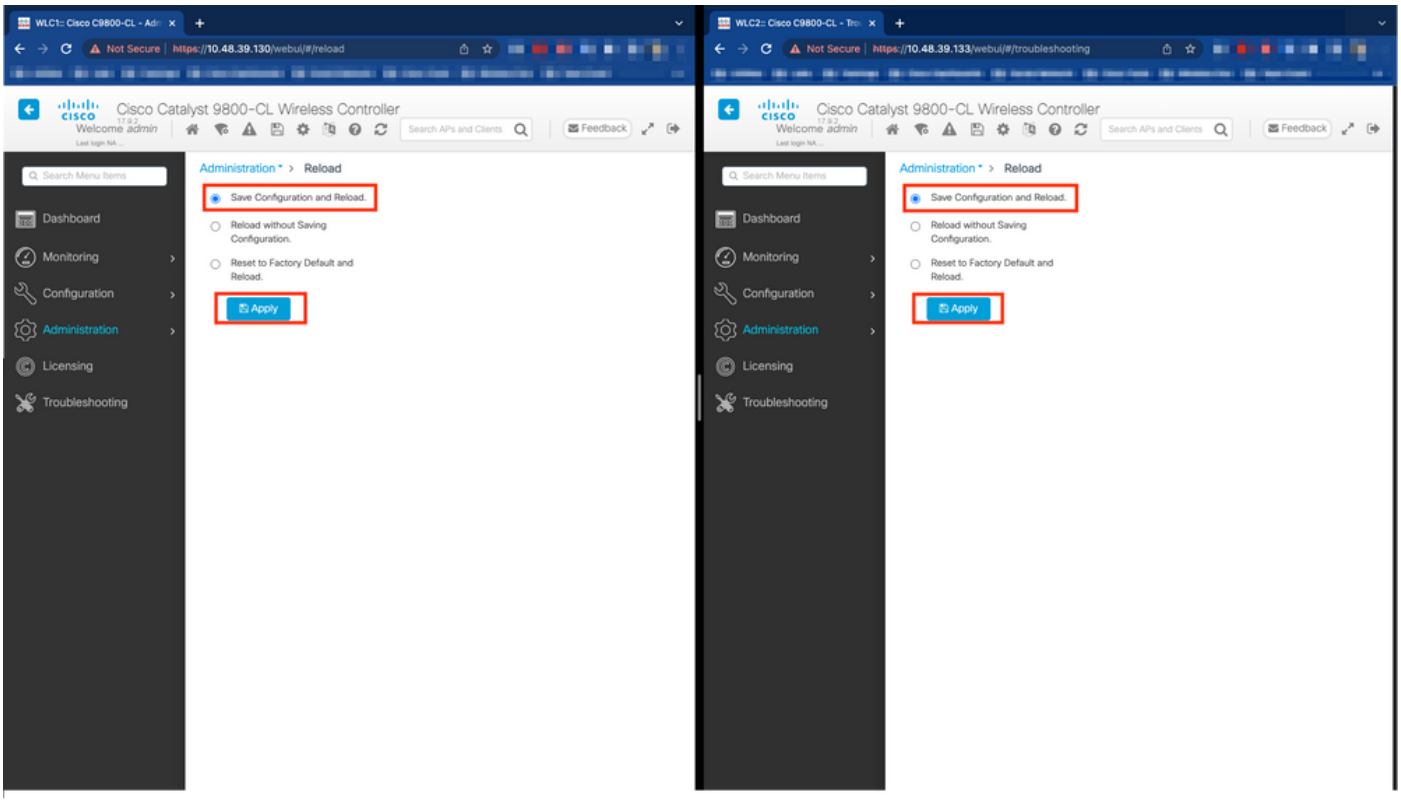
Observação: quanto à configuração da GUI, no Catalyst 9800 virtual, a interface usada pelo controlador deve ser selecionada entre as disponíveis. Como recomendado, GigabitEthernet 3 é usado aqui e configurado graças ao chassis redundancy ha-interface GigabitEthernet 3 comando. Esse comando não faz parte da configuração de execução, no entanto, a interface usada pelo HA pode ser vista nas variáveis de ambiente da instância do ROMMON. Eles podem ser vistos com o show romvar comando.

Etapa 4. Recarregue os controladores.

Para que o par HA seja formado e a configuração seja efetiva, ambos os controladores devem ser recarregados ao mesmo tempo, uma vez que a configuração feita na etapa 3 tenha sido salva.

Da GUI:

Pode-se usar a página Recarregar administração de ambas as GUI para reiniciar os controladores, como descrito nesta captura de tela.



Do CLI:

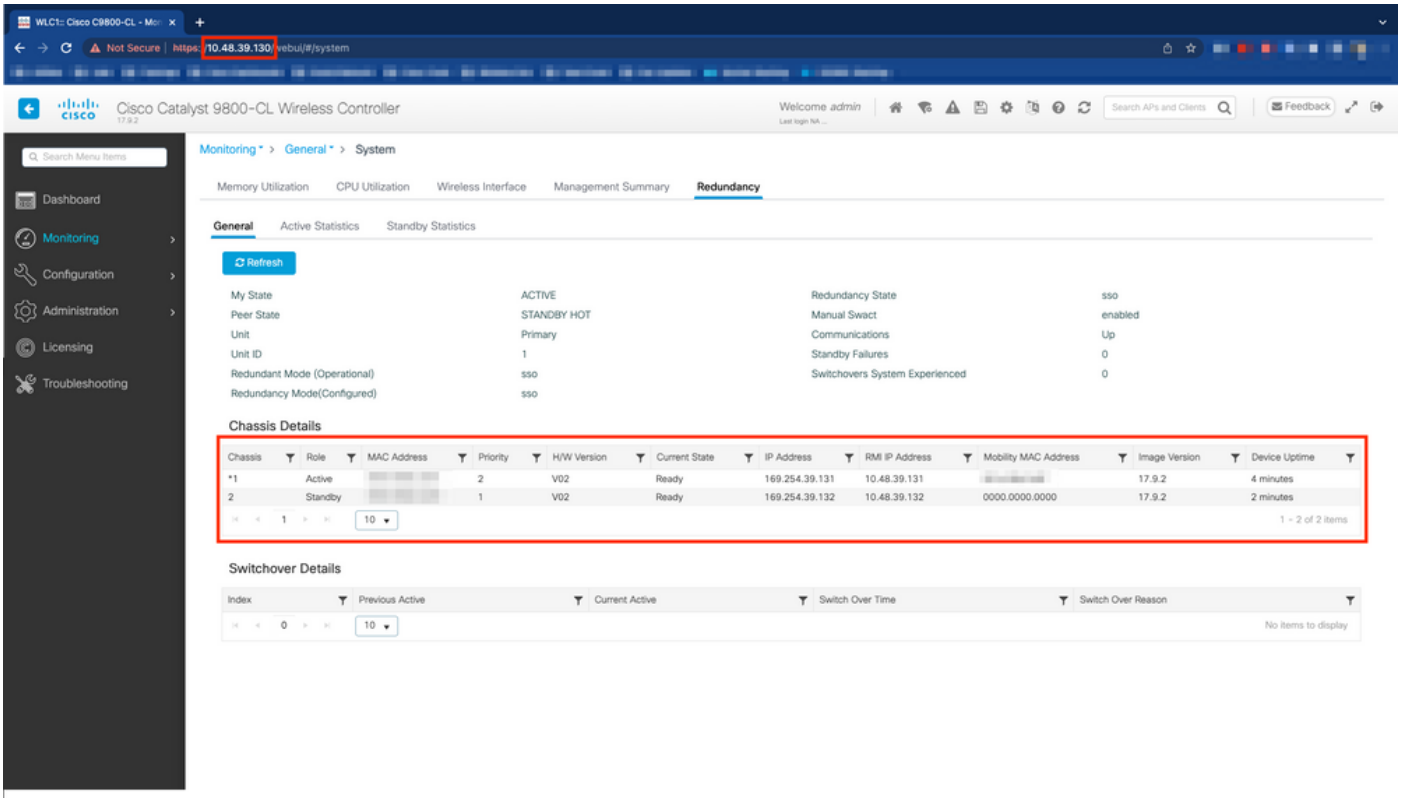
```
WLCx#reload Reload command is being issued on Active unit, this will reload the whole stack Proceed wit
```

Verificar

Quando os dois controladores do par HA se descobrem e criam o par HA desejado, um controlador (o principal) é capaz de monitorar os dois chassis a partir da GUI ou CLI.

Da GUI:

Para monitorar a configuração de redundância da GUI 9800, navegue até a guia Redundancy (Redundância) na página Monitoring > General > System (Monitoramento > Geral > Sistema), conforme mostrado nesta captura de tela.



Do CLI:

```
WLC#show chassis rmi Chassis/Stack Mac Address : 0050.568d.cdf4 - Local Mac Address Mac persistency wai
```

```
WLC#show redundancy Redundant System Information : ------------------------------ Available system upti
```

Troubleshooting

Reflexo de um único ponto de venda

O comum show tech wireless não inclui comandos que permitam compreender os failovers de HA de um par de HA nem seu status atual corretamente. Colete este comando para ter a maioria dos comandos relacionados ao HA em uma única operação:

```
WLC#show tech wireless redundancy
```

comandos show

Para o status das portas de redundância, esses comandos podem ser usados.

```
WLC#show chassis detail Chassis/Stack Mac Address : 0050.568d.2a93 - Local Mac Address Mac persistency
```

Esse comando mostra o número do chassi e o Status da Porta de Redundância, útil como solução de problemas na primeira etapa.

Para verificar os contadores keepalive na porta keepalive, é possível usar esses comandos.

```
WLC#show platform software stack-mgr chassis active R0 sdp-counters Stack Discovery Protocol (SDP) Coun
```

Outros comandos

É possível fazer uma captura de pacote na porta de redundância do controlador com esses comandos

```
WLC#test wireless redundancy packetdump start Redundancy Port PacketDump Start Packet capture started o
```

As capturas feitas usando esses comandos são salvas na bootflash: do controlador, sob o nome haIntCaptureLo.pcap.

Também é possível executar um teste de keepalive na porta de redundância com esse comando.

```
WLC#test wireless redundancy rping Redundancy Port ping PING 169.254.39.131 (169.254.39.131) 56(84) byt
```

Entre em mais detalhes

Para visualizar a configuração das variáveis ROMMON, que nos mostra como a configuração real está sendo refletida nas variáveis, você pode usar este comando.

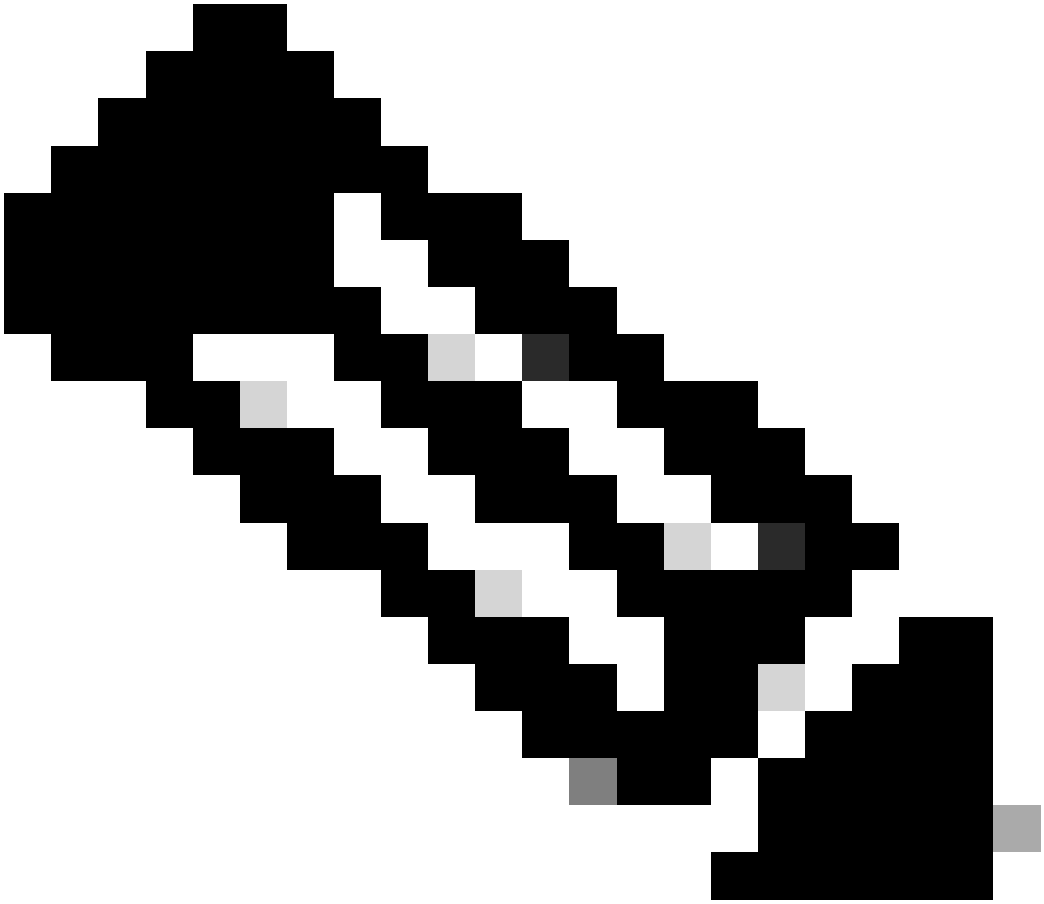
```
WLC#show romvar ROMMON variables: MCP_STARTUP_TRACEFLAGS = 00000000:00000000 SWITCH_NUMBER = 2 CONFIG_F
```

Esse comando mostra a prioridade do chassi, detalhes de RMI e RP, intervalo de peer juntamente com detalhes mais úteis.

Também podemos monitorar os processos que executam HA SSO no WLC, que são dois processos, ou seja, stack_mgr e rif_mgr.

Para fazer isso, colete os rastreamentos sempre ativos em um arquivo de texto usando o comando, o parâmetro de tempo aqui pode ser ajustado para cobrir o intervalo de tempo que queremos solucionar problemas.

```
show logging process stack_mgr start last 30 minutes to-file bootflash:stack_mgr_logs.txt show logging
```



Observação: é importante observar que a porta de serviço do WLC em standby está desativada e inacessível enquanto o controlador está atuando como em standby.

Cenários típicos

Usuário Forçado

Se você observar o histórico de switchover, poderá ver "user forced", que aparece quando um usuário iniciou um switchover entre os controladores, usando o redundancy force-switchover comando.

```
WLC#show redundancy switchover history Index Previous Current Switchover Switchover active active reaso
```

Unidade Ativa Removida

Se você observar o histórico do switchover, poderá ver "unidade ativa removida", que aponta para uma perda de comunicação na porta de redundância entre os dois controladores.

```
WLC#show redundancy switchover history Index Previous Current Switchover Switchover active active reaso
```

Isso pode acontecer se o link entre os dois controladores cair, mas também pode acontecer se uma unidade WLC cair repentinamente (falha de energia) ou travar. É interessante monitorar as duas WLCs para ver se elas têm relatórios de sistema que indicam travamentos/reinicializações inesperados.

Ativo GW perdido

Se você observar o histórico do switchover, poderá ver "GW perdido ativo", que aponta para uma perda de comunicação com o gateway na porta RMI.

```
WLC#show redundancy switchover history Index Previous Current Switchover Switchover active active reaso
```

Isso acontece se o link entre o controlador ativo e seu gateway for desativado.

Outras considerações

HA SSO para Catalyst 9800-CL

Em ambientes virtuais, você precisa aceitar que a latência é introduzida, e a latência não é algo que o HA tolera corretamente. Isso é legítimo, já que o SSO HA tende a detectar rápida e eficientemente qualquer falha no chassi. Para conseguir isso, cada chassi verifica o status do outro usando keepalives em links RP e RMI, bem como pings em direção ao gateway de seus RMIs (e este, o de seus WMI que deve ser o mesmo). Se algum desses for perdido, a pilha reage de acordo com os sintomas, conforme detalhado no "System and Network Fault Handling" do guia HA SSO.

Ao trabalhar com pilhas HA SSO virtuais do Catalyst 9800, é comum observar switchovers devido a keepalive perdido no link RP. Isso pode ocorrer devido à latência introduzida pelo ambiente virtualizado.

Para determinar se a pilha de HA SSO sofre de quedas de keepalive RP, você pode usar os logs do gerenciador de stack/rif.

```
! Keepalives are missed 004457: Feb 4 02:15:50.959 Paris: %STACKMGR-6-KA_MISSED: Chassis 1 R0/0: stack_
```

Se ambos os chassis estiverem operando, o switchover cria uma "detecção ativa dupla", que é uma consequência das quedas no RP.

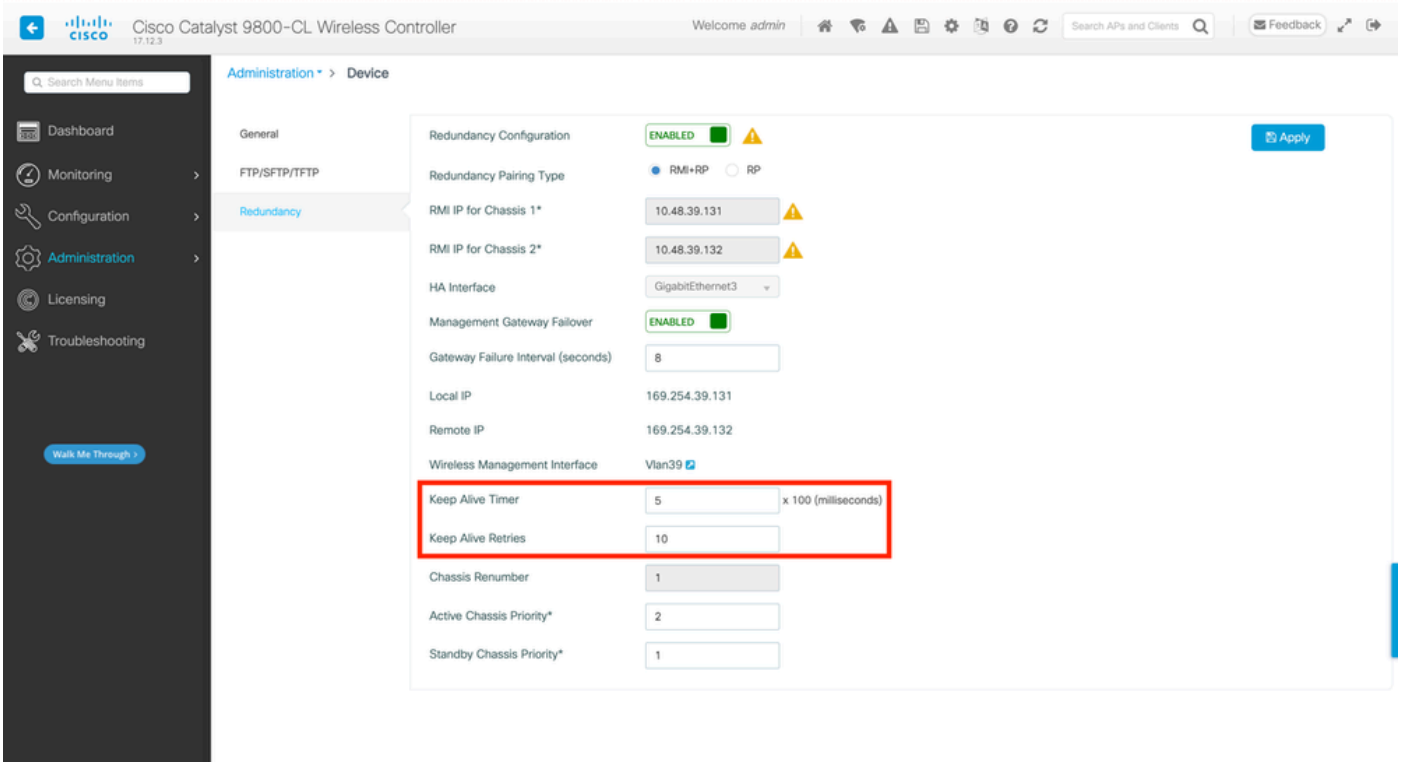
Em tal situação, ajustar os parâmetros de manutenção de atividade de HA para evitar esses switchovers desnecessários pode ajudar. Dois parâmetros podem ser configurados,

- **Temporizador Keep Alive:** o período de tempo que separa o envio de duas mensagens de keepalive entre cada chassi.
- **Tentativas de Keep Alive:** o número de keepalive que precisa ser perdido para declarar um peer inativo.

Por padrão, o temporizador keep alive é definido como 1ms e as novas tentativas como 5. Isso significa que após 5 ms de keepalive perdidos no link RP, ocorre um switchover. Esses valores podem ser muito baixos para implantações virtuais. Se você estiver passando por um switchover recorrente devido à perda de keepalives de RP, tente aumentar esses parâmetros para estabilizar a pilha.

Da GUI:

Para monitorar ou modificar os parâmetros de manutenção de atividade de SSO de HA da GUI 9800, navegue até a guia Redundancy (Redundância) na página *Administration > Device*, conforme descrito nesta captura de tela.



Do CLI:

```
WLC#chassis redundancy keep-alive retries <5-10> WLC#chassis redundancy keep-alive timer <1-10>
```

Junto com a configuração desses parâmetros, outra otimização pode ajudar com tal comportamento na pilha de HA SSO. Para dispositivos físicos, o hardware permite conectar um chassi a outro, normalmente usando um único fio. Em um ambiente virtual, a interconexão da porta RP para cada chassi deve ser feita por um switch virtual (vSwitch), que pode mais uma vez introduzir latência em comparação com conexões físicas. Usar um vSwitch dedicado para criar o link RP é outra otimização que pode evitar a perda de manutenções de atividades de HA devido à latência. Isso também está documentado no Guia de implantação de nuvem do Cisco Catalyst 9800-CL Wireless Controller. Portanto, o melhor é usar um link vSwitch dedicado para RP entre as VMs 9800-CL e garantir que nenhum outro tráfego interfira nele.

Implantações do Catalyst 9800 HA SSO Inside ACI

Quando um switchover ocorre em uma pilha de HA SSO, o chassi recém-ativo usa o mecanismo ARP gratuito (GARP) para atualizar o mapeamento MAC para IP na rede e certificar-se de que ele receba o tráfego dedicado ao controlador. Em particular, o chassi envia GARP para se tornar o novo "proprietário" do WMI e certificar-se de que o tráfego CAPWAP alcance o chassi apropriado.

O chassi que está se tornando ativo na verdade não está enviando um único GARP, mas um burst deles para garantir que qualquer dispositivo na rede atualize seu IP para o mapeamento MAC. Essa rajada pode sobrecarregar o recurso de aprendizagem ARP da ACI e, assim, quando a ACI é usada, é recomendável reduzir essa rajada o máximo possível na configuração do Catalyst 9800.

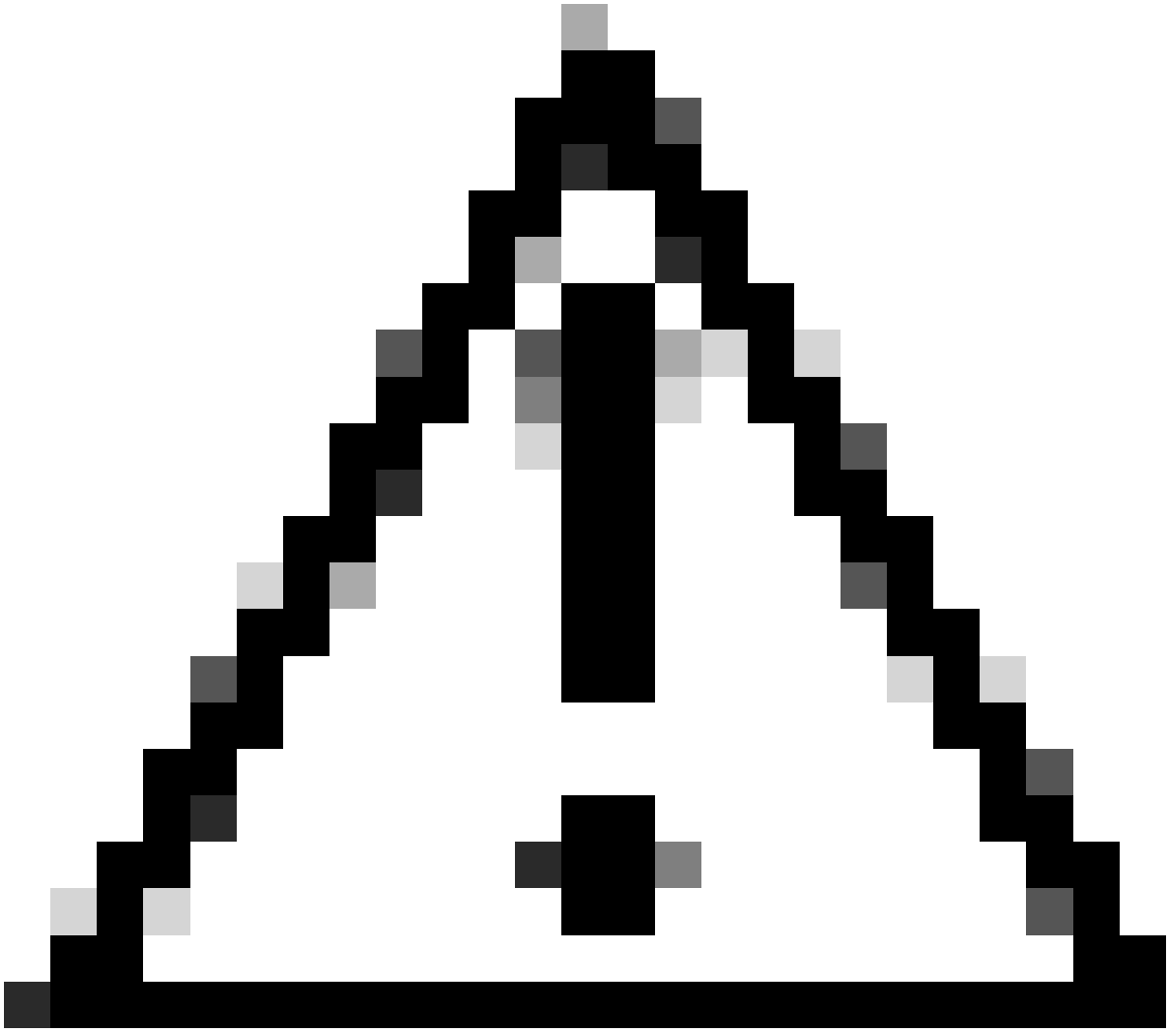
Do CLI:

```
WLC# configure terminal WLC(config)# redun-management garp-retransmit burst 0 interval 0
```

Junto com a limitação do burst GARP iniciado pelo 9800 durante um switchover, também é recomendável desativar o recurso fast switchover nesta plataforma. Quando o fast switchover é configurado, o controlador ativo envia uma notificação explícita ao controlador em standby, informando que ele está sendo desativado. Ao usar isso, o tráfego de intercalação pode existir (APs e clientes sendo descartados) entre as duas WLCs que formam a pilha de HA até que uma delas fique inativa. Assim, desativar esse recurso ajuda a estabilizar sua infraestrutura sem fio enquanto trabalha com implantações da ACI.

Do CLI:

```
WLC#configure terminal WLC(config)#no redun-management fast-switchover
```



Cuidado: lembre-se de que quando a alternância rápida é desativada, o controlador em espera depende exclusivamente das falhas de tempo limite de keepalive para detectar quando o controlador ativo foi desativado. Estes devem, portanto, ser configurados com o

---

maior cuidado.

Os detalhes sobre as considerações para implantações de HA SSO para o Catalyst 9800 dentro da rede ACI podem ser vistos na seção "Informações sobre a implantação da rede ACI no controlador" do Guia de Configuração de Software do Cisco Catalyst 9800 Series Wireless Controller.

Referências

- 17.3 Guia de HA SSO
- 17.6 Guia de HA SSO

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.