

Catalyst 9800에서 고가용성 SSO 구성 | 빠른 시작 설명서

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[네트워크 다이어그램](#)

[설정](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[원스톱 반사](#)

[명령 표시](#)

[기타 명령](#)

[자세히 보기](#)

[일반적인 시나리오](#)

[사용자 강제](#)

[액티브 유닛 제거됨](#)

[활성 Lost GW](#)

[추가 고려 사항](#)

[Catalyst 9800-CL용 HA SSO](#)

[Catalyst 9800 HA SSO Inside ACI 구축](#)

[참조](#)

소개

이 문서에서는 Catalyst 9800 WLC에서 RP+RMI 방식으로 SSO(High Availability Stateful Switchover)를 구성하는 방법을 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는

- Catalyst wireless 9800 구성 모델.
- HA SSO 가이드에서 설명하는 고가용성의 개념

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- C9800-CL v17.9.2

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

HA SSO 컨피그레이션에는 이 중 3개만 필요할 수 있지만, 여기서는 컨트롤러 GUI에 쉽게 액세스할 수 있도록 WMI(Wireless Management Interface)와 동일한 네트워크의 IP 주소 4개가 사용되었습니다.

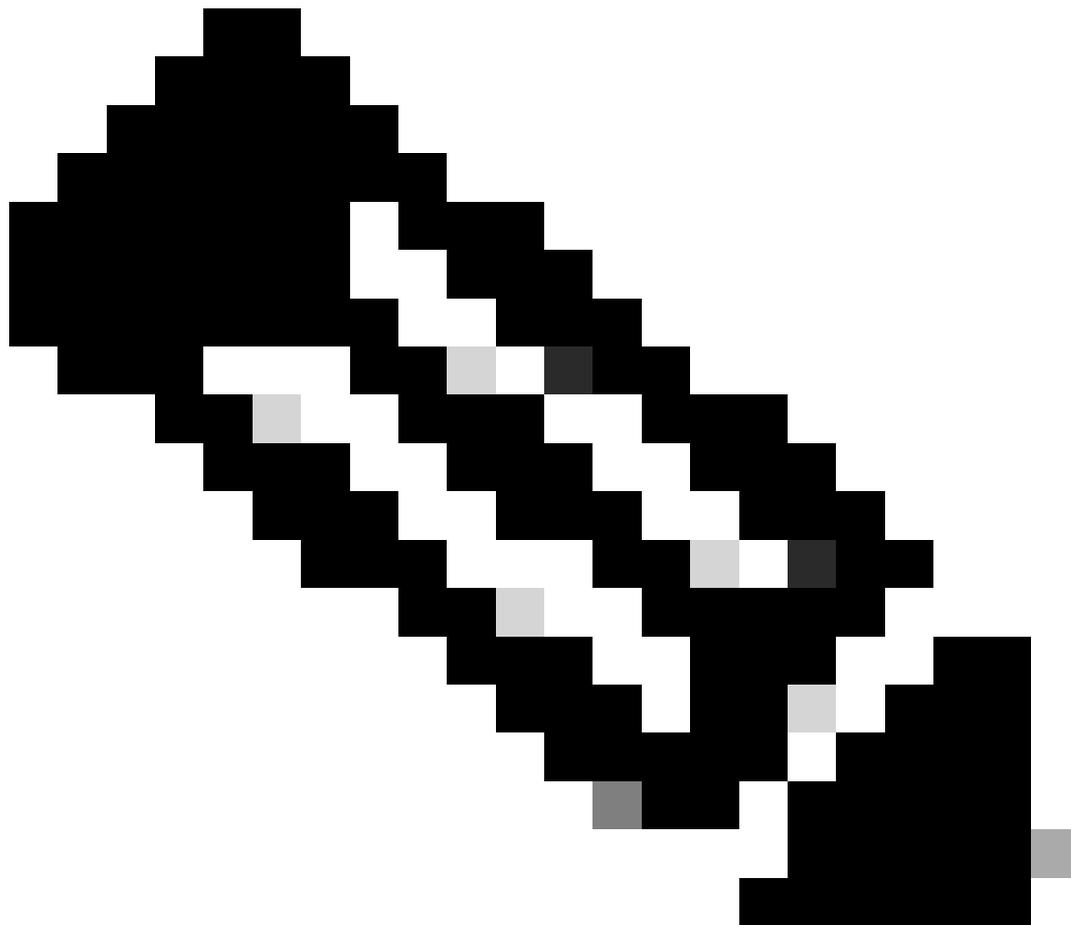
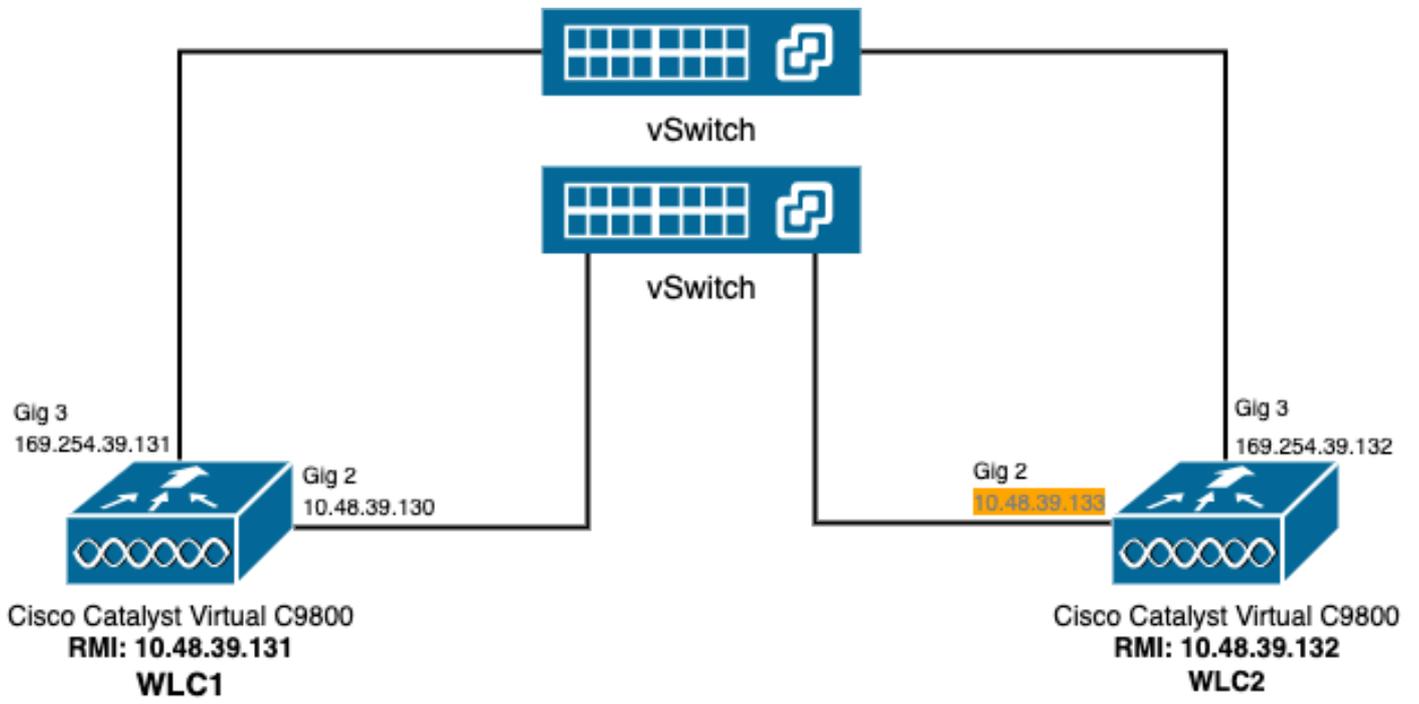
배경 정보

무선 컨트롤러의 고가용성 SSO 기능을 통해 액세스 포인트는 활성 무선 컨트롤러 및 활성 무선 컨트롤러와 CAPWAP 터널을 설정하여 AP 및 클라이언트 데이터베이스의 미러 복사본을 대기 무선 컨트롤러와 공유할 수 있습니다. 전환이 발생할 경우(즉, 액티브 컨트롤러가 실패하여 Standby 컨트롤러가 작동함), 연결된 AP가 검색 상태로 전환되지 않으며 클라이언트의 연결이 끊어지지 않습니다. AP와 활성 상태인 무선 컨트롤러 사이에는 한 번에 하나의 CAPWAP 터널만 유지됩니다.

두 유닛은 전용 RP 포트(또는 VM용 가상 인터페이스)를 통해 피어 연결을 형성하고, 두 컨트롤러 모두 관리 인터페이스에서 동일한 IP 주소를 공유합니다. RP 인터페이스는 런타임에 대량 컨피그레이션과 증분 컨피그레이션을 동기화하고 HA 쌍의 두 컨트롤러의 작동 상태를 확인하는 데 사용됩니다. 또한 RMI + RP를 사용할 경우 스탠바이 컨트롤러와 액티브 컨트롤러 모두 IP 주소가 할당된 RMI(Redundancy Management Interface)를 갖습니다. 즉, 게이트웨이 연결성을 보장하는 데 사용됩니다. 실행 상태인 액세스 포인트의 CAPWAP 상태도 활성 무선 컨트롤러에서 핫 스탠바이 무선 컨트롤러로 동기화됩니다. 그러면 활성 무선 컨트롤러에 장애가 발생할 때 액세스 포인트가 상태 전체를 전환할 수 있습니다. 활성 무선 컨트롤러에 장애가 발생할 경우 AP는 검색 상태로 전환되지 않으며, 대기 무선 컨트롤러가 활성 무선 컨트롤러로 작동하여 네트워크를 지원합니다.

구성

네트워크 다이어그램



참고: WLC2로 지정된 9800-CL 컨트롤러의 가상 인터페이스 GigabitEthernet 2에 할당된 임시 IP 주소가 주황색으로 강조 표시됩니다. 이 IP 주소는 WLC2의 WMI로 임시로 정의되며 HA SSO 컨피그레이션을 쉽게 하기 위해 이 인스턴스의 GUI에 액세스할 수 있습니다. HA SSO가 구성되면 단일 WMI만 HA SSO 컨트롤러 쌍에 사용되므로 이 주소가 해제됩니다.

설정

이 예에서 HA(High Availability) SSO(stateful switchover)는 동일한 Cisco IOS 소프트웨어 버전을 실행하는 두 개의 9800-CL 인스턴스 간에 구성됩니다. 이 인스턴스는 분리된 WMI와 액세스 가능한 GUI로 구성되었습니다.

- WLC1이라고 하는 첫 번째 IP 주소 10.48.39.130;
- 두 번째 IP 주소 10.48.39.133(WLC2라고 함).

이러한 IP 주소 외에 동일한 서브넷(및 VLAN)에 추가된 2개(10.48.39.131 및 10.48.39.132)가 사용되었습니다. 이는 각각 쉐시 1(WLC1) 및 쉐시 2(WLC2)에 대한 RMI(Redundancy Management Interface) IP 주소입니다.



참고: 두 컨트롤러 간에 HA가 구성되면 10.48.39.133이 해제되고 10.48.39.130이 내 구성의 유일한 WMI가 됩니다. 따라서 컨피그레이션 후에는 WMI 및 RMI 중 하나인 3개의 IP 주소만 사용됩니다.

두 디바이스가 HA 컨피그레이션을 시작하기도 전에 두 디바이스의 인터페이스 컨피그레이션은 이 예에서 제공한 것과 유사해야 합니다.

```
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
```

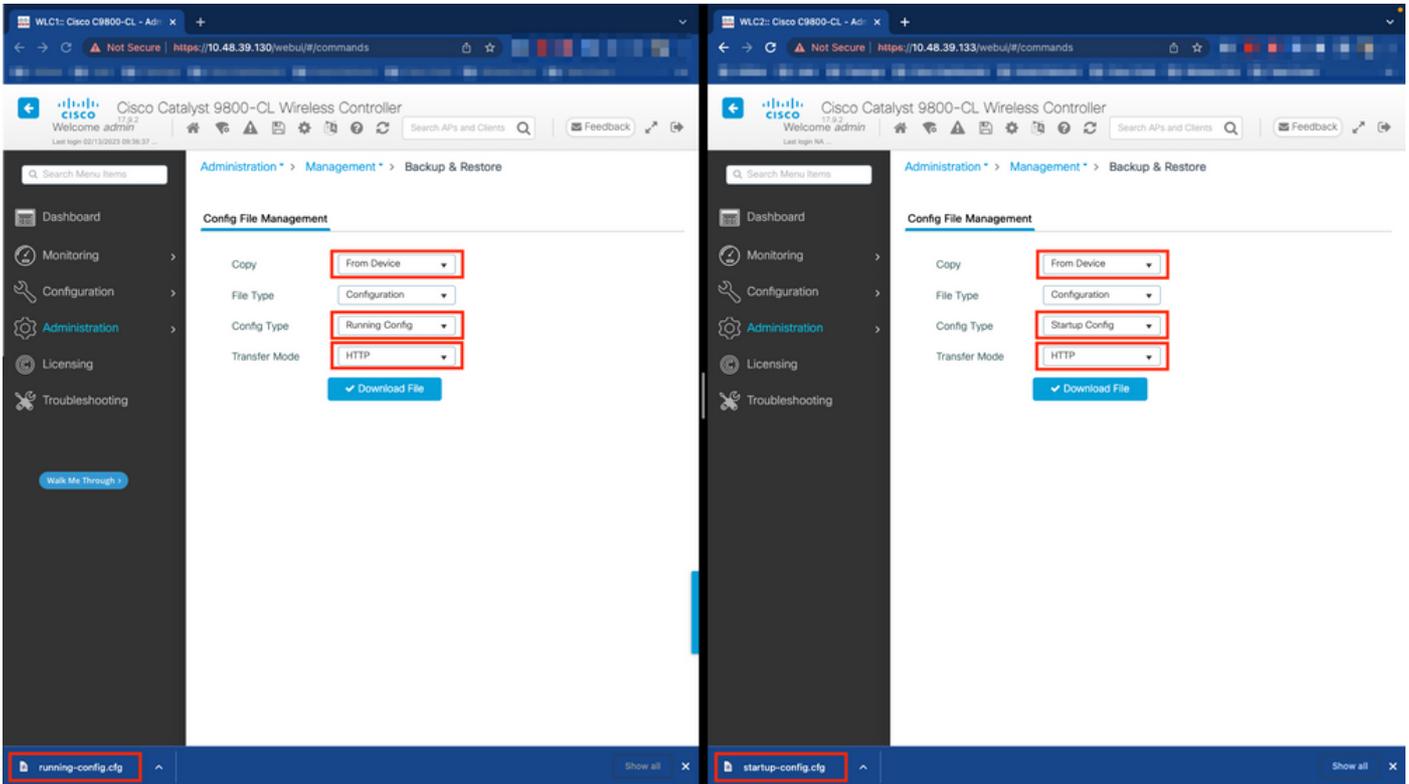
이 예에서 WLC1은 기본 컨트롤러(샐시 1)로 지정되고 WLC2는 보조 컨트롤러(샐시 2)로 지정됩니다. 즉, 2개의 컨트롤러로 구성된 HA 쌍에서 WLC1의 컨피그레이션을 사용하며 프로세스 후 WLC2 중 하나가 손실됩니다.

1단계(선택 사항) 컨트롤러의 Startup Config 및 Running Config 파일을 백업합니다.

잘못된 처리가 발생하여 컨피그레이션이 손실될 수 있습니다. 이를 방지하려면 HA 컨피그레이션에 사용되는 두 컨트롤러에서 시작 컨피그레이션과 실행 중인 컨피그레이션을 모두 백업하는 것이 좋습니다. 이 작업은 9800 GUI 또는 CLI를 사용하여 쉽게 수행할 수 있습니다.

GUI에서 다음과 같이 표시되어야 합니다.

9800 GUI의 *Administration* → *Management* → *Backup & Restore* 탭(스크린샷 참조)에서 컨트롤러에서 현재 사용 중인 시작 및 실행 중인 컨피그레이션을 다운로드할 수 있습니다.



이 예에서는 시작(왼쪽) 및 컨피그레이션(오른쪽) 모두 HTTP를 통해 WLC의 GUI에 액세스하는 데 사용되는 브라우저를 호스팅하는 디바이스에서 직접 다운로드됩니다. Transfer Mode 필드를 사용하면 백업할 파일의 전송 모드 및 대상을 쉽게 조정할 수 있습니다.

CLI에서:

```
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)
```

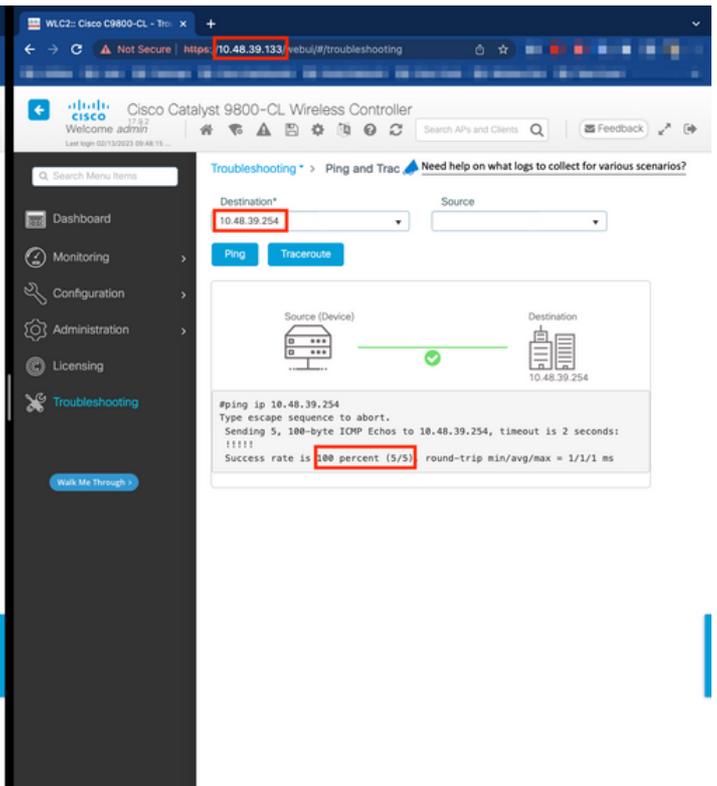
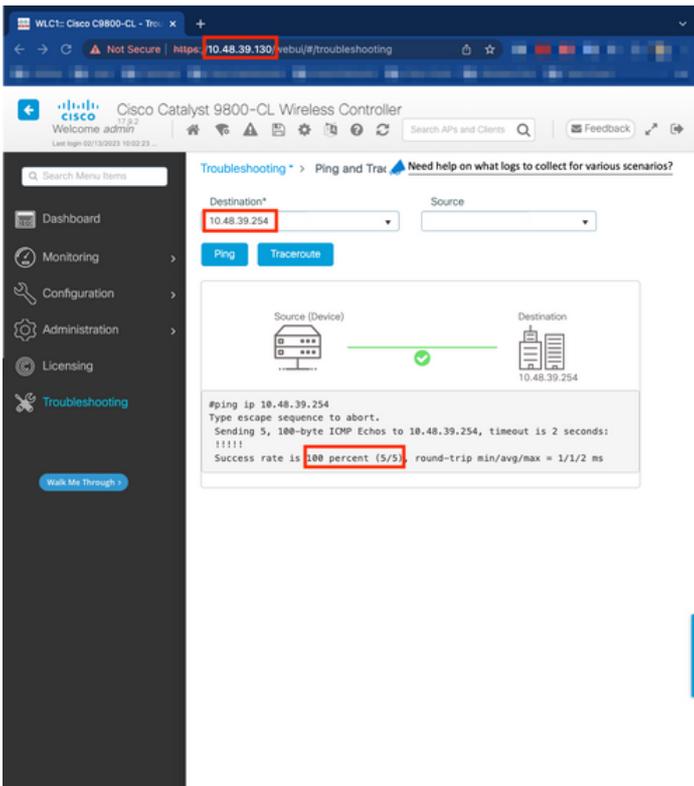
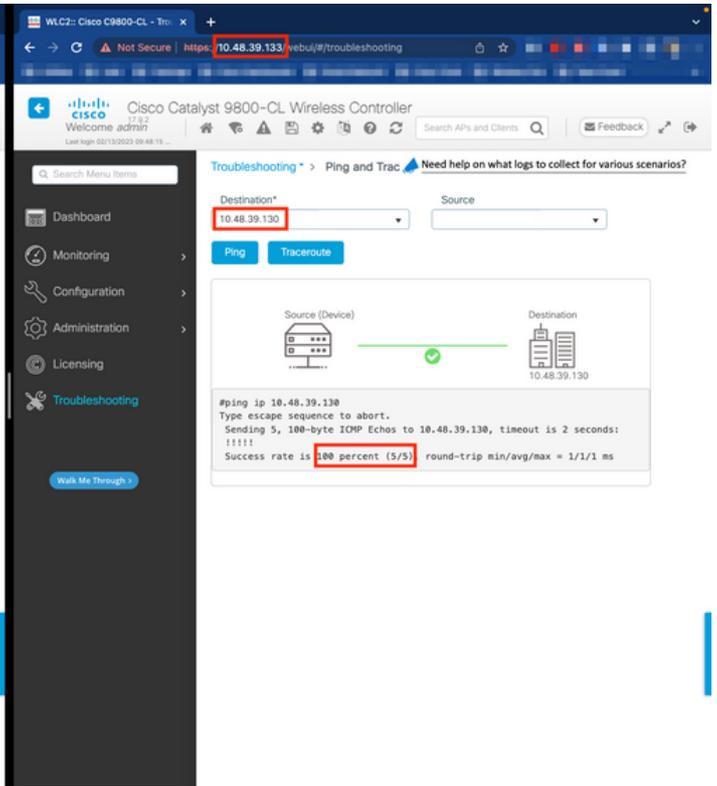
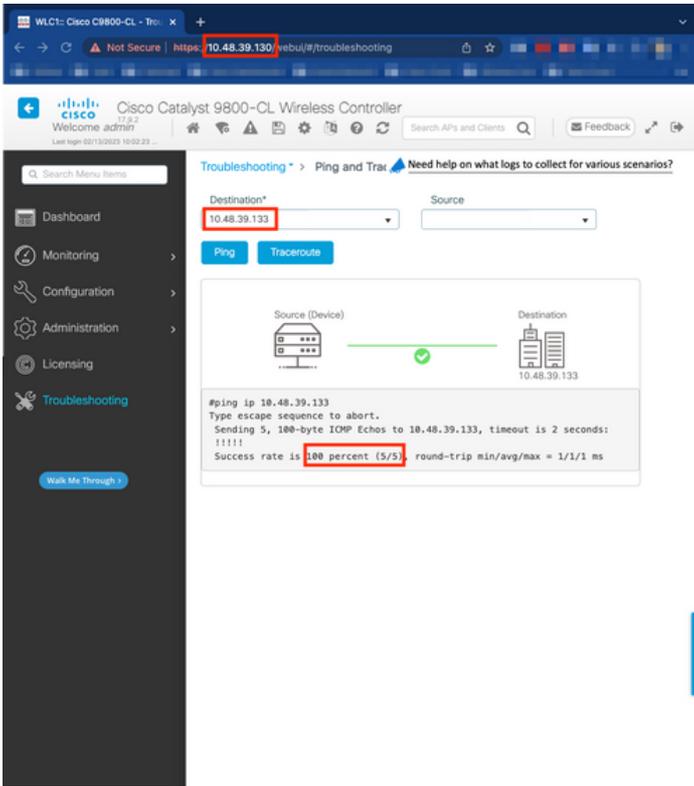
를 시작<SERVER-IP> 실행 중인 컨피그레이션 파일이 복사되는 TFTP 서버 IP로 교체합니다.

2단계. (선택 사항) 네트워크 연결을 확인합니다.

두 WLC GUI 또는 CLI에서 간단한 연결 테스트, 즉 두 디바이스에서 게이트웨이를 ping하고 디바이스 간에 ping을 수행할 수 있습니다. 이렇게 하면 두 컨트롤러 모두 HA를 구성하는 데 필요한 연결을 갖게 됩니다.

GUI에서 다음과 같이 표시되어야 합니다.

다음 그림에 표시된 것처럼 컨트롤러 자체와 각 WLC와 네트워크 게이트웨이 간의 연결을 테스트하기 위해 9800 GUI의 *Troubleshooting*(트러블슈팅) 탭에 있는 *Ping and Traceroute* 툴을 사용할 수 있습니다.



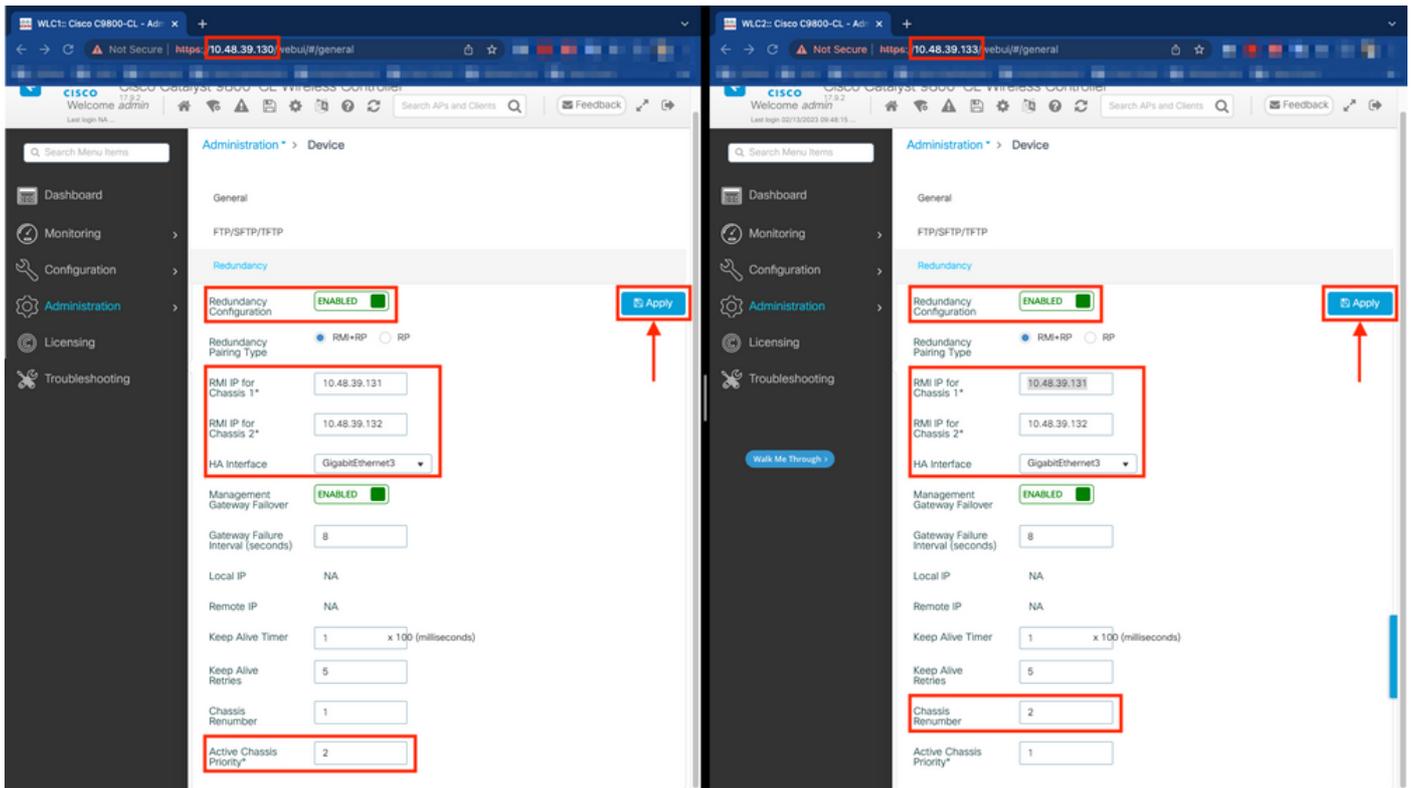
CLI에서:

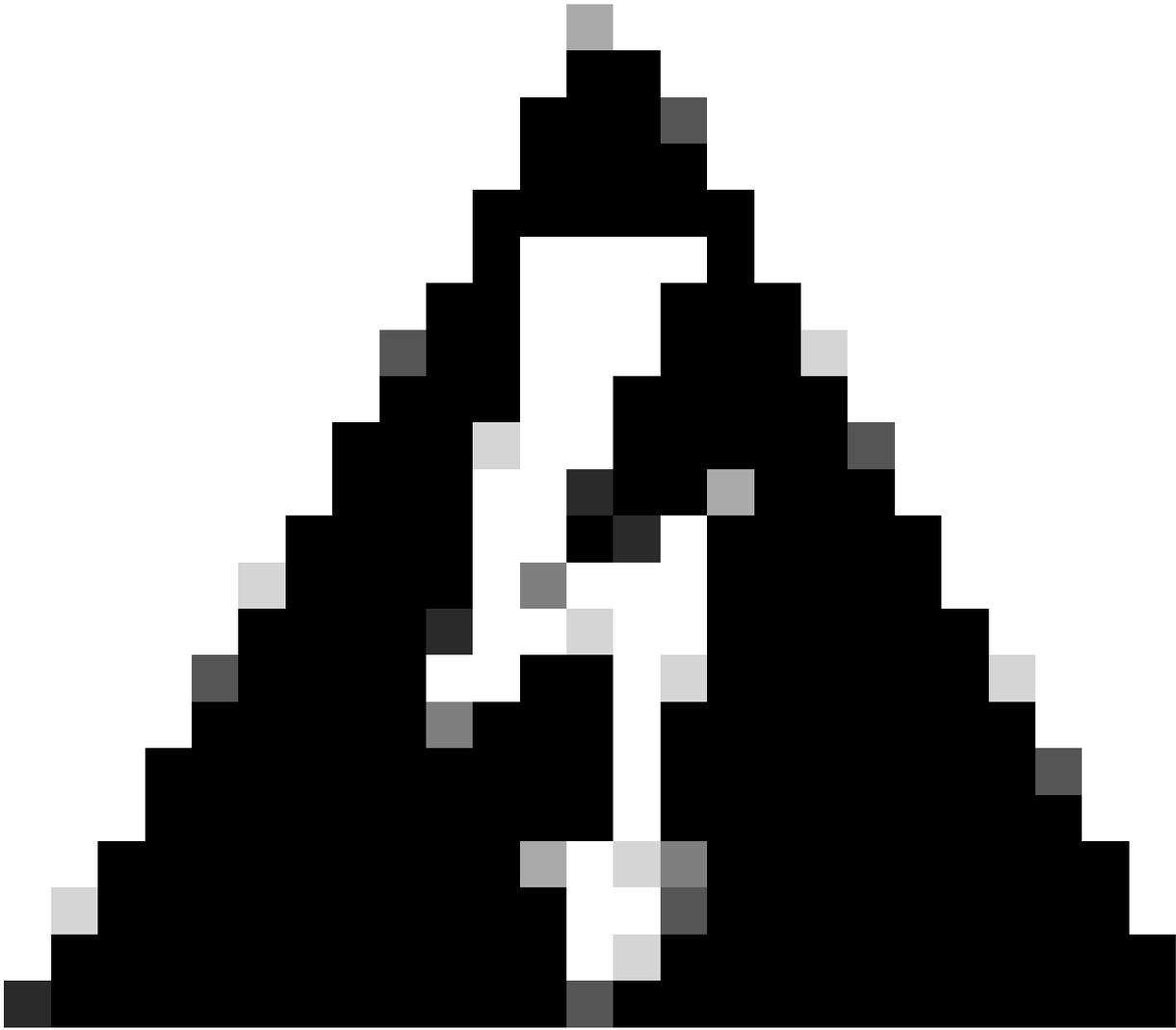
WLCx#ping 10.48.39.133 Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to 10.48.39.133, t

3단계. RMI + RP 페어링 유형으로 이중화를 구성합니다.

각 디바이스 간의 연결이 보장되므로 컨트롤러 간에 이중화를 구성할 수 있습니다. 이 스크린샷은 9800 GUI의 Administration→

Device 페이지의 Redundancy(이중화) 탭에서 컨피그레이션을 수행하는 방법을 보여줍니다.





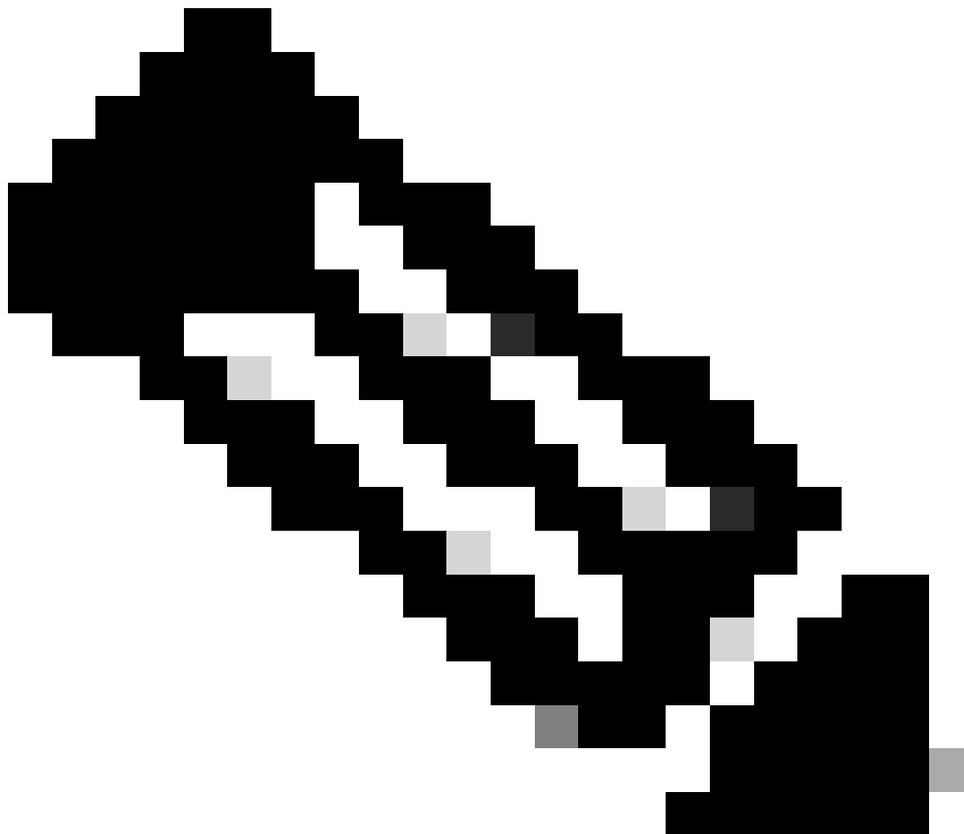
경고: 이 예에서는 WLC1이 기본 컨트롤러로 지정되었습니다. 이는 해당 컨피그레이션이 다른 컨트롤러에 복제되었음을 의미합니다. HA 쌍에서 적절한 컨피그레이션을 사용하고 일부를 잃지 않도록 적절한 새시 우선순위/번호 재설정을 적용해야 합니다.

이제 구성된 필드와 그 용도를 살펴보겠습니다

- **이중화 컨피그레이션:** WLC 간 이중화를 사용하려면 이 옵션을 활성화해야 합니다.
- **이중화 페어링 유형:** 이 가이드에서는 RMI 컨피그레이션을 사용하는 HA SSO를 다루므로, 이중화 관리 인터페이스와 이

중화 포트를 모두 사용하여 구성된 페어링 유형은 RMI + RP여야 합니다. 이중화 포트만 사용하여 이중화를 구성하도록 선택할 수도 있습니다. 그러나 RP만 선택한 경우 게이트웨이의 연결성을 확인하지 않으며 이중화 WLC 상태만 확인합니다

- **RMI IP for Chassis 1/2:** 이 필드는 제공된 IP 주소를 두 인스턴스 모두에 대해 지정된 이중화 인터페이스에 할당합니다. 이 예에서 샤프 1과 2의 두 RMI IP는 이전에 설명되고 [네트워크 다이어그램](#)에 표시된 대로 각각 10.48.39.131 및 10.48.39.132로 [구성되었습니다](#).
- **HA 인터페이스:** 가상 어플라이언스를 사용할 때 하이퍼바이저의 vNIC(가상 네트워크 인터페이스 카드)와 가상 머신의 네트워크 인터페이스 간의 매핑은 다른 방법으로 구성할 수 있습니다. 따라서 이중화에 사용되는 인터페이스는 Cisco Catalyst 9800-CL에 맞게 구성할 수 있습니다. 여기서는 9800-[CL](#) 구축 가이드에서 권장하는 대로 [GigabitEthernet 3](#)을 사용했습니다.



참고: 물리적 C9800 어플라이언스를 사용할 경우 HA 및 RP에서 사용되는 인터페이스는 기본 인터페이스이며 구성할 수 없습니다. 실제로 하드웨어 9800 WLC는 네트워크 이중화 인터페이스와 분리된 전용 이중화 인터페이스를 갖추고 있습니다.

- **관리 게이트웨이 장애 조치:** HA SSO 컨피그레이션 가이드에 자세히 설명된 대로 이 이중화 방법은 게이트웨이에 ICMP(Internet Control Message Protocol) ping을 주기적으로 전송하여 수행하는 기본 게이트웨이 확인을 구현합니다. 액티브 컨트롤러와 스탠바이 컨트롤러 모두 RMI IP를 이러한 확인의 소스 IP로 사용합니다. 이 메시지는 1초 간격으로 전송됩니다.

- **Gateway Failure Interval(게이트웨이 실패 간격):** 이 값은 게이트웨이가 연결 불가로 선언되기 전에 게이트웨이 검사가 연속적으로 실패해야 하는 시간을 나타냅니다. 기본적으로 이는 8초로 구성됩니다. 게이트웨이 검사는 매초마다 전송되므로, 이는 게이트웨이에 도달하는 데 연속적으로 8번 실패했음을 나타냅니다.

- **로컬/원격 IP:** 새시 1 및 2에 대해 구성된 RP IP입니다. 이러한 IP 주소는 169.254.x.x로 자동 생성되며, 여기서 x.x는 관리 인터페이스의 마지막 두 옥텟에서 파생됩니다.

- **Keep Alive Timer:** HA SSO 컨피그레이션 가이드에 자세히 설명된 대로, 활성 및 대기 새시는 서로 keep-alive 메시지를 전송하여 둘 다 계속 사용할 수 있도록 합니다. keep alive 타이머는 각 새시 간에 2개의 keepalive 메시지 전송을 분리하는 시간입니다. 기본적으로 keep-alive 메시지는 100ms마다 전송됩니다. VM 인프라에서 적은 지연(스냅샷 등..)이 발생할 때마다 악의적인 전환을 방지하려면 9800-CL로 이 값을 늘리는 것이 좋습니다.

- **Keep Alive Retries(킵얼라이브 재시도):** 이 필드는 피어가 다운되었다고 주장하기 전에 피어 킵얼라이브 재시도 값을 구성합니다. keep-alive 타이머와 재시도된 기본값을 모두 사용할 경우, 100ms 시간 간격으로 전송된 5개의 keep alive 메시지가 응답하지 않은 상태로 남아 있으면(즉, 이중화 링크가 500ms 동안 다운된 경우) 피어가 다운된 것입니다.

- **새시 번호 다시 매기기:** 어플라이언스에서 사용해야 하는 새시 번호(1 또는 2)입니다.

WLC2(10.48.39.133)에서는 새시의 번호가 2로 다시 지정됩니다. 기본적으로 새시 번호는 1입니다. RP 포트의 IP 주소는 RMI에서 파생됩니다. 새시 번호가 두 컨트롤러에서 동일하면 로컬 RP 포트 IP 파생이 동일하며 검색이 실패합니다. 이러한 활성-활성 시나리오를 방지하려면 새시의 번호를 다시 지정합니다.

- **활성 새시 우선순위:** HA 쌍에서 사용해야 하는 컨피그레이션을 정의하는 데 사용되는 우선순위입니다. 우선순위가 가장 높은 어플라이언스는 다른 어플라이언스에 복제되는 어플라이언스입니다. 따라서 우선순위가 가장 낮은 새시의 컨피그레이션

은 손실됩니다.

WLC1(10.48.39.130)에서 활성 새시 우선순위가 2로 설정되었습니다. 이는 이 새시가 생성된 HA 쌍에서 활성 새시로 선택되었는지(따라서 해당 컨피그레이션이 사용되었는지) 확인하기 위한 것입니다.

이러한 컨피그레이션이 완료되면 Apply(적용) 버튼을 사용하여 컨트롤러에 컨피그레이션을 적용합니다.

CLI에서

먼저 두 디바이스에서 RMI를 구성하는 데 사용되는 가상 인터페이스에서 보조 IP 주소를 구성합니다.

```
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
```

그런 다음 두 디바이스 모두에서 이중화를 활성화합니다

```
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
```

WLC1이 기본 컨트롤러가 되는 것과 같은 새시 우선순위를 구성합니다

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

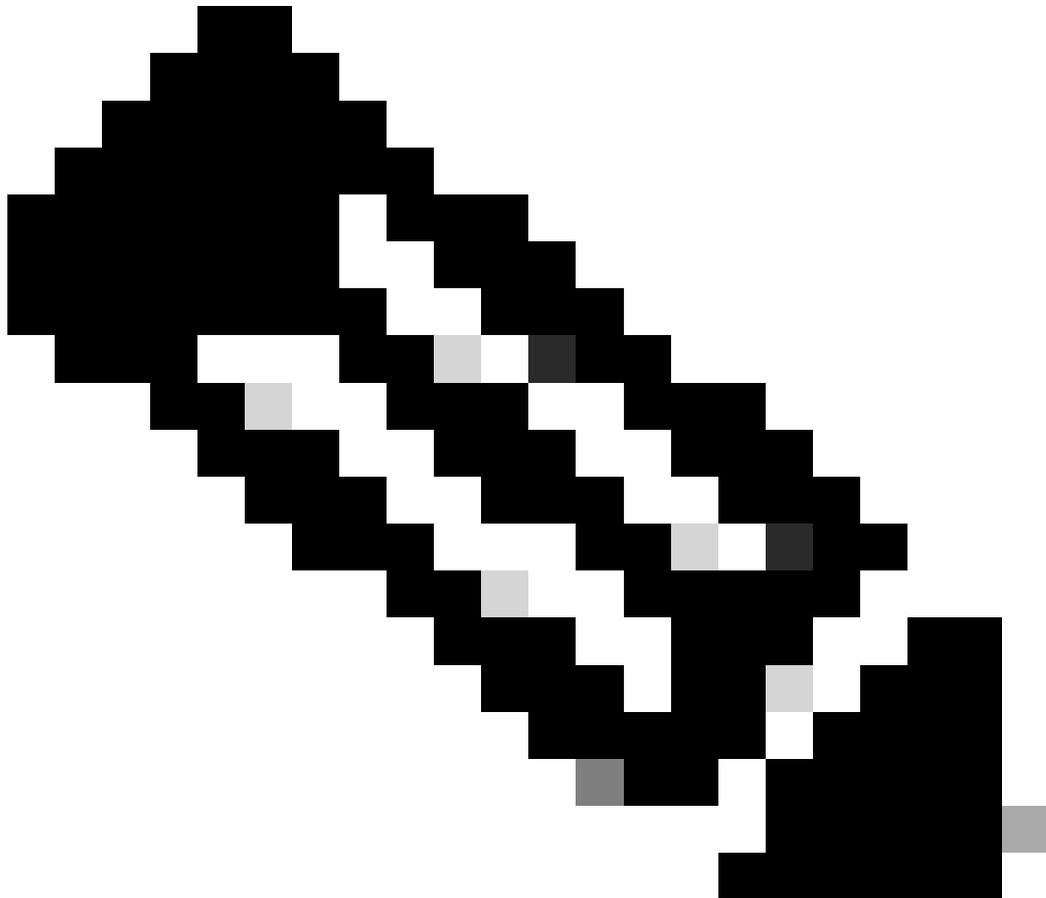
보조 컨트롤러가 되는 WLC2의 새시 번호 다시 매기기

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

마지막으로, 두 디바이스 모두에서 RMI를 구성합니다

```
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
```



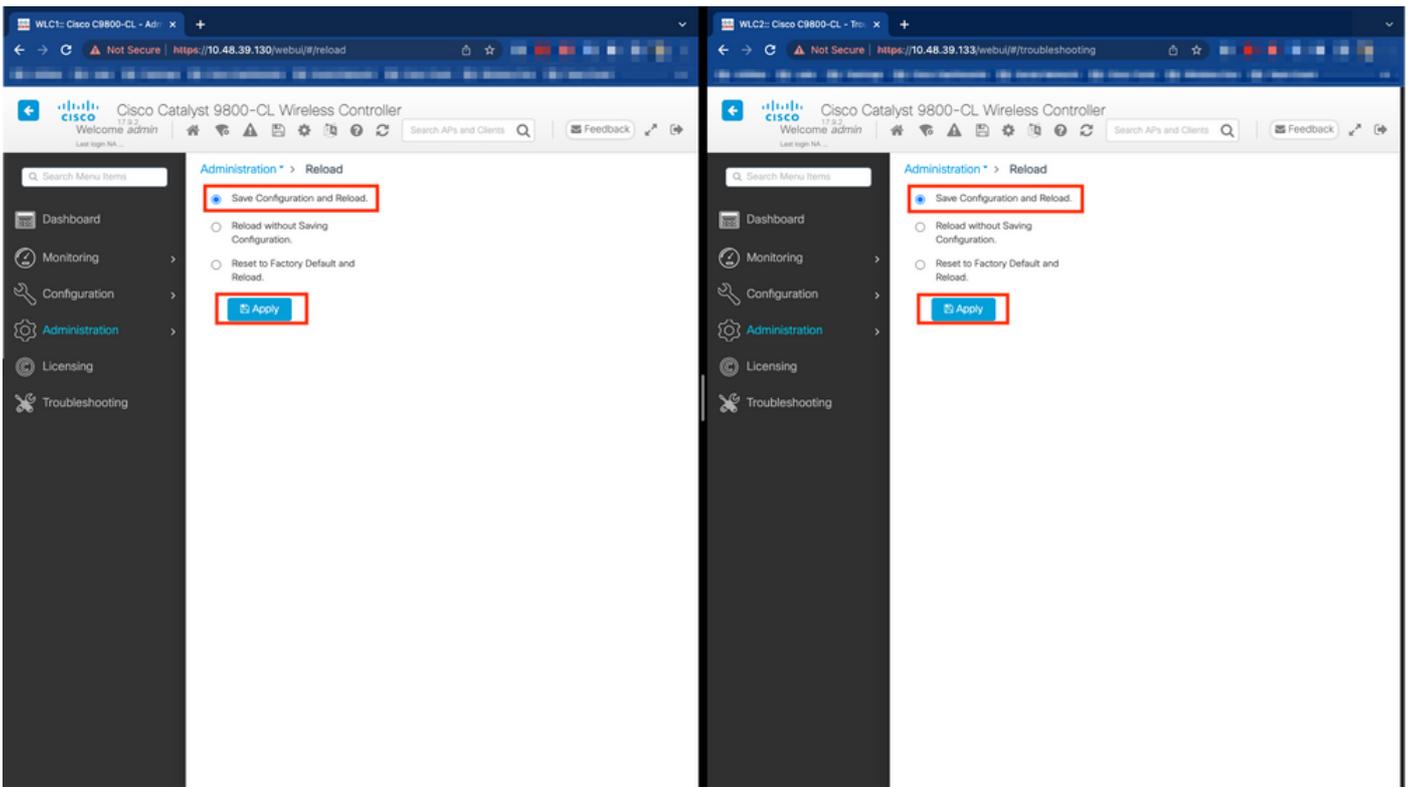
참고: GUI 컨피그레이션의 경우, 가상 Catalyst 9800에서는 컨트롤러에서 사용하는 인터페이스를 사용 가능한 인터페이스 중에서 선택해야 합니다. 권장되는 대로, GigabitEthernet 3가 여기에서 사용되며 이 명령 덕분에 chassis redundancy ha-interface GigabitEthernet 3 구성됩니다. 이 명령은 실행 중인 컨피그레이션의 일부가 아니지만 HA에서 사용하는 인터페이스는 인스턴스 ROMMON 환경 변수에 표시됩니다. 이러한 항목은 명령을 사용하여 확인할 수 show romvar 있습니다.

4단계. 컨트롤러 다시 로드

HA 쌍을 구성하고 컨피그레이션을 적용하려면 3단계에서 구성한 컨피그레이션을 저장한 후 두 컨트롤러를 동시에 다시 로드해야 합니다.

GUI에서:

두 GUI의 Administration Reload(관리 다시 로드) 페이지를 사용하여 이 스크린샷과 같이 컨트롤러를 다시 시작할 수 있습니다.



CLI에서:

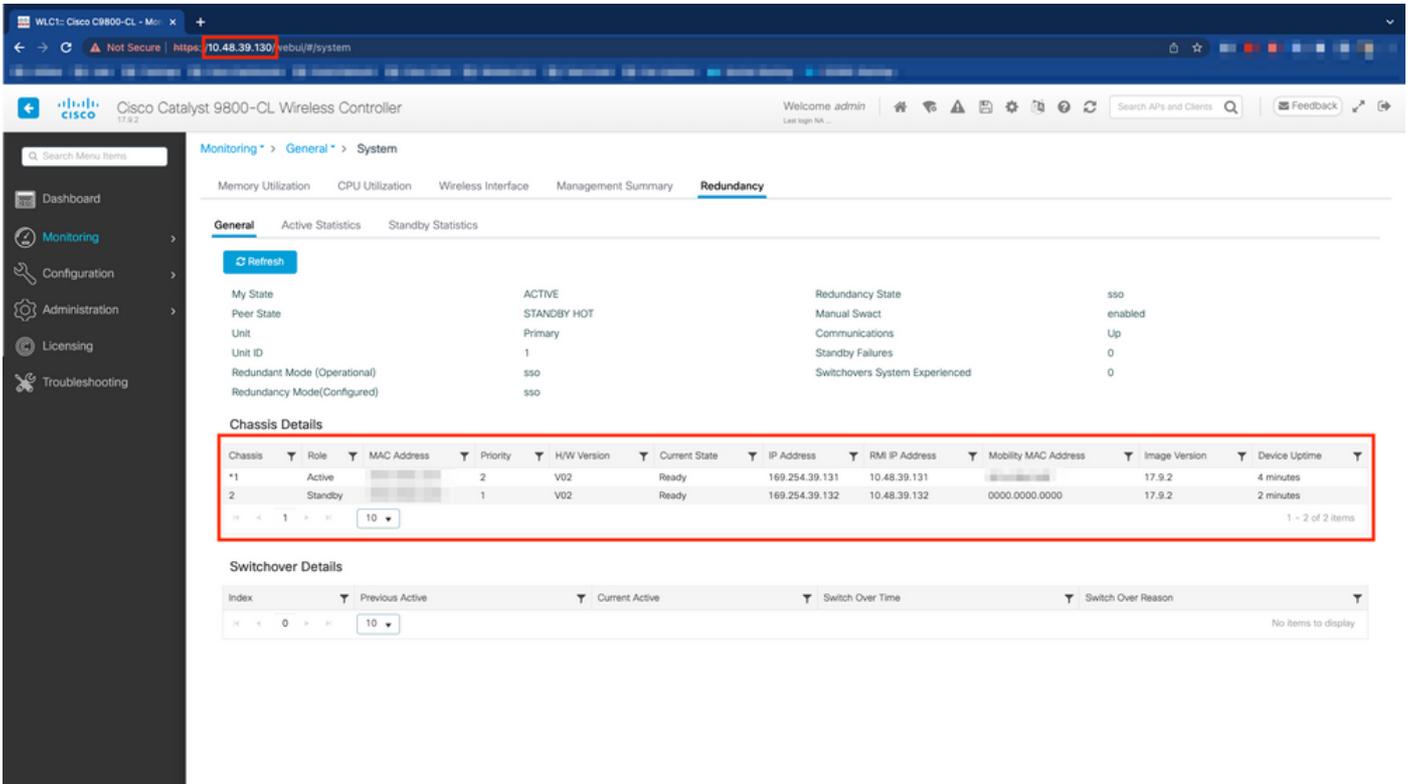
WLCx#reload Reload command is being issued on Active unit, this will reload the whole stack Proceed with

다음을 확인합니다.

HA 쌍의 두 컨트롤러가 서로를 검색하고 원하는 HA 쌍을 생성하면, 하나의 컨트롤러(기본)가 GUI 또는 CLI에서 두 새시를 모니터링할 수 있습니다.

GUI에서:

9800 GUI에서 이중화 컨피그레이션을 모니터링하려면 이 스크린샷에 표시된 대로 Monitoring(모니터링) > General(일반) > System(시스템) 페이지에서 Redundancy(이중화) 탭으로 이동합니다.



CLI에서:

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

WLC#show redundancy Redundant System Information : ----- Available system uptime

문제 해결

원스톱 반사

일반에는 HA 쌍의 HA 장애 조치와 현재 상태를 제대로 파악할 수 있는 명령이 포함되어 있지 show tech wireless 않습니다. 단일 작업에서 대부분의 HA 관련 명령을 사용하려면 이 명령을 수집합니다.

WLC#show tech wireless redundancy

명령 표시

이중화 포트의 상태에는 이러한 명령을 사용할 수 있습니다.

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

이 명령은 첫 번째 단계 트러블슈팅으로 유용한 새시 번호 및 이중화 포트 상태를 표시합니다.

keepalive 포트에서 keepalive 카운터를 확인하려면 다음 명령을 사용할 수 있습니다.

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

기타 명령

이러한 명령을 사용하여 컨트롤러의 이중화 포트에서 패킷 캡처를 수행할 수 있습니다

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

이러한 명령을 사용하여 만든 캡처는 컨트롤러bootflash: 의 이름 아래에 저장됩니다haIntCaptureLo.pcap.

이 명령을 사용하여 이중화 포트에서 keepalive 테스트를 실행할 수도 있습니다.

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

자세히 보기

실제 컨피그레이션이 변수에 어떻게 반영되는지 보여 주는 ROMMON Variables 컨피그레이션을 보려면 이 명령을 사용할 수 있습니다.

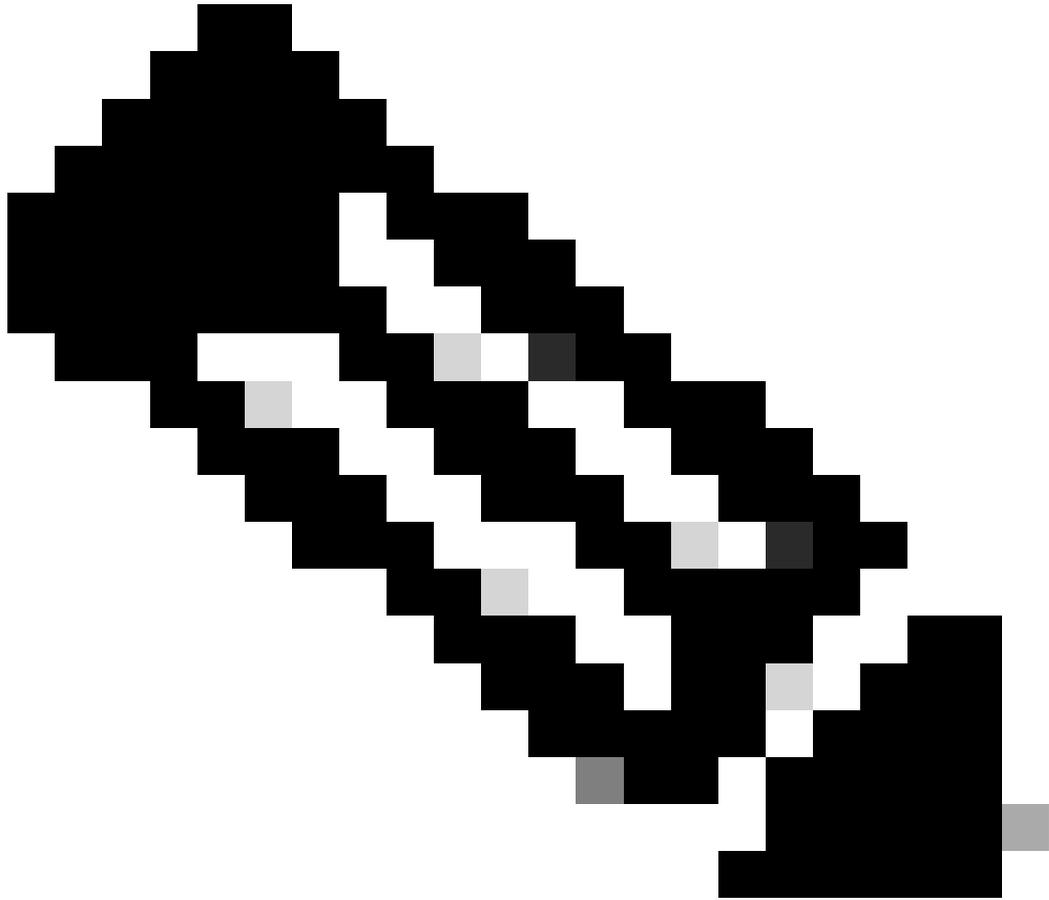
```
WLC#show romvar ROMMON variables: MCP_STARTUP_TRACEFLAGS = 00000000:00000000 SWITCH_NUMBER = 2 CONFIG_F
```

이 명령은 새시의 우선순위, RMI 및 RP 세부사항, 피어 시간 초과 및 더 유용한 세부사항을 표시합니다.

또한 WLC에서 HA SSO를 실행하는 프로세스(stack_mgr 및 rif_mgr)를 모니터링할 수 있습니다.

이렇게 하려면 명령을 사용하여 텍스트 파일에 대한 always on 추적을 수집합니다. 여기서 시간 매개변수를 조정하여 문제를 해결할 수 있습니다.

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



참고: 컨트롤러가 스탠바이 상태로 작동하는 동안 스탠바이 WLC의 서비스 포트가 비활성화되고 연결할 수 없다는 점에 유의해야 합니다.

일반적인 시나리오

사용자 강제

전환 기록을 보면 사용자가 명령을 사용하여 컨트롤러 간 전환을 시작했을 때 나타나는 "사용자 강제"를 볼 수 redundancy force-switchover 있습니다.

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

액티브 유닛 제거됨

전환 내역을 보면 두 컨트롤러 간 이중화 포트에서 통신 손실을 가리키는 "액티브 유닛이 제거됨"을 확인할 수 있습니다.

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

두 컨트롤러 간의 링크가 중단될 경우 이러한 현상이 발생할 수 있지만, 하나의 WLC 유닛이 갑자기 중단되거나(정전) 충돌할 경우에도 발생할 수 있습니다. 두 WLC를 모니터링하여 예기치 않은 충돌/재부팅을 나타내는 시스템 보고서가 있는지 확인하는 것이 좋습니다.

활성 Lost GW

전환 이력을 살펴보면 RMI 포트에서 게이트웨이와의 통신 손실을 가리키는 "Active lost GW"가 표시됩니다.

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

활성 컨트롤러와 해당 게이트웨이 간의 링크가 중단될 경우 이러한 현상이 발생합니다.

추가 고려 사항

Catalyst 9800-CL용 HA SSO

가상 환경에서는 레이턴시가 도입되는 것을 받아들여야 하며, 레이턴시는 HA가 적절히 용인하는 것이 아닙니다. HA SSO는 새시 결합을 빠르고 효율적으로 탐지하는 경향이 있으므로 이는 합법적입니다. 이를 위해 각 새시는 RP 및 RMI 링크의 킥얼라이브와 RMI의 게이트웨이를 향하는 ping을 사용하여 다른 새시의 상태를 확인합니다(WMI 중 하나가 동일해야 함). 이러한 사항 중 하나라도 누락된 경우, 스택은 [HA SSO 가이드](#)의 "시스템 및 네트워크 결합 처리"에 설명된 대로 증상에 따라 [반응합니다](#).

Catalyst 9800의 가상 HA SSO 스택으로 작업할 때 RP 링크를 통해 킥얼라이브가 누락되어 스위치오버가 발생하는 것이 일반적입니다. 이는 가상화된 환경에 의해 도입된 레이턴시 때문일 수 있습니다.

HA SSO 스택에서 RP keepalive 삭제로 인한 문제를 확인하려면 stack/rif 관리자 로그를 사용할 수 있습니다.

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

두 새시가 모두 작동 중이면 스위치오버는 RP의 삭제에 따른 "듀얼 액티브 탐지"를 생성합니다.

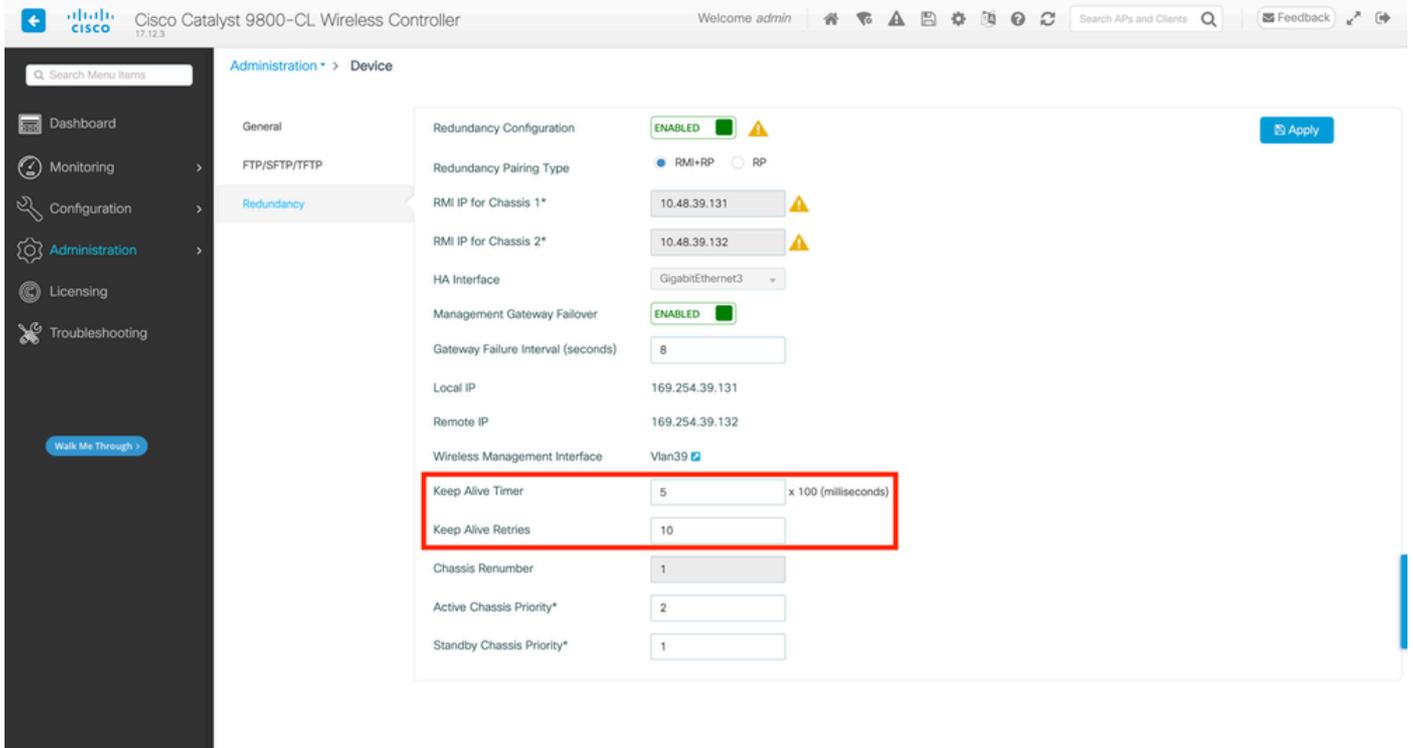
이러한 상황에서는 이러한 불필요한 전환을 방지하기 위해 HA 킥얼라이브 매개변수를 변경하는 것이 도움이 될 수 있습니다. 두 가지 매개변수를 구성할 수 있습니다.

- **Keep Alive Timer:** 각 새시 간 2개의 keepalive 메시지 전송을 분리하는 시간입니다.
- **Keep Alive Retries(킥얼라이브 재시도):** 피어를 다운으로 선언하기 위해 누락해야 하는 킥얼라이브 횟수입니다.

기본적으로 keep alive 타이머는 1ms로 설정되고 재시도는 5로 설정됩니다. 이는 RP 링크에서 keepalive 5ms가 누락되고 나면 전환이 발생할 수 있습니다. 이러한 값은 가상 구축에 비해 너무 낮을 수 있습니다. RP 킥얼라이브가 누락되어 반복적인 전환이 발생하는 경우, 이러한 매개변수를 늘려 스택을 안정화해 보십시오.

GUI에서:

9800 GUI에서 HA SSO 킥얼라이브 매개변수를 모니터링하거나 수정하려면 이 스크린샷에 표시된 대로 Administration(관리) > Device(디바이스) 페이지에서 Redundancy(이중화) 탭으로 이동합니다.



CLI에서:

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

이러한 매개변수의 컨피그레이션과 함께 또 다른 최적화는 HA SSO 스택의 이러한 동작에 도움이 될 수 있습니다. 물리적 어플라이언스의 경우 하드웨어는 일반적으로 단일 와이어를 사용하여 새시를 다른 새시에 연결할 수 있습니다. 가상 환경에서 각 새시에 대한 RP 포트의 상호 연결은 vSwitch(가상 스위치)를 통해 이루어져야 하는데, 이 경우 물리적 연결에 비해 레이턴시가 다시 발생할 수 있습니다. 전용 vSwitch를 사용하여 RP 링크를 생성하는 것은 레이턴시로 인한 HA 킥얼라이브의 손실을 방지할 수 있는 또 다른 최적화입니다. 이 내용은 [Cisco Catalyst 9800-CL Wireless Controller for Cloud Deployment Guide](#)에도 설명되어 있습니다. 따라서 가장 좋은 방법은 9800-CL VM 간의 RP 링크에 전용 vSwitch를 사용하고 다른 트래픽이 이를 방해하지 않도록 하는 것입니다.

Catalyst 9800 HA SSO Inside ACI 구축

HA SSO 스택에서 전환이 발생하면 새로 활성화된 새시는 GARP(Gratuitous ARP) 메커니즘을 사용하여 네트워크에서 MAC-IP 매핑을 업데이트하고 컨트롤러 전용 트래픽을 수신하는지 확인합니다. 특히 새시는 GARP를 전송하여 WMI의 새 "소유자"가 되고 CAPWAP 트래픽이 적절한 새시에 도달하는지 확인합니다.

새시가 활성화된다는 것은 실제로 단일 GARP를 보내는 것이 아니라, 네트워크의 모든 디바이스가 IP를 MAC으로 업데이트하는지 확인하기 위해 GARP를 버스트하는 것입니다. 이 버스트는 ACI의 ARP 학습 기능을 압도할 수 있으므로 ACI를 사용할 경우 Catalyst 9800 구성에서 이 버스트를 최대한 줄이는 것이 좋습니다.

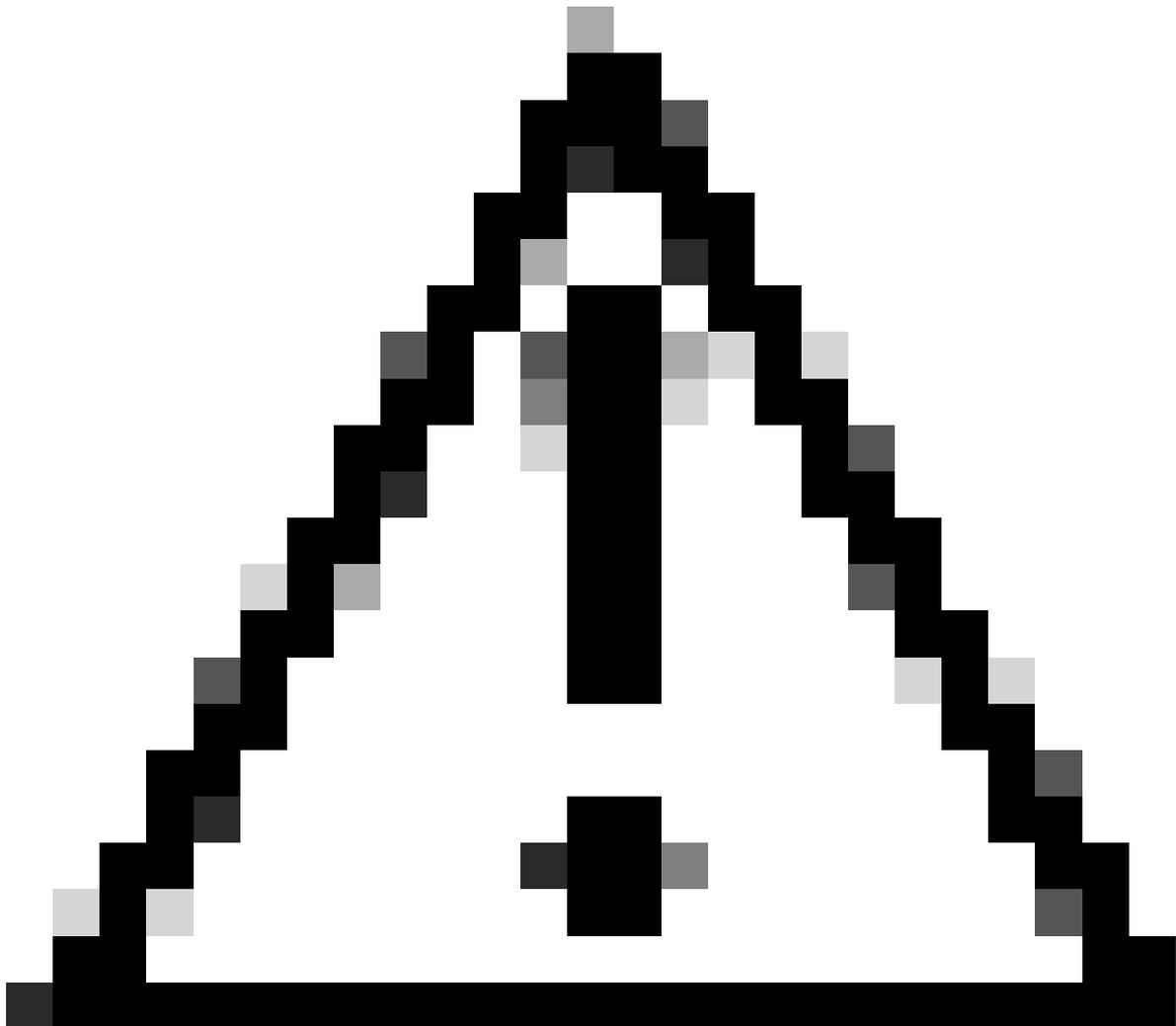
CLI에서:

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

전환 중에 9800에서 시작된 GARP 버스트를 제한하는 것과 더불어 이 플랫폼에서 빠른 전환 기능을 비활성화하는 것이 좋습니다. 빠른 전환이 구성된 경우 활성 컨트롤러는 대기 컨트롤러에 작동 중임을 알리는 명시적 알림을 보냅니다. 이를 사용하는 동안 HA 스택을 구성하는 두 WLC 사이에 인터리빙 트래픽이 존재할 수 있습니다(AP 및 클라이언트 삭제 중). 두 WLC 중 하나가 중단될 때까지 말입니다. 따라서 이 기능을 비활성화하면 ACI 구축에서 작업하는 동안 무선 인프라를 안정화하는 데 도움이 됩니다.

CLI에서:

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



주의: 빠른 전환이 비활성화된 경우 스탠바이 컨트롤러는 활성 컨트롤러의 작동이 중지된 시점을 탐지하기 위해 keepalive 시간 초과 실패에만 의존합니다. 따라서 최대한 신중하게 구성해야 합니다.

ACI 네트워크 내부에서 Catalyst 9800을 구축할 때 고려해야 할 사항에 대한 자세한 내용은 [Cisco Catalyst 9800 Series Wireless Controller Software Configuration Guide](#)의 "Information About Deploying ACI Network in Controller" 섹션에서 확인할 수 있습니다.

참조

- [17.3 HA SSO 가이드](#)
- [17.6 HA SSO 가이드](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.