

Catalyst 스위치 네트워크의 HSRP 문제 해결

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[HSRP의 이해](#)

[배경 정보](#)

[기본 작업](#)

[HSRP 용어](#)

[HSRP 주소 지정](#)

[HSRP 라우터 통신](#)

[토큰 링을 제외한 모든 미디어에서 HSRP 대기 IP 주소 통신](#)

[ICMP 리디렉션](#)

[HSRP 기능 매트릭스](#)

[HSRP 기능](#)

[패킷 형식](#)

[HSRP 상태](#)

[HSRP 타이머](#)

[HSRP 이벤트](#)

[HSRP 작업](#)

[HSRP 상태 테이블](#)

[패킷 플로우](#)

[라우터 A 설정\(활성 라우터\)](#)

[라우터 B 설정\(대기 라우터\)](#)

[HSRP 사례 연구 문제 해결](#)

[사례 연구 #1: HSRP 대기 IP 주소가 중복 IP 주소로 보고됨](#)

[사례 연구 #2: HSRP 상태가 계속 변경\(활성, 대기, 통화\) 또는 %HSRP-6-STATECHANGE](#)

[사례 연구 #3: HSRP가 피어를 인식하지 못함](#)

[사례 연구 #4: HSRP 상태 변경 및 스위치 보고서 SYS-4-P2 WARN: 1/Host](#)

[사례 연구 #5: 비대칭 라우팅 및 HSRP\(HSRP를 실행하는 라우터를 사용하는 네트워크에서 유니캐스트 트래픽의 과도한 플러딩\)](#)

[MSFC1](#)

[MSFC2](#)

[비대칭 라우팅의 결과](#)

[사례 연구 #6: HSRP 가상 IP 주소가 다른 IP 주소로 보고됨](#)

[사례 연구 #7: HSRP로 인해 보안 포트에서 MAC 위반 발생](#)

[사례 연구 #9: %Interface 하드웨어가 여러 그룹을 지원할 수 없습니다.](#)

[Catalyst 스위치에서 HSRP 문제 해결](#)

[A. HSRP 라우터 설정 확인](#)

[1. 고유한 라우터 인터페이스 IP 주소 확인](#)

[2. 대기\(HSRP\) IP 주소 및 대기 그룹 번호 확인](#)

[3. 대기 \(HSRP\) IP 주소가 인터페이스별로 다른지 확인합니다.](#)

[4. 대기 use-bia 명령을 사용해야 하는 경우](#)

[5. 액세스 목록 설정 확인](#)

[B. Catalyst Fast EtherChannel 및 트렁킹 설정 확인](#)

[1. 트렁킹 설정 확인](#)

[2. Fast EtherChannel\(포트 채널링\) 설정 확인](#)

[3. 스위치 MAC 주소 전달 테이블 조사](#)

[C. 물리적 레이어 연결 확인](#)

[1. 인터페이스 상태 확인](#)

[2. 링크 변경 및 포트 오류](#)

[3. IP 연결성 확인](#)

[4. 단방향 링크 확인](#)

[5. 추가 물리적 레이어 트러블슈팅 참조](#)

[D. 레이어 3 HSRP 디버깅](#)

[1. 표준 HSRP 디버깅](#)

[2. 조건부 HSRP 디버깅\(대기 그룹 및/또는 VLAN을 기준으로 출력 제한\)](#)

[3. 향상된 HSRP 디버깅](#)

[E. 스페닝 트리 문제 해결](#)

[1. 스페닝 트리 설정 확인](#)

[2. 스페닝 트리 루프 상태](#)

[3. 토폴로지 변경 알림](#)

[4. 연결 해제된 차단된 포트](#)

[5. 브로드캐스트 억제](#)

[6. 콘솔 및 Telnet 액세스](#)

[7. 스페닝 트리 기능: Portfast, UplinkFast 및 BackboneFast](#)

[8. BPDU Guard](#)

[9. VTP 정리](#)

[F. Divide and Conquer](#)

[알려진 문제](#)

[Cisco 2620/2621, Cisco 3600 및 고속 이더넷을 사용하는 경우 HSRP 상태 플랩/불안정함](#)

[관련 정보](#)

소개

이 문서에서는 일반적인 문제와 HSRP(Hot Standby Router Protocol) 문제를 해결하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

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.

HSRP의 이해

배경 정보

이 문서에서는 HSRP와 관련된 다음과 같은 가장 일반적인 문제를 다룹니다.

- 중복 HSRP 대기 IP 주소의 라우터 보고서
- 일정한 HSRP 상태 변경(활성, 대기, 음성)
- HSRP 피어가 없습니다.
- HSRP와 관련된 스위치 오류 메시지
- HSRP 설정에 대한 과도한 네트워크 유니캐스트

참고: 이 문서에서는 Catalyst 스위치 환경에서 HSRP 문제를 해결하는 방법을 자세히 설명합니다. 이 문서에는 소프트웨어 버전 및 네트워크 토폴로지 설계에 대한 참조 사항이 많이 포함되어 있습니다. 그럼에도 불구하고 이 문서의 유일한 목적은 HSRP 문제를 해결하는 엔지니어를 지원 및 안내하는 것입니다. 이 문서는 설계 가이드, 소프트웨어 권장 사항 또는 모범 사례 문서가 아닙니다.

미션 크리티컬 통신에 인트라넷 및 인터넷 서비스를 사용하는 기업 및 소비자는 네트워크 및 애플리케이션을 지속적으로 사용할 수 있어야 합니다. 고객은 Cisco IOS® 소프트웨어에서 HSRP를 활용하는 경우, 거의 100%에 달하는 네트워크 가동 시간에 대한 요구를 충족할 수 있습니다. 시스코 플랫폼에 고유한 HSRP는 네트워크에 엣지 디바이스 또는 액세스 회로의 첫 번째 홉 장애에서 사용자 트래픽을 즉시 투명하게 복구하는 방식으로 IP 네트워크에 대한 네트워크 이중화를 제공합니다.

IP 주소와 MAC(Layer 2 [L2]) 주소를 공유하는 경우, 두 개 이상의 라우터가 단일 가상 라우터 역할을 할 수 있습니다. 호스트 워크스테이션 기본 게이트웨이 이중화에는 주소가 필요합니다. 대부분의 호스트 워크스테이션은 라우팅 테이블을 포함하지 않으며 단일 다음 홉 IP 및 MAC 주소만 사용합니다. 이 주소를 기본 게이트웨이라고 합니다. HSRP를 사용하는 경우, 가상 라우터 그룹의 멤버는 상태 메시지를 지속적으로 교환합니다. 계획되었거나 계획되지 않은 이유로 라우터가 작동하지 않는 경우, 한 라우터가 다른 라우터의 라우팅 책임을 맡을 수 있습니다. 호스트는 단일 기본 게이트웨이로 설정되며 IP 패킷을 일관된 IP 및 MAC 주소로 계속 전달합니다. 라우팅을 수행하는 디바이스의 전환은 최종 워크스테이션에 투명하게 수행됩니다.

참고: 여러 기본 게이트웨이에 대해 Microsoft OS를 실행하는 호스트 워크스테이션을 구성할 수 있습니다. 그러나 여러 기본 게이트웨이는 동적이지 않습니다. OS는 한 번에 하나의 기본 게이트웨이만 사용합니다. 시스템은 첫 번째로 설정된 기본 게이트웨이가 ICMP(Internet Control Management Protocol)에서 연결할 수 없는 것으로 확인된 경우, 부팅 시 추가로 설정된 기본 게이트웨이만 선택합니다.

기본 작업

HSRP를 실행하는 라우터 집합은 단일 기본 게이트웨이 라우터를 LAN의 호스트에 제공하기 위해 함께 작동합니다. 이러한 라우터 집합을 HSRP 그룹 또는 대기 그룹이라고 합니다. 그룹에서 선택

된 단일 라우터는 호스트가 전송한 패킷을 가상 라우터로 전달하는 역할을 합니다. 이러한 라우터를 활성 라우터라고 합니다. 다른 라우터가 대기 라우터로 선택됩니다. 활성 라우터에 장애가 발생하면 대기는 패킷 전달 의무를 수행합니다. 임의 개수의 라우터가 HSRP를 실행할 수 있지만, 활성 라우터만 가상 라우터 IP 주소로 전송된 패킷을 전달합니다.

네트워크 트래픽을 최소화하기 위해 활성 및 대기 라우터는 프로토콜이 선택 프로세스를 완료한 후 주기적 HSRP 메시지를 전송합니다. HSRP 그룹의 추가 라우터는 대기 상태로 유지됩니다. 활성 라우터가 실패하면 대기 라우터가 활성 라우터 역할을 수행합니다. 대기 라우터가 실패하거나 활성 라우터가 되면 다른 라우터가 대기 라우터로 선택됩니다.

각 대기 그룹은 단일 가상 라우터(기본 게이트웨이)를 에뮬레이션합니다. 각 그룹에 대해 잘 알려진 단일 MAC 및 IP 주소가 해당 그룹에 할당됩니다. 여러 대기 그룹이 공존하고 LAN에 중복될 수 있으며, 개별 라우터는 여러 그룹에 참여할 수 있습니다. 이 경우 라우터는 각 그룹에 대해 별도의 상태 및 타이머를 유지 관리합니다.

HSRP 용어

용어 정의

활성 라우터 가상 라우터에 대한 패킷을 현재 전달하는 라우터

대기 라우터 기본 백업 라우터

대기 그룹 HSRP에 참여하고 가상 라우터를 공동으로 에뮬레이션하는 라우터 집합

Hello 시간 지정된 라우터에서 연속 HSRP hello 메시지 간의 간격

보류 시간 Hello 메시지를 수신한 시점부터 전송 라우터가 실패했다고 가정하는 시점까지의 간격

HSRP 주소 지정

HSRP 라우터 통신

HSRP를 실행하는 라우터는 HSRP hello 패킷을 통해 서로 간의 HSRP 정보를 전달합니다. 이러한 패킷은 UDP(User Datagram Protocol) 포트 1985에서 대상 IP 멀티캐스트 주소 224.0.0.2로 전송됩니다. IP 멀티캐스트 주소 224.0.0.2는 모든 라우터와 통신하는 데 사용되는 예약된 멀티캐스트 주소입니다. 활성 라우터는 설정된 IP 주소 및 HSRP 가상 MAC 주소에서 hello 패킷을 제공합니다. 대기 라우터는 설정된 IP 주소 및 버닝된 MAC 주소(BIA)에서 hello를 제공합니다. HSRP 라우터가 서로 올바르게 식별할 수 있도록 하려면 이 주소 지정을 사용해야 합니다.

대부분의 경우 라우터를 HSRP 그룹의 일부로 설정하는 경우, 라우터는 해당 그룹 및 자체 BIA에 대한 HSRP MAC 주소를 수신 대기합니다. 이 동작의 유일한 예외는 Cisco 2500, 4000 및 4500 라우터의 경우입니다. 이러한 라우터에는 단일 MAC 주소만 인식하는 이더넷 하드웨어가 있습니다. 따라서 이러한 라우터는 활성 라우터 역할을 할 때 HSRP MAC 주소를 사용합니다. 라우터는 대기 라우터 역할을 하는 경우, BIA를 사용합니다.

토큰 링을 제외한 모든 미디어에서 HSRP 대기 IP 주소 통신

호스트 워크스테이션은 기본 게이트웨이를 HSRP 대기 IP 주소로 사용하여 설정되므로 호스트는 HSRP 대기 IP 주소와 연결된 MAC 주소와 통신해야 합니다. 이 MAC 주소는 0000.0c07.ac**로 구성된 가상 MAC 주소입니다. **은(는) 각 인터페이스를 기반으로 하는 16진수의 HSRP 그룹 번호입니다. 예를 들어 HSRP 그룹 1은 0000.0c07.ac01의 HSRP 가상 MAC 주소를 사용합니다. 인접한 LAN 세그먼트의 호스트는 일반 ARP(Address Resolution Protocol) 프로세스를 사용하여 연결된 MAC 주소를 확인합니다.

ICMP 리디렉션

서브넷을 보호하는 HSRP 피어 라우터는 네트워크의 다른 모든 서브넷에 대한 액세스를 제공할 수 있습니다. 이는 HSRP의 기본입니다. 따라서 활성 HSRP 라우터가 되는 라우터는 중요하지 않습니다. Cisco IOS 소프트웨어 릴리스 12.1(3)T 이전의 Cisco IOS 소프트웨어 릴리스에서 ICMP 리디렉션은 인터페이스에서 HSRP가 사용되는 경우 해당 인터페이스에서 자동으로 비활성화됩니다. 이 설정이 없으면 호스트가 HSRP 가상 IP 주소에서 단일 라우터의 인터페이스 IP 및 MAC 주소로 리디렉션될 수 있습니다. 이중화가 손실됩니다.

Cisco IOS Software에서는 HSRP를 사용하여 ICMP 리디렉션을 허용하는 방법을 도입합니다. 이 방법은 HSRP를 통해 아웃바운드 ICMP 리디렉션 메시지를 필터링합니다. 다음 홉 IP 주소는 HSRP 가상 주소로 변경됩니다. 아웃바운드 ICMP 리디렉션 메시지의 게이트웨이 IP 주소는 해당 네트워크에 있는 HSRP 활성 라우터 목록과 비교됩니다. 게이트웨이 IP 주소에 해당하는 라우터가 HSRP 그룹에 대한 활성 라우터인 경우, 게이트웨이 IP 주소는 해당 그룹 가상 IP 주소로 대체됩니다. 이 솔루션을 사용하면 호스트가 원격 네트워크에 대한 최적의 경로를 학습하고, 동시에 HSRP가 제공하는 복원력을 유지 관리할 수 있습니다.

HSRP 기능 매트릭스

HSRP를 지원하는 기능 및 Cisco IOS 소프트웨어 릴리스에 대해 알아보려면 [Hot Standby Router Protocol](#) 특징 및 기능의 [Cisco IOS 릴리스 및 HSRP 기능 매트릭스](#) 섹션을 참조하십시오.

HSRP 기능

대부분의 HSRP 기능에 대한 정보는 [Hot Standby Router Protocol 특징 및 기능](#)을 참조하십시오. 이 문서에서는 이러한 HSRP 기능에 대한 정보를 제공합니다.

- 선점
- 인터페이스 추적
- BIA 사용
- 여러 HSRP 그룹
- MAC 주소 설정
- 시스템 로그 지원
- HSRP 디버깅
- 향상된 HSRP 디버깅
- 인증
- IP 이중화
- SNMP(Simple Network Management Protocol) MIB
- MPLS(Multiprotocol Label Switching)의 HSRP

참고: 브라우저에서 찾기 기능을 사용하여 문서 내에서 이러한 섹션을 찾을 수 있습니다.

패킷 형식

이 표에는 UDP HSRP 프레임의 데이터 부분 형식이 나와 있습니다.

버전	Op 코드	상태	Hellotime
Holdtime	우선순위	그룹	예약됨
인증 데이터			
인증 데이터			

가상 IP 주소

이 표에서는 HSRP 패킷의 각 필드에 대해 설명합니다.

패킷 필드 설명

Op 코드(1 octet)	Op 코드는 패킷에 포함된 메시지 유형을 설명합니다. 가능한 값은 0 - hello, 1 - coup 및 2 - resign입니다. Hello 메시지는 라우터가 HSRP를 실행하고 활성 라우터가 될 수 있음을 나타내기 위해 전송됩니다. 라우터가 활성 라우터가 되기를 원하는 경우 Coup 메시지가 전송됩니다. 라우터가 더 이상 활성 라우터가 되기를 원하지 않는 경우 Resign 메시지가 전송됩니다.
상태(1 octet)	대기 그룹의 각 라우터는 상태 시스템을 구현합니다. 상태 필드는 메시지를 전송하는 라우터의 현재 상태를 설명합니다. 개별 상태에 대한 세부 정보입니다. 0 - 초기, 1 - 학습, 2 - 듣기, 4 - 말기, 8 - 대기, 16 - 활성.
Hellotime(1 octet)	이 필드는 hello 메시지에서만 의미가 있습니다. 여기에는 라우터가 전송하는 hello 메시지 간의 대략적인 기간이 포함됩니다. 시간은 초 단위로 제공됩니다.
보류 시간 (1 octet)	이 필드는 hello 메시지에서만 의미가 있습니다. 여기에는 라우터가 상태 변경을 시작하기 전에 hello 메시지를 기다리는 시간이 포함됩니다.
우선순위(1 octet)	이 필드는 활성 및 대기 라우터를 선택하는 데 사용됩니다. 두 라우터의 우선순위를 비교하면 가장 높은 값을 가진 라우터가 활성 라우터가 됩니다. 타이 브레이커는 IP 주소가 더 높은 라우터입니다.
그룹(1 octet)	이 필드는 대기 그룹을 식별합니다.
인증 데이터(8 octet)	이 필드에는 일반 텍스트의 8자 비밀번호가 포함됩니다.
가상 IP 주소(4 octet)	가상 IP 주소가 라우터에 설정되지 않은 경우, 활성 라우터의 hello 메시지에서 주소를 학습할 수 있습니다. HSRP 대기 IP 주소가 설정되지 않은 경우에만 주소를 학습하고 hello 메시지가 인증됩니다(인증이 설정된 경우).

HSRP 상태

상태 정의

이는 시작 시의 상태입니다. 이 상태는 HSRP가 실행되지 않음을 나타냅니다. 이 상태는 설정 변경을 시작되거나 인터페이스를 처음 사용할 수 있게 되면 시작됩니다.
라우터가 가상 IP 주소를 확인하지 않았으며 활성 라우터에서 인증된 hello 메시지를 아직 확인하지 않습니다. 이 상태에서 라우터는 활성 라우터에서 수신 대기합니다.
라우터는 가상 IP 주소를 알고 있지만 라우터는 활성 라우터도 아니고 대기 라우터도 아닙니다. 해당 라우터에서 hello 메시지를 수신합니다.
라우터는 주기적으로 hello 메시지를 전송하고 활성 및/또는 대기 라우터의 선택에 적극적으로 참여합니다. 라우터에 가상 IP 주소가 없으면 라우터는 상태를 시작할 수 없습니다.
라우터는 다음 활성 라우터가 될 후보이며 정기적인 hello 메시지를 전송합니다. 일시적인 조건을 제외하고 상태의 그룹에는 최대 하나의 라우터가 있습니다.
라우터는 현재 그룹 가상 MAC 주소로 전송되는 패킷을 전달합니다. 라우터는 주기적 hello 메시지를 전송합니다. 일시적인 조건을 제외하면 그룹의 상태에는 최대 하나의 라우터가 있어야 합니다.

HSRP 타이머

각 라우터는 HSRP에서 3개의 타이머만 사용합니다. 타이머는 hello 메시지를 시간 처리합니다. HSRP는 실패가 발생하는 경우 HSRP hello 및 보류 타이머가 설정된 방식에 따라 수렴됩니다. 기본적으로 이러한 타이머는 각각 3초와 10초로 설정됩니다. 즉, hello 패킷이 3초마다 HSRP 대기 그룹 디바이스 간에 전송되고, hello 패킷이 10초 동안 수신되지 않은 경우 대기 디바이스는 활성 상태가 됩니다. 이러한 타이머 설정을 낮추어 장애 조치 또는 선점 속도를 높일 수 있지만, CPU 사용량이 증가하고 불필요한 대기 상태 플래핑을 방지하려면 hello 타이머를 1초 미만으로 설정하거나 보류 타이머를 4초 미만으로 설정하지 마십시오. HSRP 추적 메커니즘을 사용하고 추적된 링크가 실패

하면 hello 및 보류 타이머에 관계없이 페일오버 또는 선점이 즉시 발생합니다. 타이머가 만료되면 라우터가 새 HSRP 상태로 전환됩니다. 타이머는 standby [group-number] timers hellotime holdtime 명령으로 변경할 수 있습니다. 예: 대기 1 타이머 5 15.

다음 표에서는 이러한 타이머에 대한 자세한 정보를 제공합니다.

타이머 설명

- 활성 타이머** 이러한 타이머는 활성 라우터를 모니터링하는 데 사용됩니다. 이러한 타이머는 활성 라우터가 hello 패킷을 수신할 때마다 시작됩니다. 이러한 타이머는 HSRP hello 메시지의 관련 필드에 설정된 보류 시간 값에 따라 만료됩니다.
- 대기 타이머** 이러한 타이머는 대기 라우터를 모니터링하는 데 사용됩니다. 대기 라우터가 hello 패킷을 수신할 때마다 타이머가 시작됩니다. 이러한 타이머는 각 hello 패킷에 설정된 보류 시간 값에 따라 만료됩니다.
- Hello 타이머** 이러한 타이머는 hello 패킷을 클럭하는 데 사용됩니다. 모든 HSRP 상태의 모든 HSRP 라우터는 0 타이머 hello 타이머가 만료되면 hello 패킷을 생성합니다.

HSRP 이벤트

이 표는 HSRP finite state machine의 이벤트를 제공합니다.

키 이벤트

- 1 HSRP는 활성화된 인터페이스에서 설정됩니다.
- 2 HSRP가 인터페이스에서 비활성화되어 있거나 인터페이스가 비활성화되어 있습니다.
- 3 활성 타이머 만료, 활성 타이머는 활성 라우터에서 마지막 hello 메시지가 표시되는 보류 시간으로 설정됩니다.
- 4 대기 타이머 만료, 대기 타이머는 대기 라우터에서 마지막 hello 메시지가 표시되는 보류 시간으로 설정됩니다.
- 5 Hello 타이머 만료, hello 메시지 전송을 위한 주기적인 타이머가 만료되었습니다.
- 6 상태의 라우터에서 우선순위가 더 높은 hello 메시지 수신
- 7 활성 라우터에서 우선순위가 더 높은 hello 메시지 수신
- 8 활성 라우터에서 우선순위가 더 낮은 hello 메시지 수신
- 9 활성 라우터에서 resign 메시지 수신
- 10 우선순위가 더 높은 라우터에서 coup 메시지 수신
- 11 대기 라우터에서 우선순위가 더 높은 hello 메시지 수신
- 12 대기 라우터에서 우선순위가 더 낮은 hello 메시지 수신

HSRP 작업

이 표는 상태 시스템의 일부로 수행할 작업을 지정합니다.

서신 작업

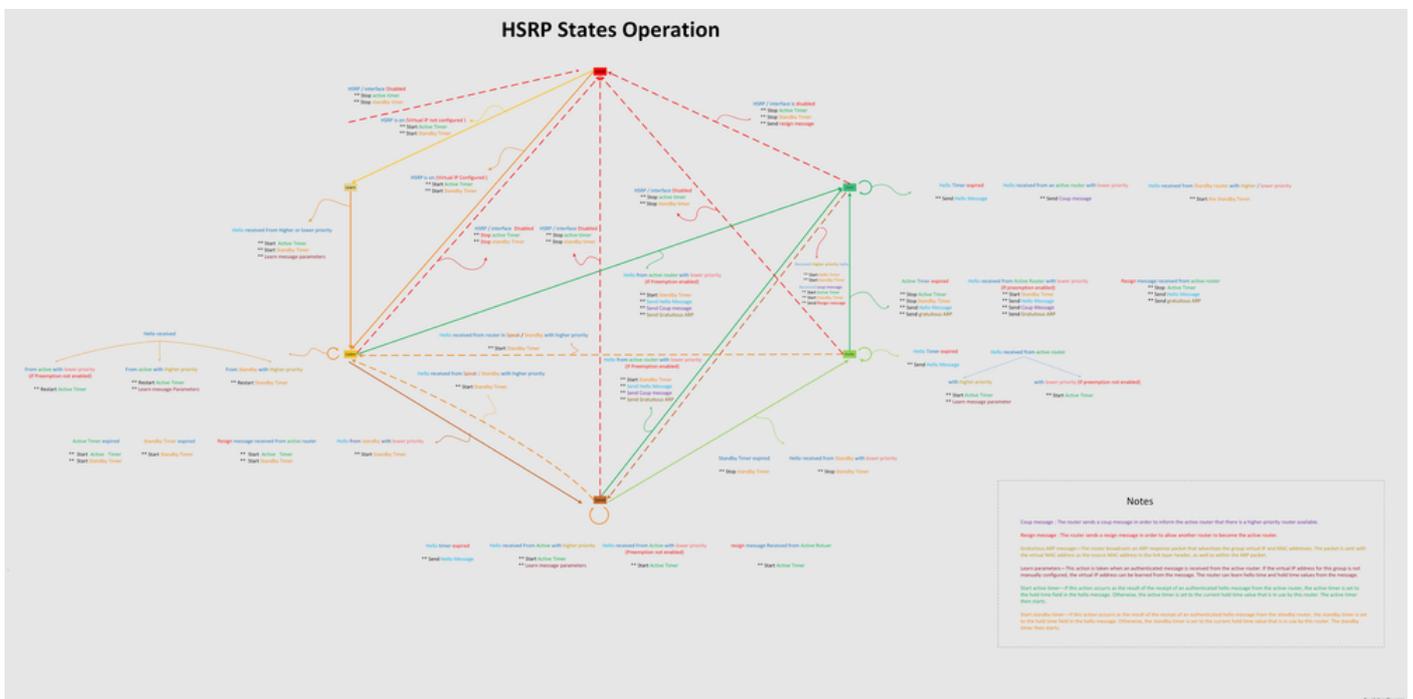
- A Start active timer(활성 타이머 시작)** - 활성 라우터에서 인증된 hello 메시지를 수신한 결과로 이 작업이 진행되는 경우 활성 타이머가 hello 메시지의 hold time(보류 시간) 필드로 설정됩니다. 그렇지 않으면 타이머는 이 라우터에서 사용 중인 현재 보류 시간 값으로 설정됩니다. 그런 다음 활성 타이머가 시작됩니다.
- B Start standby timer(대기 타이머 시작)** - 대기 라우터에서 인증된 hello 메시지를 수신한 결과로 이 작업이 수행되는 경우 대기 타이머가 hello 메시지의 hold time(보류 시간) 필드로 설정됩니다. 그렇지 않으면 타이머는 이 라우터에서 사용 중인 현재 보류 시간 값으로 설정됩니다. 그런 다음 대기 타이머가 시작됩니다.
- C 활성 타이머 중지** — 활성 타이머가 중지됩니다.
- D 대기 타이머 중지** - 대기 타이머가 중지됩니다.
- E 매개변수 학습** - 이 작업은 활성 라우터에서 인증된 메시지가 수신될 때 수행됩니다. 이 그룹의 가상 IP 주소는 메시지에서 자동으로 설정하지 않은 경우, 메시지에서 가상 IP 주소를 학습할 수 있습니다. 라우터는 메시지 hello 시간 및 보류 시간 값을 학습할 수 있습니다.

- F Hello 메시지 전송 - 라우터가 현재 상태, hello 시간 및 보류 시간과 함께 hello 메시지를 전송합니다.
- G Coup 메시지 전송 - 라우터는 우선순위가 더 높은 라우터를 사용할 수 있음을 활성 라우터에 알리기 위해 coup 메시지를 전송합니다.
- H Resign 메시지 전송 - 다른 라우터가 활성 라우터가 될 수 있도록 라우터가 resign 메시지를 전송합니다.
- I Gratuitous ARP 메시지 전송 - 라우터가 그룹 가상 IP 및 MAC 주소를 알리는 ARP 응답 패킷을 브로드캐스트합니다. 패킷은 ARP 패킷 내에서 뿐만 아니라 링크 레이어 헤더의 소스 MAC 주소로 가상 MAC 주소로 함께 전송됩니다.

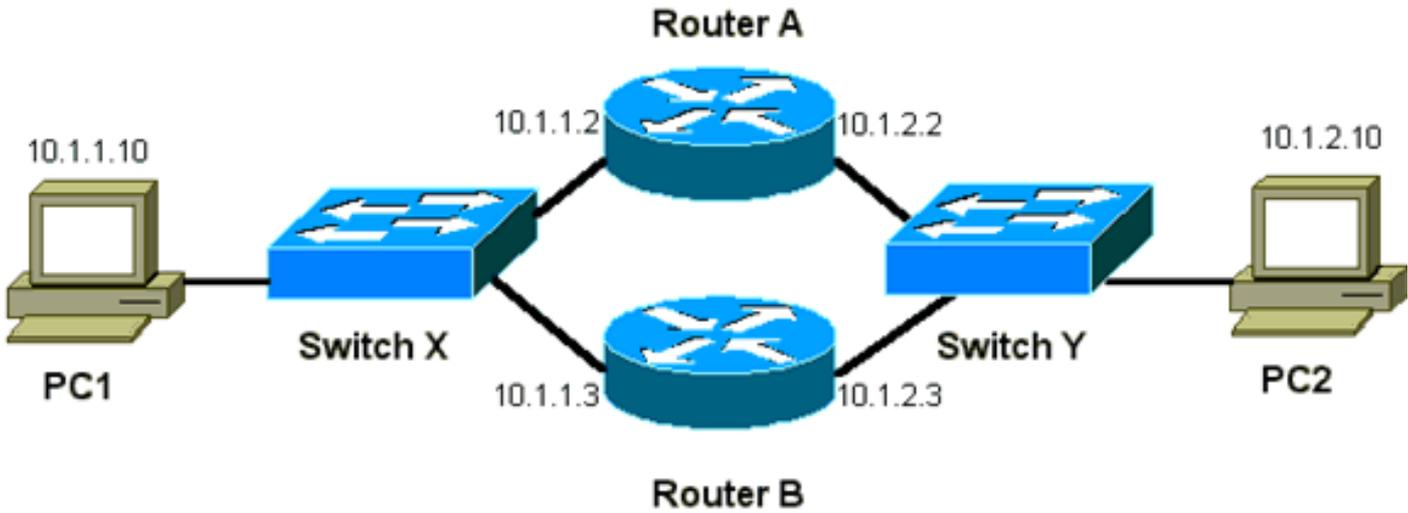
HSRP 상태 테이블

이 섹션의 다이어그램은 HSRP 상태 시스템의 상태 전환을 보여줍니다. 이벤트가 발생할 때마다 관련 작업이 수행되고 라우터가 다음 HSRP 상태로 전환됩니다. 다이어그램에서 숫자는 이벤트를 지정하고 문자는 관련 작업을 지정합니다. [HSRP 이벤트](#) 섹션의 표는 숫자를 정의하고, [HSRP 작업](#) 섹션의 표는 문자를 정의합니다. 이 다이어그램은 참조용으로만 사용하십시오. 다이어그램은 상세하며 일반적인 트러블슈팅 목적에는 필요하지 않습니다.

다이어그램의 고화질 이미지는 HSRP 상태 작업을 참조하십시오.



패킷 플로우



디바이스 MAC 주소 IP 주소 서브넷 마스크 기본 게이트웨이

PC1	0000.0c00.0001	10.1.1.10	255.255.255.0	10.1.1.1
PC2	0000.0c00.1110	10.1.2.10	255.255.255.0	10.1.2.1

라우터 A 설정(활성 라우터)

```
interface GigabitEthernet 0/0
 ip address 10.1.1.2 255.255.255.0
 mac-address 4000.0000.0010
 standby 1 ip 10.1.1.1
 standby 1 priority 200
```

```
interface GigabitEthernet 0/1 ip address 10.1.2.2 255.255.255.0 mac-address 4000.0000.0011
 standby 1 ip 10.1.2.1 standby 1 priority 200
```

라우터 B 설정(대기 라우터)

```
interface GigabitEthernet 0/0
 ip address 10.1.1.3 255.255.225.0
 mac-address 4000.0000.0020
 standby 1 ip 10.1.1.1
```

```
interface GigabitEthernet 0/1 ip address 10.1.2.3 255.255.255.0 mac-address 4000.0000.0021
 standby 1 ip 10.1.2.1
```

참고: 이 예에서는 설명을 위해서만 고정 MAC 주소를 구성합니다. 반드시 필요한 경우가 아니면 고정 MAC 주소를 설정하지 마십시오.

HSRP 문제를 해결하기 위해 스니퍼 추적을 가져올 때 패킷 흐름의 개념을 이해해야 합니다. 라우터 A는 우선순위 200을 사용하며 두 인터페이스 모두에서 활성 라우터가 됩니다. 이 섹션의 예에서 호스트 워크스테이션으로 향하는 라우터의 패킷에는 라우터 BIA(물리적 MAC 주소)의 소스 MAC 주소가 있습니다. HSRP IP 주소로 향하는 호스트 머신의 패킷에는 HSRP 가상 MAC 주소의 대상 MAC 주소가 있습니다. MAC 주소는 라우터와 호스트 간의 각 플로우에서 동일하지 않습니다.

이 표는 스위치 X에서 가져온 스니퍼 추적을 기반으로 플로우당 각 MAC 및 IP 주소 정보를 보여줍니다.

패킷 플로우	소스 MAC	대상 MAC	소스 IP	대상 IP
PC2로 향하는 PC1의 패킷	PC1(0000.0c00.0001)	라우터 A 인터페이스 이더넷 0(0000.0c07.ac01)의 HSRP 가상 MAC 주소	10.1.1.10	10.1.1.10
PC2에서 라우터 A를 통해 반환되고 PC1로 향하는 패킷	라우터 A 이더넷 0 BIA(4000.0000.0010)	PC1(0000.0c00.0001)	10.1.2.10	10.1.1.10
HSRP 대기 IP 주소(ICMP, Telnet)로 향하는 PC1의 패킷	PC1(0000.0c00.0001)	라우터 A 인터페이스 이더넷 0(0000.0c07.ac01)의 HSRP 가상 MAC 주소	10.1.1.10	10.1.1.10
활성 라우터의 실제 IP 주소로 향하는 패킷(ICMP, Telnet)	PC1(0000.0c00.0001)	라우터 A 이더넷 0 BIA(4000.0000.0010)	10.1.1.10	10.1.1.10
대기 라우터의 실제 IP 주소로 향하는 패킷(ICMP, Telnet)	PC1(0000.0c00.0001)	라우터 B 이더넷 0 BIA(4000.0000.0020)	10.1.1.10	10.1.1.10

HSRP 사례 연구 문제 해결

사례 연구 #1: HSRP 대기 IP 주소가 중복 IP 주소로 보고됨

다음과 같은 오류 메시지가 나타날 수 있습니다.

```
Oct 12 13:15:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
on Vlan25, sourced by 0000.0c07.ac19
Oct 13 16:25:41: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:31:02: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
on Vlan25, sourced by 0000.0c07.ac19
Oct 15 22:41:01: %STANDBY-3-DUPADDR: Duplicate address 10.25.0.1
on Vlan25, sourced by 0000.0c07.ac19
```

이러한 오류 메시지가 반드시 HSRP 문제를 나타내는 것은 아닙니다. 오히려 오류 메시지는 STP(Spanning Tree Protocol) 루프 또는 라우터/스위치 설정 문제를 나타냅니다. 오류 메시지는 다른 문제의 증상일 뿐입니다.

또한 이러한 오류 메시지는 HSRP의 올바른 작동을 방해하지 않습니다. 중복 HSRP 패킷은 무시됩니다. 이러한 오류 메시지는 30초 간격으로 제한됩니다. 그러나 HSRP 주소의 `STANDBY-3-DUPADDR` 오류 메시지를 유발하는 네트워크 불안정으로 인해 네트워크 성능이 저하되고 패킷 손실이 발생할 수 있습니다.

이러한 메시지는 구체적으로 라우터가 VLAN 25의 HSRP IP 주소에서 MAC 주소 0000.0c07.ac19로 소싱된 데이터 패킷을 받았음을 나타냅니다. HSRP MAC 주소가 0000.0c07.ac19이므로 해당 라우터가 자체 패킷을 다시 받았거나 HSRP 그룹의 두 라우터 모두로 전환되었습니다. 라우터가 자체 패킷을 수신했기 때문에 라우터가 아닌 네트워크에 문제가 있을 가능성이 높습니다. 다양한 문제로 인해 이 동작이 발생할 수 있습니다. 오류 메시지를 유발할 수 있는 네트워크 문제는 다음과 같습니다.

- 일시적 STP 루프
- EtherChannel 설정 문제
- 중복된 프레임

이러한 오류 메시지를 트러블슈팅하는 경우 이 문서의 [Catalyst Switches](#)에서 HSRP 트러블슈팅 [섹션](#)의 트러블슈팅 단계를 참조하십시오. 모든 트러블슈팅 모듈은 컨피그레이션의 모듈을 포함하는 이 섹션에 적용됩니다. 또한 스위치 로그에 오류가 있는지 확인하고 필요에 따라 추가 사례 연구를 참조하십시오.

활성 라우터가 자체 멀티캐스트 hello 패킷을 수신하는 것을 방지하기 위해 액세스 목록을 사용할 수 있습니다. 그러나 이는 오류 메시지에 대한 해결 방법일 뿐이며 실제로는 문제의 증상을 숨깁니다. 해결 방법은 HSRP 인터페이스에 확장 인바운드 액세스 목록을 적용하는 것입니다. 액세스 목록은 물리적 IP 주소에서 시작되고 모든 라우터 멀티캐스트 주소 224.0.0.2로 향하는 모든 트래픽을 차단 합니다.

```
access-list 101 deny ip host 172.16.12.3 host 224.0.0.2
access-list 101 permit ip any any
```

```
interface GigabitEthernet 0/0
 ip address 172.16.12.3 255.255.255.0
 standby 1 ip 172.16.12.1
 ip access-group 101 in
```

사례 연구 #2: HSRP 상태가 계속 변경(활성, 대기, 통화) 또는 %HSRP-6-STATECHANGE

다음과 같은 오류 메시지가 나타날 수 있습니다.

```
Jan 9 08:00:42.623: %STANDBY-6-STATECHANGE: Standby: 49:
Vlan149 state Standby -> Active
Jan 9 08:00:56.011: %STANDBY-6-STATECHANGE: Standby: 49:
Vlan149 state Active -> Speak
Jan 9 08:01:03.011: %STANDBY-6-STATECHANGE: Standby: 49:
Vlan149 state Speak -> Standby
Jan 9 08:01:29.427: %STANDBY-6-STATECHANGE: Standby: 49:
Vlan149 state Standby -> Active
Jan 9 08:01:36.808: %STANDBY-6-STATECHANGE: Standby: 49:
Vlan149 state Active -> Speak
Jan 9 08:01:43.808: %STANDBY-6-STATECHANGE: Standby: 49:
Vlan149 state Speak -> Standby
```

```
Jul 29 14:03:19.441: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Standby -> Active Jul 29 16:27:04.133: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Active -> Speak Jul 29 16:31:49.035: %HSRP-5-STATECHANGE: Vlan10 Grp 110 state Speak -> Standby
```

이러한 오류 메시지는 대기 HSRP 라우터가 HSRP 피어에서 3개의 연속 HSRP hello 패킷을 수신하지 못한 상황을 설명합니다. 출력은 대기 라우터가 상태에서 상태로 이동하는 것을 보여줍니다. 잠시 후에 라우터는 상태로 돌아갑니다. 초기 설치 중에 이 오류 메시지가 발생하지 않는 한 HSRP 문제로 인해 오류 메시지를 발생하지 않을 수 있습니다. 오류 메시지는 피어 간의 HSRP hello 손실을 나타냅니다. 이러한 문제를 해결하는 경우, HSRP 피어 간의 통신을 확인해야 합니다. 피어 간의 임의의 일시적인 데이터 통신 손실은 이러한 메시지가 나타나는 가장 일반적인 문제입니다. HSRP 상태 변경은 높은 CPU 사용률로 인해 발생하는 경우가 많습니다. 높은 CPU 사용률로 인한 오류 메시지인 경우, 네트워크에 스니퍼를 배치하고 높은 CPU 사용률을 유발하는 시스템을 추적합니다.

피어 간 HSRP 패킷 손실을 유발하는 몇 가지 원인이 있습니다. 가장 일반적인 문제는 [물리적 레이어 문제](#), 스페닝 트리 문제로 인한 [과도한 네트워크 트래픽](#) 또는 각 Vlan으로 인한 과도한 트래픽입니다. [사례 연구 #1](#)과 마찬가지로, 모든 트러블슈팅 모듈은 HSRP 상태 변경 사항, 특히 [레이어 3 HSRP 디버깅](#)의 해결에 적용할 수 있습니다.

피어 간 HSRP 패킷 손실이 각 VLAN에 의해 발생하는 과도한 트래픽으로 인해 발생하는 경우 SPD를 조정하거나 늘리고 입력 큐 삭제 문제를 해결하기 위해 큐 크기를 유지할 수 있습니다.

SPD(Selective Packet Discard) 크기를 늘리려면 컨피그레이션 모드로 이동하여 Cat6500 스위치에서 다음 명령을 실행합니다.

```
(config)#ip spd queue max-threshold 600
```

```
!--- Hidden Command
```

```
(config)#ip spd queue min-threshold 500
```

```
!--- Hidden Command
```

보류 대기열 크기를 늘리려면 VLAN 인터페이스 모드로 이동하여 이 명령을 실행합니다.

```
(config-if)#hold-queue 500 in
```

SPD 및 보류 대기열 크기를 늘린 후 `clear counter interface` 명령을 실행하면 인터페이스 카운터를 수 있습니다.

사례 연구 #3: HSRP가 피어를 인식하지 못함

이 섹션의 라우터 출력은 HSRP에 대해 설정되었지만 HSRP 피어를 인식하지 않는 라우터를 보여줍니다. 이렇게 하려면 라우터가 인접 라우터에서 HSRP hello 수신에 실패해야 합니다. 이러한 문제를 해결 시에는 이 문서의 [물리적 레이어 연결 확인](#) 섹션 및 [HSRP 라우터 설정 확인](#) 섹션을 참조하십시오. 물리적 레이어 연결이 올바른 경우, 일치하지 않는 VTP 모드를 확인합니다.

```
Vlan8 - Group 8
Local state is Active, priority 110, may preempt
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.168
Hot standby IP address is 10.1.2.2 configured
Active router is local
Standby router is unknown expired
Standby virtual mac address is 0000.0c07.ac08
5 state changes, last state change 00:05:03
```

사례 연구 #4: HSRP 상태 변경 사항 및 스위치 보고서 SYS-4-P2_WARN: 1/Host <mac_address>가 Syslog의 포트 <port_1>과 포트 <port_2> 사이에서 플래핑 중입니다.

다음과 같은 오류 메시지가 나타날 수 있습니다.

```
2001 Jan 03 14:18:43 %SYS-4-P2_WARN: 1/Host 00:00:0c:14:9d:08
  is flapping between port 2/4 and port 2/3
```

```
Feb 4 07:17:44 AST: %SW_MATM-4-MACFLAP_NOTIF: Host 0050.56a9.1f28 in vlan 1027 is flapping between port Te1/0/7 and port Te2/0/2
```

Catalyst Switches에서 스위치는 호스트 MAC 주소가 15초 내에 두 번 이동할 경우 이동하는 호스트 MAC 주소를 보고합니다. 가능한 원인은 STP 루프입니다. 스위치는 STP 루프의 영향을 최소화하기 위해 약 15초 동안 이 호스트에서 패킷을 삭제합니다. 보고된 두 포트 간에 MAC 주소 이동이 HSRP 가상 MAC 주소인 경우, 두 HSRP 라우터 모두가 상태로 전환되는 문제일 가능성이 높습니다.

보고된 MAC 주소가 HSRP 가상 MAC 주소가 아닌 경우, 이 문제는 네트워크에서 패킷의 루프, 중복 또는 리플렉션을 나타낼 수 있습니다. 이러한 유형의 조건은 HSRP 문제의 원인이 될 수 있습니다. MAC 주소 이동에 대한 가장 일반적인 원인은 [스패닝 트리 문제](#) 또는 [물리적 레이어 문제](#)입니다.

이 오류 메시지의 문제를 해결하는 경우 다음 단계를 완료하십시오.

참고: 이 문서의 [Catalyst Switches](#)에서 HSRP [트러블슈팅 섹션](#)의 단계도 완료합니다.

1. 호스트 MAC 주소의 올바른 소스(포트)를 확인합니다.
2. 호스트 MAC 주소를 소싱하지 않아야 하는 포트의 연결을 해제합니다.
3. VLAN 별로 STP 토폴로지를 문서화하고 STP 장애를 확인합니다.
4. 포트 채널 설정을 확인합니다. 포트 채널 설정이 올바르지 않으면 호스트 MAC 주소별로 오류 메시지가 플랩핑될 수 있습니다. 이는 포트 채널링의 로드 밸런싱 특성 때문입니다.

사례 연구 #5: 비대칭 라우팅 및 HSRP(HSRP를 실행하는 라우터를 사용하는 네트워크에서 유니캐스트 트래픽의 과도한 플러딩)

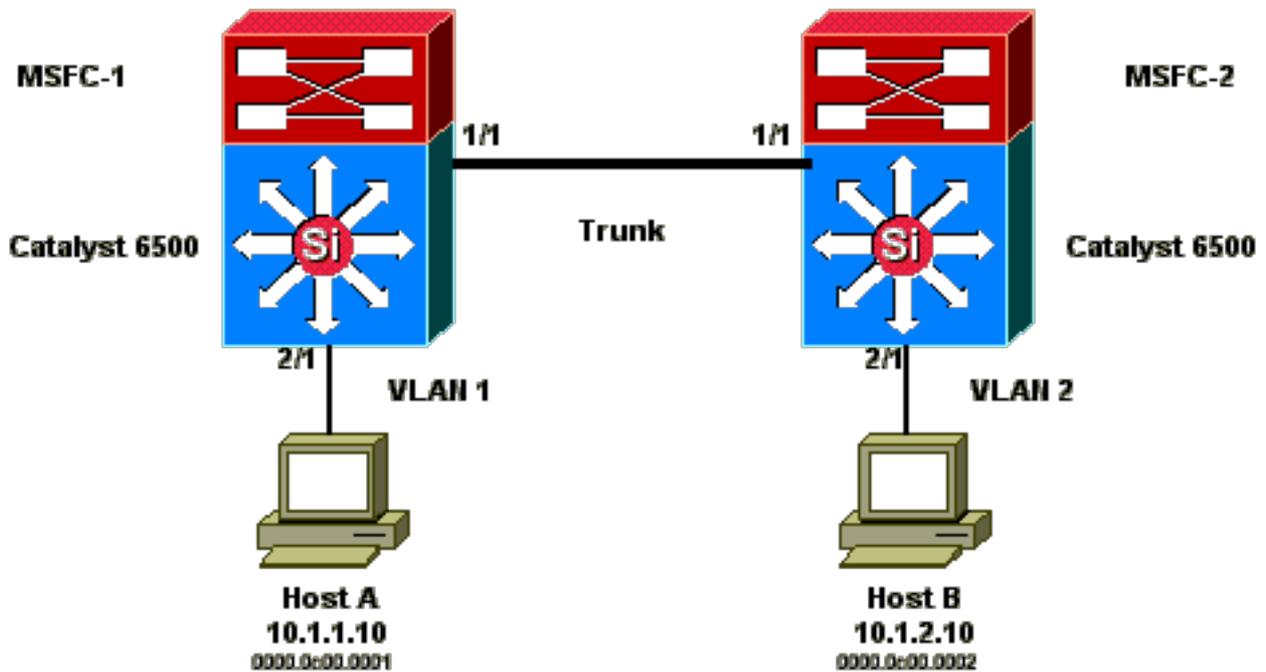
비대칭 라우팅의 경우, 전송 및 수신 패킷은 호스트와 통신하는 피어 간에 서로 다른 경로를 사용합니다. 이 패킷 흐름은 HSRP 우선순위를 기반으로 HSRP 라우터 간 로드 밸런싱 컨피그레이션에서 HSRP를 액티브 또는 스탠바이로 설정한 결과입니다. 스위칭 환경에서 이러한 유형의 패킷 플로우로 인해 알 수 없는 유니캐스트 플러딩이 과도하게 발생할 수 있습니다. 또한 MLS(Multilayer Switching) 항목이 없을 수 있습니다. 알 수 없는 유니캐스트 플러딩은 스위치가 모든 포트에서 유니캐스트 패킷을 플러딩할 때 발생합니다. 대상 MAC 주소에 대한 항목이 없으므로 스위치가 패킷을 초과합니다. 이 동작은 패킷이 계속 전달되므로 연결을 끊지 않습니다. 그러나 이 동작은 호스트 포트에서 추가 패킷의 플러드를 설명합니다. 이 사례에서는 비대칭 라우팅의 동작 및 유니캐스트 플러딩 결과의 이유를 연구합니다.

비대칭 라우팅의 증상은 다음과 같습니다.

- 과도한 유니캐스트 패킷 플러딩
- 플로우에 대한 MLS 항목 없음
- 호스트 포트의 패킷이 호스트로 향하지 않음을 보여주는 스니퍼 추적
- 서버 로드 밸런서, 웹 캐시 디바이스 및 네트워크 어플라이언스와 같은 L2 기반 패킷 재작성 엔진을 사용하는 네트워크 레이턴시 증가Cisco LocalDirector 및 Cisco Cache Engine을 예로 들 수 있습니다.
- 추가 유니캐스트 플러딩 트래픽 로드를 처리할 수 없는 연결된 호스트 및 워크스테이션에서 삭제된 패킷

참고: 라우터의 기본 ARP 캐시 에이징 시간은 4시간입니다. 스위치 CAM(content-addressable memory) 항목의 기본 에이징 시간은 5분입니다. 호스트 워크스테이션의 ARP 에이징 시간은 이 논의에서 중요하지 않습니다. 그러나 이 예에서는 ARP 에이징 시간을 4시간으로 설정합니다.

이 다이어그램이 이 문제를 보여줍니다. 이 토폴로지 예시에는 각 스위치에 MSFC(Multilayer Switch Feature Card)가 있는 Catalyst 6500이 포함되어 있습니다. 이 예에서는 MSFC를 사용하지 않고 MSFC 대신 모든 라우터를 사용할 수 있습니다. 사용할 수 있는 라우터의 예로는 RSM(Route Switch Module), GSR(Gigabit Switch Router) 및 Cisco 7500이 있습니다. 호스트는 스위치의 포트에 직접 연결됩니다. 스위치는 VLAN 1 및 VLAN 2에 대한 트래픽을 전달하는 트렁크를 통해 상호 연결됩니다.



이러한 출력은 각 MSF의 **show standby** 명령 설정에서 발췌한 것입니다.

MSFC1

```
interface Vlan 1
  mac-address 0003.6bf1.2a01
  ip address 10.1.1.2 255.255.255.0
  no ip redirects
  standby 1 ip 10.1.1.1
  standby 1 priority 110
```

```
interface Vlan 2
  mac-address 0003.6bf1.2a01
  ip address 10.1.2.2 255.255.255.0
  no ip redirects
  standby 2 ip 10.1.2.1
```

```
MSFC1#show standby
Vlan1 - Group 1
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.696
Hot standby IP address is 10.1.1.1 configured
Active router is local
Standby router is 10.1.1.3 expires in 00:00:07
Standby virtual mac address is 0000.0c07.ac01
2 state changes, last state change 00:20:40
Vlan2 - Group 2
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.776
Hot standby IP address is 10.1.2.1 configured
Active router is 10.1.2.3 expires in 00:00:09, priority 110
Standby router is local
4 state changes, last state change 00:00:51
MSFC1#exit
Console> (enable)
```

MSFC2

```
interface Vlan 1
  mac-address 0003.6bf1.2a02
  ip address 10.1.1.3 255.255.255.0
  no ip redirects
  standby 1 ip 10.1.1.1
```

```
interface Vlan 2
  mac-address 0003.6bf1.2a02
  ip address 10.1.2.3 255.255.255.0
  no ip redirects
  standby 2 ip 10.1.2.1
  standby 2 priority 110
```

```
MSFC2#show standby
Vlan1 - Group 1
Local state is Standby, priority 100
Hellotime 3 holdtime 10
Next hello sent in 00:00:01.242
Hot standby IP address is 10.1.1.1 configured
Active router is 10.1.1.2 expires in 00:00:09, priority 110
Standby router is local
7 state changes, last state change 00:01:17
Vlan2 - Group 2
Local state is Active, priority 110
Hellotime 3 holdtime 10
Next hello sent in 00:00:00.924
Hot standby IP address is 10.1.2.1 configured
Active router is local
Standby router is 10.1.2.2 expires in 00:00:09
Standby virtual mac address is 0000.0c07.ac02
2 state changes, last state change 00:40:08
MSFC2#exit
```

참고: MSFC1에서 VLAN 1은 HSRP 상태이고 VLAN 2는 HSRP 상태입니다. MSFC2에서 VLAN 2는 HSRP 상태이고 VLAN 1은 HSRP 상태입니다. 각 호스트의 기본 게이트웨이는 각 대기 IP 주소입니다.

1. 처음에는 모든 캐시가 비어 있습니다. 호스트 A는 MSFC1을 기본 게이트웨이로 사용합니다. 호스트 B는 MSFC2를 사용합니다. **Ping이 시작되기 전의 ARP 및 MAC 주소 테이블 참고:** 간단한 설명을 위해 라우터 HSRP의 스위치 1 MAC 주소와 MAC 주소는 이 섹션에 나타나는 다른 테이블에 포함되지 않습니다.
2. 호스트 A는 호스트 B를 ping합니다. 이는 호스트 A가 ICMP 에코 패킷을 전송함을 의미합니다. 각 호스트가 별도의 VLAN에 상주하므로 호스트 A는 호스트 B로 향하는 패킷을 기본 게이트웨이로 전달합니다. 해당 프로세스가 발생하려면 호스트 A가 기본 게이트웨이 MAC 주소 10.1.1.1을 확인하기 위해 ARP를 전송해야 합니다. **호스트 A가 기본 게이트웨이에 대해 ARP를 전송한 후의 ARP 및 MAC 주소 테이블**
3. MSFC1은 패킷을 수신하고, 패킷을 재작성하며, 패킷을 호스트 B에 전달합니다. 호스트가 직접 연결된 인터페이스에 상주하므로 패킷을 재작성하기 위해 MSFC1은 호스트 B에 대한 ARP 요청을 전송합니다. MSFC2는 이 플로우에서 패킷을 아직 수신하지 않았습니다. MSFC1가 호스트 B에서 ARP 응답을 수신하면 두 스위치 모두 호스트 B와 연결된 소스 포트를 학습합니다. **호스트 A가 기본 게이트웨이에 패킷을 전송하고 MSFC1이 호스트 B에 대한 ARP를 전송한 이후의 ARP 및 MAC 주소 테이블**
4. 호스트 B는 MSFC1을 통해 호스트 A로부터 에코 패킷을 수신합니다. 호스트 B는 이제 에코 응답을 호스트 A에 보내야 합니다. 호스트 A는 다른 VLAN에 상주하므로 호스트 B는 기본 게

이트웨이인 MSFC2를 통해 응답을 전달합니다. MSFC2를 통해 패킷을 전달하려면 호스트 B에서 기본 게이트웨이 IP 주소인 10.1.2.1에 대한 ARP를 전송해야 합니다.**호스트 B가 기본 게이트웨이에 대해 ARP를 전송한 후의 ARP 및 MAC 주소 테이블**

- 이제 호스트 B가 에코 응답 패킷을 MSFC2에 전달합니다. MSFC2는 VLAN 1에 직접 연결되어 있으므로 호스트 A에 대한 ARP 요청을 보냅니다. 스위치 2는 MAC 주소 테이블을 호스트 B의 MAC 주소로 채웁니다.**호스트 A에서 에코 패킷을 수신한 후의 ARP 및 MAC 주소 테이블**
- 에코 응답이 호스트 A에 도달하고 플로우가 완료됩니다.

비대칭 라우팅의 결과

호스트 A가 호스트 B를 계속 ping하는 경우를 고려해 보십시오. 호스트 A는 에코 패킷을 MSFC1로 전송하고 호스트 B는 비대칭 라우팅 상태에 있는 MSFC2에 에코 응답을 전송합니다. 스위치 1이 호스트 B의 소스 MAC을 학습하는 유일한 시간은 호스트 B가 MSFC1의 ARP 요청에 응답할 때입니다. 이는 호스트 B가 MSFC2를 기본 게이트웨이로 사용하고 MSFC1 및 결과적으로 스위치 1로 패킷을 전송하지 않기 때문입니다. ARP 시간 제한은 기본적으로 4시간이므로 스위치 1은 기본적으로 5분 후에 호스트 B의 MAC 주소를 에이징합니다. 스위치 2는 5분 후에 호스트 A를 에이징합니다. 따라서 스위치 1은 호스트 B의 대상 MAC를 사용하는 모든 패킷을 알 수 없는 유니캐스트로 처리해야 합니다. 스위치는 호스트 A에서 전송되는 패킷을 플러딩하여 모든 포트에서 호스트 B로 향하는 패킷을 플러딩합니다 또한 스위치 1에는 MAC 주소 항목 호스트 B가 없으므로 MLS 항목도 없습니다.

호스트 A가 호스트 B를 5분 동안 지속적으로 Ping한 후의 ARP 및 MAC 주소 테이블

호스트 A ARP 테이블	스위치 1 MAC 주소 테이블 MAC VLAN 포트	MSFC1 ARP 테이블	MSFC2 ARP 테이블	스위치 2 MAC 주소 테이블 MAC VLAN 포트	호스트 B ARP 테이블
10.1.1.1 : 0000.0c07.ac01	0000.0c00.0001 1 2/1	10.1.1.10 : 0000.0c00.0001	10.1.2.10 0000.0c00.0002	0000.0c00.0002 2 2/1	10.1.2.2 : 0003.6bf1.2a01
10.1.1.3 : 0003.6bf1.2a0		10.1.2.10 : 0000.0c00.0001	10.1.1.10 0000.0c00.0001		10.1.2.1 : 0000.0c07.ac01

호스트 A의 MAC 주소 항목이 스위치 2에서 에이징된 후 호스트 B에서 오는 에코 응답 패킷에 동일한 문제가 발생합니다. 호스트 B는 에코 응답을 MSFC2에 전달하며, MSFC2는 패킷을 라우팅하고 VLAN 1에서 전송합니다. 스위치에는 MAC 주소 테이블에 엔트리 호스트 A가 없으며 VLAN 1의 모든 포트에서 패킷을 플러딩해야 합니다.

비대칭 라우팅 문제는 연결을 끊지 않습니다. 그러나 비대칭 라우팅은 과도한 유니캐스트 플러딩 및 누락된 MLS 항목을 초래할 수 있습니다. 이 상황을 해결할 수 있는 세 가지 설정 변경 사항이 있습니다.

- 각 스위치의 MAC 에이징 시간을 14,400초(4시간) 이상으로 조정합니다.
- 라우터의 ARP 시간 제한을 5분(300초)으로 변경합니다.
- MAC 에이징 시간 및 ARP 시간 제한을 동일한 시간 제한 값으로 변경합니다.

바람직한 방법은 MAC 에이징 시간을 14,400초로 변경하는 것입니다. 설정 지침은 다음과 같습니다.

- Cisco IOS 소프트웨어: `mac address-table aging-time <seconds> vlan <vlan_id>`

사례 연구 #6: HSRP 가상 IP 주소가 다른 IP 주소로 보고됨

스위치의 브리징 루프로 인해 interVLAN 누수가 있는 경우 STANDBY-3-DIFFVIP1 오류 메시지가 발생 합니다.

이 오류 메시지가 표시되고 스위치의 브리징 루프로 인해 interVLAN 누수가 있는 경우, 다음 단계를 완료하여 오류를 해결합니다.

1. 패킷이 엔드 노드 간에 이동하는 경로를 식별합니다. 이 경로에 라우터가 있는 경우 다음 단계를 완료합니다. 첫 번째 스위치에서 라우터로의 경로 문제를 해결합니다. 라우터에서 두 번째 스위치로의 경로 문제를 해결합니다.
2. 경로의 각 스위치에 연결하고 엔드 노드 간 경로에서 사용되는 포트의 상태를 확인합니다.

사례 연구 #7: HSRP로 인해 보안 포트에서 MAC 위반 발생

HSRP 활성화 라우터에 연결된 스위치 포트에 포트 보안이 설정된 경우, 둘 이상의 인터페이스에서 동일한 보안 MAC 주소를 가질 수 없으므로 MAC 위반이 발생합니다. 보안 위반은 다음 상황 중 하나인 보안 포트에서 발생합니다.

- 보안 MAC 주소의 최대 수가 주소 테이블에 추가되고, MAC 주소가 주소 테이블에 없는 스테이션이 인터페이스에 액세스하려고 시도합니다.
- 하나의 보안 인터페이스에서 학습되거나 설정된 주소는 동일한 VLAN의 다른 보안 인터페이스에 표시됩니다.

기본적으로 포트 보안 위반으로 인해 스위치 인터페이스가 오류를 비활성화하고 즉시 종료하며, 이는 라우터 간의 HSRP 상태 메시지를 차단합니다.

해결 방법

- 라우터에서 **standby use-bia** 명령을 실행합니다. 이렇게 하면 라우터가 가상 MAC 주소 대신 HSRP에 버닝(burned-in)된 주소를 사용합니다.
- HSRP 활성화 라우터에 연결하는 스위치 포트에서 포트 보안을 비활성화합니다.

사례 연구 #9: %Interface 하드웨어가 여러 그룹을 지원할 수 없습니다.

여러 HSRP 그룹이 인터페이스에서 생성된 경우 이 오류 메시지가 수신됩니다.

```
%Interface hardware cannot support multiple groups
```

이 오류 메시지는 일부 라우터 또는 스위치의 하드웨어 제한으로 인해 수신됩니다. 어떤 소프트웨어 방법으로도 제한을 극복할 수 없습니다. 문제는 각 HSRP 그룹이 인터페이스에서 하나의 추가 MAC 주소를 사용하므로 이더넷 MAC 칩이 여러 HSRP 그룹을 활성화하기 위해 다양한 프로그래밍이 가능한 MAC 주소를 지원해야 한다는 것입니다.

해결 방법은 **standby use-bia** 인터페이스 설정 명령을 사용하는 것입니다. 이 명령은 사전 할당된 MAC 주소 대신 인터페이스의 BIA(Burned-In Address)를 가상 MAC 주소로 사용합니다.

Catalyst 스위치에서 HSRP 문제 해결

A. HSRP 라우터 설정 확인

1. 고유한 라우터 인터페이스 IP 주소 확인

각 HSRP 라우터에 인터페이스별로 각 서브넷에 대한 고유한 IP 주소가 있는지 확인합니다. 또한 각 인터페이스에 회선 프로토콜이 있는지 인지 확인합니다. 각 인터페이스의 현재 상태를 신속하게 확인하려면 **show ip interface brief** 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
Router_1#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.1 YES manual up up Vlan10 192.168.10.1 YES manual up up Vlan11 192.168.11.1 YES manual up up
```

```
Router_2#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.2 YES manual up up Vlan10 192.168.10.2 YES manual up up Vlan11 192.168.11.2 YES manual up up
```

2. 대기(HSRP) IP 주소 및 대기 그룹 번호 확인

설정된 대기 (HSRP) IP 주소 및 대기 그룹 번호가 각 HSRP 참여 라우터와 일치하는지 확인합니다. 대기 그룹 또는 HSRP 대기 주소가 일치하지 않으면 HSRP 문제가 발생할 수 있습니다. **show standby** 명령은 각 인터페이스의 standby 그룹 및 standby IP 주소 설정을 자세히 설명합니다. 예를 들면 다음과 같습니다.

```
Router_1#show standby Vlan10 - Group 110 State is Active 2 state changes, last state change 00:01:34 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.144 secs Preemption enabled Active router is local Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec) Priority 110 (configured 110) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:00:27 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.096 secs Preemption enabled Active router is local Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec) Priority 110 (configured 110) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1 Router_2#show standby Vlan10 - Group 110 State is Standby 1 state change, last state change 00:03:15 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.088 secs Preemption disabled Active router is 192.168.10.1, priority 110 (expires in 11.584 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Standby 1 state change, last state change 00:02:53 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.352 secs Preemption disabled Active router is 192.168.11.1, priority 110 (expires in 9.120 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1
```

3. 대기 (HSRP) IP 주소가 인터페이스별로 다른지 확인합니다.

대기 (HSRP) IP 주소가 각 인터페이스에 설정된 IP 주소에서 고유한지 확인합니다. **show standby** 명령은 이 정보를 보기 위한 빠른 참조입니다. 예를 들면 다음과 같습니다.

```
Router_1#show standby Vlan10 - Group 110 State is Active 2 state changes, last state change 00:01:34 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.144 secs Preemption enabled Active router is local Standby router is 192.168.10.2, priority 109 (expires in 10.784 sec) Priority 110 (configured 110) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:00:27 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.096 secs Preemption enabled Active router is local Standby router is 192.168.11.2, priority 109 (expires in 8.944 sec) Priority 110 (configured 110) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1 Router_2#show standby Vlan10 - Group 110 State is Standby 1 state change, last state change 00:03:15 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 1.088 secs Preemption disabled Active router is 192.168.10.1, priority 110 (expires in 11.584 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Standby 1 state change, last state change 00:02:53 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 2.352 secs Preemption disabled Active router is 192.168.11.1, priority 110 (expires in 9.120 sec) Standby router is local Priority 109 (configured 109) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1
```

4. 대기 use-bia 명령을 사용해야 하는 경우

HSRP가 토큰 링 인터페이스에 설정되지 않은 경우, 특별한 상황에서는 **standby use-bia** 명령만 사용합니다. 이 명령은 HSRP 그룹에 대한 가상 HSRP MAC 주소 대신 BIA를 사용하도록 라우터에 지시합니다. 토큰 링 네트워크에서 SRB(source-route bridging)를 사용 중인 경우, **standby use-bia** 명령을 사용하면 새 활성 라우터가 Gratuitous ARP를 사용하여 호스트 RIF(Routing Information Field) 캐시를 업데이트할 수 있습니다. 그러나 모든 호스트 구현이 Gratuitous ARP를 올바르게 처리하는 것은 아닙니다. **standby use-bia** 명령에 대한 또 다른 주의 사항은 proxy ARP와 관련이 있습니다. 대기 라우터는 장애가 발생한 액티브 라우터의 손실된 프록시 ARP 데이터베이스를 처리할 수 없습니다.

5. 액세스 목록 설정 확인

모든 HSRP 피어에 설정된 액세스 목록이 해당 인터페이스에 설정된 HSRP 주소를 필터링하지 않는지 확인합니다. 특히 서브넷의 모든 라우터에 트래픽을 전송하는 데 사용되는 멀티캐스트 주소를 확인합니다(**224.0.0.2**). 또한 HSRP 포트 **1985**로 향하는 UDP 트래픽이 필터링되지 않았는지 확인합니다. HSRP는 이 주소 및 포트를 사용하여 피어 간에 hello 패킷을 전송합니다. 라우터에 설정된 액세스 목록을 기록하려면 **show access-lists** 명령을 빠른 참조로 실행합니다. 예를 들면 다음과 같습니다.

```
Router_1#show access-lists
Standard IP access list 77
  deny 10.19.0.0, wildcard bits 0.0.255.255
  permit any
Extended IP access list 144
  deny pim 238.0.10.0 0.0.0.255 any
  permit ip any any (58 matches)
```

B. Catalyst Fast EtherChannel 및 트렁킹 설정 확인

1. 트렁킹 설정 확인

HSRP 라우터를 연결하기 위해 트렁크를 사용하는 경우, 라우터 및 스위치에서 트렁킹 설정을 확인합니다. 5개의 가능한 트렁킹 모드가 있습니다.

- on
- desirable
- 자동
- 꺼짐
- nonegotiate

설정된 트렁킹 모드가 원하는 트렁킹 방법을 제공하는지 확인합니다.

HSRP 문제를 해결할 때 스위치 대 스위치 연결에 대해 *desirable* 설정을 사용합니다. 이 설정은 스위치 포트가 트렁크를 올바르게 설정할 수 없는 문제를 격리할 수 있습니다. 대부분의 Cisco IOS 라우터는 트렁크 협상을 지원하지 않으므로 라우터 대 스위치 설정을 *nonegotiate*로 설정합니다.

IEEE 802.1Q(dot1q) 트렁킹 모드의 경우 트렁크의 양쪽이 동일한 네이티브 VLAN 및 캡슐화를 사용하도록 구성되었는지 확인합니다. 시스코 제품은 기본적으로 네이티브 VLAN에 태그를 지정하지 않으므로 네이티브 VLAN 설정이 일치하지 않으면 일치하지 않는 VLAN에 연결되지 않습니다. 마지막으로, 트렁크가 라우터에 설정된 VLAN을 전달하도록 설정되었는지 확인하고, VLAN이 정리되지 않고 라우터 연결 포트에 대한 STP 상태에 있는지 확인합니다. 이 정보를 보여주는 빠른 참조를 위해 **show interfaces <interface> trunk** 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
L2Switch_1#show interfaces gigabitEthernet1/0/13 trunk Port Mode Encapsulation Status Native vlan Gi1/0/13 on 802.1q trunking
1 Port Vlans allowed on trunk Gi1/0/13 1-4094 Port Vlans allowed and active in management domain Gi1/0/13 1,10-11,70,100,300-309
Port Vlans in spanning tree forwarding state and not pruned Gi1/0/13 1,10-11,70,100,300-309
Router_1#show interfaces gigabitEthernet1/0/1 trunk Port Mode Encapsulation Status Native vlan Gi1/0/1 on 802.1q trunking 1
Port Vlans allowed on trunk Gi1/0/1 1-4094 Port Vlans allowed and active in management domain Gi1/0/1 1,10-11,100,206,301,307,401,900,3001-3002
Port Vlans in spanning tree forwarding state and not pruned Gi1/0/1 1,10-11,100,206,301,307,401,900,3001-3002
```

2. Fast EtherChannel(포트 채널링) 설정 확인

HSRP 라우터를 연결하기 위해 포트 채널을 사용하는 경우, 라우터와 스위치 모두에서 EtherChannel 설정을 확인합니다. 하나 이상의 측에서 스위치 대 스위치 포트 채널을 적절하게 설정합니다. 다른 쪽은 다음 모드 중 하나일 수 있습니다.

- on
- desirable
- 자동

그러나 이 예에서 인터페이스는 포트 채널의 멤버가 아닙니다.

```
Router_1#show etherchannel summary Flags: D - down P - bundled in port-channel I - stand-alone s - suspended H - Hot-standby
(LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator M - not in use, minimum links not met u - unsuitable
for bundling w - waiting to be aggregated d - default port A - formed by Auto LAG Number of channel-groups in use: 0 Number of
aggregators: 0 Group Port-channel Protocol Ports -----+-----+-----+----- Router_1#
Router_2#show etherchannel summary Flags: D - down P - bundled in port-channel I - stand-alone s - suspended H - Hot-standby
(LACP only) R - Layer3 S - Layer2 U - in use f - failed to allocate aggregator M - not in use, minimum links not met u - unsuitable
for bundling w - waiting to be aggregated d - default port A - formed by Auto LAG Number of channel-groups in use: 0 Number of
aggregators: 0 Group Port-channel Protocol Ports -----+-----+-----+----- Router_2#
```

3. 스위치 MAC 주소 전달 테이블 조사

HSRP 가상 MAC 주소 및 물리적 BIA에 대한 HSRP 라우터의 스위치에 MAC 주소 테이블 항목이 있는지 확인합니다. 라우터의 **show standby** 명령은 가상 MAC 주소를 제공합니다. **show interface** 명령은 물리적 BIA를 제공합니다. 다음은 샘플 출력입니다.

```
Router_1#show standby Vlan10 - Group 110 State is Active 2 state changes, last state change 00:37:03 Virtual IP address is
192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1
default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.768 secs Preemption enabled Active router is local Standby router is
192.168.10.2, priority 109 (expires in 10.368 sec) Priority 110 (configured 110) Group name is "hsrp-VI10-110" (default) FLAGS:
0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:35:56 Virtual IP address is 192.168.11.100 Active
virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec,
hold time 10 sec Next hello sent in 1.472 secs Preemption enabled Active router is local Standby router is 192.168.11.2, priority
109 (expires in 8.336 sec) Priority 110 (configured 110) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1
```

```
Router_1#show interfaces vlan 10 Vlan10 is up, line protocol is up, Autostate Enabled Hardware is Ethernet SVI, address is
d4e8.801f.4846 (bia d4e8.801f.4846) Internet address is 192.168.10.1/24 MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive not supported ARP type: ARPA,
ARP Timeout 04:00:00 Last input 00:00:00, output 00:00:01, output hang never Last clearing of "show interface" counters never
Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5
minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 9258 packets input, 803066 bytes, 0 no
buffer Received 0 broadcasts (0 IP multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
3034 packets output, 368908 bytes, 0 underruns Output 0 broadcasts (0 IP multicasts) 0 output errors, 2 interface resets 0
unknown protocol drops 0 output buffer failures, 0 output buffers swapped out
```

```
L2Switch_1#show mac address-table address 0000.0c07.ac6e Mac Address Table ----- Vlan Mac
Address Type Ports ----
10 0000.0c07.ac6e DYNAMIC Gi1/0/13 Total Mac Addresses for this criterion: 1
L2Switch_1#show mac address-table address 0000.0c07.ac6f Mac Address Table ----- Vlan Mac
```

Address Type Ports ----- 11 0000.0c07.ac6f DYNAMIC Gi1/0/13 Total Mac Addresses for this criterion: 1

항목의 에이징 속도를 확인하려면 CAM 에이징 시간을 확인해야 합니다. 시간이 STP 전달 지연에 대해 설정된 값과 같고 이것이 기본적으로 15초인 경우, 네트워크에 STP 루프가 있을 가능성이 높습니다. 다음은 샘플 명령 출력입니다.

```
L2Switch_1#show mac address-table aging-time vlan 10 Global Aging Time: 300 Vlan Aging Time ----- 10 300
L2Switch_1#show mac address-table aging-time vlan 11 Global Aging Time: 300 Vlan Aging Time ----- 11 300
```

C. 물리적 레이어 연결 확인

HSRP 그룹에서 둘 이상의 라우터가 활성화되면 해당 라우터는 동료 HSRP 피어에서 hello 패킷을 일관되게 수신하지 않습니다. 물리적 레이어 문제로 인해 피어 간의 트래픽이 일관되게 전달되지 않아 이러한 시나리오가 발생할 수 있습니다. HSRP 문제를 해결하는 경우 HSRP 피어 간의 물리적 연결 및 IP 연결을 확인해야 합니다. 연결을 확인하려면 **show standby** 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
Router_1#show standby Vlan10 - Group 110 State is Active 2 state changes, last state change 00:54:03 Virtual IP address is 192.168.10.100 Active virtual MAC address is 0000.0c07.ac6e (MAC In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.848 secs Preemption enabled Active router is local Standby router is unknown Priority 110 (configured 110) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Active 2 state changes, last state change 00:52:56 Virtual IP address is 192.168.11.100 Active virtual MAC address is 0000.0c07.ac6f (MAC In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Next hello sent in 0.512 secs Preemption enabled Active router is local Standby router is unknown Priority 110 (configured 110) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1
```

```
Router_2#show standby Vlan10 - Group 110 State is Init (interface down) 2 state changes, last state change 00:00:42 Virtual IP address is 192.168.10.100 Active virtual MAC address is unknown (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6e (v1 default) Hello time 3 sec, hold time 10 sec Preemption disabled Active router is unknown Standby router is unknown Priority 109 (configured 109) Group name is "hsrp-VI10-110" (default) FLAGS: 0/1 Vlan11 - Group 111 State is Init (interface down) 2 state changes, last state change 00:00:36 Virtual IP address is 192.168.11.100 Active virtual MAC address is unknown (MAC Not In Use) Local virtual MAC address is 0000.0c07.ac6f (v1 default) Hello time 3 sec, hold time 10 sec Preemption disabled Active router is unknown Standby router is unknown Priority 109 (configured 109) Group name is "hsrp-VI11-111" (default) FLAGS: 0/1
```

1. 인터페이스 상태 확인

인터페이스 확인 이 예시에 나와있는 것처럼 모든 HSRP 설정 인터페이스가 / 상태인지 확인합니다

```
Router_1#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.1 YES manual up up Vlan10 192.168.10.1 YES manual up up Vlan11 192.168.11.1 YES manual up up Router_2#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.2 YES manual up up Vlan10 192.168.10.2 YES manual administratively down down Vlan11 192.168.11.2 YES manual administratively down down
```

인터페이스가 관리상 / 된 경우, 라우터에 설정 모드를 입력하고 **no shutdown** 인터페이스 전용 명령을 실행합니다. 예를 들면 다음과 같습니다.

```
Router_2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router_2(config)#interface vlan 10
Router_2(config-if)#no shutdown
Router_2(config-if)#end
```

```
Router_2#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router_2(config)#interface vlan 11
Router_2(config-if)#no shutdown Router_2(config-if)#end
```

```
Router_2#show ip interface brief Interface IP-Address OK? Method Status Protocol Vlan1 192.168.1.2 YES manual up up Vlan10
```

192.168.10.2 YES manual up down Vlan11 192.168.11.2 YES manual up up

인터페이스가 / 또는 / 상태인 경우, 로그에서 인터페이스 변경 알림을 검토합니다. Cisco IOS 소프트웨어 기반 스위치의 경우, 링크 / 상황에 대해 다음 메시지가 표시됩니다.

```
%LINK-3-UPDOWN: Interface "interface", changed state to up
%LINK-3-UPDOWN: Interface "interface", changed state to down
```

Router_1#show log

```
3d04h: %STANDBY-6-STATECHANGE: Standby: 0: Vlan10 state Active-> Speak
3d04h: %LINK-5-CHANGED: Interface Vlan10, changed state to down
3d04h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down
```

HSRP 피어 사이에 있는 포트, 케이블 및 트랜시버 또는 기타 디바이스를 검사합니다. 누군가가 연결을 제거하거나 느슨하게 하였습니까? 링크가 반복적으로 손실되는 인터페이스가 있습니까? 올바른 케이블 유형이 사용되었습니까? 다음 예시와 같이 인터페이스에 오류가 있는지 확인합니다.

```
Router_2#show interface vlan 10 Vlan10 is down, line protocol is down , Autostate Enabled Hardware is Ethernet SVI, address is 1880.90d8.5946 (bia 1880.90d8.5946) Internet address is 192.168.10.2/24 MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive not supported ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:10, output 00:00:08, output hang never Last clearing of "show interface" counters never Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 0 bits/sec, 0 packets/sec 5 minute output rate 0 bits/sec, 0 packets/sec 1243 packets input, 87214 bytes, 0 no buffer Received 0 broadcasts (0 IP multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 23 packets output, 1628 bytes, 0 underruns Output 0 broadcasts (0 IP multicasts) 0 output errors, 2 interface resets 0 unknown protocol drops 0 output buffer failures, 0 output buffers swapped out
```

2. 링크 변경 및 포트 오류

스위치 포트 링크 변경 사항 및 기타 오류를 확인합니다. 다음 명령을 실행하고 출력을 검토합니다.

- 로깅 표시
- **show interfaces <interface> 카운터**
- **show interfaces <interface> status**

이러한 명령을 사용하면 스위치와 다른 디바이스 간의 연결에 문제가 있는지 확인할 수 있습니다.

이러한 메시지는 링크 / 상황에서 정상적으로 표시됩니다.

```
L2Switch_1#show logging Syslog logging: enabled (0 messages dropped, 5 messages rate-limited, 0 flushes, 0 overruns, xml disabled, filtering disabled) No Active Message Discriminator. No Inactive Message Discriminator. Console logging: level informational, 319 messages logged, xml disabled, filtering disabled Monitor logging: level debugging, 0 messages logged, xml disabled, filtering disabled Buffer logging: level debugging, 467 messages logged, xml disabled, filtering disabled Exception Logging: size (4096 bytes) Count and timestamp logging messages: disabled File logging: disabled Persistent logging: disabled No active filter modules. Trap logging: level informational, 327 message lines logged Logging Source-Interface: VRF Name: Log Buffer (10000 bytes): *Jul 26 17:52:07.526: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to up *Jul 26 17:52:09.747: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/13, changed state to down *Jul 26 17:57:11.716: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307. *Jul 26 17:57:11.716: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type. *Jul 26 17:57:13.583: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up *Jul 26 17:57:16.237: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down *Jul 26 18:02:16.481: %SPANTREE-7-RECV_1Q_NON_TRUNK: Received 802.1Q BPDU on non trunk GigabitEthernet1/0/16 VLAN307. *Jul 26 18:02:16.481: %SPANTREE-7-BLOCK_PORT_TYPE: Blocking GigabitEthernet1/0/16 on VLAN0307. Inconsistent port type. *Jul 26 18:02:18.367: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to up *Jul 26 18:02:20.561: %LINK-3-UPDOWN: Interface GigabitEthernet1/0/16, changed state to down
```

포트의 일반적인 상태를 확인하려면 **show interfaces <interface> status** 명령을 실행합니다. 예를 들면 다음과 같습니다.

Cisco IOS에서 debug standby 명령을 사용하여 HSRP 디버그 기능을 활성화합니다. 이 정보는 문제가 간헐적으로 발생하고 일부 인터페이스에만 영향을 미치는 경우에 유용합니다. 디버그를 사용하면 해당 HSRP 라우터가 특정 간격으로 HSRP hello 패킷을 수신하고 전송하는지 확인할 수 있습니다. 라우터가 hello 패킷을 수신하지 않는 경우 피어가 hello 패킷을 전송하지 않거나 네트워크가 패킷을 삭제하는 것을 유추할 수 있습니다.

명령을 사용합니다 목적

디버그 대기 HSRP 디버깅 활성화

다음은 샘플 명령 출력입니다.

```
Router_1#debug standby HSRP debugging is on Jul 29 16:12:16.889: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100 Jul 29 16:12:16.996: HSRP: V111 Grp 111 Hello in 192.168.11.2 Standby pri 109 vIP 192.168.11.100 Jul 29 16:12:17.183: HSRP: V110 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100 Jul 29 16:12:17.366: HSRP: V111 Grp 111 Hello out 192.168.11.1 Active pri 110 vIP 192.168.11.100 Jul 29 16:12:18.736: HSRP: V110 Interface adv in, Passive, active 0, passive 1, from 192.168.10.2 Jul 29 16:12:19.622: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
```

2. 조건부 HSRP 디버깅(대기 그룹 및/또는 VLAN을 기준으로 출력 제한)

Cisco IOS 소프트웨어 릴리스 12.0(3)에는 debug standby 명령의 출력을 인터페이스 및 그룹 번호를 기준으로 필터링할 수 있는 디버그 조건이 도입되었습니다. 이 명령은 Cisco IOS 소프트웨어 릴리스 12.0에 도입된 디버그 조건 패러다임을 활용합니다.

명령을 사용합니다

목적

디버그 조건 standby <interface> <group> 그룹의 HSRP 조건부 디버깅을 활성화합니다(0-255)

인터페이스는 HSRP를 지원할 수 있는 유효한 인터페이스여야 합니다. 그룹은 0~255의 모든 그룹일 수 있습니다. 존재하지 않는 그룹에 대해 디버그 조건을 설정할 수 있습니다. 이렇게 하면 새 그룹을 초기화하는 동안 디버그를 캡처할 수 있습니다. 디버그 출력을 생성하려면 디버그 대기를 활성화해야 합니다. 대기 디버그 조건이 없으면 모든 인터페이스의 모든 그룹에 대해 디버그 출력이 생성됩니다. 하나 이상의 대기 디버그 조건이 있는 경우 모든 대기 디버그 조건을 기준으로 대기 디버그 출력이 필터링됩니다. 다음은 샘플 명령 출력입니다.

```
Router_1#debug condition standby vlan 10 110
Condition 1 set
Router_1#
Jul 29 16:16:20.284: V110 HSRP110 Debug: Condition 1, hsrp V110 HSRP110 triggered, count 1
Router_1#debug standby
HSRP debugging is on
Router_1#
Jul 29 16:16:44.797: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:45.381: HSRP: V110 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
Jul 29 16:16:47.231: HSRP: V110 Grp 110 Hello out 192.168.10.1 Active pri 110 vIP 192.168.10.100
Jul 29 16:16:48.248: HSRP: V110 Grp 110 Hello in 192.168.10.2 Standby pri 109 vIP 192.168.10.100
```

3. 향상된 HSRP 디버깅

Cisco IOS 소프트웨어 릴리스 12.1(1)에는 향상된 HSRP 디버깅이 추가되었습니다. 유용한 정보를 찾기 위해 향상된 HSRP 디버깅은 주기적인 hello 메시지의 노이즈를 제한하고 추가 상태 정보를 포함합니다. 이 정보는 서비스 요청을 생성하는 경우 시스코 기술 지원 엔지니어와 작업할 때 특히 유용합니다.

명령을 사용합니다

디버그 대기

목적

모든 HSRP 오류, 이벤트 및 패킷을 포

16:54:36.378: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:38.856: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100 *Jul 29 16:54:38.876: HSRP: V110 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:41.688: HSRP: V110 Grp 110 Hello out 192.168.10.2 Standby pri 109 vIP 192.168.10.100 *Jul 29 16:54:41.717: HSRP: V110 Grp 110 Hello in 192.168.10.1 Active pri 110 vIP 192.168.10.100

E. 스페닝 트리 문제 해결

네트워크의 STP 루프 상태 또는 불안정성은 HSRP 피어의 적절한 통신을 방해할 수 있습니다. 이러한 부적절한 통신으로 인해 각 피어가 활성 라우터가 됩니다. STP 루프는 브로드캐스트 스톱, 중복 프레임 및 MAC 테이블 불일치를 유발할 수 있습니다. 이러한 모든 문제는 전체 네트워크, 특히 HSRP에 영향을 줍니다. HSRP 오류 메시지는 STP 문제의 첫 번째 지표가 될 수 있습니다.

STP 문제를 해결하는 경우 각 VLAN에서 네트워크의 STP 토폴로지를 반드시 이해해야 합니다. 루트 브리지인 스위치와 차단 및 전달에 있는 스위치의 포트를 확인해야 합니다. 각 VLAN에는 자체 STP 토폴로지가 있으므로 이 정보는 각 VLAN에서 매우 중요합니다.

1. 스페닝 트리 설정 확인

네트워크의 모든 스위치 및 브리징 디바이스에 STP가 설정되어 있는지 확인합니다. 각 스위치에서 루트 브리지가 있을 것으로 간주되는 위치를 확인합니다. 또한 다음 타이머의 값을 확인합니다.

-
- Hello Time
-

이 모든 정보를 보려면 `show spanning-tree` 명령을 실행합니다. 기본적으로 이 명령은 모든 VLAN에 대해 이 정보를 표시합니다. 그러나 명령과 함께 VLAN 번호를 제공하면 다른 VLAN 정보도 필터링할 수 있습니다. 이 정보는 STP 문제를 트러블슈팅할 때 매우 유용합니다.

`show spanning-tree` 출력에서 참고하는 이 세 타이머는 루트 브리지에서 학습됩니다. 이러한 타이머는 해당 특정 브리지에 설정된 타이머와 일치하지 않아도 됩니다. 그러나 이 스위치가 언제든지 루트 브리지가 되는 경우 타이머가 루트 브리지와 일치하는지 확인합니다. 루트 브리지에 대한 이러한 타이머의 일치는 연속성과 관리 편의성을 유지하는 데 도움이 됩니다. 또한 일치하면 잘못된 타이머를 가진 스위치가 네트워크를 손상시키는 것을 방지할 수 있습니다.

참고: 네트워크에 이중화 링크가 있는지 여부와 상관없이 모든 VLAN에 대해 항상 STP를 활성화합니다. 비중복 네트워크에서 STP를 활성화하면 중단이 방지됩니다. 누군가가 허브 또는 다른 스위치와 함께 스위치를 브리징하고 실수로 물리적 루프를 생성하는 경우 손상이 발생할 수 있습니다. STP는 특정 문제를 격리하는 데에도 매우 유용합니다. STP를 활성화하여 네트워크의 일부 작업에 영향을 주는 경우 격리해야 하는 기존 문제가 있을 수 있습니다.

다음은 `show spanning-tree` 명령의 샘플 출력입니다.

```
L2Switch_1#show spanning-tree vlan 10 VLAN0010 Spanning tree enabled protocol rstp Root ID Priority 32778 Address 00fe.c8d3.8680 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32778 (priority 32768 sys-id-ext 10) Address 00fe.c8d3.8680 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 300 sec Interface Role Sts Cost Prio.Nbr Type ----- Gi1/0/3 Desg FWD 4 128.3 P2p Gi1/0/10 Desg FWD 4 128.10 P2p Edge Gi1/0/11 Desg FWD 4 128.11 P2p Gi1/0/13 Desg FWD 4 128.13 P2p Gi1/0/14 Desg FWD 4 128.14 P2p Gi1/0/15 Desg FWD 4 128.15 P2p Gi1/0/16 Desg FWD 4 128.16 P2p Gi1/0/35 Desg FWD 4 128.35 P2p
L2Switch_1#show spanning-tree vlan 11 VLAN0011 Spanning tree enabled protocol rstp Root ID Priority 32779 Address 00fe.c8d3.8680 This bridge is the root Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Bridge ID Priority 32779 (priority 32768 sys-id-ext 11) Address 00fe.c8d3.8680 Hello Time 2 sec Max Age 20 sec Forward Delay 15 sec Aging Time 300 sec Interface Role Sts Cost Prio.Nbr Type ----- Gi1/0/3 Desg FWD 4 128.3 P2p Gi1/0/10 Desg FWD 4 128.10 P2p Edge Gi1/0/11 Desg FWD 4 128.11 P2p Gi1/0/13 Desg FWD 4 128.13 P2p Gi1/0/14 Desg FWD 4 128.14 P2p Gi1/0/15 Desg FWD 4 128.15 P2p Gi1/0/16 Desg FWD 4 128.16 P2p Gi1/0/35 Desg FWD 4 128.35 P2p
```

스위치 L2Switch_1은 VLAN 10 및 VLAN 11의 루트입니다.

2. 스페닝 트리 루프 상태

STP 루프가 발생하려면 네트워크에 L2 물리적 이중화가 있어야 합니다. 물리적 루프 조건의 가능성이 없는 경우 STP가 발생하지 않습니다. STP 루프 조건의 증상은 다음과 같습니다.

- 총 네트워크 중단
- 연결 손실
- 프로세스 및 시스템 사용률이 높은 네트워크 장비별 보고서

STP 루프 조건이 발생하는 단일 VLAN은 링크를 혼잡하게 하고 대역폭의 다른 VLAN을 부족하게 할 수 있습니다. `show interfaces <interface> controller` 명령은 어떤 포트가 과도한 수의 패킷을 전송 또는 수신하는지 알려줍니다. 과도한 브로드캐스트 및 멀티캐스트는 일부 STP 루프의 포트를 나타낼 수 있습니다. 일반적으로 멀티캐스트 또는 브로드캐스트가 유니캐스트 패킷의 수를 초과할 때마다 STP 루프 조건의 링크가 의심됩니다.

참고: 스위치에서는 멀티캐스트 프레임으로 수신 및 전송된 STP BPDU(Bridge Protocol Data Unit)도 계산합니다. STP 차단 상태에 있는 포트는 여전히 STP BPDU를 전송 및 수신합니다.

```
Router_2#show interfaces gi1/0/1 controller GigabitEthernet1/0/1 is up, line protocol is up (connected) Hardware is Gigabit Ethernet, address is 1880.90d8.5901 (bia 1880.90d8.5901) Description: PNP STARTUP VLAN MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec, reliability 255/255, txload 1/255, rxload 1/255 Encapsulation ARPA, loopback not set Keepalive set (10 sec) Full-duplex, 1000Mb/s, media type is 10/100/1000BaseTX input flow-control is on, output flow-control is unsupported ARP type: ARPA, ARP Timeout 04:00:00 Last input 00:00:00, output 00:00:04, output hang never Last clearing of "show interface" counters never Input queue: 0/2000/0/0 (size/max/drops/flushes); Total output drops: 0 Queueing strategy: fifo Output queue: 0/40 (size/max) 5 minute input rate 33000 bits/sec, 31 packets/sec 5 minute output rate 116000 bits/sec, 33 packets/sec 9641686 packets input, 1477317083 bytes, 0 no buffer Received 1913802 broadcasts (1151766 multicasts) 0 runts, 0 giants, 0 throttles 0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored 0 watchdog, 1151766 multicast, 0 pause input 0 input packets with dribble condition detected 10702696 packets output, 4241534645 bytes, 0 underruns Output 3432 broadcasts (0 multicasts) 0 output errors, 0 collisions, 2 interface resets 9582 unknown protocol drops 0 babbles, 0 late collision, 0 deferred 0 lost carrier, 0 no carrier, 0 pause output 0 output buffer failures, 0 output buffers swapped out Transmit GigabitEthernet1/0/1 Receive 4241534645 Total bytes 1477317083 Total bytes 10562003 Unicast frames 7727884 Unicast frames 4229489212 Unicast bytes 1291270617 Unicast bytes 137261 Multicast frames 1151766 Multicast frames 11812065 Multicast bytes 91096867 Multicast bytes 3432 Broadcast frames 762036 Broadcast frames 233368 Broadcast bytes 94949599 Broadcast bytes 0 System FCS error frames 0 IpgViolation frames 0 MacUnderrun frames 0 MacOverrun frames 0 Pause frames 0 Pause frames 0 Cos 0 Pause frames 0 Cos 0 Pause frames 0 Cos 1 Pause frames 0 Cos 1 Pause frames 0 Cos 2 Pause frames 0 Cos 2 Pause frames 0 Cos 3 Pause frames 0 Cos 3 Pause frames 0 Cos 4 Pause frames 0 Cos 4 Pause frames 0 Cos 5 Pause frames 0 Cos 5 Pause frames 0 Cos 6 Pause frames 0 Cos 6 Pause frames 0 Cos 7 Pause frames 0 Cos 7 Pause frames 0 Oam frames 0 OamProcessed frames 0 Oam frames 0 OamDropped frames 38144 Minimum size frames 4165201 Minimum size frames 4910833 65 to 127 byte frames 3126489 65 to 127 byte frames 1237675 128 to 255 byte frames 750243 128 to 255 byte frames 1029126 256 to 511 byte frames 1279281 256 to 511 byte frames 2205966 512 to 1023 byte frames 103668 512 to 1023 byte frames 1280952 1024 to 1518 byte frames 205229 1024 to 1518 byte frames 0 1519 to 2047 byte frames 11575 1519 to 2047 byte frames 0 2048 to 4095 byte frames 0 2048 to 4095 byte frames 0 4096 to 8191 byte frames 0 4096 to 8191 byte frames 0 8192 to 16383 byte frames 0 8192 to 16383 byte frames 0 16384 to 32767 byte frame 0 16384 to 32767 byte frame 0 > 32768 byte frames 0 > 32768 byte frames 0 Late collision frames 0 SymbolErr frames 0 Excess Defer frames 0 Collision fragments 0 Good (1 coll) frames 0 ValidUnderSize frames 0 Good (>1 coll) frames 0 InvalidOverSize frames 0 Deferred frames 0 ValidOverSize frames 0 Gold frames dropped 0 FcsErr frames 0 Gold frames truncated 0 Gold frames successful 0 1 collision frames 0 2 collision frames 0 3 collision frames 0 4 collision frames 0 5 collision frames 0 6 collision frames 0 7 collision frames 0 8 collision frames 0 9 collision frames 0 10 collision frames 0 11 collision frames 0 12 collision frames 0 13 collision frames 0 14 collision frames 0 15 collision frames 0 Excess collision frames 0 LAST UPDATE 2384 msecs AGO
```

3. 토폴로지 변경 알림

STP 문제 진단에 필수적인 또 다른 명령은 `show spanning-tree detail` 명령입니다. 이 명령은 TCN(Topology Change Notification) 메시지를 다시 발신자로 추적합니다. 스위치 간에 특수 BPDU로 전송되는 이러한 메시지는 스위치에서 토폴로지가 변경되었음을 나타냅니다. 이 스위치는

루트 포트에 TCN을 전송합니다. TCN은 업스트림을 루트 브리지로 이동합니다. 그런 다음 루트 브리지는 모든 포트에서 또 다른 특수 BPDU인 TCA(Topology Change Acknowledgment)를 전송합니다. 루트 브리지는 설정 BPDU에서 TCN 비트를 설정합니다. 이렇게 하면 모든 비 루트 브리지가 MAC 주소 테이블 에이징 타이머를 설정 STP 전달 지연으로 설정합니다.

이 문제를 격리하려면 각 VLAN의 루트 브리지에 액세스하고 스위치 연결 포트에 대해 **show spanning-tree <interface> detail** 명령을 실행합니다. 마지막 항목은 마지막 TCN이 수신된 시간을 제공합니다. 이 상황에서는 너무 늦어서 가능한 STP 루프를 유발할 수 있는 TCN을 발급한 사람을 확인할 수 없습니다. `Number of topology changes` (수) 항목은 발생하는 TCN 수에 대한 아이디어를 제공합니다. STP 루프 중에 이 카운터는 1분마다 증가할 수 있습니다. 더 자세한 사항은 [스패닝 트리 프로토콜 문제 및 관련 설계 고려 사항](#)을 참조하십시오.

기타 유용한 정보는 다음과 같습니다.

- 마지막 TCN의 포트
- 마지막 TCN 시간
- 현재 TCN 수

다음은 샘플 명령 출력입니다.

```
L2Switch_1#show spanning-tree vlan 10 detail VLAN0010 is executing the rstp compatible Spanning Tree protocol Bridge Identifier has priority 32768, sysid 10, address 00fe.c8d3.8680 Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6 We are the root of the spanning tree Topology change flag not set, detected flag not set Number of topology changes 8 last change occurred 03:21:48 ago from GigabitEthernet1/0/35 Times: hold 1, topology change 35, notification 2 hello 2, max age 20, forward delay 15 Timers: hello 0, topology change 0, notification 0, aging 300 Port 3 (GigabitEthernet1/0/3) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.3. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.3, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 0 Port 10 (GigabitEthernet1/0/10) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.10. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.10, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 The port is in the portfast mode by portfast trunk configuration Link type is point-to-point by default BPDU: sent 6063, received 0 Port 11 (GigabitEthernet1/0/11) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.11. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.11, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 0 Port 13 (GigabitEthernet1/0/13) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.13. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.13, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 3 Port 14 (GigabitEthernet1/0/14) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.14. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.14, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6066, received 3 Port 15 (GigabitEthernet1/0/15) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.15. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.15, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6067, received 0 Port 16 (GigabitEthernet1/0/16) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.16. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.16, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6067, received 0 Port 35 (GigabitEthernet1/0/35) of VLAN0010 is designated forwarding Port path cost 4, Port priority 128, Port Identifier 128.35. Designated root has priority 32778, address 00fe.c8d3.8680 Designated bridge has priority 32778, address 00fe.c8d3.8680 Designated port id is 128.35, designated path cost 0 Timers: message age 0, forward delay 0, hold 0 Number of transitions to forwarding state: 1 Link type is point-to-point by default BPDU: sent 6067, received 0
```

이 출력은 마지막 토폴로지 변경이 인터페이스 GigabitEthernet1/0/35에 연결되지 않은 디바이스에서 발생했음을 보여줍니다. 그런 다음 이 디바이스에서 동일한 **show spanning-tree detail** 명령을 실행하여 문제를 추적합니다. TCN을 생성하는 이 스위치가 PC 또는 엔드포인트에만 연결되어 있는 경우 STP PortFast가 이러한 포트에서 활성화되어 있는지 확인하십시오. STP PortFast는 포트가

상태를 전환할 때 STP TCN을 억제합니다.

STP에 대한 정보 및 NIC(Network Interface Card)와 연결된 링크 전환 문제를 해결하는 방법에 대한 정보는 다음 문서를 참조하십시오.

- [PortFast 및 기타 명령을 사용하여 워크스테이션 시작 연결 지연 해결](#)
- [Rapid Spanning Tree Protocol 이해\(802.1w\)](#)
- [STP 문제 및 관련 설계 고려 사항](#)

4. 연결 해제된 차단된 포트

FEC(Fast EtherChannel) (포트 채널링)의 로드 밸런싱 특성으로 인해 FEC 문제는 HSRP 및 STP 문제에 모두 기여할 수 있습니다. STP 또는 HSRP의 문제를 해결할 때 모든 FEC 연결에 대한 컨피그레이션을 제거할 수 있습니다. 컨피그레이션 변경 사항이 적용된 후 두 스위치에서 **show spanning-tree blockedports** 명령을 실행합니다. 포트 중 하나 이상이 연결 양쪽에서 차단을 시작하는지 확인합니다.

Fast EtherChannel에 대한 자세한 내용은 다음 문서를 참조하십시오.

- [Catalyst 스위치의 EtherChannel 로드 밸런싱 및 이중화 이해](#)
- [EtherChannel 구성](#)

5. 브로드캐스트 억제

브로드캐스트 스톱의 영향을 줄이기 위해 브로드캐스트 억제를 활성화합니다. 브로드캐스트 스톱은 STP 루프의 주요 부작용 중 하나입니다. 다음은 샘플 명령 출력입니다.

```
L2Switch_1#show run interface TenGigabitEthernet1/1/5 Building configuration... Current configuration : 279 bytes ! interface TenGigabitEthernet1/1/5 switchport trunk allowed vlan 300-309 switchport mode trunk storm-control broadcast level 30.00 storm-control multicast level 30.00 storm-control unicast level 30.00 spanning-tree guard root end L2Switch_1#show storm-control broadcast Key: U - Unicast, B - Broadcast, M - Multicast Interface Filter State Upper Lower Current Action Type -----  
----- Te1/1/5 Forwarding 30.00% 30.00% 0.00% None B Te1/1/7 Link Down 30.00% 30.00% 0.00% None B Te1/1/8 Forwarding 10.00% 10.00% 0.00% None B L2Switch_1#show storm-control multicast Key: U - Unicast, B - Broadcast, M - Multicast Interface Filter State Upper Lower Current Action Type -----  
---- Te1/1/5 Forwarding 30.00% 30.00% 0.00% None M Te1/1/7 Link Down 30.00% 30.00% 0.00% None M
```

6. 콘솔 및 Telnet 액세스

스위치에 대한 콘솔 또는 Telnet 트래픽은 STP 루프 중에 문제가 되는 디바이스를 적절하게 추적하기에는 너무 느려지는 경우가 많습니다. 네트워크를 즉시 복구하려면 모든 중복된 물리적 링크를 제거합니다. STP가 새로운 비이중화 토폴로지에서 다시 통합하도록 허용된 후 한 번에 하나의 이중화된 링크를 재연결합니다. 하나의 특정 세그먼트를 추가한 후 STP 루프가 반환되면 문제가 되는 디바이스를 식별한 것입니다.

7. 스페닝 트리 기능: Portfast, UplinkFast 및 BackboneFast

PortFast, UplinkFast 및 BackboneFast가 올바르게 설정되어 있는지 확인합니다. STP 문제를 해결하는 경우, 모든 고급 STP(UplinkFast 및 BackboneFast)를 비활성화합니다. 또한 비 브리징 호스트에 직접 연결된 포트에서만 STP PortFast가 활성화되어 있는지 확인합니다. 비 브리징 호스트에는 브리지 그룹이 없는 사용자 워크스테이션 및 라우터가 포함됩니다. 허브 또는 다른 스위치에 연결된 포트에서 PortFast를 활성화하지 마십시오. 다음은 이러한 기능을 이해하고 구성하는 데 도움이

되는 몇 가지 문서입니다.

[스패닝 트리 PortFast, BPDU Guard, BPDU Filter, UplinkFast, BackboneFast 및 Loop Guard 구성](#)
[Cisco UplinkFast 기능 이해 및 구성](#)

8. BPDU Guard

PortFast BPDU 가드를 활성화하면 비 트렁킹 PortFast 활성화 포트는 해당 포트에서 BPDU를 수신할 때 errdisable 상태로 이동합니다. 이 기능을 사용하면 PortFast에 대해 잘못 설정된 포트를 찾을 수 있습니다. 이 기능은 또한 디바이스가 패킷을 반영하거나 네트워크에 STP BPDU를 삽입하는 위치도 탐지합니다. STP 문제를 해결할 때 이 기능을 활성화하여 STP 문제를 격리할 수 있습니다.

```
L2Switch_1#configure terminal Enter configuration commands, one per line. End with CNTL/Z. L2Switch_1(config)#spanning-tree portfast bpduguard L2Switch_1(config)#end
```

9. VTP 정리

네트워크에서 VTP 정리가 활성화되면 HSRP 그룹의 디바이스가 활성화될 수 있습니다. 이로 인해 게이트웨이 간에 IP 충돌이 일어나고 트래픽 문제가 발생합니다. HSRP 그룹의 VLAN이 네트워크에서 VTP에 의해 정리되지 않았는지 확인합니다.

F. Divide and Conquer

HSRP를 격리하거나 해결하기 위한 다른 모든 시도가 실패하는 경우 "분할 및 정복" 방법이 다음 방법입니다. 이 방법은 네트워크 및 네트워크를 구성하는 구성 요소를 격리하는 데 도움이 됩니다. 분할 및 정복에는 다음 목록에 있는 지침 중 하나가 포함됩니다.

참고: 이 목록은 이 문서의 다른 섹션에서 제공하는 일부 지침을 반복합니다.

- HSRP 라우터로 스위치하기 위해 HSRP 및 격리된 VLAN에 대한 테스트 VLAN을 생성합니다.
- 모든 이중화 포트를 분리합니다.
- FEC 포트를 단일 연결 포트로 분리합니다.
- HSRP 그룹 멤버를 단 두 개의 멤버로 줄입니다.
- 필요한 VLAN만 해당 포트에서 전파되도록 트렁크 포트를 정리합니다.
- 문제가 중단될 때까지 네트워크에서 연결된 스위치의 연결을 끊습니다.

알려진 문제

Cisco 2620/2621, Cisco 3600 및 고속 이더넷을 사용하는 경우 HSRP 상태 플랩/불안정함

이러한 문제는 네트워크 연결을 중단하거나 네트워크에 우선순위가 더 높은 HSRP 라우터를 추가할 때 Fast Ethernet 인터페이스에서 발생할 수 있습니다. HSRP 상태가 활성에서 음성으로 변경되면 라우터는 인터페이스 MAC 주소 필터에서 HSRP MAC 주소를 제거하기 위해 인터페이스를 재설정합니다. Cisco 2600s, 3600s 및 7500s에 대한 Fast Ethernet 인터페이스에서 사용되는 특정 하드웨어에만 이러한 문제가 있습니다. 라우터 인터페이스를 재설정하면 Fast Ethernet 인터페이스에서

링크 상태가 변경되고 스위치가 변경 사항을 탐지합니다. 스위치가 STP를 실행하는 경우 변경 사항으로 인해 STP 전환이 발생합니다. STP는 포트를 전달 상태로 전환하는 데 30초가 걸립니다. 이 시간은 기본 전달 지연 시간인 15초의 두 배입니다. 동시에, 음성 라우터는 HSRP 보류 시간인 10초 후에 상태로 전환됩니다. STP가 아직 전달되지 않으므로 활성 라우터에서 HSRP hello 메시지가 수신되지 않습니다. 이렇게 하면 약 10초 후에 대기 라우터가 활성화됩니다. 이제 두 라우터가 모두 상태입니다. STP 포트가 전달되면 우선순위가 더 낮은 라우터가 활성에서 음성으로 변경되고 전체 프로세스가 반복됩니다.

플랫폼	설명	Cisco 버그 ID	수정	해결 방법
Cisco 2620/2621	HSRP가 설정되고 케이블이 분리되면 Fast Ethernet 인터페이스가 플랩을 시작합니다. HSRP 상태가		소프트웨어 업그레이드 . 개정 정보는 버그를 참조하십시오.	연결된 스위치 포트에서 스페닝 트리 PortFast를 활성화합니다.
Cisco 2620/2621	2600 Fast Ethernet에서 플래핑됩니다. HSRP 상태가		Cisco IOS Software 릴리스 12.1.3	연결된 스위치 포트에서 스페닝 트리 PortFast를 활성화합니다.
Cisco 3600(NM-1FE-TX ¹)	2600 및 3600 Fast Ethernet에서 플래핑됩니다.		Cisco IOS Software 릴리스 12.1.3	연결된 스위치 포트에서 스페닝 트리 PortFast를 활성화합니다.
Cisco 4500(Fast Ethernet 인터페이스)	4500 Fast Ethernet에서 HSRP 상태가 플래핑됩니다.	Cisco 버그 ID CSCds16055	Cisco IOS Software 릴리스 12.1.5	연결된 스위치 포트에서 스페닝 트리 PortFast를 활성화합니다.

¹ NM-1FE-TX = one-port Fast Ethernet(10/100BASE-TX 인터페이스) 네트워크 모듈.

대체 해결 방법은 STP 전달 지연이 기본 HSRP 보류 시간의 절반 미만이 되도록 HSRP 타이머를 조정하는 것입니다. 기본 STP 전달 지연은 15초이고, 기본 HSRP 보류 시간은 10초입니다.

HSRP 프로세스에서 **track** 명령을 사용하는 경우 HSRP 플랩을 방지하기 위해 특정 감소값을 사용하는 것이 좋습니다.

다음은 **track** 명령을 사용하는 경우 HSRP 활성 라우터의 샘플 설정입니다.

```
standby 1 ip 10.0.0.1
standby 1 priority 105
standby 1 preempt delay minimum 60
standby 1 name TEST
standby 1 track <object> decrement 15
```

여기서 15는 객체가 플랩할 때의 감소 값입니다. track 명령에 대해 자세히 알아보려면 HSRPv2 컨피그레이션 예제의 [Track Option 문서로 이동하십시오.](#)

관련 정보

- [캠퍼스 LAN Catalyst 스위치 - 액세스](#)

- [LAN 스위칭](#)
- [기술 지원 및 문서 - Cisco Systems](#)

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.