

# 캠퍼스 스위치 네트워크에서 IntraVLAN 및 InterVLAN 연결 저하의 일반적인 원인

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기 규칙](#)

[IntraVLAN 및 InterVLAN 연결 저하의 일반적인 원인](#)

[3가지 원인 범주](#)

[네트워크 속도 저하의 원인](#)

[원인 문제 해결](#)

[충돌 도메인 문제 해결](#)

[느린 IntraVLAN\(브로드캐스트 도메인\) 문제 해결](#)

[느린 InterVLAN 연결 문제 해결](#)

[관련 정보](#)

## 소개

이 문서에서는 네트워크 지연에 영향을 줄 수 있는 가장 일반적인 문제를 다룹니다. 이 문서에서는 일반적인 네트워크 속도 증상을 분류하고 문제 진단 및 해결 방법에 대한 개요를 설명합니다.

## [사전 요구 사항](#)

### [요구 사항](#)

이 문서에 대한 특정 요건이 없습니다.

### [사용되는 구성 요소](#)

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

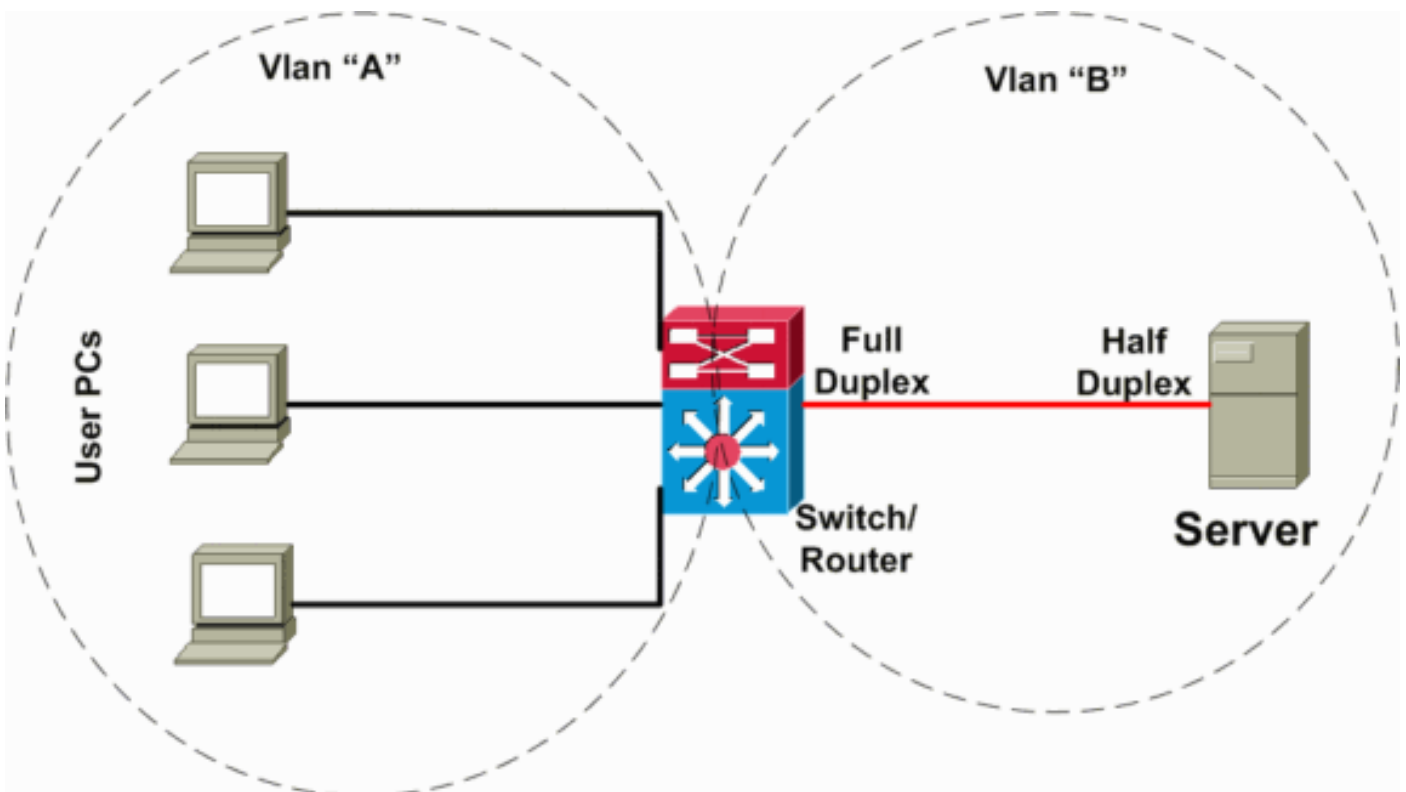
### [표기 규칙](#)

문서 규칙에 대한 자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

## [IntraVLAN 및 InterVLAN 연결 저하의 일반적인 원인](#)

VLAN에서 느린 연결의 증상은 서로 다른 네트워크 레이어의 여러 요인에 의해 발생할 수 있습니다. 일반적으로 네트워크 속도 문제는 더 낮은 수준에서 발생할 수 있지만, 문제가 "느린 VLAN"이라는 용어로 자체 마스크 처리되므로 더 높은 수준에서 증상을 관찰할 수 있습니다. 이 문서는 다음과 같은 새로운 용어를 정의합니다. "slow collision domain", "slow broadcast domain"(즉, slow VLAN) 및 "slow interVLAN forwarding" 이러한 정보는 아래의 [세 가지 원인 카테고리](#)에 정의되어 있습니다.

다음 시나리오(아래 네트워크 다이어그램에 표시됨)에는 서버와 클라이언트 VLAN 간에 VLAN 간 라우팅을 수행하는 레이어 3(L3) 스위치가 있습니다. 이 장애 시나리오에서는 서버 하나가 스위치에 연결되고 포트 이중 모드는 서버 측에서 반이중으로 구성되고 스위치 측에서 전이중으로 구성됩니다. 이러한 컨피그레이션 오류는 서버가 연결된 링크에서 트래픽 속도가 더 높을 때 패킷 손실이 증가하여 패킷 손실과 속도가 느려집니다. 이 서버와 통신하는 클라이언트의 경우 동일한 VLAN에 있는 다른 디바이스나 클라이언트와 통신하는 데 문제가 없으므로 이 문제는 VLAN 간 포워딩 속도가 느린 것으로 보입니다. 이 문제는 다른 VLAN에서 서버와 통신할 때만 발생합니다. 따라서 이 문제는 단일 충돌 도메인에서 발생했지만 VLAN 간 포워딩 속도가 느린 것으로 보입니다.



### [3가지 원인 범주](#)

느린 연결의 원인은 다음과 같이 세 가지 범주로 나눌 수 있습니다.

#### [느린 충돌 도메인 연결](#)

충돌 도메인은 반이중 포트 컨피그레이션에 구성된 연결된 디바이스로 정의되며, 서로 연결되거나 허브에 연결됩니다. 디바이스가 스위치 포트에 연결되어 있고 전이중 모드가 구성된 경우 포인트-투-포인트 연결은 분리되지 않습니다. 이러한 세그먼트의 느린 연결은 여러 가지 이유로 발생할 수 있습니다.

#### [느린 브로드캐스트 도메인 연결\(느린 VLAN\)](#)

전체 VLAN(즉, 동일한 VLAN의 모든 디바이스)에서 속도가 느려질 때 브로드캐스트 도메인 연결이 느려집니다.

## 느린 InterVLAN 연결(VLAN 간의 느린 전달)

느린 interVLAN 연결(VLAN 간 느린 전달)은 로컬 VLAN에 느린 속도가 없지만 트래픽은 대체 VLAN으로 전달되어야 하며 예상된 속도로 전달되지 않을 때 발생합니다.

## 네트워크 속도 저하의 원인

### 패킷 손실

대부분의 경우, 일반적으로 더 빨리 실행되는 작업을 완료하기 위해 상위 계층 프로토콜(애플리케이션)이 더 많은 시간이 필요한 경우 네트워크는 느린 것으로 간주됩니다. 이러한 느림은 네트워크에서 일부 패킷이 손실되어 TCP 또는 애플리케이션과 같은 고급 프로토콜이 시간 초과되어 재전송을 시작합니다.

### 하드웨어 포워딩 문제

네트워크 장비에 의해 발생하는 또 다른 유형의 느림에서는 포워딩(레이어 2[L2] 또는 L3)이 느리게 수행되는지 여부. 이는 정상적인(설계) 작동 및 느린 경로 포워딩으로 전환되는 편차 때문입니다. 스위치의 MLS(Multilayer Switching)가 하드웨어의 VLAN 간에 L3 패킷을 전달하지만 컨피그레이션이 잘못되어 MLS가 제대로 작동하지 않으며 소프트웨어의 라우터에서 전달이 수행되며 이는 interVLAN 전달 속도를 크게 떨어뜨립니다.

## 원인 문제 해결

### 충돌 도메인 문제 해결

따라서 VLAN이 느린 것으로 나타나면 먼저 충돌 도메인 문제를 격리합니다. 동일한 충돌 도메인의 사용자만 연결 문제를 겪고 있는지 또는 여러 도메인에서 발생하는 경우 설정해야 합니다. 이렇게 하려면 동일한 충돌 도메인에 있는 사용자 PC 간에 데이터를 전송하고 이 성능을 다른 충돌 도메인의 성능과 비교하거나 예상한 성능과 비교합니다.

충돌 도메인에서만 문제가 발생하고 동일한 VLAN에 있는 다른 충돌 도메인의 성능이 정상인 경우 스위치의 포트 카운터를 확인하여 이 세그먼트에서 어떤 문제가 발생할 수 있는지 확인합니다. 이중 불일치와 같은 원인은 간단합니다. 덜 자주 발생하는 또 다른 원인은 오버로드되거나 초과 가입한 세그먼트입니다. 단일 세그먼트 문제 해결에 대한 자세한 내용은 [이더넷 10/100/1000Mb 반이중/전 이중 자동 협상 구성 및 문제 해결 문서](#)를 참조하십시오.

동일한 VLAN에서 서로 다른 충돌 도메인의 사용자가 동일한 성능 문제를 가지고 있는 경우 소스와 대상 간에 하나 이상의 이더넷 세그먼트의 이중 불일치로 인해 발생할 수 있습니다. 다음 시나리오가 자주 발생합니다. 스위치는 VLAN의 모든 포트에서 전이중(full-duplex)을 갖도록 수동으로 구성되며(기본 설정은 "auto"입니다), 포트에 연결된 사용자(NIC[network interface card])는 자동 협상 절차를 수행합니다. 따라서 모든 포트에서 듀플렉스 불일치가 발생하므로 각 포트(충돌 도메인)의 성능이 저하됩니다. 따라서 전체 VLAN(브로드캐스트 도메인)에 성능 문제가 있는 것처럼 보이지만 각 포트의 충돌 도메인에 대해 여전히 이중 불일치로 분류됩니다.

또 다른 고려 사항은 특정 NIC 성능 문제입니다. 성능 문제가 있는 NIC가 공유 세그먼트에 연결된 경우 전체 세그먼트가 느려지는 것으로 나타날 수 있습니다. 특히 NIC가 다른 세그먼트나 VLAN을 제공하는 서버에 속하는 경우 그러합니다. 문제를 해결할 때 잘못 인식할 수 있으므로 이 사례를 염두에 두십시오. 다시 한 번 말하지만, 이 문제를 좁히는 가장 좋은 방법은 동일한 세그먼트의 두 호스트(문제가 있는 NIC가 연결된 경우) 간에 데이터 전송을 수행하거나, 해당 포트에 NIC만 있는 경우

격리가 쉽지 않으므로, 이 호스트에서 다른 NIC를 시도하거나, 의심되는 호스트를 별도의 포트에 연결하여 포트와 NIC를 올바르게 구성하도록 하는 것입니다.

그래도 문제가 있는 경우 스위치 포트 문제를 해결하십시오. [Troubleshooting Switch Port and Interface Problems](#) 문서를 참조하십시오.

가장 심각한 경우는 호환되지 않는 NIC의 일부 또는 전부가 Cisco 스위치에 연결될 때입니다. 이 경우 스위치에 성능 문제가 있는 것으로 보입니다. NIC와 Cisco 스위치의 호환성을 확인하려면 [Troubleshooting Cisco Catalyst Switches to NIC Compatibility Issues\(Cisco Catalyst 스위치에서 NIC 호환성 문제 해결\)](#) 문서를 참조하십시오.

처음 두 가지 케이스(충돌 도메인 느림과 VLAN 느림 문제 해결)를 구분해야 합니다. 이 두 가지 원인은 서로 다른 도메인입니다. 충돌 도메인 속도가 느려지면 스위치 외부(또는 스위치 에지, 스위치 포트) 또는 스위치 외부에 문제가 발생합니다. 세그먼트에만 문제가 있을 수 있습니다(예: 세그먼트 길이를 초과하는 초과 서브스크립션 세그먼트, 세그먼트의 물리적 문제 또는 허브/리피터 문제). VLAN 속도가 느린 경우 스위치(또는 여러 스위치) 내부에 문제가 있을 수 있습니다. 문제를 잘못 진단하면 잘못된 위치에서 문제를 찾는 데 시간을 낭비할 수 있습니다.

따라서, 케이스를 진단한 후 아래 나열된 항목을 확인하십시오.

공유 세그먼트의 경우

- 세그먼트가 오버로드되었는지 또는 초과 가입되었는지 확인
- 세그먼트가 정상인지 확인합니다(케이블 길이가 올바른지, 감쇠가 표준인지 여부, 미디어의 물리적 손상이 있는지 여부 포함).
- 네트워크 포트 및 세그먼트에 연결된 모든 NIC에 호환 설정이 있는지 확인
- NIC가 제대로 작동하는지 확인(그리고 최신 드라이버를 실행 중)
- 네트워크 포트에서 계속 증가하는 오류가 표시되는지 확인
- 네트워크 포트가 오버로드되었는지 확인(특히 서버 포트인 경우)

포인트-투-포인트 공유 세그먼트 또는 컬렉션이 없는(전이중) 세그먼트의 경우:

- 포트 및 NIC 호환 구성 결정
- 세그먼트의 상태를 확인합니다.
- NIC의 상태를 확인합니다.
- 네트워크 포트 오류 또는 초과 서브스크립션 찾기

## [느린 IntraVLAN\(브로드캐스트 도메인\) 문제 해결](#)

위의 섹션에서 설명한 대로 이중 불일치나 충돌 도메인 문제가 없는지 확인한 후 이제 IntraVLAN 속도 문제를 해결할 수 있습니다. 속도 저하의 위치를 격리하는 다음 단계는 동일한 VLAN에 있는 호스트 간(다른 포트에 있음) 데이터 전송을 수행하는 것입니다. 즉, 서로 다른 충돌 도메인에서 성능을 대체 VLAN에서 동일한 테스트와 비교합니다.

다음과 같은 경우 VLAN 속도가 느려질 수 있습니다.

- [트래픽 루프](#)
- [오버로드 또는 오버서브스크립션된 VLAN](#)
- [스위치 인밴드 경로의 혼잡](#)
- [스위치 관리 프로세서 높은 CPU 사용률](#)
- [컷스루 스위치의 인그레스 오류](#)

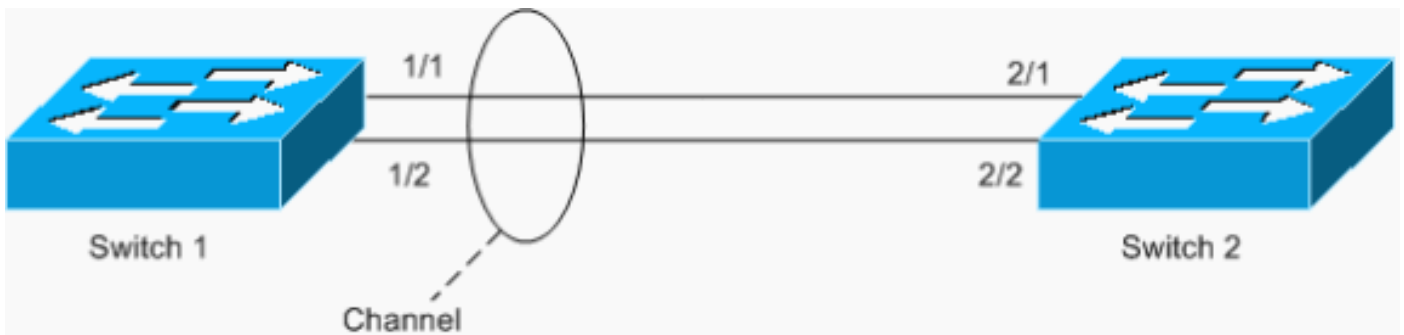
- <sup>1</sup> [소프트웨어 또는 하드웨어 컨피그레이션 오류](#)
- <sup>1</sup> [소프트웨어 버그](#)
- <sup>1</sup> [하드웨어 문제](#)

<sup>1</sup>. 이 세 가지 이유로 인해 intraVLAN 연결이 느려집니다. 이 문서에서는 Cisco 기술 지원 엔지니어의 문제 해결이 필요할 수 있습니다. 위에 나열된 첫 번째 5가지 가능한 원인을 확인한 후 [Cisco 기술 지원](#)을 통해 서비스 요청을 열어야 할 수 있습니다.

## 트래픽 루프

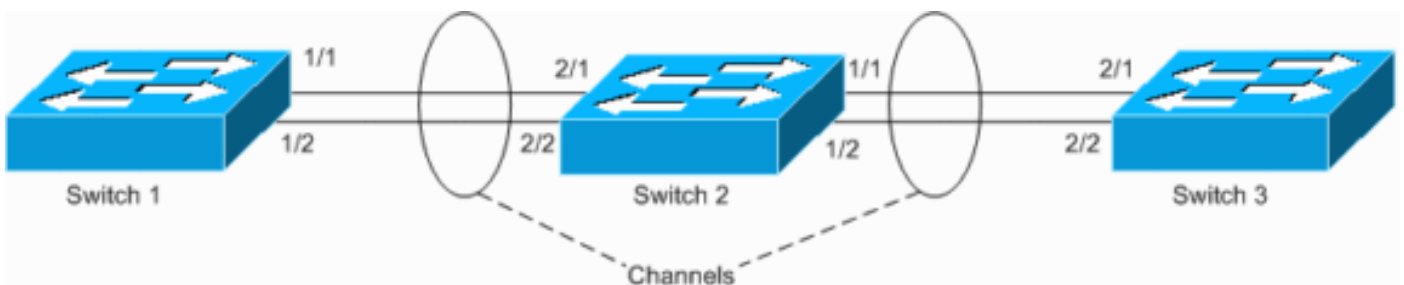
트래픽 루프는 느린 VLAN의 가장 일반적인 원인입니다. 루프와 함께 루프를 경험하고 있음을 나타내는 다른 증상들이 표시되어야 합니다. STP(Spanning Tree Protocol) 루프의 문제 해결에 대한 자세한 내용은 [STP\(Spanning Tree Protocol\) Problems and Related Design Considerations\(스패닝 트리 프로토콜 문제 및 관련 설계 고려 사항\) 문서](#)를 참조하십시오. 기가비트 지원 백플레인인 있는 강력한 스위치(예: Cisco Catalyst 6500/6000)는 관리 CPU 성능을 저하시키지 않고 일부(STP) 루프를 처리할 수 있지만, 루프된 패킷은 스위치에서 입력 버퍼가 오버플로우되고 Rx/Tx(Receive/Transmit) 버퍼가 스위치에서 오버플로우되어 다른 디바이스에 연결할 때 성능이 저하될 수 있습니다.

루프의 또 다른 예는 다음 시나리오와 같이 비대칭적으로 구성된 EtherChannel입니다.



이 예에서는 포트 1/1 및 1/2가 채널에 있지만 포트 2/1 및 2/2는 채널에 없습니다.

스위치 1에는 구성된 채널(강제 채널)이 있으며 스위치 2에는 해당 포트에 대한 채널 구성이 없습니다. 플러딩된 트래픽(멀티캐스트/캐스트/알 수 없는 유니캐스트)이 스위치 1에서 스위치 2로 흐르면 스위치 2는 다시 채널로 루프됩니다. 트래픽이 계속 반복되지 않고 한 번만 반영되기 때문에 완전한 루프가 아닙니다. 전체 루프의 1/2입니다. 이러한 컨피그레이션이 두 개 있으면 아래 예와 같이 완전한 루프를 생성할 수 있습니다.



이러한 컨피그레이션이 잘못되면 트래픽이 잘못 전환되어 패킷 손실이 발생하므로 잘못된 포트에서 MAC 주소를 학습할 수 있습니다. 예를 들어, 위 다이어그램에 표시된 것처럼 스위치 1에 연결된 활성 HSRP(Hot Standby Router Protocol)가 있는 라우터를 고려해 보십시오. 라우터가 패킷을 브로드캐스트한 후, 유니캐스트 패킷이 라우터에서 다시 전송될 때까지 MAC은 스위치 2에 의해 루프되고 스위치 1에 의해 채널을 학습합니다.

## 오버로드 또는 오버서브스크립션 VLAN

VLAN에 병목 지점(초과 서브스크립션 세그먼트)이 있는지 확인하고 찾아냅니다.VLAN이 오버로드 되는 첫 번째 표시는 포트의 Rx 또는 Tx 버퍼가 오버서브스크립션된 경우입니다.일부 포트에서 아웃페기 또는 폐기되는 것이 표시되면 해당 포트가 오버로드되었는지 확인합니다.(폐기 수가 증가해도 전체 Rx 버퍼가 표시되는 것은 아닙니다.) Catalyst OS(CatOS)에서 실행할 수 있는 유용한 명령은 **show mac mod/port** 또는 **show top [M]**입니다.Cisco IOS® Software(네이티브)에서 **show interfaces slot#/port#counters errors** 명령을 실행하여 폐기를 확인할 수 있습니다.오버로드되거나 초과 가입한 VLAN 시나리오와 [트래픽 루프](#) 시나리오는 서로 자주 동반되지만 별도로 존재할 수도 있습니다.

대부분의 경우 트래픽의 집계 대역폭을 과소평가하면 백본 포트에서 과부하가 발생합니다.이 문제를 해결하는 가장 좋은 방법은 포트가 병목 현상이 발생한 디바이스 간에 EtherChannel을 구성하는 것입니다.네트워크 세그먼트가 이미 채널인 경우 채널 그룹에 포트를 더 추가하여 채널 용량을 늘립니다.

또한 Cisco CEF(Express Forwarding) 양극화 문제에 대해서도 숙지하십시오.이 문제는 라우터에 의해 트래픽이 로드 밸런싱되는 네트워크에서 발생하지만 Cisco Express Forwarding의 알고리즘 균일성으로 인해 모든 트래픽이 양극화되고 다음 홉에서는 로드 밸런싱되지 않습니다.그러나 로드 밸런싱된 L3 링크가 있는 특정 토폴로지가 필요하므로 이 문제는 자주 발생하지 않습니다.Cisco Express Forwarding 및 로드 밸런싱에 대한 자세한 내용은 Supervisor [Engine 2 및 Running CatOS System Software를 사용하여 Catalyst 6500/600 Series 스위치에서 CEF를 포함하는 유니캐스트 IP 라우팅 문제 해결을 참조하십시오.](#)

오버로드된 VLAN의 또 다른 원인은 비대칭 라우팅 문제입니다.이러한 유형의 컨피그레이션으로 인해 VLAN이 과도하게 많은 트래픽이 발생할 수도 있습니다.자세한 내용은 [원인 1:Switched Campus Networks의 Unicast Flooding 문서의 Asymmetric Routing 섹션](#)입니다.

때로는 병목 현상이 네트워크 장치 자체일 수도 있습니다.예를 들어 3기가비트 백플레인을 사용하여 스위치를 통해 4기가비트 트래픽을 펌프하려고 하면 트래픽이 크게 손실됩니다.네트워크 스위치 아키텍처에 대한 이해는 이 문서의 범위를 벗어납니다.그러나 네트워크 스위치의 용량을 고려할 때 다음 사항에 유의하십시오.

- 백플레인 용량
- 주요 차단 문제
- 차단 및 비차단 스위치/포트 아키텍처

## 스위치 인밴드 경로의 혼잡

스위치 인밴드 경로의 혼잡으로 인해 스페닝 트리 루프나 네트워크의 다른 유형이 불안정해질 수 있습니다.Cisco 스위치의 인밴드 포트는 관리 프로세서에 대한 관리 트래픽(예: Cisco Discovery Protocol 및 PAgP[Port Aggregation Protocol])을 위한 인터페이스를 제공하는 가상 포트입니다.인밴드 포트는 사용자가 이를 볼 수 없으며 인밴드 기능이 정상적인 포트 운영과 결합되기 때문에 가상으로 간주됩니다.예를 들어 Catalyst 4000, Catalyst 5000 및 Catalyst 6500/6000 시리즈 스위치(CatOS 실행)의 SC0 인터페이스는 인밴드 포트의 하위 집합입니다.인터페이스 SC0은 구성된 VLAN 내에서 관리 프로세서에 대한 IP 스택만 제공하는 반면, 인밴드 포트는 구성된 VLAN의 브리지 프로토콜 데이터 유닛(BPDU)과 기타 여러 관리 프로토콜(예: Cisco Discovery Protocol, IGMP(Internet Group Management Protocol), Cisco Group Management Protocol, DTP(Dynamic Trunking Protocol))에 대한 관리 프로세서에 대한 액세스를 제공합니다.

인밴드 포트가 오버로드되는 경우(잘못 구성된 애플리케이션 또는 사용자 트래픽으로 인해), 프로토콜 상태 안정성이 일반 메시지 또는 "hello"를 수신한 프로토콜이 불안정해질 수 있습니다.이 상태

가 되면 임시 루프, 인터페이스 플랩 및 기타 문제가 발생하여 이러한 유형의 속도가 느려질 수 있습니다.

DoS(Denial of Service) 공격이 성공할 수 있지만 스위치에서 인밴드 포트가 혼잡을 일으키기 어렵습니다. 인밴드 포트의 트래픽을 제한하거나 줄일 방법은 없습니다. 솔루션에는 스위치 관리자의 개입과 조사가 필요합니다. 인밴드 포트는 일반적으로 혼잡을 매우 잘 차단합니다. 인밴드 포트 오작동을 일으키거나 Rx 또는 Tx 방향에 문제가 발생하는 경우는 거의 없습니다. 이는 심각한 하드웨어 중단이 발생할 수 있으며 전체 스위치에 영향을 미칩니다. 이 상태는 인식하기 어렵고 일반적으로 [Cisco 기술 지원](#) 엔지니어가 진단합니다. 이러한 증상은 스위치가 갑자기 "청각 장애"가 되고 Cisco Discovery Protocol 인접 디바이스 업데이트와 같은 제어 트래픽이 표시되지 않는다는 것입니다. 이는 Rx 인밴드 문제를 나타냅니다. (그러나 Cisco Discovery Protocol 인접 디바이스 하나가 확인되면 인밴드가 작동하고 있음을 확신할 수 있습니다.) 이에 따라 연결된 모든 스위치가 단일 스위치(기타 모든 관리 프로토콜 포함)에서 Cisco Discovery Protocol을 분실할 경우 해당 스위치의 인밴드 인터페이스에서 Tx 문제를 나타냅니다.

### [스위치 관리 프로세서 높은 CPU 사용률](#)

인밴드 경로가 오버로드되면 스위치에서 높은 CPU 조건을 경험할 수 있습니다. CPU가 이러한 불필요한 트래픽을 모두 처리하므로 상황이 악화됩니다. CPU 사용률이 높은 경우 대역내 경로가 오버로드되거나 대체 문제로 인해 발생하는 경우 위의 [Congestion on Switch Inband Path](#) 섹션에 설명된 대로 관리 프로토콜에 영향을 줄 수 있습니다.

일반적으로 관리 CPU는 모든 스위치의 취약한 지점이라고 가정합니다. 올바르게 구성된 스위치를 사용하면 CPU 사용률이 높아서 발생하는 문제의 위험을 줄일 수 있습니다.

Catalyst 4000 시리즈 스위치의 Supervisor Engine I 및 II 아키텍처는 관리 CPU가 스위칭 오버헤드에 관련되도록 설계되었습니다. 다음 사항에 유의하십시오.

- CPU는 새로운 경로(Supervisor Engine I와 II는 경로 기반임)가 스위치에 들어올 때마다 스위치 패브릭을 프로그래밍합니다. 인밴드 포트가 오버로드되면 새 경로가 삭제됩니다. 따라서 포트 간에 트래픽이 전환될 때 패킷이 손실되고(무음 폐기) 상위 레이어 프로토콜이 느려집니다. (위의 [스위치 인밴드 경로의 혼잡](#) 섹션을 참조하십시오.)
- CPU가 Supervisor Engine I 및 II에서 부분적으로 스위칭을 수행하므로 CPU 조건이 높으면 Catalyst 4000의 스위칭 기능에 영향을 줄 수 있습니다. Supervisor Engine I 및 II에서 높은 CPU 사용률은 스위칭 오버헤드 자체에서 발생할 수 있습니다.

Catalyst 4500/4000 Series의 Supervisor Engine II+, III 및 IV는 상당히 트래픽 톨러런트(traffic-tolerant) 하지만 Cisco IOS Software 기반 Supervisor Engine의 MAC 주소 학습은 여전히 소프트웨어(관리 CPU에 의한)에서 완전히 수행됩니다. CPU 사용률이 높으면 이 프로세스에 영향을 미치고 속도가 느려질 수 있습니다. Supervisor Engine I 및 II와 마찬가지로, 대규모 MAC 주소 학습 또는 재학습으로 Supervisor Engine II+, III 및 IV의 CPU 사용률이 높아질 수 있습니다.

CPU는 Catalyst 3500XL 및 2900XL 시리즈 스위치에서도 MAC 학습에 관련되어 있으므로 빠른 주소 재학습을 통해 CPU 성능에 영향을 주는 프로세스가 있습니다.

또한 MAC 주소 학습 프로세스(하드웨어에서 완전히 구현된 경우에도)는 스위칭 프로세스에 비해 상대적으로 느린 프로세스입니다. MAC 주소 재학습이 지속적으로 높은 경우 원인을 찾아 제거해야 합니다. 네트워크의 스페닝 트리 루프로 인해 이러한 유형의 MAC 주소가 재학습될 수 있습니다. MAC 주소 재학습(또는 MAC 주소 플래핑)은 포트 기반 VLAN을 구현하는 서드파티 스위치에서도 발생할 수 있습니다. 즉, MAC 주소가 VLAN 태그와 연결되지 않습니다. 특정 컨피그레이션에서 Cisco 스위치에 연결된 이러한 종류의 스위치로 인해 VLAN 간에 MAC이 유출될 수 있습니다. 따라서 MAC 주소 재학습이 높은 속도로 진행되어 성능이 저하될 수 있습니다.

## 컷스루 스위치의 인그레스 오류

컷스루 인그레스(cut-through) 오류 패킷 전파는 [슬로우 충돌 도메인 연결과](#) 관련이 있지만 오류 패킷이 다른 세그먼트로 전송되기 때문에 세그먼트 간에 스위칭되는 문제가 발생한 것으로 보입니다. 컷스루 스위치(예: Catalyst 8500 Series Campus Switch Routers(CSR) 및 Catalyst 4000 시리즈용 Catalyst 2948G-L3 또는 L3 스위칭 모듈)는 패킷의 L2/L3 헤더를 읽고 패킷을 목적지 포트 또는 포트에 전달할 수 있는 충분한 정보가 있는 즉시 패킷/프레임 스위칭을 시작합니다. 따라서 패킷이 인그레스 포트와 이그레스 포트 간에 스위칭되는 동안 패킷의 시작 부분이 이미 이그레스 포트에서 전달되고 나머지 패킷은 인그레스 포트에서 계속 수신됩니다. 인그레스 세그먼트가 정상적이지 않다면 CRC(cyclic redundancy check) 오류 또는 런트를 생성할 경우 어떻게 됩니까? 스위치는 프레임 끝을 수신하고 그 시점에는 대부분의 프레임이 이그레스 포트에서 전송될 때만 이 점을 인식합니다. 잘못된 프레임의 나머지를 전송하는 것은 의미가 없으므로 나머지는 삭제되고 이그레스 포트는 "언더런" 오류를 증가시키고 인그레스 포트는 해당 오류 카운터를 증가시킵니다. 여러 인그레스 포트가 비정상 상태이고 해당 서버가 이그레스 포트에 상주하는 경우 문제가 발생하지 않더라도 서버 세그먼트에 문제가 있는 것으로 나타납니다.

컷스루 L3 스위치의 경우 언더런이 있는지 확인하고 모든 인그레스 포트에서 오류를 확인합니다.

## 소프트웨어 또는 하드웨어 구성 오류

컨피그레이션이 잘못되면 VLAN이 느려질 수 있습니다. 이러한 부정적인 효과는 VLAN이 초과 서브스크립션되거나 오버로드되는 결과로 나타날 수 있지만, 대부분 잘못된 설계나 간과된 컨피그레이션으로 인해 발생합니다. 예를 들어, 멀티캐스트 트래픽 제한 기술이 해당 VLAN에 올바르게 구성되지 않은 경우 VLAN(세그먼트)은 멀티캐스트 트래픽(예: 비디오 또는 오디오 스트림)에 의해 쉽게 압도될 수 있습니다. 이러한 멀티캐스트 트래픽은 데이터 전송에 영향을 미칠 수 있으며, 모든 사용자에 대해 전체 VLAN에서 패킷 손실을 초래할 수 있습니다(그리고 멀티캐스트 스트림을 받지 않으려는 사용자의 세그먼트가 플러딩).

## 소프트웨어 버그 및 하드웨어 문제

소프트웨어 버그 및 하드웨어 문제는 편차를 유발하므로 식별하기 어려우며 이는 트러블슈팅이 어렵습니다. 소프트웨어 버그 또는 하드웨어 문제로 인해 문제가 발생한다고 생각되면 [Cisco 기술 지원](#) 엔지니어에게 문의하여 문제를 조사하십시오.

## 느린 InterVLAN 연결 문제 해결

느린 VLAN 간 연결(VLAN 간)을 트러블슈팅하기 전에 이 문서의 [충돌 도메인 문제 해결](#) 및 [느린 IntraVLAN\(Broadcast Domain\)](#) 섹션에서 설명하는 문제를 조사하고 해결합니다.

대부분의 경우 사용자 컨피그레이션 오류 때문에 VLAN 간 연결이 느립니다. 예를 들어, MLS 또는 MMLS(Multicast Multicast Multilayer Switching)를 잘못 구성한 경우 라우터 CPU에서 패킷 전달을 수행하는데, 이는 느린 경로입니다. 컨피그레이션 오류를 방지하고 필요한 경우 효율적으로 문제를 해결하려면 L3 포워딩 디바이스에서 사용하는 메커니즘을 이해해야 합니다. 대부분의 경우 L3 포워딩 메커니즘은 라우팅 및 ARP(Address Resolution Protocol) 테이블의 컴파일을 기반으로 하며 추출된 패킷 포워딩 정보를 하드웨어(바로 가기)로 프로그래밍합니다. 바로 가기를 프로그래밍하는 과정에서 오류가 발생하면 소프트웨어 패킷 포워딩(느린 경로), 포워딩(잘못된 포트에 전달) 또는 트래픽 블랙홀링으로 이어집니다.

일반적으로 바로 가기 프로그래밍 실패 또는 불완전한 바로 가기 생성(소프트웨어 패킷 전달, 전달 오류 또는 트래픽 블랙홀링으로 이어질 수 있음)은 소프트웨어 버그의 결과입니다. 이 문제가 있다고 생각되면 [Cisco 기술 지원](#) 엔지니어에게 조사하도록 하십시오. 다른 이유로 interVLAN 포워딩이



느려지는 경우 하드웨어 오작동이 발생하지만 이러한 원인은 이 문서의 범위를 벗어납니다. 하드웨어 오작동 때문에 하드웨어에서 성공적으로 바로가기를 생성하는 것을 방지할 수 있으므로 트래픽이 느린(소프트웨어) 경로를 사용하거나 블랙홀링될 수 있습니다. [Cisco 기술 지원](#) 엔지니어가 하드웨어 장애를 처리해야 합니다.

장비가 올바르게 구성되었지만 하드웨어 스위칭이 수행되지 않는 경우 소프트웨어 버그 또는 하드웨어 오작동이 원인일 수 있습니다. 그러나 이러한 결론을 내리기 전에 디바이스 기능을 숙지하십시오.

다음은 하드웨어 포워딩이 중단되거나 전혀 수행되지 않을 때 가장 자주 발생하는 두 가지 상황입니다.

- 바로 가기를 저장하는 메모리가 모두 사용되었습니다. 메모리가 가득 차면 소프트웨어는 일반적으로 더 이상 바로 가기를 만들지 않습니다. (예를 들어, NetFlow 또는 Cisco Express Forwarding 기반 MLS는 새 바로가기가 필요하지 않은 경우 비활성화되고 [slow path] 소프트웨어로 전환됩니다.)
- 장비는 하드웨어 스위칭을 수행하도록 설계되지 않았지만 명확하게 표시되지 않습니다. 예를 들어 Catalyst 4000 Series Supervisor Engines III 이상은 하드웨어 포워드만 IP 트래픽을 처리하도록 설계되었습니다. 다른 모든 트래픽 유형은 CPU에서 처리하는 소프트웨어입니다. 또 다른 예는 CPU 개입이 필요한 ACL(Access Control List)의 컨피그레이션입니다(예: "log" 옵션 사용). 이 규칙에 적용되는 트래픽은 소프트웨어의 CPU에 의해 처리됩니다.

[컷스루 스위치의 인그레스\(ingress\) 오류](#)는 VLAN 간 라우팅 속도 저하에 기여할 수 있습니다. 컷스루 스위치는 L3 및 L2 트래픽을 전달하기 위해 동일한 아키텍처 원칙을 사용하므로 위의 [Troubleshoot Slow IntraVLAN\(Broadcast Domain\)](#) 섹션에 제공된 문제 해결 방법을 L2 트래픽에도 적용할 수 있습니다.

interVLAN 라우팅에 영향을 주는 또 다른 유형의 잘못된 컨피그레이션은 최종 사용자 디바이스(예: PC 및 프린터)의 컨피그레이션 오류입니다. 일반적으로 잘못 구성된 PC가 있습니다. 예를 들어, 기본 게이트웨이가 잘못 구성되거나, PC ARP 테이블이 유효하지 않거나, IGMP 클라이언트가 제대로 작동하지 않습니다. 일반적인 경우는 여러 라우터 또는 라우팅 가능 디바이스가 있고 최종 사용자 PC의 일부 또는 전체가 잘못된 기본 게이트웨이를 사용하도록 잘못 구성된 경우입니다. 모든 네트워크 장치가 구성되어 제대로 작동하기 때문에 가장 심각한 문제가 될 수 있지만, 최종 사용자 디바이스는 이러한 잘못된 컨피그레이션 때문에 이러한 장치를 사용하지 않습니다.

네트워크의 디바이스가 하드웨어 가속화 유형이 없는 일반 라우터인 경우(NetFlow MLS에 참여하지 않음), 트래픽 포워딩 속도는 CPU 속도 및 사용 속도에 전적으로 따라 달라집니다. 높은 CPU 사용률은 전달 속도에 확실히 영향을 미칩니다. 그러나 L3 스위치에서 CPU 조건이 높더라도 전송 속도에 영향을 주지 않습니다. 높은 CPU 사용률은 하드웨어 바로가기를 생성(프로그램)하는 CPU의 기능에 영향을 미칩니다. 바로가기가 하드웨어에 이미 설치되어 있는 경우 CPU가 많이 사용되더라도 바로가기가 만료될 때까지(만료 타이머가 있는 경우) 트래픽이 하드웨어에서 전환되거나 CPU에서 제거됩니다. 그러나 라우터가 모든 유형의 소프트웨어 가속화(예: 고속 스위칭 또는 Cisco Express Forwarding 스위칭)에 대해 구성된 경우 소프트웨어 바로가기의 영향을 받을 수 있습니다. 바로가기가 끊어졌거나 메커니즘 자체가 실패하는 경우 전달 속도가 가속화되는 대신 트래픽이 CPU에 펀딩되어 데이터 전달 속도가 느려집니다.

## [관련 정보](#)

- [IP 멀티레이어 스위칭 문제 해결](#)
- [Supervisor Engine 2 및 Running CatOS System Software를 사용하여 Catalyst 6500/6000 Series 스위치에서 CEF를 포함하는 유니캐스트 IP 라우팅 문제 해결](#)

- [Catalyst 3550 Series 스위치로 VLAN 간 라우팅 구성](#)
- [스위치 제품 지원](#)
- [LAN 스위칭 기술 지원](#)
- [기술 지원 및 문서 - Cisco Systems](#)