

# Catalyst SPAN(Switched Port Analyzer) 구성: 예

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[SPAN, RSPAN, ERSPAN을 지원하는 Catalyst Switch](#)

[요구 사항](#)

[사용되는 구성 요소](#)

#### [배경 정보](#)

[SPAN에 대한 간단한 설명](#)

[SPAN 용어](#)

[소스 포트의 특성](#)

[소스 VLAN의 특성](#)

[목적지 포트의 특성](#)

[리플렉터 포트의 특성](#)

#### [Catalyst Express 500/520의 SPAN](#)

#### [Catalyst 2900XL/3500XL 스위치의 SPAN](#)

[제공되는 기능 및 제한 사항](#)

[컨피그레이션 예시](#)

[네트워크 다이어그램](#)

[Catalyst 2900XL/3500XL의 샘플 컨피그레이션](#)

[컨피그레이션 단계 설명](#)

#### [Catalyst 2948G-L3 및 4908G-L3의 SPAN](#)

#### [Catalyst 8500의 SPAN](#)

#### [CatOS를 실행하는 Catalyst 2900, 4500/4000, 5500/5000, 6500/6000 Series Switch의 SPAN](#)

##### [로컬 SPAN](#)

[PSPAN, VSPAN: 일부 포트 또는 전체 VLAN 모니터링](#)

[SPAN으로 단일 포트 모니터링](#)

[SPAN으로 여러 포트 모니터링](#)

[SPAN으로 VLAN 모니터링](#)

[인그레스/이그레스 SPAN](#)

[트렁크에 SPAN 구현](#)

[트렁크에 속한 VLAN의 하위 집합 모니터링](#)

[목적지 포트에서의 트렁킹](#)

[여러 개의 동시 세션 생성](#)

[기타 SPAN 옵션](#)

##### [원격 SPAN](#)

[RSPAN 개요](#)

[RSPAN 컨피그레이션 예](#)

[두 스위치 S1과 S2 간 ISL 트렁크 설정](#)

[RSPAN VLAN 생성](#)

[S2의 포트 5/2 컨피그레이션\(RSPAN 목적지 포트로 구성\)](#)

[S1의 RSPAN 소스 포트 컨피그레이션](#)

[구성 확인](#)

---

[set rspan 명령으로 가능한 기타 컨피그레이션](#)

[기능 요약 및 제한](#)

[Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750, 3750-E Series Switch의 SPAN](#)

[Cisco IOS System Software를 실행하는 Catalyst 4500/4000 및 Catalyst 6500/6000 Series Switch의 SPAN](#)

[컨피그레이션 예시](#)

[기능 요약 및 제한](#)

[SPAN이 각종 Catalyst 플랫폼의 성능에 미치는 영향](#)

[Catalyst 2900XL/3500XL 시리즈](#)

[아키텍처 개요](#)

[성능에 미치는 영향](#)

[Catalyst 4500/4000 시리즈](#)

[아키텍처 개요](#)

[성능에 미치는 영향](#)

[Catalyst 5500/5000 및 6500/6000 시리즈](#)

[아키텍처 개요](#)

[성능에 미치는 영향](#)

[FAQ 및 일반적인 문제](#)

[잘못된 SPAN 컨피그레이션으로 인한 연결 문제](#)

[SPAN 목적지 포트 가동/중지](#)

[SPAN 세션에서 브리징 루프를 생성하는 이유?](#)

[SPAN이 성능에 영향을 미칩니까?](#)

[EtherChannel 포트에서 SPAN을 설정할 수 있습니까?](#)

[여러 SPAN 세션이 동시에 실행될 수 있습니까?](#)

[오류 "% Local Session Limit Has Been Exceeded"](#)

[VPN 서비스 모듈에서 SPAN 세션을 삭제할 수 없습니다. "% Session \[Session No.\] Used by Service Module" 오류 메시지가 표시됩니다.](#)

[손상된 패킷을 SPAN으로 캡처할 수 없는 이유는 무엇입니까?](#)

[오류: 서비스 모듈에서 사용하는 세션 2의 비율\(%\)](#)

[리플렉터 포트에서 패킷 삭제](#)

[Catalyst 6500 Chassis에서는 항상 SPAN 세션을 FWSM과 함께 사용](#)

[같은 스위치 내에서 SPAN 세션과 RSPAN 세션의 ID가 같을 수 있습니까?](#)

[RSPAN 세션은 서로 다른 여러 VTP 도메인에서 작동할 수 있습니까?](#)

[RSPAN 세션은 WAN에서 또는 서로 다른 여러 네트워크에서 작동할 수 있습니까?](#)

[RSPAN 소스 세션과 목적지 세션이 같은 Catalyst Switch에 있을 수 있습니까?](#)

[SPAN 목적지 포트에 연결된 네트워크 분석기/보안 디바이스에 연결할 수 없습니다.](#)

[관련 정보](#)

---

## 소개

이 문서에서는 최근에 구현된 SPAN(Switched Port Analyzer)의 기능을 설명합니다.

## 사전 요구 사항

## SPAN, RSPAN, ERSPAN을 지원하는 Catalyst Switch

Catalyst 스위치	SPAN 지원	RSPAN 지원	ERSPAN 지원
Catalyst Express 500/520 시리즈	예	아니요	아니요
Catalyst 6500/6000 시리즈	예	예	예. Cisco IOS Software Release 12.2(18)SXE 이상을 실행하는 Supervisor 2T(PFC4), Supervisor 720(PFC3B 또는 PFC3BXL). 하드웨어 버전이 3.2 이상이고 Cisco IOS Software Release 12.2(18)SXE 이상을 실행하는 Supervisor 720(PFC3A)
Catalyst 5500/5000 시리즈	예	아니요	아니요
Catalyst 4900 시리즈	예	예	아니요
Catalyst 4500/4000 시리즈(4912G 포함)	예	예	아니요
Catalyst 3750 Metro 시리즈	예	예	아니요
Catalyst 3750/3750E/3750X 시리즈	예	예	아니요
Catalyst 3560/3560E/3650X 시리즈	예	예	아니요
Catalyst 3550 시리즈	예	예	아니요
Catalyst 3500 XL 시리즈	예	아니요	아니요
Catalyst 2970 시리즈	예	예	아니요
Catalyst 2960 시리즈	예	예	아니요
Catalyst 2955 시리즈	예	예	아니요
Catalyst 2950 시리즈	예	예	아니요
Catalyst 2940 시리즈	예	아니요	아니요
Catalyst 2948G-L3	아니요	아니요	아니요
Catalyst 2948G-L2, 2948G-GE-TX, 2980G-A	예	예	아니요
Catalyst 2900XL 시리즈	예	아니요	아니요
Catalyst 1900 시리즈	예	아니요	아니요

요구 사항

이 문서에 대한 특정 조건이 없습니다.

## 사용되는 구성 요소

이 문서에 수록된 이 정보는 Catalyst 4500/4000, 5500/5000, 6500/6000 시리즈 스위치에 대한 참조로 CatOS 5.5를 사용합니다. Catalyst 2900XL/3500XL 시리즈 스위치에서는 Cisco IOS® Software Release 12.0(5)XU를 사용합니다.

이 문서는 SPAN의 변경 사항을 반영하여 업데이트되지만, SPAN 기능의 최신 개발 현황은 해당 스위치 플랫폼 문서의 릴리스 노트를 참조하십시오.

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.

## 배경 정보

포트 미러링 또는 포트 모니터링이라고도 하는 이 SPAN 기능은 네트워크 분석기를 통한 분석을 위해 네트워크 트래픽을 선택합니다. 네트워크 분석기는 Cisco SwitchProbe 디바이스 또는 다른 RMON(Remote Monitoring) 프로브일 수 있습니다.

예전의 SPAN은 Cisco Catalyst 시리즈 스위치의 기본적인 수준의 기능이었습니다. 그러나 CatOS(Catalyst OS)의 최신 릴리스에서 크게 향상되었고, 사용자를 위한 여러 새로운 기능이 도입되었습니다.

이 문서를 SPAN 기능의 컨피그레이션 가이드 대신 사용할 수 없습니다. 이 문서에서는 SPAN과 관련하여 자주 묻는 질문과 답을 확인할 수 있습니다.

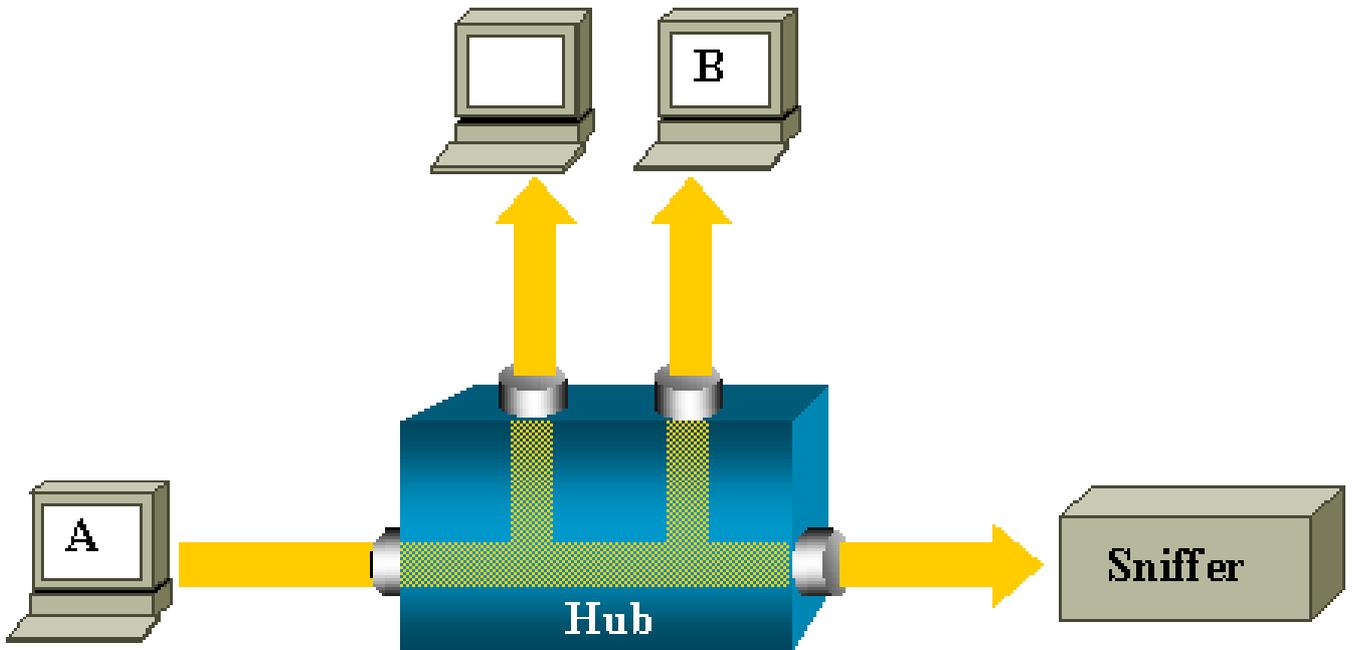
- SPAN이란 무엇이고 어떻게 구성합니까?
- 어떤 다양한 기능이 제공되며(특히 다중 동시 SPAN 세션), 그 기능을 실행하려면 어떤 소프트웨어 레벨이 필요합니까?
- SPAN이 스위치 성능에 영향을 미칩니까?

## SPAN에 대한 간단한 설명

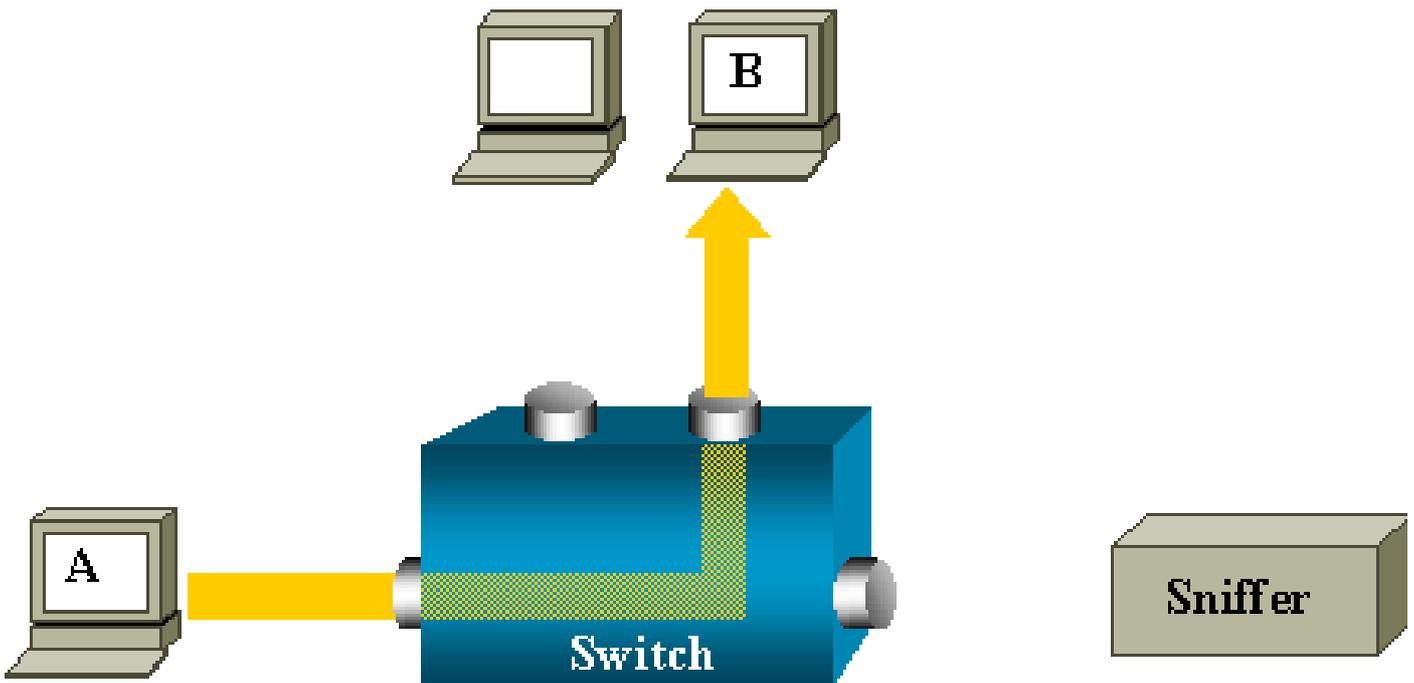
스위치와 허브의 근본적인 차이 때문에 SPAN 기능이 스위치에 도입되었습니다. 허브는 어떤 포트에서 패킷을 수신하면, 이 포트를 제외한 모든 포트에서 해당 패킷의 복사본을 보냅니다.

스위치가 부팅되면 수신하는 각기 다른 패킷의 소스 MAC 주소를 기반으로 레이어 2 포워딩 테이블을 구축하기 시작합니다. 이 포워딩 테이블이 빌드되면, 스위치는 어떤 MAC 주소를 목적지로 하는 트래픽을 해당 포트에 직접 포워딩합니다.

예를 들어, 호스트 A가 호스트 B로 전송하고 둘 다 허브에 연결된 이더넷 트래픽을 캡처하려면 이 허브에 스니퍼를 연결하기만 하면 됩니다. 나머지 모든 포트는 호스트 A와 호스트 B 간의 트래픽을 인식합니다.



스위치에서는 호스트 B MAC 주소를 확인한 다음 A에서 B로 보내는 유니캐스트 트래픽이 오로지 B 포트에 포워딩됩니다. 따라서 스니퍼에서는 이 트래픽을 인식하지 않습니다.



이러한 컨피그레이션에서는 다음과 같이 모든 포트에 플러딩되는 트래픽만 스니퍼에서 캡처합니다

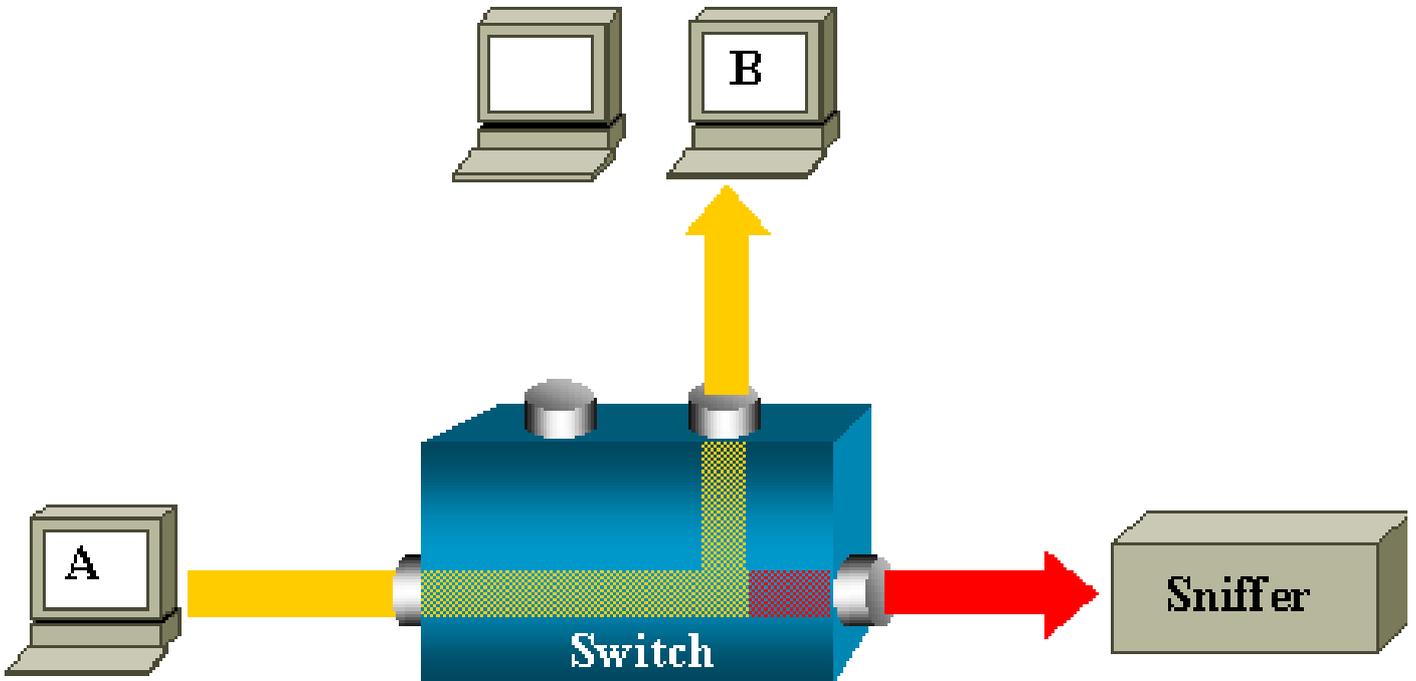
- 브로드캐스트 트래픽
- CGMP 또는 IGMP(Internet Group Management Protocol) 스누핑이 비활성화된 멀티캐스트 트래픽
- 알 수 없는 유니캐스트 트래픽

유니캐스트 플러딩은 스위치의 CAM(content-addressable memory) 테이블에 목적지 MAC이 없을

경우 발생합니다.

스위치는 트래픽을 어디에 보내야 하는지 모릅니다. 이 스위치는 목적지 VLAN의 모든 포트에 패킷을 플러딩합니다.

호스트 A가 스니퍼 포트에 보내는 유니캐스트 패킷을 인위적으로 복사하는 추가 기능이 필요합니다.

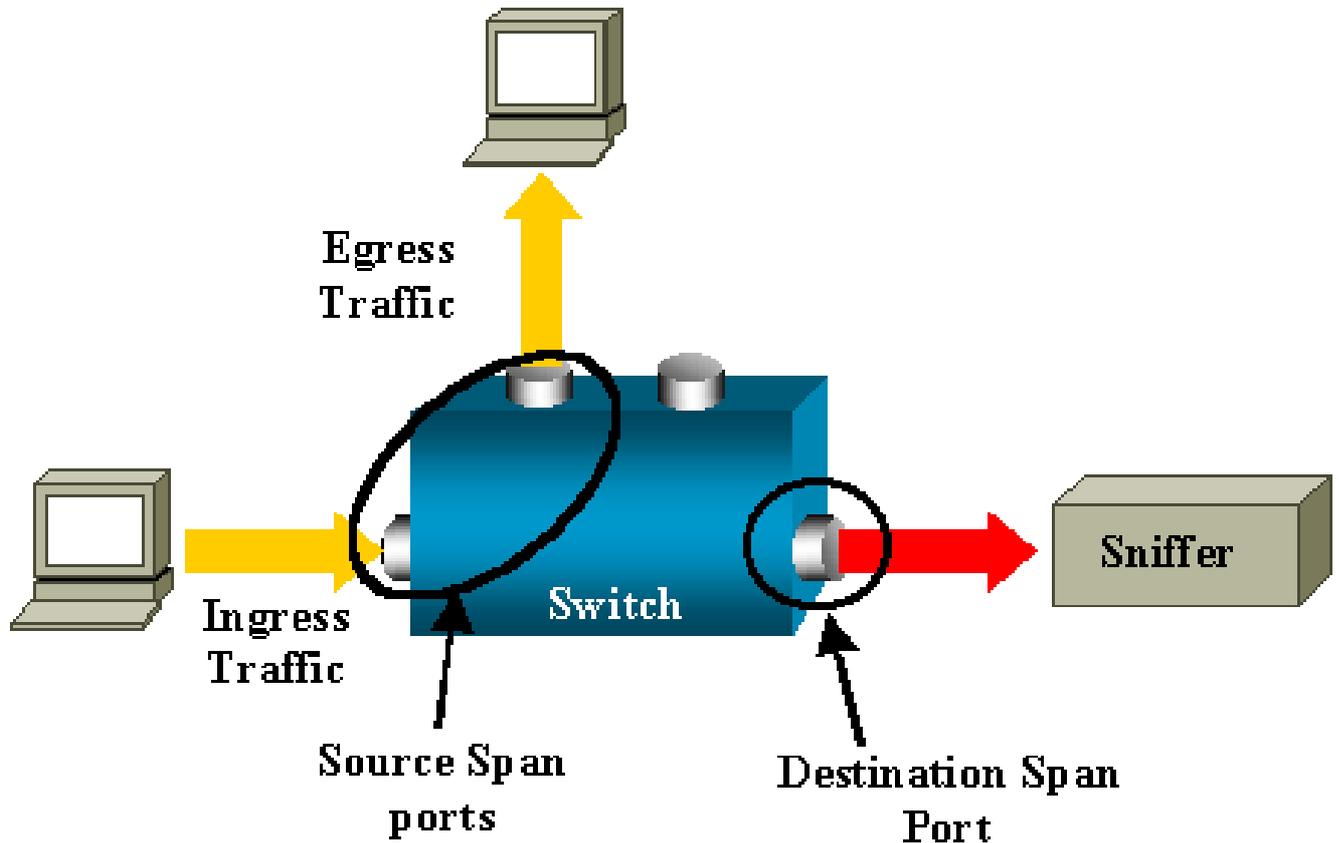


이 다이어그램에서 스니퍼가 연결된 포트는 호스트 A가 보내는 모든 패킷의 복사본을 수신하도록 구성되어 있습니다. 이 포트를 SPAN 포트라고 합니다.

이 문서의 나머지 섹션에서는 이 기능을 고도로 정밀하게 조정하여 포트 모니터링 이외의 작업도 수행하는 방법을 설명합니다.

## SPAN 용어

- 인그레스 트래픽 — 스위치에 들어가는 트래픽입니다.
- 이그레스 트래픽 — 스위치에서 나오는 트래픽입니다.
- [소스\(SPAN\) 포트 — SPAN 기능을 사용하여 모니터링하는 포트입니다.](#)
- [소스\(SPAN\) VLAN — SPAN 기능을 사용하여 트래픽을 모니터링하는 VLAN입니다.](#)
- [목적지\(SPAN\) 포트 — 대개 네트워크 분석기가 연결된 상태에서 소스 포트를 모니터링하는 포트입니다.](#)
- [리플렉터 포트 — RSPAN VLAN에 패킷을 복사하는 포트입니다.](#)
- 모니터 포트 - 모니터 포트는 Catalyst 2900XL/3500XL/2950 용어의 대상 SPAN 포트이기도 합니다.



- 로컬 SPAN — 모니터링되는 포트가 모두 목적지 포트와 같은 스위치에 있을 경우 SPAN 기능은 로컬입니다. 이 기능은 역시 이 목록에서 정의하는 RSPAN(Remote SPAN)과 대비됩니다.
- RSPAN(Remote SPAN) — 일부 소스 포트는 목적지 포트와 같은 스위치에 있지 않습니다.

RSPAN은 고급 기능이며, 스위치 사이에서 SPAN이 모니터링하는 트래픽을 전달하기 위해 특별한 VLAN이 필요합니다.

RSPAN이 모든 스위치에서 지원되지는 않습니다. 구축하는 스위치에서 RSPAN을 사용할 수 있는지를 각 릴리스 노트 또는 컨피그레이션 가이드에서 확인하십시오.

- PSPAN(Port-based SPAN) — 사용자가 스위치의 소스 포트를 하나 이상 그리고 목적지 포트 하나를 지정합니다.
- VSPAN(VLAN-based SPAN) — 사용자는 특정 스위치에서 하나의 명령으로 특정 VLAN에 속한 모든 포트를 모니터링하도록 선택할 수 있습니다.
- ESPAN - 향상된 SPAN 버전을 의미합니다. 이 용어는 SPAN을 발전시키는 동안 추가 기능의 이름을 지정하기 위해 여러 번 사용되었으므로 이 문서에서는 용어가 명확하지 않으며 사용하지 않습니다.
- 관리 소스 — 모니터링되도록 구성된 소스 포트 또는 VLAN의 목록입니다.
- 운영 소스 — 실제로 모니터링되는 포트의 목록입니다. 이 포트의 목록이 관리 소스와 다를 수 있습니다.

예를 들어, 섀다운 모드인 포트는 관리 소스에 나타날 수 있으나, 실제로 모니터링되지 않습니다.

## 소스 포트의 특성

모니터링되는 포트라고도 하는 소스 포트는 네트워크 트래픽 분석을 위해 모니터링하는 스위치드 포트 또는 라우티드 포트입니다.

단일 로컬 SPAN 세션 또는 RSPAN 소스 세션에서 수신(Rx), 전송(Tx) 또는 양방향(both)과 같은 소스 포트 트래픽을 모니터링할 수 있습니다.

이 스위치는 (스위치의 가용 포트 최대 개수 한도에서) 임의 개수의 소스 포트 및 임의 개수의 소스 VLAN을 지원합니다.

소스 포트의 특성은 다음과 같습니다.

- EtherChannel, 고속 이더넷, 기가 비트 이더넷 등 어떤 포트 유형도 가능합니다.
- 다중 SPAN 세션에서 모니터링할 수 있습니다.
- 이는 목적지 포트가 될 수 없습니다.
- 각 소스 포트에 모니터링 방향(인그레스, 이그레스 또는 둘 다)을 구성할 수 있습니다. EtherChannel 소스의 경우, 모니터링 방향이 그룹의 모든 물리적 포트에 적용됩니다.
- 소스 포트는 같은 VLAN 또는 서로 다른 VLAN에 속할 수 있습니다.
- VLAN SPAN 소스의 경우, 소스 VLAN의 모든 활성 포트가 소스 포트에 포함됩니다.

## VLAN 필터링

트렁크 포트를 소스 포트에 모니터링하는 경우, 기본적으로 트렁크의 모든 활성 VLAN을 모니터링합니다. VLAN 필터링을 사용하여 트렁크 소스 포트의 SPAN 트래픽 모니터링을 특정 VLAN으로 제한할 수 있습니다.

- VLAN 필터링은 트렁크 포트 또는 음성 VLAN 포트에만 적용됩니다.
- VLAN 필터링은 포트 기반 세션에만 적용되며, VLAN 소스를 사용하는 세션에서는 허용되지 않습니다.
- VLAN 필터 목록이 지정되면, 목록에 있는 VLAN만 트렁크 포트 또는 음성 VLAN 액세스 포트에서 모니터링됩니다.
- 다른 포트 유형으로부터 수신한 SPAN 트래픽은 VLAN 필터링의 영향을 받지 않습니다. 즉, 모든 VLAN이 다른 포트에서 허용됩니다.
- VLAN 필터링은 목적지 SPAN 포트에 포워딩된 트래픽에만 적용되며, 일반 트래픽의 스위칭에는 영향을 주지 않습니다.
- 하나의 세션에서 소스 VLAN과 필터 VLAN을 혼합할 수 없습니다. 소스 VLAN 또는 필터 VLAN 중 하나만 가능하며, 동시에 둘 다 사용할 수 없습니다.

## 소스 VLAN의 특성

VSPAN은 하나 이상의 VLAN에서 네트워크 트래픽을 모니터링하는 것입니다. VSPAN의 SPAN 또는 RSPAN 소스 인터페이스는 VLAN ID이며, 해당 VLAN에 대한 모든 포트에서 트래픽이 모니터링됩니다.

VSPAN의 특징은 다음과 같습니다.

- 소스 VLAN의 모든 활성 포트는 소스 포트에 포함되며, 두 방향 중 하나로 또는 양방향으로 모니터링될 수 있습니다.
- 지정된 포트에서 모니터링되는 VLAN의 트래픽만 목적지 포트에 보내집니다.
- 목적지 포트가 소스 VLAN에 속하는 경우, 소스 목록에서 제외되어 모니터링되지 않습니다.
- 포트가 소스 VLAN에 추가되거나 소스 VLAN에서 제거될 경우, 이 포트가 수신하는 소스 VLAN의 트래픽은 모니터링되는 소스에 추가되거나 제거됩니다.
- 필터 VLAN을 VLAN 소스와 같은 세션에서 사용할 수 없습니다.
- 이더넷 VLAN만 모니터링할 수 있습니다.

## 목적지 포트의 특성

각 로컬 SPAN 세션 또는 RSPAN 목적지 세션에는 소스 포트 및 VLAN으로부터 트래픽의 사본을 수신할 (모니터링 포트라고도 하는) 목적지 포트가 있어야 합니다.

목적지 포트의 특성은 다음과 같습니다.

- 목적지 포트는 소스 포트와 같은 스위치에 상주해야 합니다(로컬 SPAN 세션의 경우).
- 어떤 이더넷 물리적 포트도 목적지 포트가 될 수 있습니다.
- 목적지 포트는 한 번에 하나의 SPAN 세션에만 참여할 수 있습니다. 어떤 SPAN 세션의 목적지 포트가 다른 SPAN 세션을 위한 목적지 포트가 될 수 없습니다.
- 목적지 포트는 소스 포트일 수 없습니다.
- 목적지 포트는 EtherChannel 그룹일 수 없습니다.

---

 참고: Cisco IOS Software Release 12.2(33)SXH 이상에서는 PortChannel 인터페이스가 목적지 포트가 될 수 있습니다. 대상 EtherChannel은 PAgP(Port Aggregation Control Protocol) 또는 LACP(Link Aggregation Control Protocol) EtherChannel 프로토콜을 지원하지 않습니다. 모든 EtherChannel 프로토콜 지원을 비활성화한 상태에서 on 모드만 지원됩니다.

---

 참고: 자세한 내용은 [로컬 SPAN, RSPAN 및 ERSPAN](#) 대상을 참조하십시오.

---

- 목적지 포트는 EtherChannel 그룹에 지정된 물리적 포트일 수 있습니다. 해당 EtherChannel 그룹이 SPAN 소스로 지정되었더라도 가능합니다. SPAN 목적지 포트에 구성된 포트는 그룹

에서 제거됩니다.

- 학습이 활성화되지 않는 한, 이 포트는 SPAN 세션에 필요한 트래픽을 제외하고 어떤 트래픽도 전송하지 않습니다. 학습이 활성화된 경우, 포트는 목적지 포트에서 학습된 호스트로 향하는 트래픽도 전송합니다.



참고: 자세한 내용은 [로컬 SPAN, RSPAN 및 ERSPAN](#) 대상을 참조하십시오.

- 목적지 포트의 상태는 up/down으로 설계됩니다. 인터페이스에서 이 상태의 포트를 표시하여 현재는 프로덕션 포트로는 사용할 수 없음을 확실히 알려줍니다.
- 네트워크 보안 디바이스에 대해 인그레스 트래픽 포워딩이 활성화된 경우, 목적지 포트는 레이어 2에서 트래픽을 포워딩합니다.
- SPAN 세션이 활성 상태일 때는 목적지 포트가 스페닝 트리에 참여하지 않습니다.
- 목적지 포트인 경우, 어떤 레이어 2 프로토콜(STP, VTP, CDP, DTP, PagP)에도 참여하지 않습니다.
- 목적지 포트가 어떤 SPAN 세션의 소스 VLAN에 속하는 경우, 소스 목록에서 제외되어 모니터링되지 않습니다.
- 목적지 포트는 모니터링되는 모든 소스 포트에 대해 송수신된 트래픽의 복사본을 수신합니다. 목적지 포트가 오버서브스크립션되는 경우 혼잡이 발생할 수 있습니다. 이러한 혼잡은 하나 이상의 소스 포트에서 트래픽 포워딩에 영향을 줄 수 있습니다.

## 리플렉터 포트의 특성

리플렉터 포트는 RSPAN VLAN에 패킷을 복사하는 메커니즘입니다. 리플렉터 포트는 연결된 RSPAN 소스 세션의 트래픽만 포워딩합니다.

어떤 디바이스가 리플렉터 포트에 설정된 포트에 연결되면, RSPAN 소스 세션이 비활성화될 때까지는 연결되지 않습니다.

리플렉터 포트의 특성은 다음과 같습니다.

- 루프백으로 설정된 포트입니다.
- EtherChannel 그룹일 수 없고, 트렁킹하지 않으며, 프로토콜 필터링을 수행할 수 없습니다.
- EtherChannel 그룹에 지정된 물리적 포트일 수 있습니다. 해당 EtherChannel 그룹이 SPAN 소스로 지정되었다고 가능합니다. 리플렉터 포트에 구성된 포트는 그룹에서 제거됩니다.
- 리플렉터 포트에 사용되는 포트는 SPAN 소스 또는 목적지 포트가 될 수 없습니다. 또한 하나의 포트가 동시에 2개 이상 세션의 리플렉터 포트일 수 없습니다.
- 모든 VLAN에 보이지 않습니다.
- 리플렉터 포트에서 루프백된 트래픽의 기본 VLAN은 RSPAN VLAN입니다.

- 리플렉터 포트는 태그 없는 트래픽을 스위치에 루프백합니다. 그러면 이 트래픽은 RSPAN VLAN에 배치되고, 이 RSPAN VLAN을 전달하는 모든 트렁크 포트에 플러딩됩니다.
- 스페닝 트리는 리플렉터 포트에서 자동으로 비활성화됩니다.
- 리플렉터 포트는 모니터링되는 모든 소스 포트에 대해 송수신된 트래픽의 복사본을 수신합니다.

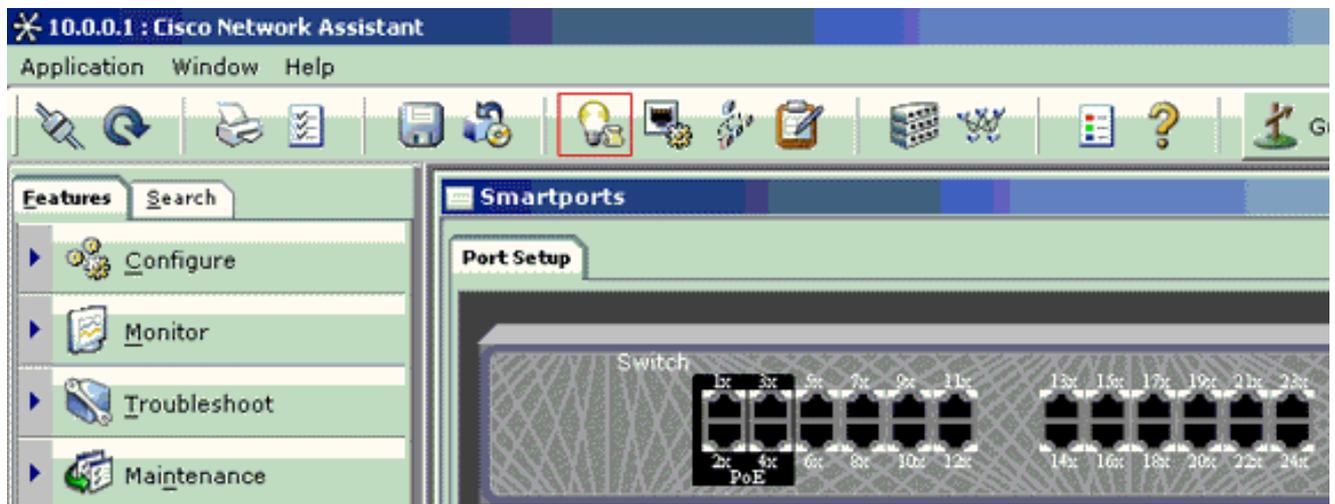
## Catalyst Express 500/520의 SPAN

Catalyst Express 500 또는 Catalyst Express 520은 SPAN 기능만 지원합니다. SPAN에 대해 Catalyst Express 500/520 포트를 구성하려면 CNA(Cisco Network Assistant)만 사용해야 합니다. 다음 단계에 따라 SPAN을 구성합니다.

1. PC에 CNA를 다운로드하고 설치합니다.

[Download Software\(소프트웨어 다운로드\) 페이지\(등록된 고객 전용\)에서 CNA를 다운로드할 수 있습니다.](#)

2. [Catalyst Express 500 스위치 12.2\(25\)FY 시작 가이드의 단계에 따라 Catalyst Express 500에 대한 스위치 설정을 맞춤설정합니다.](#) Catalyst Express 520에 대한 자세한 내용은 [Catalyst Express 520 스위치 시작 가이드를 참조하십시오.](#)
3. CNA를 사용하여 스위치에 로그인하고 Smartport(스마트 포트)를 클릭합니다.

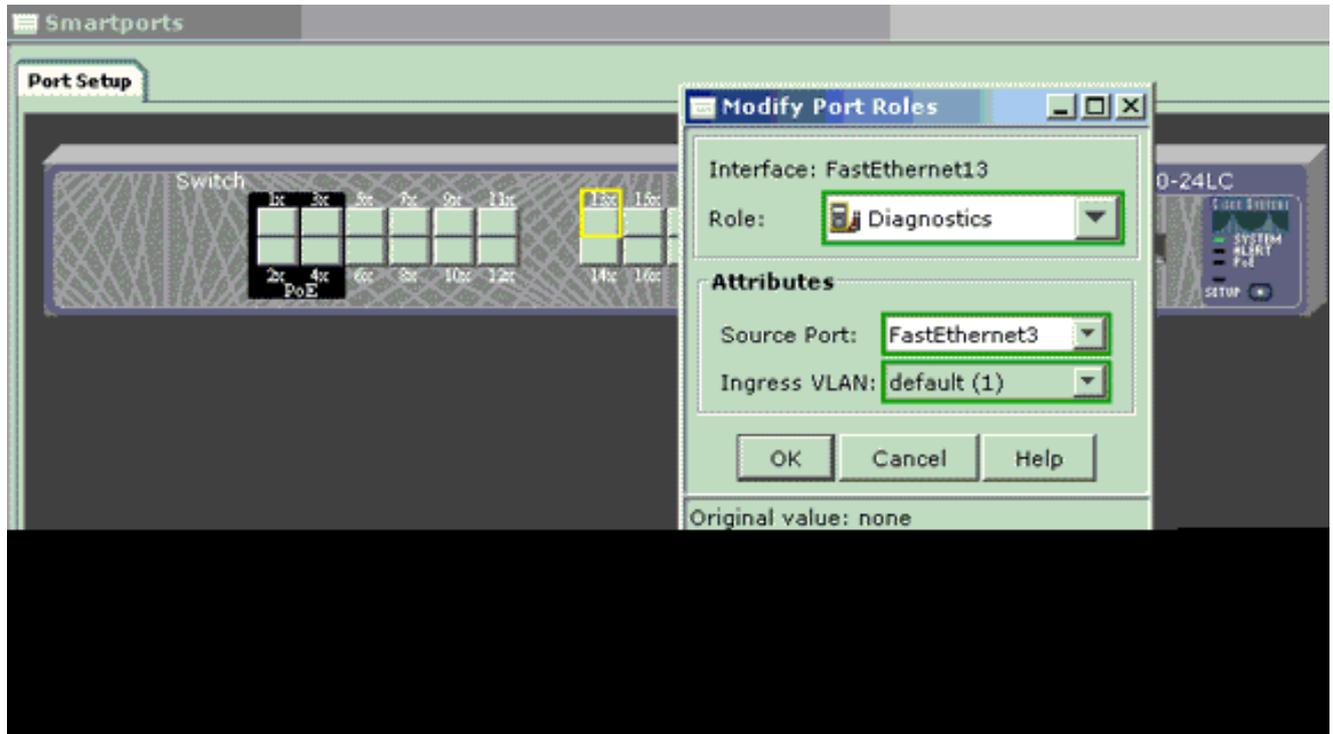


4. 스니퍼 추적을 캡처하기 위해 PC를 연결할 임의의 인터페이스를 클릭합니다.
5. 수정을 클릭합니다.

작은 팝업 상자가 나타납니다.

6. 포트에 대해 Diagnostics(진단) 역할을 선택합니다.
7. 소스 포트를 선택하고 모니터링할 VLAN을 선택합니다.

none(없음)을 선택하면 포트는 트래픽을 수신할 뿐입니다. 인그레스 VLAN을 사용하면 진단 포트에 연결된 PC에서 해당 VLAN을 사용하는 네트워크에 패킷을 보낼 수 있습니다.



8. 팝업 상자를 닫으려면 OK(확인)를 클릭합니다.
9. OK(확인)를 클릭한 다음 이 설정을 Apply(적용)합니다.
10. 진단 포트를 설정해두면 어떤 스니퍼 소프트웨어든지 사용하여 트래픽을 추적할 수 있습니다.

## Catalyst 2900XL/3500XL 스위치의 SPAN

### 제공되는 기능 및 제한 사항

Catalyst 2900XL/3500XL에서는 포트 모니터링 기능이 그다지 포괄적이지 않습니다. 따라서 이 기능은 비교적 쉽게 이해할 수 있습니다.

로컬 PSPAN 세션을 필요한 개수만큼 생성할 수 있습니다. 예를 들어, 목적지 SPAN 포트에 선택한 컨피그레이션 포트에서 PSPAN 세션을 생성할 수 있습니다. 이 경우 [포트 모니터](#) 인터페이스를 실행합니다 명령을 사용하여 모니터링할 소스 포트를 나열합니다. 모니터 포트는 Catalyst 2900XL/3500XL 용어로 하면 목적지 SPAN 포트입니다.

- 기본적으로, 특정 세션과 관련된 모든 포트(소스 또는 목적지)는 같은 VLAN에 속해야 한다는 제한이 있습니다.
- IP 주소를 사용하여 VLAN 인터페이스를 구성하는 경우 port monitor 명령은 해당 IP 주소를 목적지로 하는 트래픽만 모니터링합니다. 또한 VLAN 인터페이스에서 수신하는 브로드캐스트 트래픽도 모니터링합니다. 그러나 실제 VLAN에서 이동하는 트래픽 자체는 캡처하지 않습니다. port monitor 명령에서 어떤 인터페이스도 지정하지 않을 경우, 같은 VLAN을 인터페이스로 하는 나머지 모든 포트가 모니터링됩니다.

이 목록에는 몇 가지 제한 사항이 있습니다. 자세한 내용은 명령 참조 가이드(Catalyst 2900XL/3500XL)에서 확인하십시오.

 참고: ATM 포트만 모니터 포트가 될 수 없습니다. 그러나 ATM 포트를 모니터링할 수는 있습니다. 이 목록의 제한 사항은 포트 모니터 기능이 있는 포트에 적용됩니다.

- 모니터 포트는 Fast EtherChannel 또는 기가비트 EtherChannel 포트 그룹에 포함될 수 없습니다.
- 포트 보안상 모니터 포트를 활성화할 수 없습니다.
- 모니터 포트는 다중 VLAN 포트일 수 없습니다.
- 모니터 포트는 모니터링되는 포트와 같은 VLAN의 멤버여야 합니다. 모니터 포트와 모니터링되는 포트에 대해서는 VLAN 멤버십 변경이 허용되지 않습니다.
- 모니터 포트는 동적 액세스 포트 또는 트렁크 포트일 수 없습니다. 그러나 정적 액세스 포트는 트렁크의 VLAN, 다중 VLAN 또는 동적 액세스 포트를 모니터링할 수 있습니다. 모니터링되는 VLAN은 정적 액세스 포트와 연결된 VLAN입니다.
- 모니터 포트와 모니터링되는 포트 모두 보호되는 포트인 경우에는 포트 모니터링이 작동하지 않습니다.

모니터 상태에 있는 포트가 미러링 대상 포트의 VLAN에 계속 속해 있다면 STP(Spanning Tree Protocol)를 실행하지 않도록 주의해야 합니다. 포트 모니터가 루프의 일부일 수 있습니다. 이를테면 허브 또는 브리지에 연결하고 네트워크의 다른 부분으로 루프합니다. 이러한 경우 STP가 더는 보호해주지 않으므로, 최악의 브리징 루프 조건이 될 수 있습니다. 이 조건이 발생할 수 있는 방법의 예제는 [이 문서](#)의 SPAN 세션이 브리징 루프를 생성하는 이유를 참조하십시오.

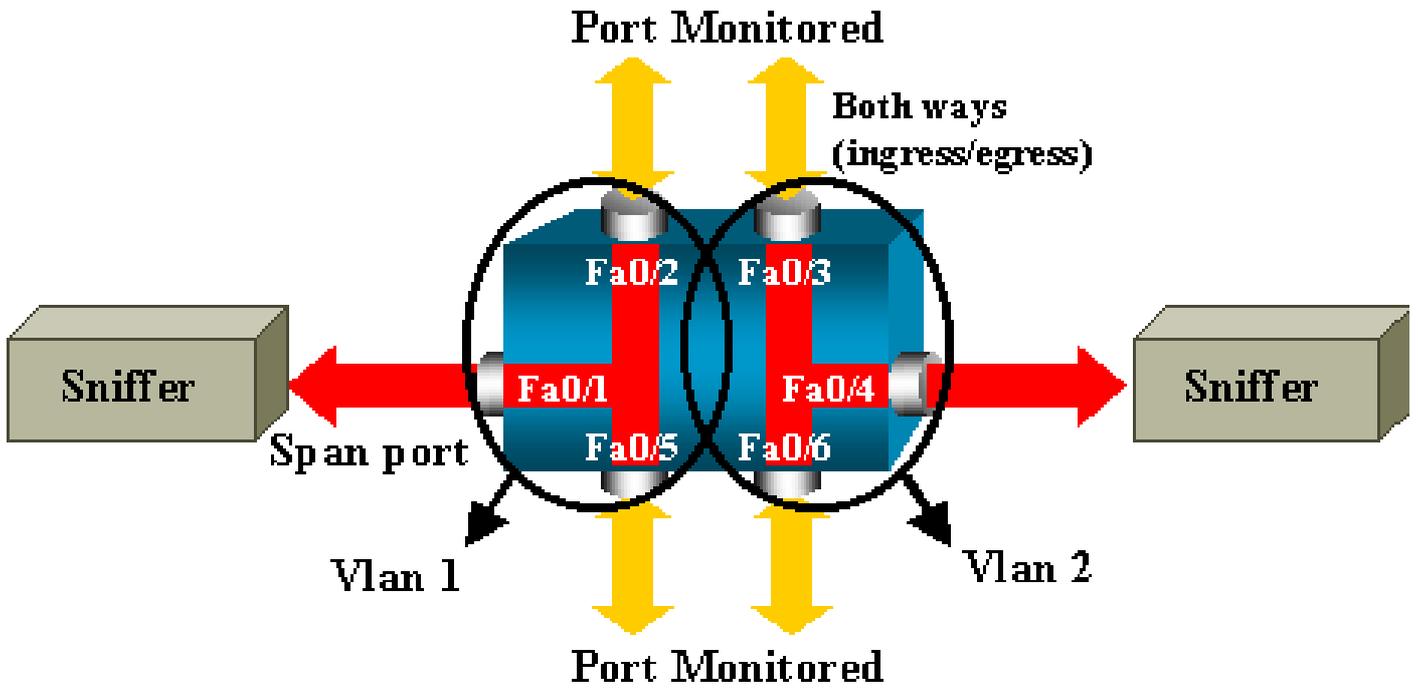
## 컨피그레이션 예시

이 예에서는 두 개의 동시 SPAN 세션을 생성합니다.

- 포트 Fa0/1(Fast Ethernet 0/1)은 포트 Fa0/2 및 Fa0/5가 송수신하는 트래픽을 모니터링합니다. 포트 Fa0/1은 관리 인터페이스 VLAN 1로 오가는 트래픽도 모니터링합니다.
- 포트 Fa0/4는 포트 Fa0/3 및 Fa0/6을 모니터링합니다.

포트 Fa0/3, Fa0/4, Fa0/6 모두 VLAN 2에 구성되어 있습니다. 다른 포트 및 관리 인터페이스는 기본 VLAN 1에서 구성됩니다.

## 네트워크 다이어그램



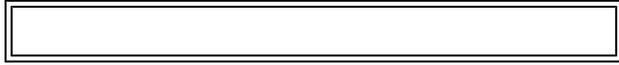
### Catalyst 2900XL/3500XL의 샘플 컨피그레이션

#### 2900XL/3500XL SPAN 샘플 컨피그레이션

```

!--- Output suppressed.
!
interface FastEthernet0/1
port monitor FastEthernet0/2
port monitor FastEthernet0/5
port monitor VLAN1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
switchport access vlan 2
!
interface FastEthernet0/4
port monitor FastEthernet0/3
port monitor FastEthernet0/6
switchport access vlan 2
!
interface FastEthernet0/5
!
interface FastEthernet0/6
switchport access vlan 2
!
!--- Output suppressed.
!
interface VLAN1
ip address 10.200.8.136 255.255.252.0
no ip directed-broadcast
no ip route-cache
!
!--- Output suppressed.

```



## 컨피그레이션 단계 설명

포트 Fa0/1을 목적지 포트 구성하고 소스 포트 Fa0/2 및 Fa0/5, 관리 인터페이스(VLAN 1)도 구성하려면 컨피그레이션 모드에서 인터페이스 Fa0/1을 선택합니다.

```
<#root>
```

```
Switch(config)#
```

```
interface fastethernet 0/1
```

모니터링할 포트의 목록을 입력합니다.

```
<#root>
```

```
Switch(config-if)#
```

```
port monitor fastethernet 0/2
```

```
Switch(config-if)#
```

```
port monitor fastethernet 0/5
```

이 명령을 사용하면, 이 두 포트에서 송수신하는 모든 패킷이 포트 Fa0/1에도 복사됩니다. 관리 인터페이스에 대한 모니터링을 구성하려면 port monitor 명령을 변형하여 실행합니다.

```
<#root>
```

```
Switch(config-if)#
```

```
port monitor vlan 1
```

---

 참고: 이 명령은 포트 Fa0/1이 전체 VLAN 1을 모니터링한다는 의미는 아닙니다. vlan 1 키워드는 단지 스위치의 관리 인터페이스를 가리킵니다.

---

이 명령의 예는 다른 VLAN에 속한 포트에 대한 모니터링이 불가능함을 보여줍니다.

```
<#root>
```

```
Switch(config-if)#
```

```
port monitor fastethernet 0/3
```

FastEthernet0/1 and FastEthernet0/3 are in different vlan

컨피그레이션을 완료하려면 다른 세션을 구성합니다. 이번에는 Fa0/4를 목적지 SPAN 포트로 사용합니다.

<#root>

```
Switch(config-if)#
```

```
interface fastethernet 0/4
```

```
Switch(config-if)#
```

```
port monitor fastethernet 0/3
```

```
Switch(config-if)#
```

```
port monitor fastethernet 0/6
```

```
Switch(config-if)#
```

```
^Z
```

show running 명령을 실행하거나 [show port monitor](#) 명령을 사용하여 컨피그레이션을 확인합니다.

<#root>

```
Switch#
```

```
show port monitor
```

```
Monitor Port Port Being Monitored
```

```
-----  
FastEthernet0/1 VLAN1
```

```
FastEthernet0/1 FastEthernet0/2
```

```
FastEthernet0/1 FastEthernet0/5
```

```
FastEthernet0/4 FastEthernet0/3
```

```
FastEthernet0/4 FastEthernet0/6
```

---

 참고: Catalyst 2900XL 및 3500XL은 Rx 방향에서만 SPAN을 지원하지 않으며(Rx SPAN 또는 인그레스 SPAN) Tx 방향에서만 SPAN을 지원하지 않습니다(Tx SPAN 또는 이그레스 SPAN). 모든 SPAN 포트는 Rx 트래픽과 Tx 트래픽을 모두 캡처하도록 설계되어 있습니다.

---

## Catalyst 2948G-L3 및 4908G-L3의 SPAN

Catalyst 2948G-L3 및 Catalyst 4908G-L3는 고정 컨피그레이션 스위치 라우터 또는 레이어 3 스위치입니다. 레이어 3 스위치의 SPAN 기능을 포트 스누핑이라고 합니다.

그러나 이 스위치에서는 포트 스누핑이 지원되지 않습니다. [Cisco IOS Release 12.0\(10\)W5\(18g\)용 Catalyst 2948G-L3 및 Catalyst 4908G-L3에 대한 문서 릴리스 노트의 지원되지 않는 기능 섹션을](#) 참조하십시오.

## Catalyst 8500의 SPAN

Catalyst 8540에서는 포트 스누핑이라는 이름으로 매우 기본적인 SPAN 기능을 제공합니다. 자세한 내용은 최신 Catalyst 8540 문서를 참조하십시오.

포트 스누핑을 사용하면 하나 이상의 소스 포트에서 어떤 목적지 포트로 가는 트래픽을 투명하게 미러링할 수 있습니다.

포트 기반 트래픽 미러링, 즉 스누핑을 설정하려면 snoop 명령을 실행합니다. 스누핑을 비활성화하려면 이 명령의 no 형식을 실행합니다.

```
<#root>
```

```
snoop interface source_port direction snoop_direction
```

```
no snoop interface source_port
```

변수 source\_port는 모니터링되는 포트를 가리킵니다. variable snoop\_direction은 모니터링되는 소스 포트의 트래픽 방향(수신, 전송 또는 둘 다)입니다.

```
<#root>
```

```
8500CSR#
```

```
configure terminal
```

```
8500CSR(config)#
```

```
interface fastethernet 12/0/15
```

```
8500CSR(config-if)#
```

```
shutdown
```

```
8500CSR(config-if)#
```

```
snoop interface fastethernet 0/0/1 direction both
```

```
8500CSR(config-if)#
```

```
no shutdown
```

show snoop 명령을 실행하면 다음과 같이 출력됩니다.

```
<#root>
```

```
8500CSR#
```

```
show snoop
```

```
Snoop Test Port Name: FastEthernet1/0/4 (interface status=SNOOPING)
Snoop option:          (configured=enabled)(actual=enabled)
Snoop direction:      (configured=receive)(actual=receive)
Monitored Port Name:
(configured=FastEthernet1/0/3)(actual=FastEthernet1/0/3)
```

---

 참고: 8540m-in-mz와 같은 멀티서비스 ATM 스위치 라우터(MSR) 이미지를 실행하는 경우 Catalyst 8540의 이더넷 포트에서는 이 명령이 지원되지 않습니다. 8540c-in-mz와 같은 CSR(Campus Switch Router) 이미지를 대신 사용해야 합니다.

---

## CatOS를 실행하는 Catalyst 2900, 4500/4000, 5500/5000, 6500/6000 Series Switch의 SPAN

이 섹션은 다음 Cisco Catalyst 2900 시리즈 스위치에만 적용됩니다.

- Cisco Catalyst 2948G-L2 스위치
- Cisco Catalyst 2948G-GE-TX 스위치
- Cisco Catalyst 2980G-A 스위치

이 섹션은 다음 Cisco Catalyst 4000 시리즈 스위치에 적용됩니다.

- 모듈형 샤페스 스위치:
  - Cisco Catalyst 4003 스위치
  - Cisco Catalyst 4006 스위치
- 고정 샤페스 스위치:
  - Cisco Catalyst 4912G 스위치

### 로컬 SPAN

SPAN 기능이 하나씩 CatOS에 추가되어 왔으며, SPAN 컨피그레이션은 단일 set span 명령으로 구성됩니다. 이제는 다양한 옵션을 이 명령과 함께 사용할 수 있습니다.

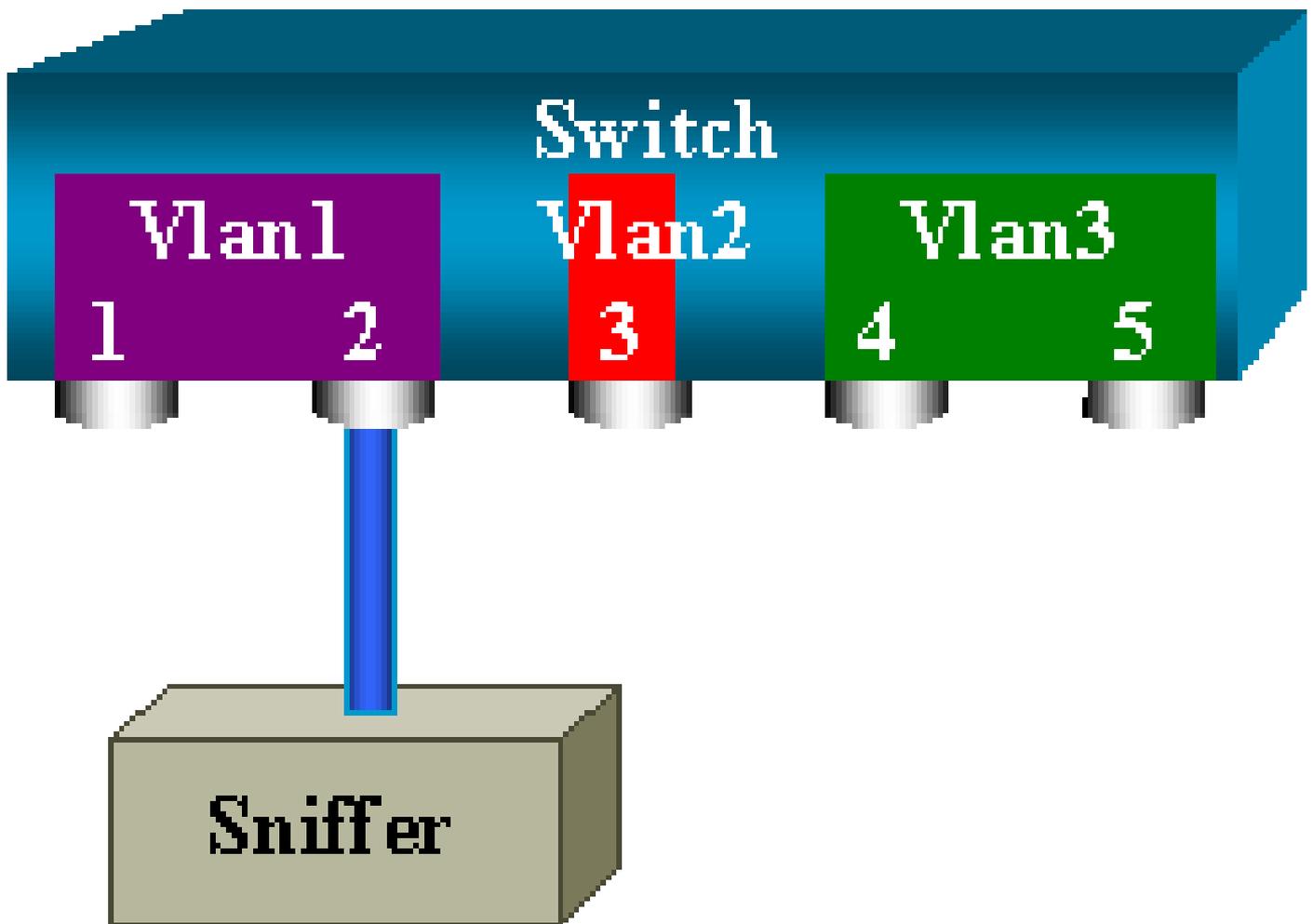
```
<#root>
```

```
switch (enable)
```

```
set span
```

```
Usage: set span disable [dest_mod/dest_port|all]  
set span <src_mod/src_ports...|src_vlans...|sc0>  
      <dest_mod/dest_port> [rx|tx|both]  
      [inpkts <enable|disable>]  
      [learning <enable|disable>]  
      [multicast <enable|disable>]  
      [filter <vlans...>]  
      [create]
```

이 네트워크 다이어그램은 다양하게 변형 가능한 SPAN을 보여줍니다.



이 다이어그램은 Catalyst 6500/6000 스위치의 슬롯 6에 있는 단일 라인 카드의 일부를 나타냅니다. 이 시나리오에서:

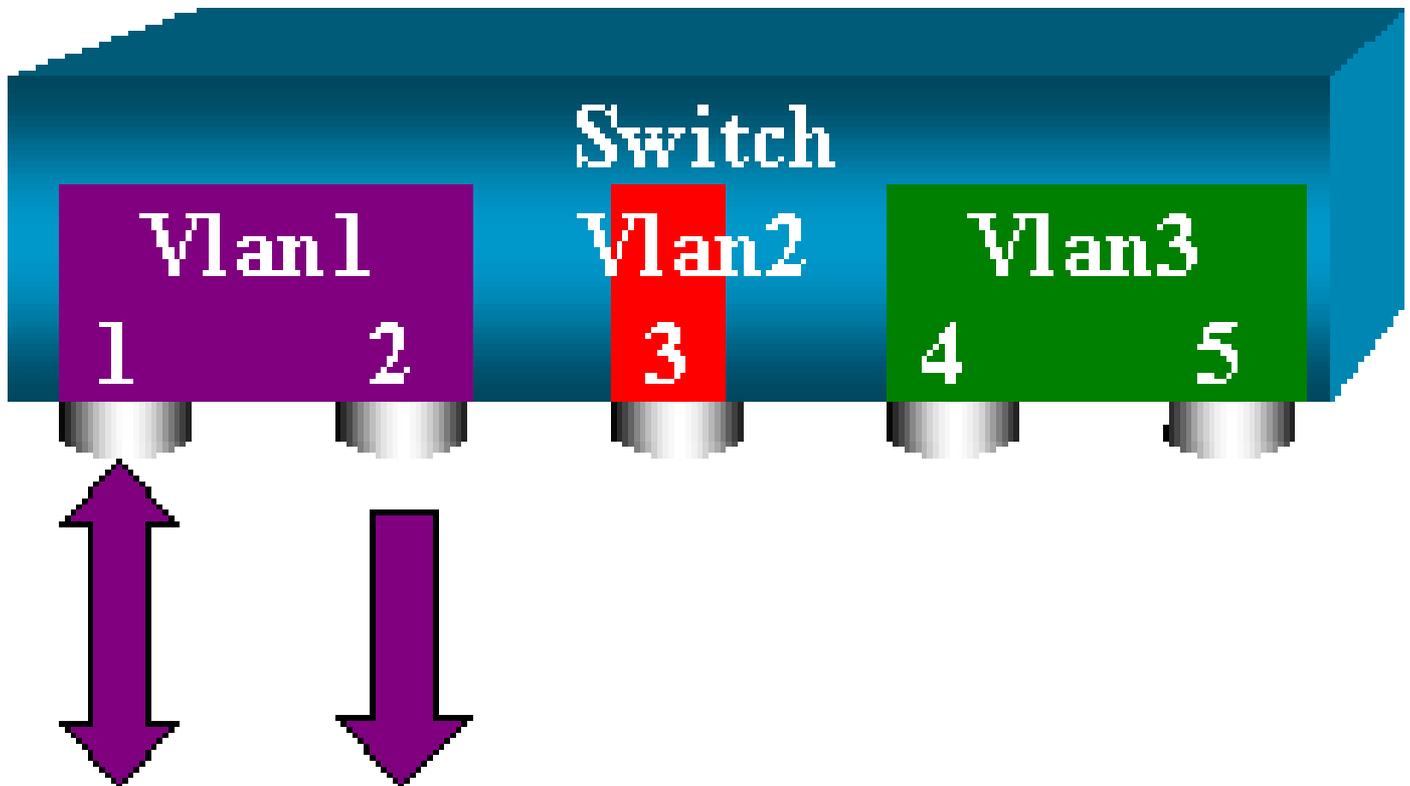
- 포트 6/1 및 6/2는 VLAN 1에 속함
- 포트 6/3은 VLAN 2에 속함
- 포트 6/4 및 6/5는 VLAN 3에 속함

스니퍼를 포트 6/2에 연결하고, 여러 가지 상황에서 모니터 포트로 사용합니다.

PSPAN, VSPAN: 일부 포트 또는 전체 VLAN 모니터링

단일 포트를 모니터링하려면 가장 단순한 형식의 set span 명령을 실행합니다. 구문은 set span source\_port destination\_port입니다.

SPAN으로 단일 포트 모니터링



```
<#root>
```

```
switch (enable)
```

```
set span 6/1 6/2
```

```
Destination : Port 6/2
```

```
Admin Source : Port 6/1
```

```
Oper Source : Port 6/1
```

```
Direction : transmit/receive
```

```
Incoming Packets: disabled
```

```
Learning : enabled
```

```
Multicast : enabled
```

```
Filter : -
```

```
Status : active
```

```
switch (enable) 2000 Sep 05 07:04:14 %SYS-5-SPAN_CFGSTATECHG:local span
```

```
session active for destination port 6/2
```

이 컨피그레이션에서는 포트 6/1에서 송수신하는 모든 패킷이 포트 6/2에 복사됩니다. 컨피그레이션을 입력하면 명확한 설명이 표시됩니다. 현재 SPAN 컨피그레이션의 요약을 보려면 show span

명령을 실행합니다.

```
<#root>
```

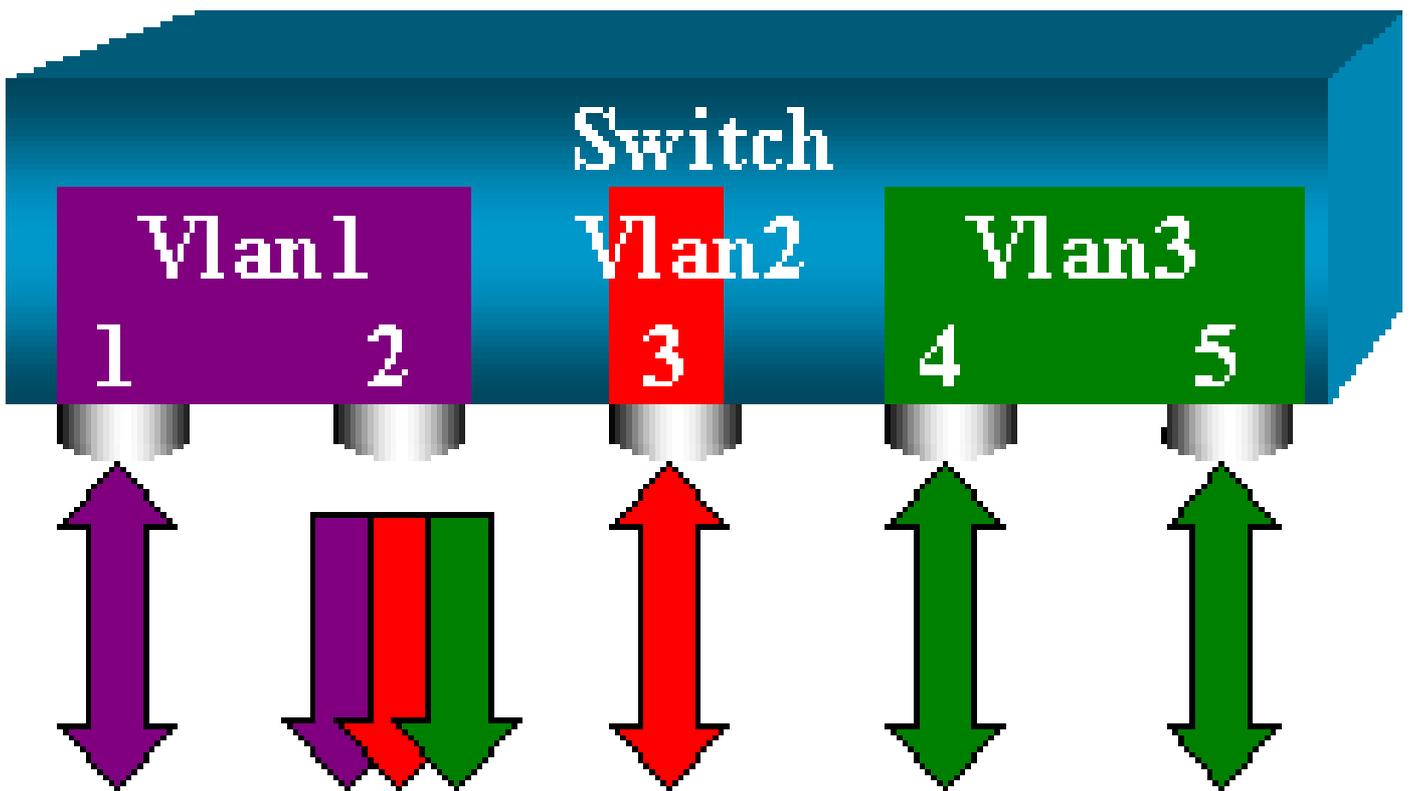
```
switch (enable)
```

```
show span
```

```
Destination : Port 6/2  
Admin Source : Port 6/1  
Oper Source : Port 6/1  
Direction : transmit/receive  
Incoming Packets: disabled  
Learning : enabled  
Multicast : enabled  
Filter : -  
Status : active
```

```
Total local span sessions: 1
```

SPAN으로 여러 포트 모니터링



set span source\_ports destination\_port 명령을 사용하면 둘 이상의 소스 포트를 지정할 수 있습니다. SPAN을 구현하려는 모든 포트를 심표로 구분하면서 나열하면 됩니다.

명령줄 인터프리터에서 하이픈을 사용하여 포트의 범위를 지정할 수도 있습니다.

이 예에서는 둘 이상의 포트를 지정하는 이 기능을 보여줍니다. 이 예에서는 포트 6/1 및 포트 3개가

포함되는 범위(6/3부터 6/5까지)에서 SPAN을 사용합니다.

---

 참고: 대상 포트는 하나만 있을 수 있습니다. 언제나 SPAN 소스 다음에 목적지 포트를 지정합니다.

---

<#root>

switch (enable)

```
set span 6/1,6/3-5 6/2
```

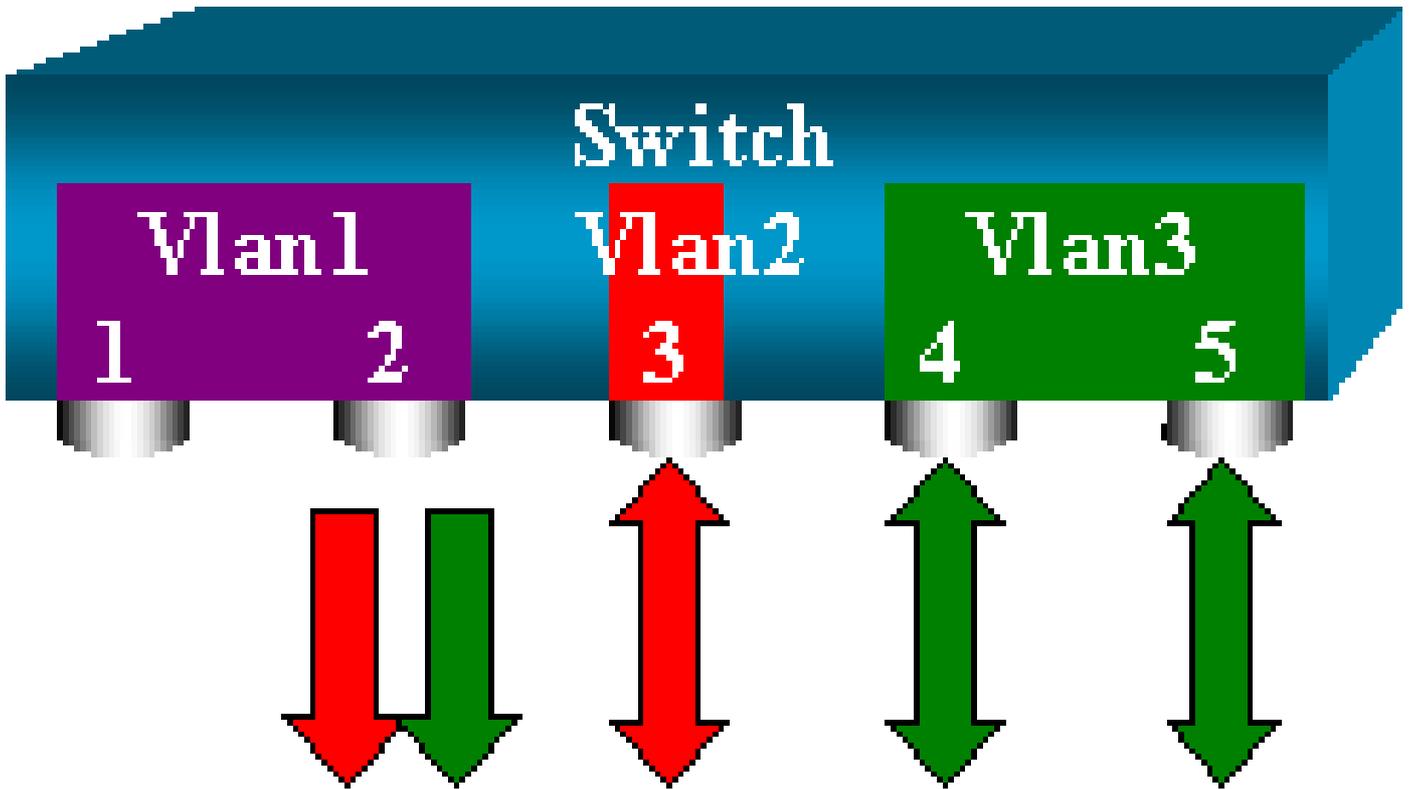
```
2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1,6/3-5
Oper Source : Port 6/1,6/3-5
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:17:36 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

 참고: Catalyst 2900XL/3500XL 스위치와 달리 Catalyst 4500/4000, 5500/5000 및 6500/6000은 5.1 이전의 CatOS 버전으로 여러 다른 VLAN에 속하는 포트를 모니터링할 수 있습니다. 여기서 미러링된 포트는 VLAN 1, 2, 3에 지정됩니다.

---

## SPAN으로 VLAN 모니터링

결국 set span 명령을 사용하면 어떤 포트에서 VLAN 전체에 대한 로컬 트래픽을 모니터링하도록 구성할 수 있습니다. 이 명령은 set span source\_vlan(s) destination\_port입니다.



포트의 목록이 아니라 하나 이상의 VLAN으로 구성된 목록을 소스로 사용합니다.

```
<#root>
```

```
switch (enable)
```

```
set span 2,3 6/2
```

```
2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 2-3
Oper Source : Port 6/3-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 07:40:10 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

이 컨피그레이션에서는 VLAN 2 또는 3에 들어오거나 나가는 모든 패킷이 포트 6/2에 복제됩니다.

 참고: 명령이 지정하는 VLAN에 속하는 모든 포트에서 개별적으로 SPAN을 구현하는 경우와 동일한 결과가 나타납니다. Oper Source(운영 소스) 필드와 Admin Source(관리 소스) 필드를 비교합니다. Admin Source(관리 소스) 필드는 기본적으로 SPAN 세션에 대해 구성된 모든 포트를 나열하고, Oper Source(운영 소스) 필드는 SPAN을 사용하는 포트를 나열합니다.

## 인그레스/이그레스 SPAN

[SPAN으로 VLAN 모니터링 섹션의 예에서는 지정된 포트를 오가는 트래픽이 모니터링됩니다.](#)

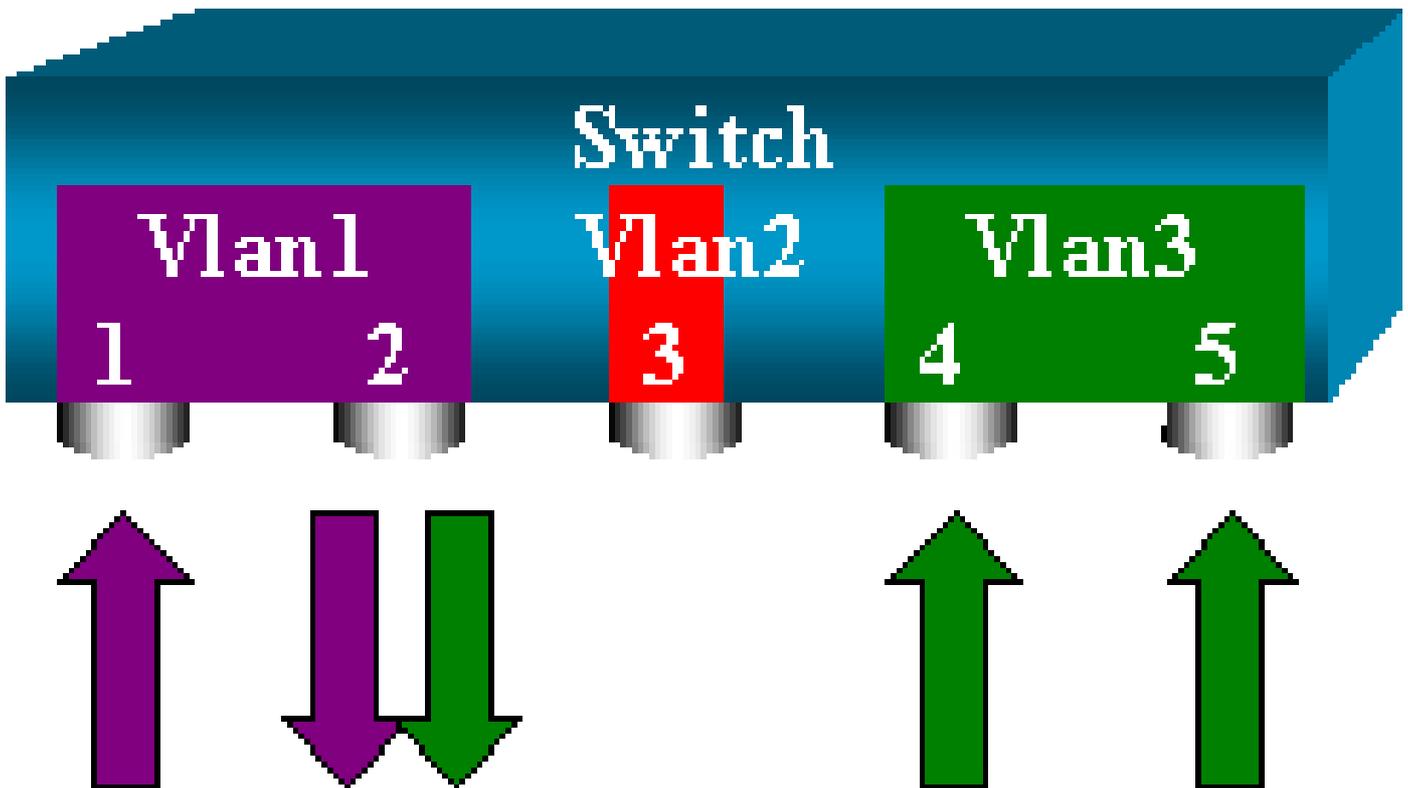
Direction: transmit/receive 필드에 표시됩니다. Catalyst 4500/4000, 5500/5000, 6500/6000 시리즈 스위치에서는 특정 포트의 이그레스(아웃바운드) 트래픽만 또는 인그레스(인바운드) 트래픽만 수집할 수 있습니다.

rx(receive) 또는 tx(transmit) 키워드를 명령의 끝에 추가합니다. 기본값은 both(tx, rx)입니다.

```
<#root>
```

```
set span source_port destination_port [rx | tx | both]
```

예시된 세션에서는 VLAN 1 및 VLAN 3의 모든 수신 트래픽을 캡처하고, 포트 6/2로 가는 트래픽을 미러링합니다.



```
<#root>
```

```
switch (enable)
```

```
set span 1,3 6/2 rx
```

```
2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span session
inactive for destination port 6/2
Destination : Port 6/2
Admin Source : VLAN 1,3
```

```
Oper Source : Port 1/1,6/1,6/4-5,15/1
Direction : receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:09:06 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
```

## 트렁크에 SPAN 구현

트렁크는 여러 VLAN을 전달하는 포트이므로 스위치에서 특별한 경우에 해당합니다. 트렁크가 소스 포트로 선택된 경우, 이 트렁크의 모든 VLAN에 대한 트래픽이 모니터링됩니다.

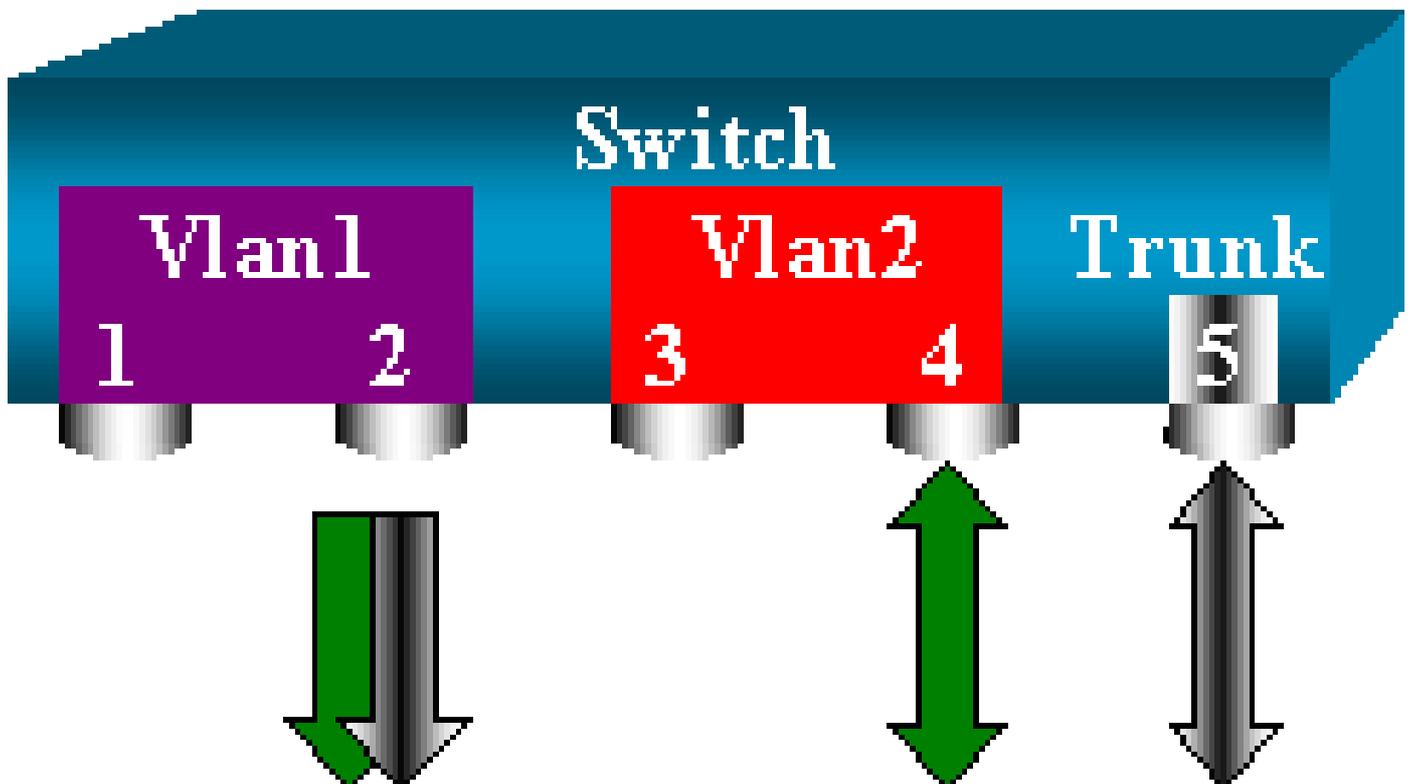
## 트렁크에 속한 VLAN의 하위 집합 모니터링

이 다이어그램에서는 이제 포트 6/5가 모든 VLAN을 전달하는 트렁크입니다. VLAN 2에서 포트 6/4 및 6/5의 트래픽에 SPAN을 사용한다고 가정합니다. 다음 명령을 실행하면 됩니다.

```
<#root>
```

```
switch (enable)
```

```
set span 6/4-5 6/2
```



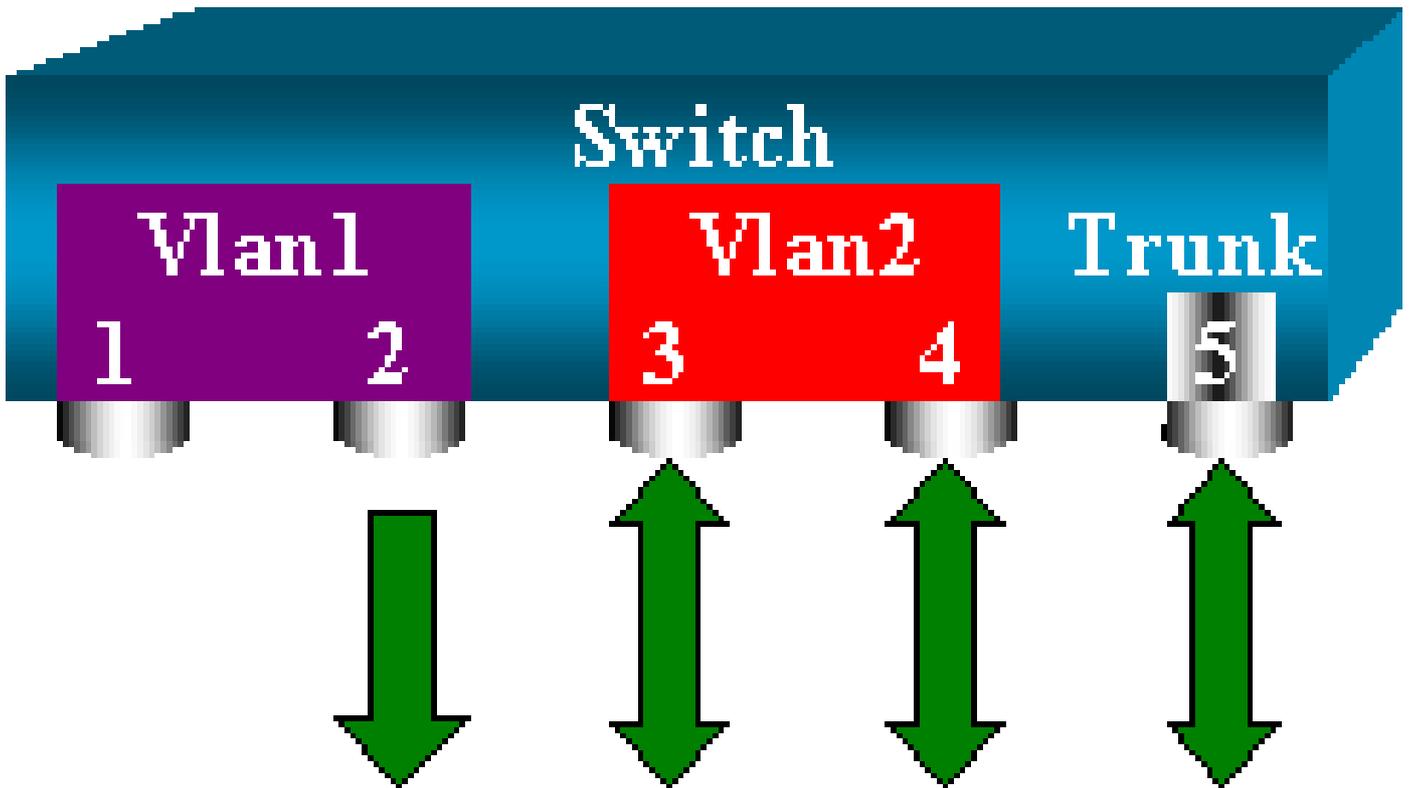
그러면 SPAN 포트에서 수신하는 트래픽에는 사용자가 원하는 트래픽 및 트렁크 6/5가 전달하는 모든 VLAN의 트래픽이 섞여 있습니다.

이러한 경우 목적지 포트에서 어떤 패킷이 VLAN 2의 포트 6/4 아니면 VLAN 1의 포트 6/5에서 오는 것인지를 구별할 방법이 없습니다. VLAN 2 전체에서 SPAN을 사용할 수도 있습니다.

```
<#root>
```

```
switch (enable)
```

```
set span 2 6/2
```



이러한 컨피그레이션에서는 최소한 트렁크에서 VLAN 2에 속하는 트래픽만 모니터링합니다. 그러면 포트 6/3에서 원치 않는 트래픽도 수신한다는 문제가 있습니다.

CatOS에는 트렁크에서 모니터링할 여러 VLAN을 선택할 수 있는 또 다른 키워드가 있습니다.

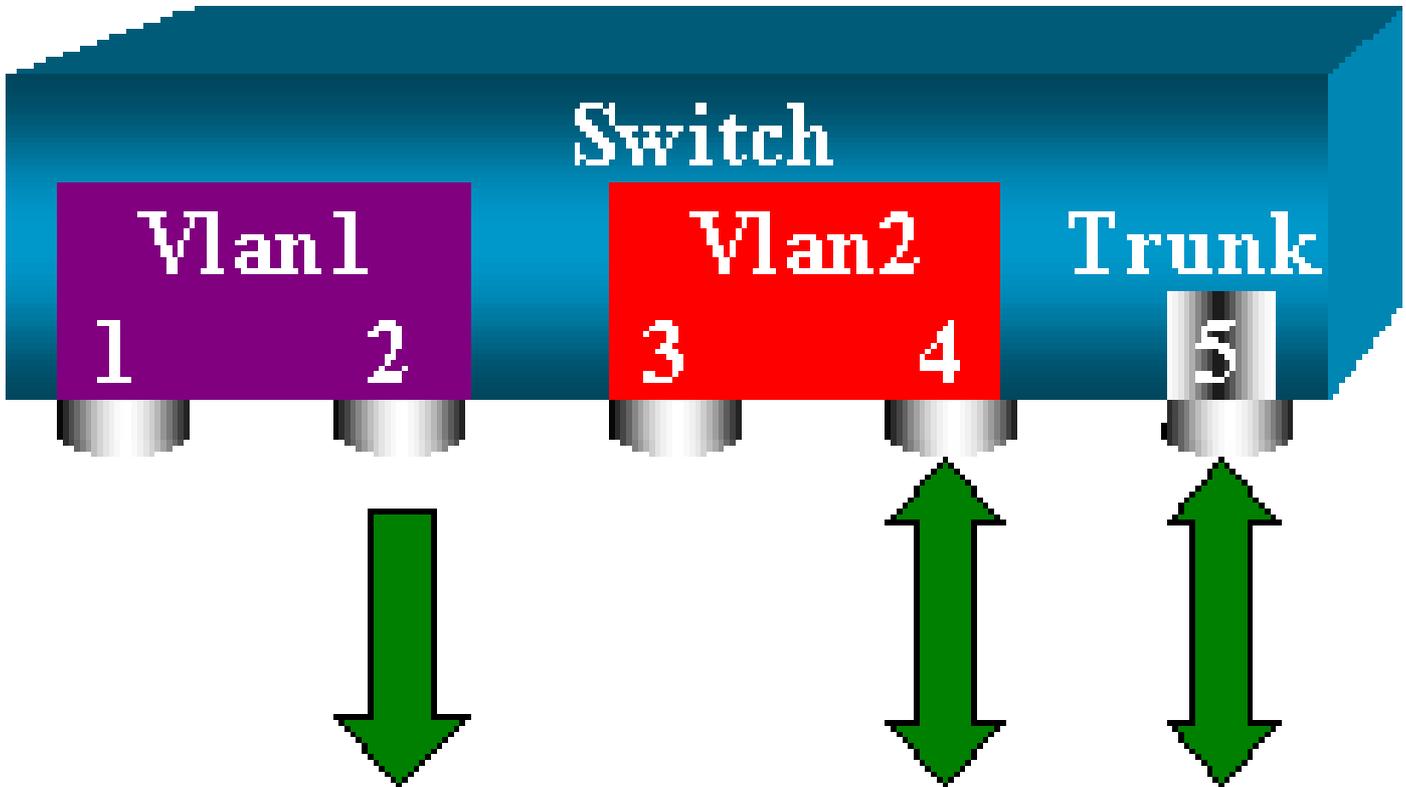
```
<#root>
```

```
switch (enable)
```

```
set span 6/4-5 6/2 filter 2
```

```
2000 Sep 06 02:31:51 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
  for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/4-5
Oper Source : Port 6/4-5
```

Direction : transmit/receive  
Incoming Packets: disabled  
Learning : enabled  
Multicast : enabled  
Filter : 2  
Status : active



이 명령에서는 모니터링되는 모든 트렁크에서 VLAN 2를 선택하기 때문에 목표한 대로 수행됩니다. 이 필터 옵션으로 여러 개의 VLAN을 지정할 수 있습니다.

 참고: 이 필터 옵션은 Catalyst 4500/4000 및 Catalyst 6500/6000 스위치에서만 지원됩니다. Catalyst 5500/5000은 set span 명령에서 사용 가능한 필터 옵션을 지원하지 않습니다.

### 목적지 포트에서의 트렁킹

소스 포트가 서로 다른 여러 VLAN에 속해 있거나 트렁크 포트에서 여러 VLAN에 SPAN을 사용할 때, 목적지 SPAN 포트에서 어떤 VLAN에 속한 패킷을 수신할지를 지정해야 하는 경우도 있습니다.

SPAN을 위해 포트를 구성하기 전에 목적지 포트에서 트렁킹을 활성화하면 그러한 지정이 가능합니다. 그러면 스니퍼로 포워딩되는 모든 패킷에 해당 VLAN ID가 태그로 지정됩니다.

 참고: 스니퍼는 해당 캡슐화를 인식해야 합니다.

<#root>

switch (enable)

```
set span disable 6/2
```

```
This command will disable your span session.  
Do you want to continue (y/n) [n]?y  
Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/4-5  
2000 Sep 06 02:52:22 %SYS-5-SPAN_CFGSTATECHG:local span session  
inactive for destination port 6/2  
switch (enable)
```

```
set trunk 6/2 nonegotiate isl
```

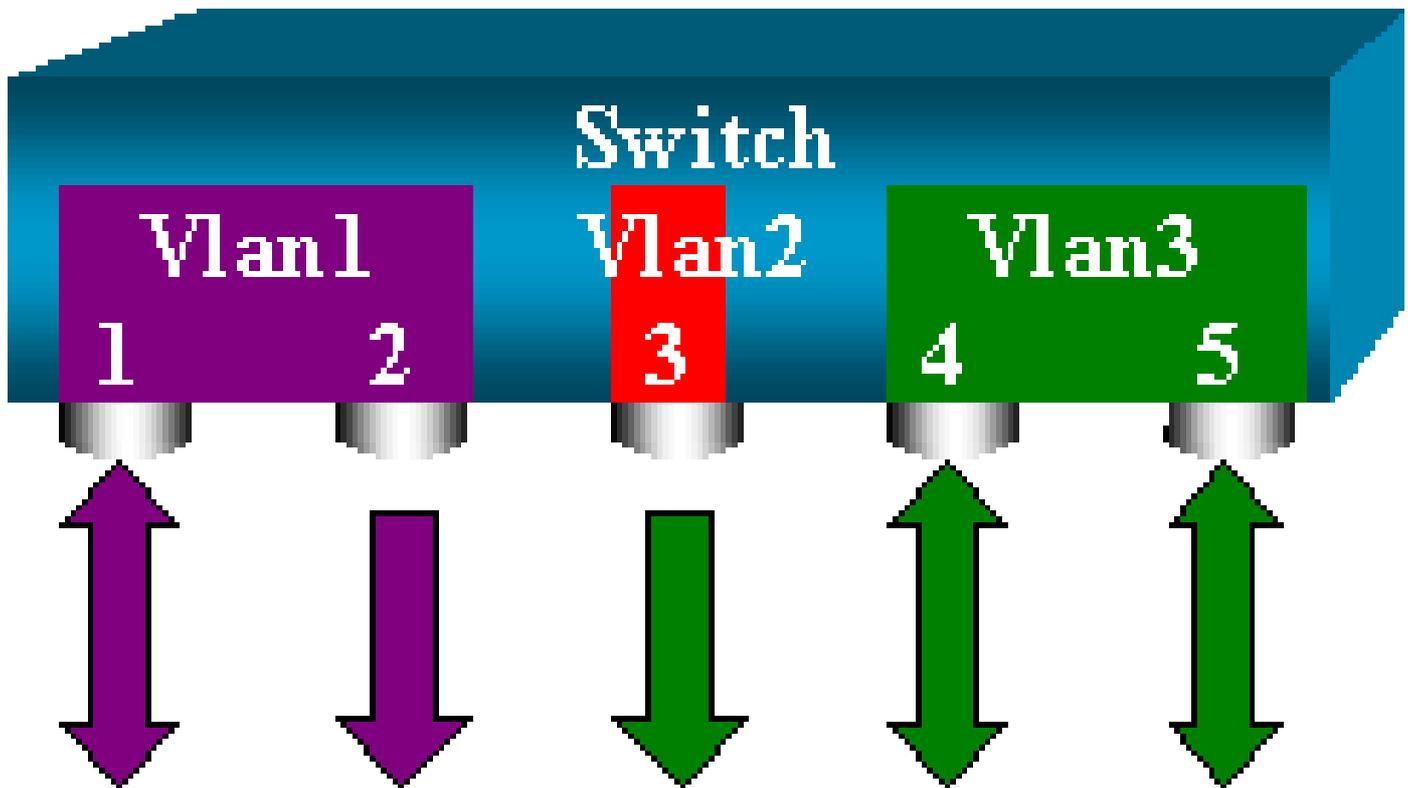
```
Port(s) 6/2 trunk mode set to nonegotiate.  
Port(s) 6/2 trunk type set to isl.  
switch (enable) 2000 Sep 06 02:52:33 %DTP-5-TRUNKPORTON:Port 6/2 has become  
isl trunk  
switch (enable)
```

```
set span 6/4-5 6/2
```

```
Destination : Port 6/2  
Admin Source : Port 6/4-5  
Oper Source : Port 6/4-5  
Direction : transmit/receive  
Incoming Packets: disabled  
Learning : enabled  
Multicast : enabled  
Filter : -  
Status : active  
2000 Sep 06 02:53:23 %SYS-5-SPAN_CFGSTATECHG:local span session active for  
destination port 6/2
```

## 여러 개의 동시 세션 생성

지금까지는 단일 SPAN 세션만 생성했습니다. 새로운 set span 명령을 실행할 때마다 이전 컨피그레이션이 무효화됩니다. 이제 CatOS에서는 여러 개의 세션을 동시에 실행할 수 있습니다. 즉, 서로 다른 목적지 포트를 동시에 가질 수 있습니다. 다른 SPAN 세션을 추가하려면 set span source destination create 명령을 실행합니다. 이 세션에서는 포트 6/1부터 6/2까지를 모니터링합니다. 그와 함께 VLAN 3에서 포트 6/3까지 모니터링합니다.



```
<#root>
```

```
switch (enable)
```

```
set span 6/1 6/2
```

```
2000 Sep 05 08:49:04 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:49:05 %SYS-5-SPAN_CFGSTATECHG:local span
session active for destination port 6/2
switch (enable)
```

```
set span 3 6/3 create
```

```
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
switch (enable) 2000 Sep 05 08:55:38 %SYS-5-SPAN_CFGSTATECHG:local span
```

```
session active for destination port 6/3
```

이제 두 세션이 동시에 있는지 확인하기 위해 show span 명령을 실행합니다.

```
<#root>
```

```
switch (enable)
```

```
show span
```

```
Destination : Port 6/2
Admin Source : Port 6/1
Oper Source : Port 6/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
```

```
-----
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
Total local span sessions: 2
```

추가 세션이 생성됩니다. 일부 세션을 삭제할 방법이 필요합니다. 명령은 다음과 같습니다.

```
<#root>
```

```
set span disable {all | destination_port}
```

목적지 포트는 세션당 하나만 가능하므로, 목적지 포트로 세션을 식별합니다. 생성된 첫 번째 세션, 즉 포트 6/2를 목적지로 사용하는 세션을 삭제합니다.

```
<#root>
```

```
switch (enable)
```

```
set span disable 6/2
```

```
This command will disable your span session.
Do you want to continue (y/n) [n]?y
Disabled Port 6/2 to monitor transmit/receive traffic of Port 6/1
```

```
2000 Sep 05 09:04:33 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/2
```

이제 세션 하나만 남았음을 확인할 수 있습니다.

```
<#root>
```

```
switch (enable)
```

```
show span
```

```
Destination : Port 6/3
Admin Source : VLAN 3
Oper Source : Port 6/4-5,15/1
Direction : transmit/receive
Incoming Packets: disabled
Learning : enabled
Multicast : enabled
Filter : -
Status : active
```

```
Total local span sessions: 1
```

모든 동시 세션을 한꺼번에 비활성화하려면 이 명령을 실행합니다.

```
<#root>
```

```
switch (enable)
```

```
set span disable all
```

```
This command will disable all span session(s).
```

```
Do you want to continue (y/n) [n]?y
```

```
Disabled all local span sessions
```

```
2000 Sep 05 09:07:07 %SYS-5-SPAN_CFGSTATECHG:local span session inactive
for destination port 6/3
```

```
switch (enable)
```

```
show span
```

```
No span session configured
```

기타 SPAN 옵션

set span 명령의 구문은 다음과 같습니다.

```
<#root>
```

switch (enable)

set span

Usage: set span disable [dest\_mod/dest\_port|all]  
set span <src\_mod/src\_ports...|src\_vlans...|sc0>  
<dest\_mod/dest\_port> [rx|tx|both]

[inpmts

]

[learning

]

[multicast

]

[filter <vlans...>  
[create]

이 섹션에서는 이 문서에서 다루는 옵션을 간략하게 설명합니다.

- sc0 - 관리 인터페이스 sc0에 대한 트래픽을 모니터링해야 할 경우 SPAN 컨피그레이션에서 sc0 키워드를 지정합니다. 이 기능은 Catalyst 5500/5000 스위치 및 6500/6000 스위치, 코드 버전 CatOS 5.1 이상에서 사용할 수 있습니다.
- inpkts enable/disable — 이 옵션은 매우 중요합니다. 이 문서의 설명대로, SPAN 목적지로 구성하는 포트는 계속 원래의 VLAN에 속해 있습니다. 그러면 일반 액세스 포트와 마찬가지로 목적지 포트에서 수신한 패킷이 VLAN에 들어갑니다. 이러한 동작이 필요할 때가 있습니다. PC를 스니퍼로 사용할 경우 해당 PC가 VLAN에 완전히 연결되어야 합니다. 그러나 네트워크에서 루프를 생성하는 다른 네트워킹 장비에 목적지 포트를 연결할 경우, 이 연결이 위험해질 수 있습니다. 목적지 SPAN 포트는 STP를 실행하지 않으므로, 결국 위험한 브리징 루프 상황이 전개될 수 있습니다. 이 상황이 발생할 수 있는 방법을 이해하려면 이 문서의 [SPAN 세션](#)에서 브리징 루프를 만드는 이유 섹션을 참조하십시오. 이 옵션의 기본 설정은 disable입니다. 즉, 목적지 SPAN 포트는 수신하는 패킷을 폐기합니다. 이러한 폐기를 통해 포트가 브리징 루프에 빠지지 않게 할 수 있습니다. 이 옵션은 CatOS 4.2에 있습니다.
- learning enable/disable — 이 옵션으로 목적지 포트에서 학습을 비활성화할 수 있습니다. 기본적으로 학습은 활성화되어 있으며, 목적지 포트는 포트에서 수신하는 패킷으로부터 MAC 주소를 학습합니다. 이 기능은 Catalyst 4500/4000 및 5500/5000의 CatOS 5.2에서 그리고 Catalyst 6500/6000의 CatOS 5.3에서 볼 수 있습니다.
- multicast enable/disable — 이름에서 알 수 있듯이 이 옵션을 사용하여 멀티캐스트 패킷 모니터링을 활성화하거나 비활성화할 수 있습니다. 기본값은 enable입니다. 이 기능은 Catalyst 5500/5000 및 6500/6000, CatOS 5.1 이상에서 사용할 수 있습니다.
- spanning port 15/1(스패닝 포트 15/1) - Catalyst 6500/6000에서 포트 15/1(또는 16/1)을 SPAN 소스로 사용할 수 있습니다. 포트에서 MSFC(Multilayer Switch Feature Card)에 포워딩되는 트래픽을 모니터링할 수 있습니다. 포트에서 소프트웨어 라우팅된 트래픽 또는 MSFC로 향하는 트래픽을 캡처합니다.

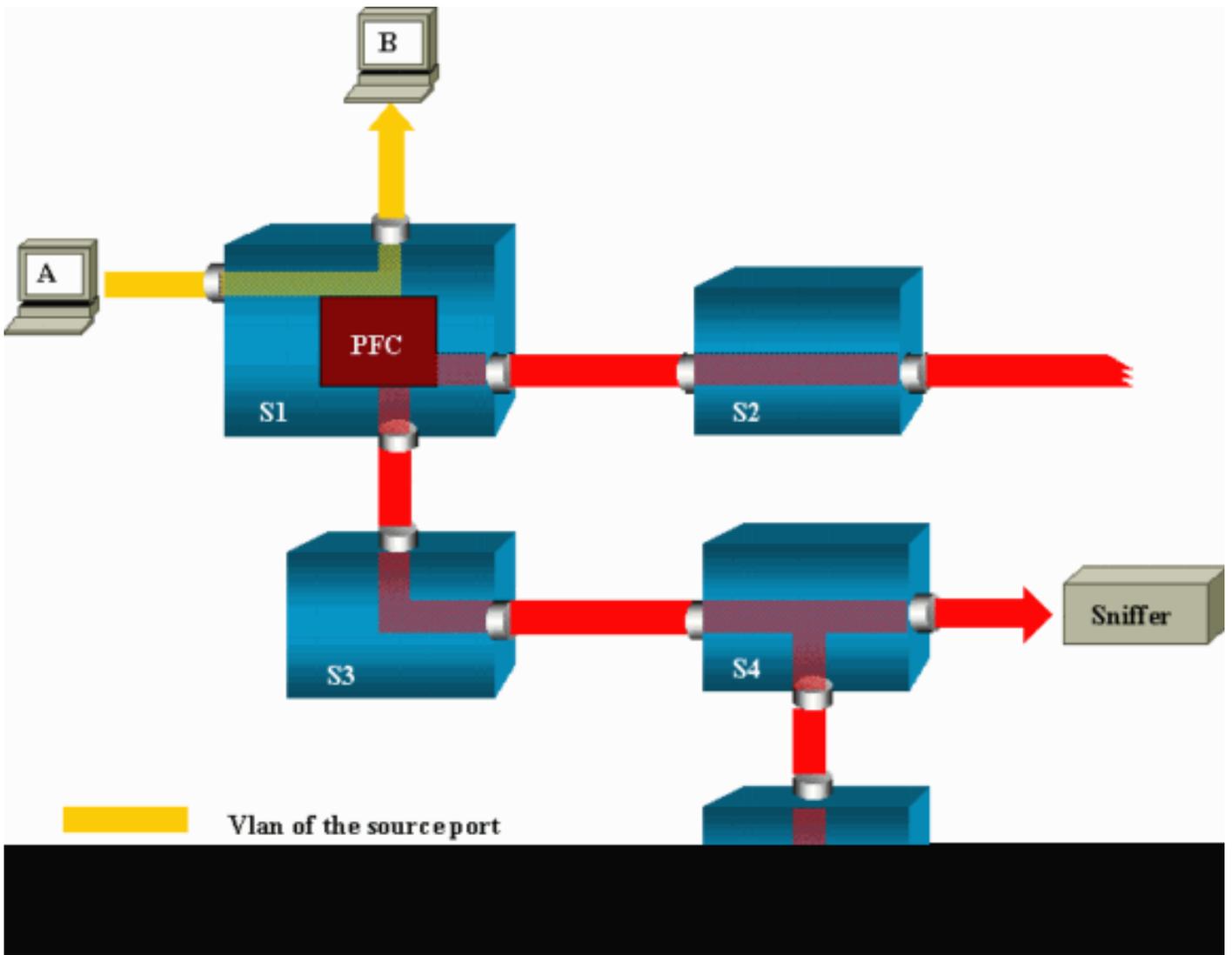
## 원격 SPAN

### RSPAN 개요

RSPAN을 사용하면 스위치 네트워크 전반에 분산된 소스 포트를 모니터링할 수 있습니다. SPAN으로 하나의 스위치에서 로컬 모니터링하는 데 머무르지 않습니다. 이 기능은 Catalyst 6500/6000 시리즈 스위치의 CatOS 5.3에서 볼 수 있으며, Catalyst 4500/4000 시리즈 스위치에서는 CatOS 6.3 이상에 추가되었습니다.

이 기능은 정확히 일반 SPAN 세션처럼 작동합니다. SPAN에서 모니터링하는 트래픽은 목적지 포트에 곧바로 복사되는 게 아니라 특별한 RSPAN VLAN에 풀러딩됩니다. 따라서 목적지 포트는 이 RSPAN VLAN의 어디에나 위치할 수 있습니다. 여러 개의 목적지 포트를 둘 수도 있습니다.

이 다이어그램에서는 RSPAN 세션의 구조를 보여줍니다.



이 예에서는 호스트 A가 보내는 트래픽을 모니터링하도록 RSPAN을 설정합니다. A가 B를 목적지로 하는 프레임을 생성하면, Catalyst 6500/6000 PFC(Policy Feature Card)의 ASIC(Application-specific Integrated Circuit)가 사전 정의된 RSPAN VLAN으로 패킷을 복사합니다. 여기에서 패킷은 RSPAN VLAN에 속하는 나머지 모든 포트에 플러딩됩니다. 여기에 그려진 모든 interswitch 링크는 트렁크이며, 이는 RSPAN의 요구 사항입니다. 액세스 포트는 스니퍼가 연결된 목적지 포트뿐입니다. 여기서는 S4, S5입니다.

이 설계에서는 몇 가지 유의할 점이 있습니다.

- S1을 소스 스위치라고 합니다. 패킷은 RSPAN 소스로 구성된 스위치의 RSPAN VLAN에만 들어갑니다. 현재는 스위치가 단일 RSPAN 세션의 소스만 될 수 있습니다. 즉, 소스 스위치는 한 번에 하나의 RSPAN VLAN에만 공급할 수 있습니다.
- S2 및 S3는 중간 스위치입니다. RSPAN 소스가 아니며 목적지 포트가 없습니다. 스위치는 임의 개수의 RSPAN 세션에서 중간 스위치가 될 수 있습니다.
- S4 및 S5는 목적지 스위치입니다. 그 포트 중 일부는 RSPAN 세션에 대한 목적지로 구성됩니다. 현재 Catalyst 6500/6000에서는 단일 세션에 대해 또는 서로 다른 여러 세션에 대해 최대 24개의 RSPAN 목적지 포트를 가질 수 있습니다. 또한 S4는 목적지 스위치이자 중간 스위치라는 것을 알 수 있습니다.

- RSPAN 패킷이 RSPAN VLAN에 플러딩되는 것을 확인할 수 있습니다. S2와 같이 목적지 포트에 대한 경로에 있지 않은 스위치도 RSPAN VLAN에 대한 트래픽을 수신합니다. 이와 같은 S1-S2 링크에서 이 VLAN을 정리하는 것이 유용할 수 있습니다.
- 이러한 플러딩을 위해 RSPAN VLAN에서 학습이 비활성화되어 있습니다.
- 루프를 방지하기 위해 STP는 RSPAN VLAN에서 유지 관리되고 있습니다. 따라서 RSPAN은 BPDU(Bridge Protocol Data Unit)를 모니터링할 수 없습니다.

### RSPAN 컨피그레이션 예

이 섹션에서는 매우 단순한 RSPAN 설계에서 이 다양한 요소를 설정하는 것을 보여줍니다. S1과 S2는 두 Catalyst 6500/6000 스위치입니다. S2에서 일부 S1 포트 또는 VLAN을 모니터링하려면 전용 RSPAN VLAN을 설정해야 합니다. 나머지 명령은 일반적인 SPAN 세션에서 사용하는 명령과 유사한 구문을 사용합니다.



### 두 스위치 S1과 S2 간 ISL 트렁크 설정

시작하려면 각 스위치에 같은 VTP(VLAN Trunk Protocol) 도메인을 두고 한쪽을 트렁킹 선호로 구성합니다. VTP 협상에서 나머지를 처리합니다. S1에서 다음 명령을 실행합니다.

```
<#root>
S1> (enable)
set vtp domain cisco

VTP domain cisco modified
```

S2에서 다음 명령을 실행합니다.

```
<#root>
```

S2> (enable)

```
set vtp domain cisco
```

VTP domain cisco modified

S2> (enable)

```
set trunk 5/1 desirable
```

Port(s) 5/1 trunk mode set to desirable.

S2> (enable) 2000 Sep 12 04:32:44 %PAGP-5-PORTFROMSTP:Port 5/1 left bridge port 5/1

2000 Sep 12 04:32:47 %DTP-5-TRUNKPORTON:Port 5/1 has become isl trunk

## RSPAN VLAN 생성

RSPAN 세션에는 별도의 RSPAN VLAN이 필요합니다. 이 VLAN을 생성해야 합니다. 기존 VLAN을 RSPAN VLAN으로 변환할 수 없습니다. 이 예에서는 VLAN 100을 사용합니다.

<#root>

S2> (enable)

```
set vlan 100 rspan
```

Vlan 100 configuration successful

VTP 서버로 구성된 하나의 스위치에서 이 명령을 실행합니다. RSPAN VLAN 100에 대한 정보가 VTP 도메인 전체에 자동으로 전파됩니다.

S2의 포트 5/2 컨피그레이션(RSPAN 목적지 포트로 구성)

<#root>

S2> (enable)

```
set rspan destination 5/2 100
```

Rspan Type : Destination

Destination : Port 5/2

Rspan Vlan : 100

Admin Source : -

Oper Source : -

Direction : -

Incoming Packets: disabled

Learning : enabled

Multicast : -

Filter : -

Status : active

2000 Sep 12 04:34:47 %SYS-5-SPAN\_CFGSTATECHG:remote span destination session

active for destination port 5/2

## S1의 RSPAN 소스 포트 컨피그레이션

이 예에서는 포트 6/2를 통해 S1으로 들어오는 수신 트래픽이 모니터링됩니다. 다음 명령을 실행합니다.

```
<#root>
```

```
S1> (enable)
```

```
set rspan source 6/2 100 rx
```

```
Rspan Type : Source
Destination : -
Rspan Vlan : 100
Admin Source : Port 6/2
Oper Source : Port 6/2
Direction : receive
Incoming Packets: -
Learning : -
Multicast : enabled
Filter : -
Status : active
S1> (enable) 2000 Sep 12 05:40:37 %SYS-5-SPAN_CFGSTATECHG:remote span
source session active for remote span vlan 100
```

포트 6/2의 모든 수신 패킷은 이제 RSPAN VLAN 100에 플러딩되고, 트렁크를 통해 S1에 구성된 목적지 포트에 도달합니다.

## 구성 확인

show rspan 명령은 스위치의 현재 RSPAN 컨피그레이션의 요약を提供합니다. 여기서도 한 번에 하나의 소스 RSPAN 세션만 있을 수 있습니다.

```
<#root>
```

```
S1> (enable)
```

```
show rspan
```

```
Rspan Type : Source
Destination : -
Rspan Vlan : 100
Admin Source : Port 6/2
Oper Source : Port 6/2
Direction : receive
Incoming Packets: -
Learning : -
Multicast : enabled
```

Filter : -  
 Status : active  
 Total remote span sessions: 1

### set rspan 명령으로 가능한 기타 컨피그레이션

RSPAN을 사용하여 소스와 목적지를 구성하기 위해 여러 명령줄을 사용합니다. 이 차이점을 제외하면, SPAN과 RSPAN은 사실상 동일하게 작동합니다. 여러 목적지 SPAN 포트를 사용하려는 경우, 단일 스위치에서 RSPAN을 로컬로 사용할 수도 있습니다.

### 기능 요약 및 제한

이 표에서는 도입된 다양한 기능을 요약하고, 지정된 플랫폼에서 기능을 실행하는 데 필요한 최소 CatOS 릴리스를 알려줍니다.

기능	Catalyst 4500/4000	Catalyst 5500/5000	Catalyst 6500/6000
inpkts enable/disable 옵션	4.4	4.2	5.1
서로 다른 VLAN의 다중 세션, 포트	5.1	5.1	5.1
sc0 옵션	—	5.1	5.1
multicast enable/disable 옵션	—	5.1	5.1
learning enable/disable 옵션	5.2	5.2	5.3
RSPAN	6.3	—	5.3

이 표에서는 가능한 SPAN 세션 수에 대해 현재 적용되는 제한을 간략하게 요약합니다.

기능	Catalyst 4500/4000 스위치 제품군	Catalyst 5500/5000 스위치 제품군	Catalyst 6500/6000 스위치 제품군
Rx 또는 두 SPAN 세션	5	1	2
Tx SPAN 세션	5	4	4
MPA(Mini Protocol Analyzer) 세션	지원되지 않음	지원되지 않음	1
Rx, Tx 또는 두 RSPAN 소스 세션	5	지원되지 않음	1 Supervisor Engine 720은 2개의 RSPAN 소스 세션을 지원합니다.
RSPAN 목적지	5	지원되지 않음	24
총 세션	5	5	30

다른 제한 사항 및 컨피그레이션 지침은 다음 문서를 참조하십시오.

- [SPAN & RSPAN 구성\(Catalyst 4500/4000\)](#)
- [SPAN & RSPAN 구성\(Catalyst 6500/6000\)](#)

# Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750, 3750-E Series Switch의 SPAN

Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750, 3750-E 시리즈 스위치의 SPAN 기능 컨피그레이션에 대한 지침입니다.

- Catalyst 2950 스위치는 한 번에 하나의 SPAN 세션만 활성화할 수 있으며, 소스 포트만 모니터링할 수 있습니다. 이 스위치에서는 VLAN을 모니터링할 수 없습니다.
- Catalyst 2950 및 3550 스위치는 Cisco IOS Software Release 12.1(13)EA1 이상에서 목적지 SPAN 포트의 트래픽을 포워딩할 수 있습니다.
- Catalyst 3550, 3560, 3750 스위치는 한 번에 최대 2개의 SPAN 세션을 지원할 수 있고, 소스 포트뿐만 아니라 VLAN도 모니터링할 수 있습니다.
- Catalyst 2970, 3560, 3750 스위치에서는 RSPAN 세션을 설정할 경우 리플렉터 포트 컨피그레이션이 필요하지 않습니다.
- Catalyst 3750 스위치의 경우 세션 컨피그레이션에서 스위치 스택 멤버에 있는 소스 및 목적지 포트를 사용할 수 있습니다.
- SPAN 세션당 하나의 목적지 포트만 허용되며, 하나의 포트가 여러 SPAN 세션의 목적지 포트가 될 수 없습니다. 따라서 두 SPAN 세션에서 같은 목적지 포트를 사용할 수 없습니다.

Catalyst 2950 및 Catalyst 3550은 SPAN 기능 컨피그레이션 명령이 비슷합니다. 그러나 Catalyst 2950은 VLAN을 모니터링할 수 없습니다. 이 예제와 같이 SPAN을 구성할 수 있습니다.

```
<#root>
```

```
C2950#
```

```
configure terminal
```

```
C2950(config)#
```

```
C2950(config)#
```

```
monitor session 1 source interface fastethernet 0/2
```

```
!--- This configures interface Fast Ethernet 0/2 as source port.
```

```
C2950(config)#
```

```
monitor session 1 destination interface fastethernet 0/3
```

```
!--- This configures interface Fast Ethernet 0/3 as destination port.
```

```
C2950(config)#
```

```
C2950#
```

```
show monitor session 1
```

```
Session 1-----  
Source Ports:  
  RX Only:      None  
  TX Only:      None  
  Both:         Fa0/2  
Destination Ports: Fa0/3  
C2950#
```

어떤 포트를 동일한 VLAN 트래픽의 로컬 SPAN 및 RSPAN의 목적지로 구성할 수도 있습니다. 직접 연결된 두 스위치에 상주하는 특정 VLAN의 트래픽을 모니터링하기 위해 목적지 포트가 있는 스위치에서 이 명령을 구성합니다. 이 예에서는 두 스위치에 분산된 VLAN 5의 트래픽을 모니터링합니다.

```
<#root>
```

```
c3750(config)#  
monitor session 1 source vlan < Remote RSPAN VLAN ID >  
  
c3750(config)#  
monitor session 1 source vlan 5  
  
c3750(config)#  
monitor session 1 destination interface fastethernet 0/3
```

*!--- This configures interface FastEthernet 0/3 as a destination port.*

원격 스위치에서 다음 컨피그레이션을 사용합니다.

```
<#root>
```

```
c3750_remote(config)#  
monitor session 1 source vlan 5
```

*!--- Specifies VLAN 5 as the VLAN to be monitored.*

```
c3750_remote(config)#  
monitor session 1 destination remote vlan
```

이전 예에서는 두 스위치에 상주하는 동일한 VLAN의 트래픽을 모니터링하기 위해 어떤 포트를 로컬 SPAN 및 RSPAN 모두의 목적지 포트로 구성했습니다.

 참고: 2900XL 및 3500XL 시리즈 스위치와 달리 Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560-E, 3750 및 3750-E 시리즈 스위치는 소스 포트 트래픽에서 Rx 방향으로만 (Rx SPAN 또는 SPAN), Tx 방향으로만(Tx SPAN 또는 SPAN) 또는 둘 다에서 SPAN을 지원합니다.

 참고: 컨피그레이션의 명령은 Cisco IOS Software 릴리스 12.0(5.2)WC(1) 또는 Cisco IOS Software 릴리스 12.1(6)EA2 이전 버전의 Catalyst 2950 소프트웨어에서 지원되지 않습니다. Cisco IOS Software Release 12.1(6)EA2 이전 버전의 소프트웨어가 있는 Catalyst 2950에서 SPAN을 구성하려면 [스위치 관리의 스위치 포트 분석기 활성화 섹션을 참조하십시오.](#)

 참고: Cisco IOS Software Release 12.1.(9)EA1d 이하 릴리스를 사용하는 Catalyst 2950 스위치는 SPAN을 지원합니다. 그러나 (스니핑 디바이스 또는 PC에 연결된) SPAN 목적지 포트에서 나타나는 모든 패킷은 SPAN 소스 포트(모니터링되는 포트)가 802.1Q 트렁크 포트가 아니라도 IEEE 802.1Q 태그를 갖습니다. 스니핑 디바이스 또는 PC의 NIC(network interface card)에서 802.1Q 태그가 지정된 패킷을 인식하지 못하면, 이 디바이스가 패킷을 삭제하거나 패킷 디코딩에 어려움을 겪을 수 있습니다. 802.1Q 태그가 지정된 프레임을 인식하는 기능은 SPAN 소스 포트가 트렁크 포트일 때만 중요합니다. Cisco IOS Software Release 12.1(11)EA1 이상에서는 SPAN 목적지 포트에서 패킷 태그 지정을 활성화하고 비활성화할 수 있습니다. 목적지 포트에서 패킷의 캡슐화를 활성화하려면 [monitor session session\\_number destination interface interface\\_id encapsulation dot1q](#) 명령을 실행합니다. encapsulation 키워드를 지정하지 않으면 패킷은 태그가 지정되지 않은 채로 전송됩니다. 이는 Cisco IOS Software Release 12.1(11)EA1 이상에서 기본 설정입니다.

기능	Catalyst 2950/3550
Ingress (inpkts) enable/disable 옵션	Cisco IOS Software Release 12.1(12c)EA1
RSPAN	Cisco IOS Software Release 12.1(12c)EA1

기능	Catalyst 2940 <sup>1</sup> , 2950, 2955, 2960, 2970, 3550, 3560, 3750
Rx 또는 두 SPAN 세션	2
Tx SPAN 세션	2
Rx, Tx 또는 두 RSPAN 소스 세션	2
RSPAN 목적지	2
총 세션	2

<sup>1</sup> Catalyst 2940 스위치는 로컬 SPAN만 지원합니다. RSPAN은 이 플랫폼에서는 지원되지 않습니다.

SPAN 및 RSPAN 컨피그레이션에 대한 자세한 내용은 다음 컨피그레이션 가이드를 참조하십시오.

- [SPAN 구성\(Catalyst 2940\)](#)

- [SPAN 및 RSPAN 구성\(Catalyst 2950, 2955\)](#)
- [SPAN 및 RSPAN 구성\(Catalyst 2960\)](#)
- [SPAN 및 RSPAN 구성\(Catalyst 3550\)](#)
- [SPAN 및 RSPAN 구성\(Catalyst 3560\)](#)
- [SPAN 및 RSPAN 구성\(Catalyst 3560-E, 3750-E\)](#)
- [SPAN 및 RSPAN 구성\(Catalyst 3750\)](#)

## Cisco IOS System Software를 실행하는 Catalyst 4500/4000 및 Catalyst 6500/6000 Series Switch의 SPAN

SPAN 기능은 Cisco IOS system software를 실행하는 Catalyst 4500/4000 및 Catalyst 6500/6000 시리즈 스위치에서 지원됩니다. 두 스위치 플랫폼 모두 [Catalyst 2940, 2950, 2955, 2960, 2970, 3550, 3560, 3560E, 3750, 3750E 시리즈 스위치의 SPAN 섹션에서 다루는 컨피그레이션과 동일한 CLI\(Command-Line Interface\) 및 비슷한 컨피그레이션을 사용합니다.](#) 관련 컨피그레이션에 대해서는 다음 문서를 참조하십시오.

- [SPAN & RSPAN 구성\(Catalyst 6500/6000\)](#)
- [SPAN & RSPAN 구성\(Catalyst 4500/4000\)](#)

### 컨피그레이션 예시

이 예제와 같이 SPAN을 구성할 수 있습니다.

```
<#root>
```

```
4507R#
```

```
configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
4507R(config)#
```

```
monitor session 1 source interface fastethernet 4/2
```

```
!--- This configures interface Fast Ethernet 4/2 as source port.
```

```
4507R(config)#
```

```
monitor session 1 destination interface fastethernet 4/3
```

```
!--- The configures interface Fast Ethernet 0/3 as destination port.
```

4507R#

show monitor session 1

Session 1-----

Type : Local Session

Source Ports :

Both : Fa4/2

Destination Ports : Fa4/3

4507R#

### 기능 요약 및 제한

이 표에서는 도입된 다양한 기능을 요약하고, 지정된 플랫폼에서 기능을 실행하는 데 필요한 최소 Cisco IOS Software 릴리스를 알려줍니다.

기능	Catalyst 4500/4000(Cisco IOS Software)	Catalyst 6500/6000(Cisco IOS Software)
Ingress (inpkts) enable/disable 옵션	Cisco IOS Software Release 12.1(19)EW	현재 지원되지 않음 <sup>1</sup>
RSPAN	Cisco IOS Software Release 12.1(20)EW	Cisco IOS Software 릴리스 12.1(13)E

<sup>1</sup> 이 기능은 현재 사용할 수 없습니다. 일반적으로 이러한 기능의 사용 가능 여부는 릴리스될 때까지 게시되지 않습니다.

 **참고:** Cisco Catalyst 6500/6000 Series 스위치의 SPAN 기능은 PIM 프로토콜과 관련하여 제한이 있습니다. 스위치가 PIM 및 SPAN 모두에 대해 구성되면, SPAN 목적지 포트에 연결된 네트워크 분석기/스니퍼에서 SPAN 소스 포트/VLAN 트래픽에 속하지 않은 PIM 패킷을 볼 수 있습니다. 이 문제는 스위치의 패킷 포워딩 아키텍처의 제약 때문에 발생합니다. SPAN 목적지 포트는 패킷의 소스를 확인하는 어떤 검사도 하지 않습니다. 이 문제는 Cisco 버그 ID [CSCdy57506](#)에서도 다루고 있습니다([등록된 고객만 이용 가능](#)).

이 표에서는 가능한 SPAN 및 RSPAN 세션 수에 대해 현재 적용되는 제한을 간략하게 요약합니다.

기능	Catalyst 4500/4000(Cisco IOS Software)
Rx 또는 두 SPAN 세션	2
Tx SPAN 세션	4
Rx, Tx 또는 두 RSPAN 소스 세션	2(Rx, Tx 또는 both), Tx에 한해 최대 4
RSPAN 목적지	2
총 세션	6

Cisco IOS software를 실행하는 Catalyst 6500/6000 스위치에 대해서는 [로컬 SPAN, RSPAN](#).

## [ERSPAN 세션 제한을 참조하십시오.](#)

Catalyst 6500 시리즈에서는 이그레스 SPAN이 Supervisor에서 수행된다는 점에 유의해야 합니다. 그러면 이그레스 SPAN 대상인 모든 트래픽이 패브릭 전반에서 Supervisor와 SPAN 목적지 포트에 차례로 전송될 수 있는데, 그러면 상당한 시스템 리소스를 사용하고 사용자 트래픽에 영향을 미칠 수도 있습니다. 인그레스 SPAN은 인그레스 모듈에서 수행되므로 SPAN 성능은 참여하는 모든 복제 엔진의 합계가 됩니다. SPAN 기능의 성능은 패킷 크기 및 복제 엔진에서 사용 가능한 ASIC의 유형에 따라 달라집니다.

Cisco IOS Software Release 12.2(33)SXH 이전의 릴리스에서는 포트-채널 인터페이스, EtherChannel이 SPAN 목적지일 수 없습니다. Cisco IOS Software Release 12.2(33)SXH 이상에서는 EtherChannel이 SPAN 목적지일 수 있습니다. 대상 EtherChannel은 PAgP(Port Aggregation Control Protocol) 또는 LACP(Link Aggregation Control Protocol) EtherChannel 프로토콜을 지원하지 않습니다. 모든 EtherChannel 프로토콜 지원을 비활성화한 상태에서 on 모드만 지원됩니다.

다른 제한 사항 및 컨피그레이션 지침은 다음 문서를 참조하십시오.

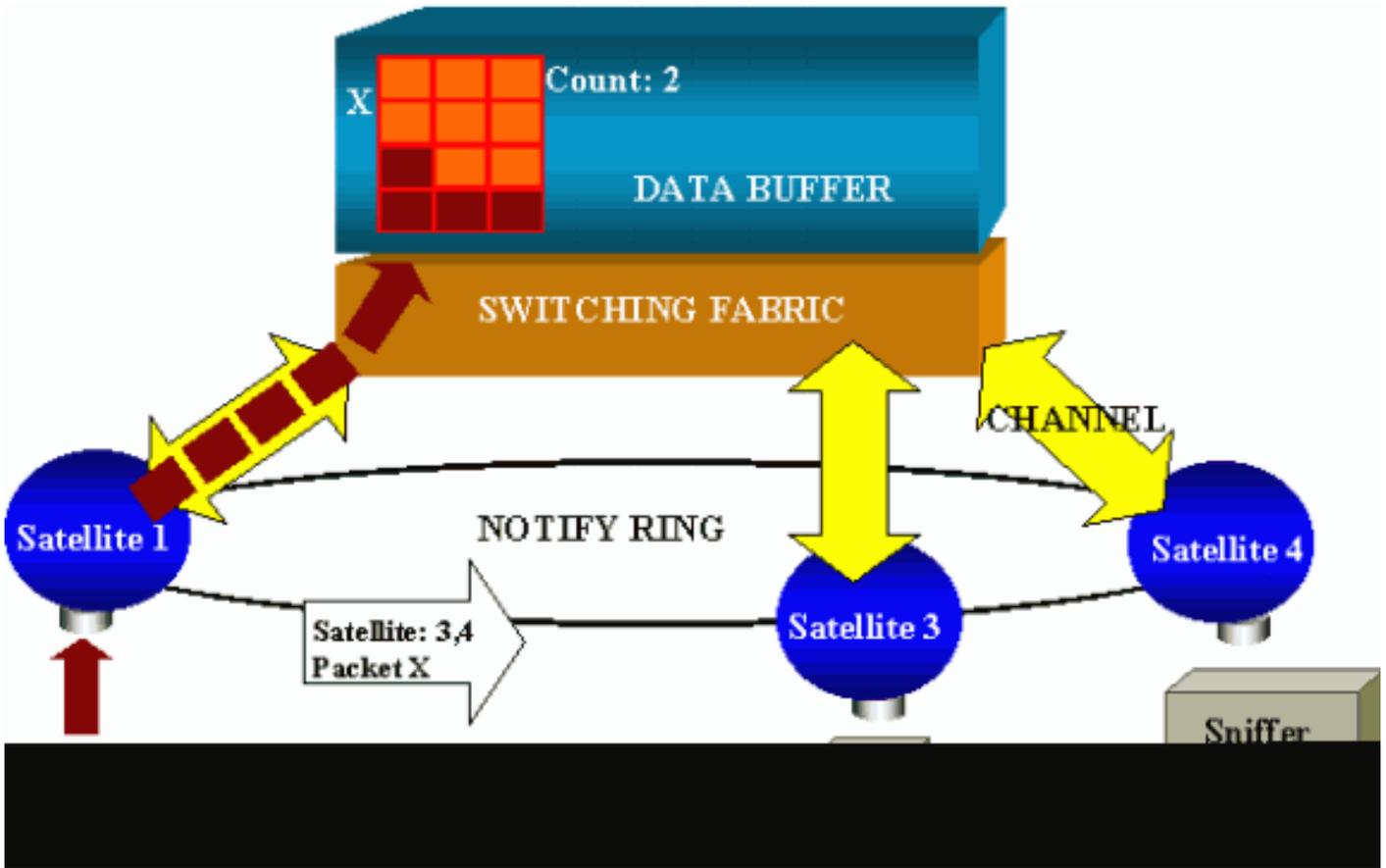
- [SPAN & RSPAN 구성\(Catalyst 4500/4000\)](#)
- [로컬 SPAN, RSPAN\(Remote SPAN\), 캡슐화된 RSPAN 구성\(Catalyst 6500/6000\)](#)

## SPAN이 각종 Catalyst 플랫폼의 성능에 미치는 영향

### Catalyst 2900XL/3500XL 시리즈

#### 아키텍처 개요

2900XL/3500XL 스위치 내부 아키텍처를 극히 단순화한 모습입니다.



스위치의 포트가 연결된 위성은 방사형 채널을 통해 스위칭 패브릭과 통신합니다. 맨 위에서 모든 위성은 트래픽 시그널링 전용 고속 알림 링을 통해 상호 연결됩니다.

어떤 위성이 포트로부터 패킷을 수신하면, 이 패킷이 여러 셀로 분할된 다음 하나 이상의 채널을 통해 스위칭 패브릭으로 전송됩니다. 그러면 패킷이 공유 메모리에 저장됩니다. 각 위성은 목적지 포트에 관해 알고 있습니다. 이 섹션의 다이어그램에서 위성 1은 패킷 X가 위성 3 및 4에 의해 수신되어야 함을 알고 있습니다. 위성 1은 알림 링을 통해 다른 위성으로 메시지를 전송합니다. 그런 다음 위성 3과 위성 4는 방사형 채널을 통해 공유 메모리로부터 셀을 받기 시작하며, 결국 패킷을 포워딩할 수 있게 됩니다. 소스 위성은 목적지를 알고 있으므로, 나머지 위성에서 이 패킷을 다운로드하는 횟수를 지정하는 인덱스도 보냅니다. 위성이 공유 메모리로부터 패킷을 받을 때마다 이 인덱스가 감소합니다. 인덱스가 0에 도달하면 공유 메모리를 해제할 수 있습니다.

### 성능에 미치는 영향

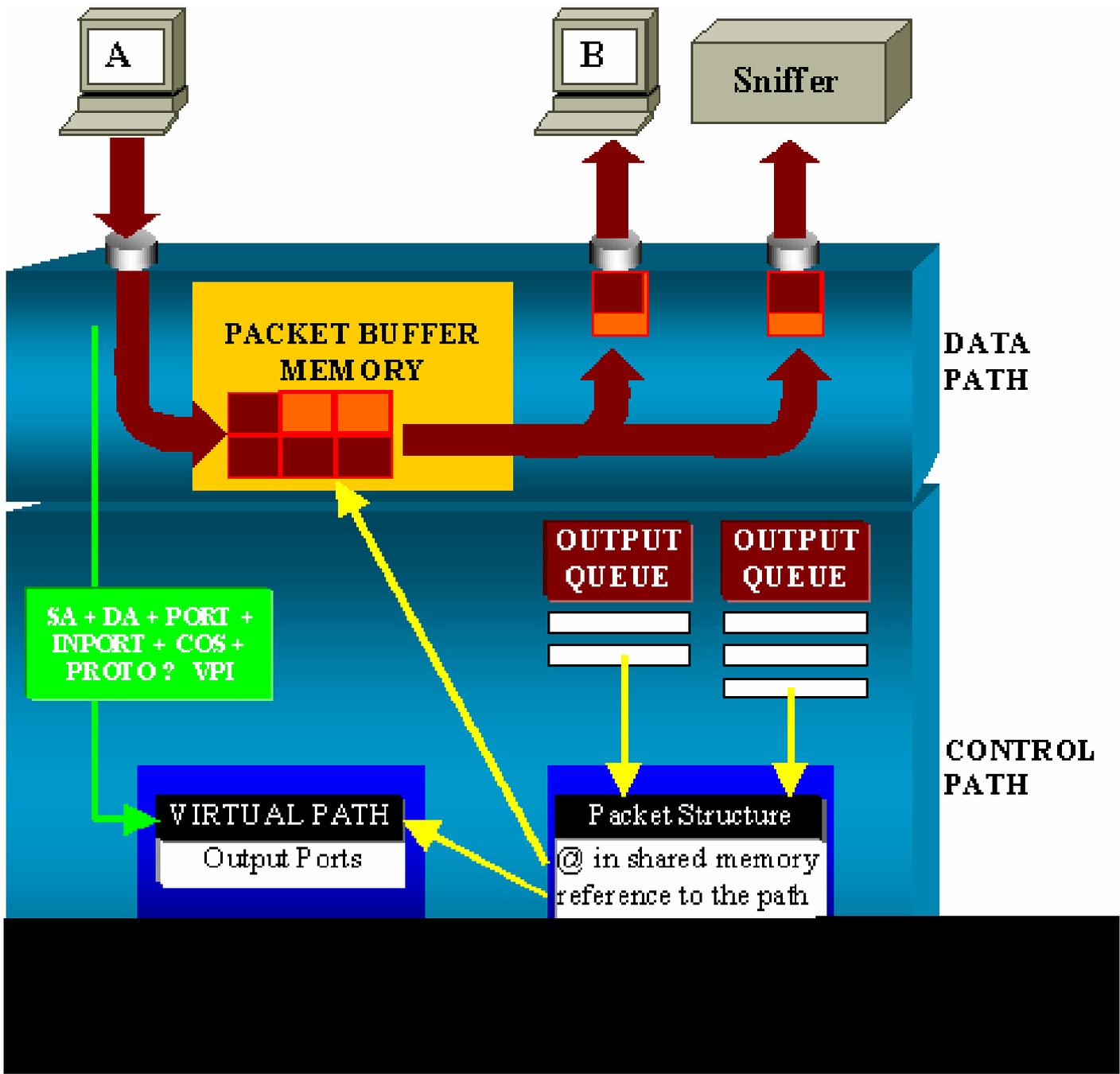
SPAN을 사용하여 일부 포트를 모니터링하려면 데이터 버퍼의 패킷을 위성으로 한 번 더 복사해야 합니다. 고속 스위칭 패브릭에는 별 영향을 미치지 않습니다.

모니터링 포트는 모니터링되는 모든 포트에 대해 송수신된 트래픽의 복사본을 수신합니다. 이 아키텍처에서는 여러 목적지로 가는 패킷의 경우 모든 복사본이 포워딩될 때까지 메모리에 저장되어 있습니다. 모니터링 포트가 장기간 50% 오버서브스크립션되는 경우, 포트가 혼잡해지고 공유 메모리의 일부를 점유할 수도 있습니다. 모니터링되는 포트 중 하나 이상에서 성능이 저하될 수 있습니다.

## Catalyst 4500/4000 시리즈

### 아키텍처 개요

Catalyst 4500/4000은 공유 메모리 스위칭 패브릭을 기반으로 합니다. 이 다이어그램은 스위치를 지나는 패킷 경로를 개괄적으로 보여줍니다. 실제 구현은 훨씬 더 복잡합니다.



Catalyst 4500/4000에서는 데이터 경로를 구별할 수 있습니다. 데이터 경로는 스위치 내의 실제 데이터 전송에 해당하는데, 모든 결정이 이루어지는 제어 경로에서 시작합니다.

패킷이 스위치에 들어가면 버퍼가 패킷 버퍼 메모리(공유 메모리)에 할당됩니다.

이 버퍼를 가리키는 패킷 구조가 PDT(Packet Descriptor Table)에서 초기화됩니다.

데이터가 공유 메모리로 복사되는 동안 제어 경로는 패킷을 스위칭할 위치를 결정합니다. 이 결정을 내리기 위해 다음 정보로 해시 값을 계산합니다.

- 패킷 소스 주소

- 대상 주소
- VLAN
- 프로토콜 유형
- 입력 포트
- CoS(Class of service)(IEEE 802.1p 태그 또는 포트 기본값)

이 값은 VPT(Virtual Path Table)에서 경로 구조의 VPI(Virtual Path Index)를 찾을 때 사용됩니다. VPT의 이 가상 경로 항목에는 이 특정 흐름과 관련된 여러 필드가 있습니다.

필드에는 목적지 포트가 포함됩니다. 이제 PDT의 패킷 구조가 가상 경로 및 카운터에 대한 참조로 업데이트됩니다.

이 섹션의 예에서는 패킷을 서로 다른 두 포트에 전송하므로 카운터가 2로 초기화됩니다. 마지막으로 패킷 구조가 두 목적지 포트의 출력 큐에 추가됩니다.

여기서 공유 메모리의 데이터가 포트의 출력 버퍼로 복사되고, 패킷 구조 카운터가 감소합니다. 0에 도달하면 공유 메모리 버퍼가 해제됩니다.

성능에 미치는 영향

SPAN 기능을 사용할 때, [아키텍처 개요 섹션의 예와 같이 패킷을 서로 다른 두 포트에 보내야 합니다.](#)

스위칭 패브릭이 비차단형이므로 패킷을 두 포트에 보내는 것은 문제가 되지 않습니다.

목적지 SPAN 포트가 혼잡하면 패킷이 출력 큐에서 삭제되고 공유 메모리에서 올바르게 해제됩니다. T

따라서 스위치 작동에 영향을 미치지 않습니다.

## Catalyst 5500/5000 및 6500/6000 시리즈

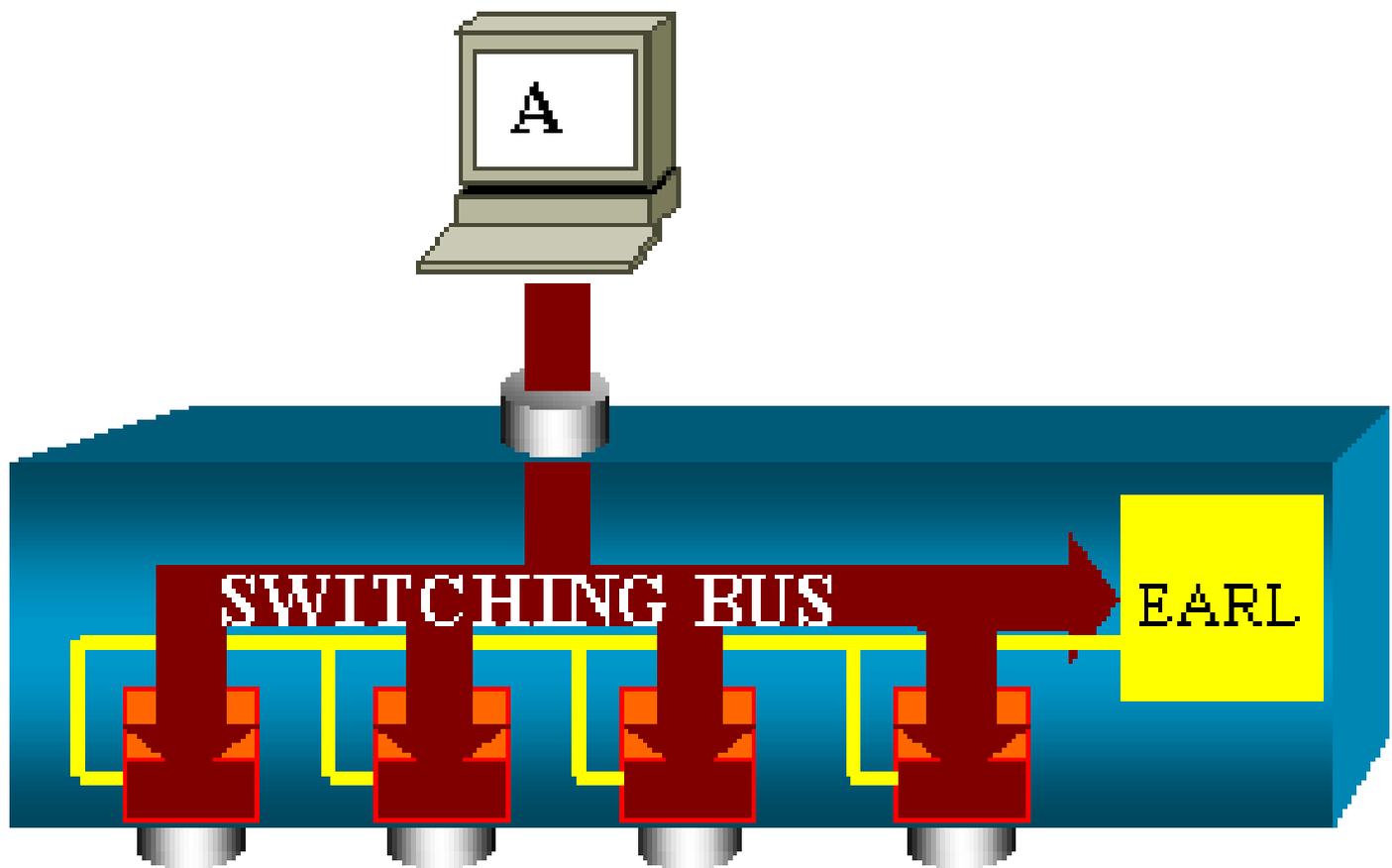
아키텍처 개요

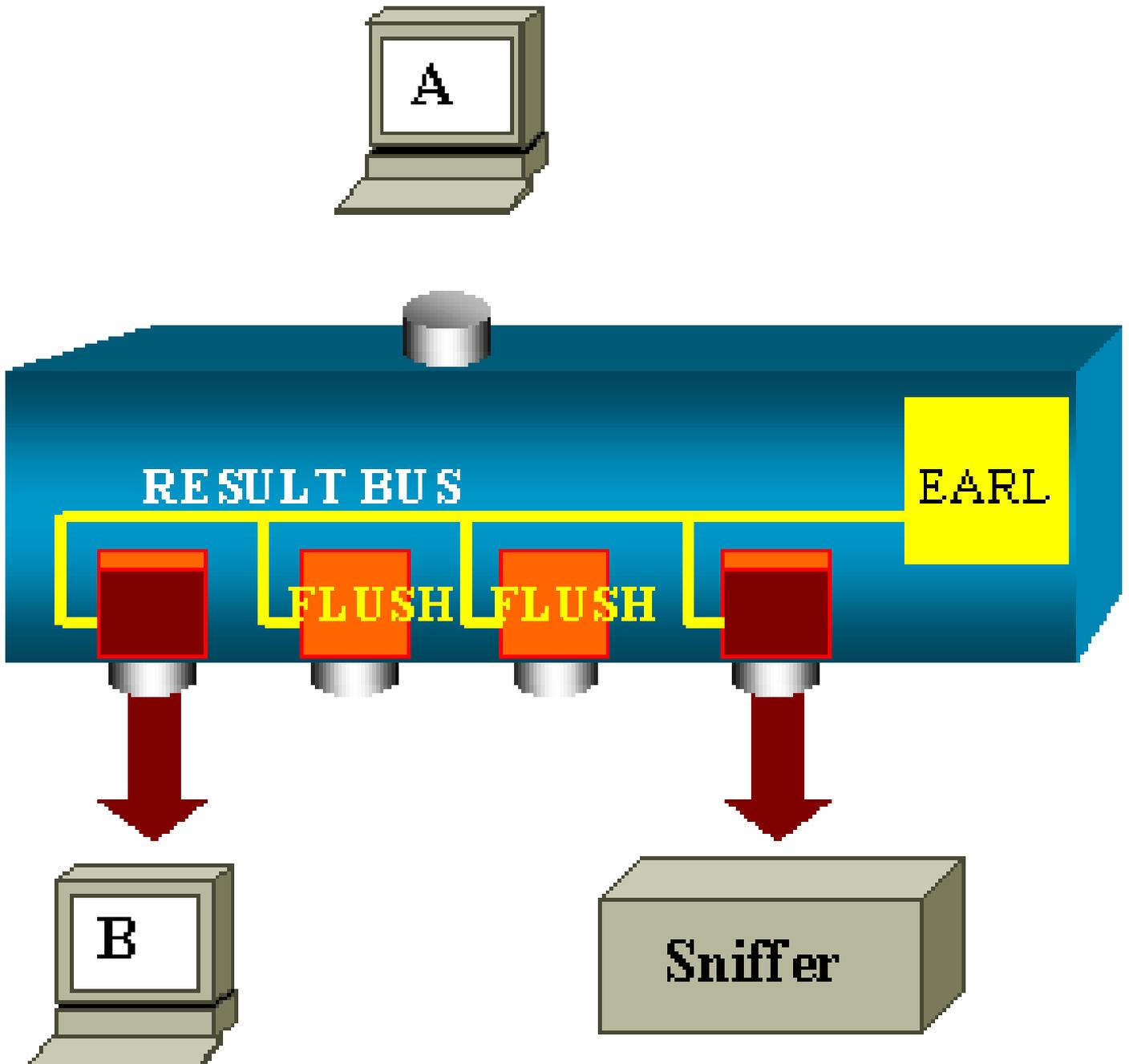
Catalyst 5500/5000 및 6500/6000 시리즈 스위치에서는 포트에서 수신되는 패킷이 내부 스위칭 버스에서 전송됩니다.

스위치의 모든 라인 카드는 이 패킷을 내부 버퍼에 저장하기 시작합니다.

그와 동시에 EARL(Encoded Address Recognition Logic)은 패킷의 헤더를 수신하고 결과 인덱스를 계산합니다. EARL은 결과 버스를 통해 모든 라인 카드에 결과 인덱스를 보냅니다.

라인 카드에서는 이 인덱스에 관한 정보를 활용하여 버퍼에서 패킷을 수신할 때 패킷을 풀러시하거나 전송할지 여부를 개별적으로 결정할 수 있습니다.





### 성능에 미치는 영향

하나 또는 여러 포트가 패킷을 전송할지 여부는 스위치 작동에 아무런 영향도 주지 않습니다. 따라서 이 아키텍처를 고려할 때 SPAN 기능이 성능에 미칠 영향은 없습니다.

### FAQ 및 일반적인 문제

#### 잘못된 SPAN 컨피그레이션으로 인한 연결 문제

잘못된 SPAN 컨피그레이션으로 인한 연결 문제가 5.1 이전의 CatOS 버전에서 자주 발생합니다. 이러한 버전에서는 하나의 SPAN 세션만 가능합니다.

SPAN을 비활성화하더라도 세션이 컨피그레이션에 남아 있습니다. `set span enable` 명령을 사용하여 저장된 SPAN 세션을 다시 활성화합니다.

이 작업은 대개 입력 오류 때문에, 이를테면 사용자가 STP를 활성화하려는 경우에 발생합니다. 목적지 포트가 사용자 트래픽 포워딩에 쓰이는 경우 심각한 연결 문제가 발생할 수 있습니다.

---

 주의: 이 문제는 아직 CatOS의 현재 구현 단계에 있습니다. SPAN 목적지로 선택하는 포트에 각별한 주의를 기울이십시오.

---

## SPAN 목적지 포트 가동/중지

모니터링을 위해 포트를 스패닝할 때 포트 상태는 UP/DOWN으로 표시됩니다.

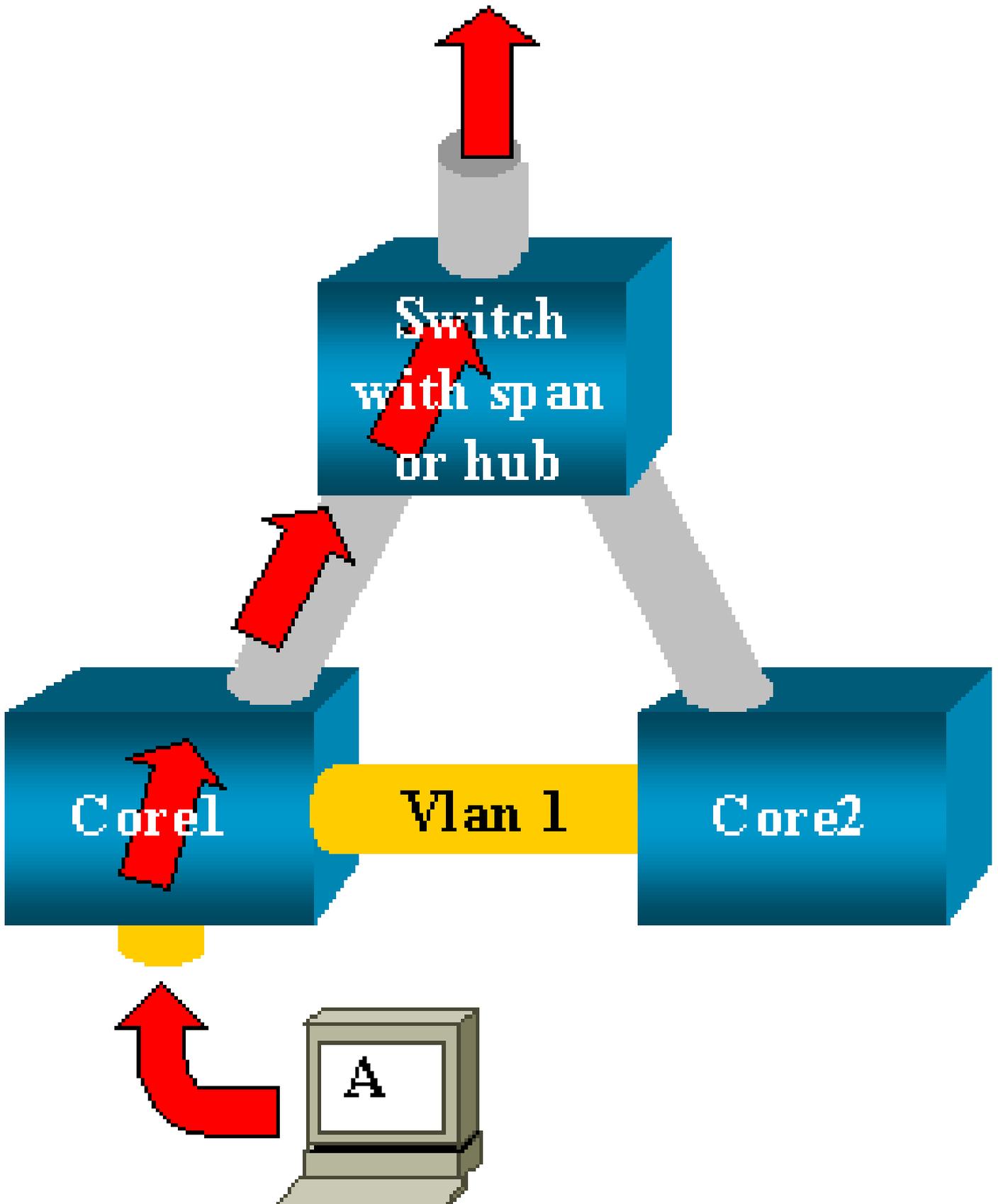
포트를 모니터링하기 위해 SPAN 세션을 구성하면, 목적지 인터페이스는 down 상태(모니터링)를 표시하도록 설계되어 있습니다.

인터페이스에서 이 상태의 포트를 표시하여 현재는 프로덕션 포트로는 사용할 수 없음을 확실히 알려 줍니다. 포트가 up/down으로 모니터링되면 정상입니다.

## SPAN 세션에서 브리징 루프를 생성하는 이유?

일반적으로 관리자가 RSPAN 기능을 흉내내려 할 때 브리징 루프가 생성됩니다. 또한 컨피그레이션 오류로 인해 이 문제가 발생할 수 있습니다.

다음과 같은 경우를 예로 들 수 있습니다.



트렁크에 의해 연결된 두 개의 코어 스위치가 있습니다. 이 경우 각 스위치에는 여러 서버, 클라이언트 또는 다른 브리지가 연결되어 있습니다.

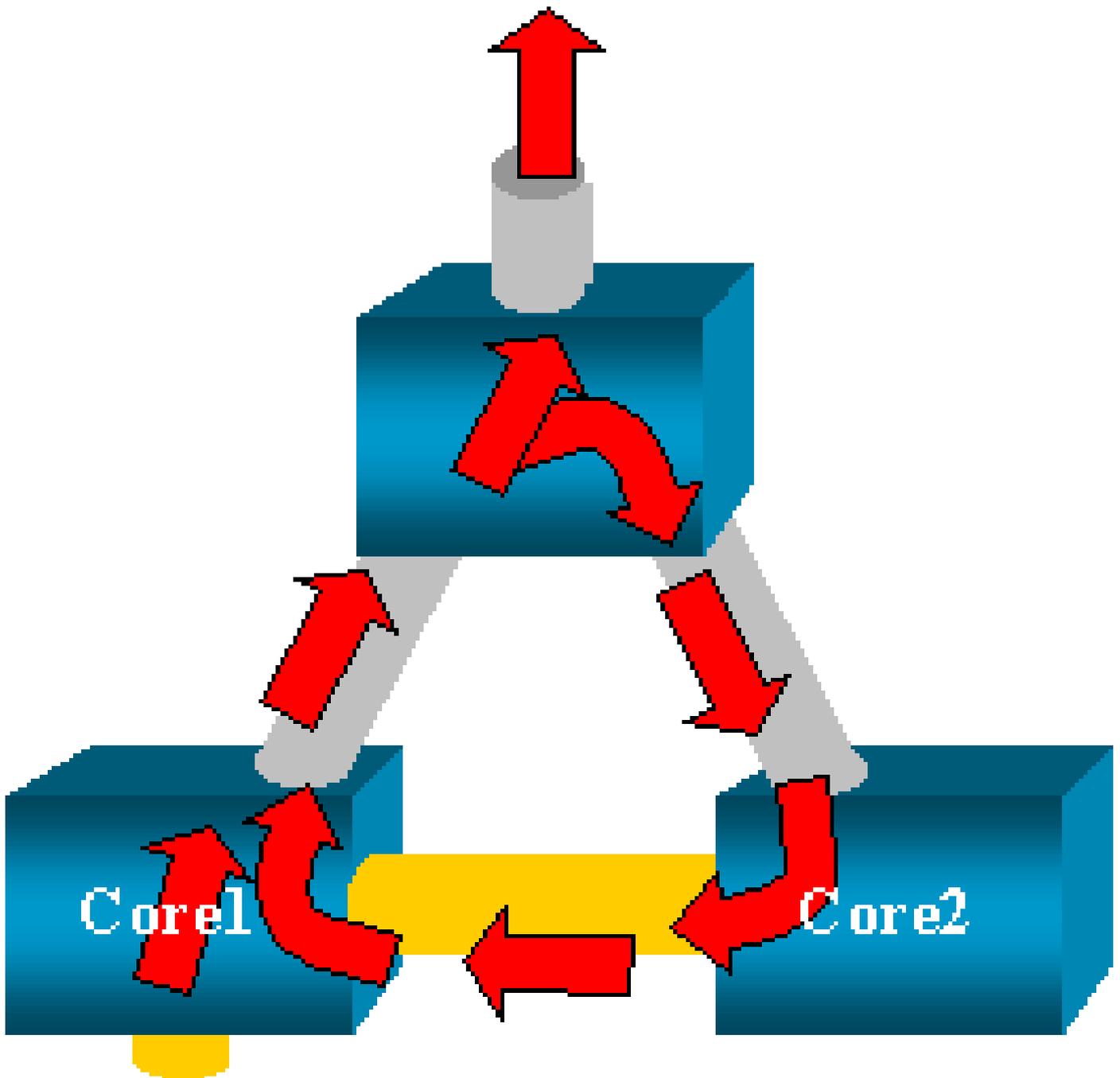
관리자는 SPAN으로 여러 브리지에 나타나는 VLAN 1을 모니터링하려고 합니다.

관리자는 각 코어 스위치에서 VLAN 1 전체를 모니터링하는 SPAN 세션을 생성합니다. 그리고 이 두 세션을 병합하기 위해 목적지 포트를 동일한 허브(또는 다른 SPAN 세션을 사용하여 동일한 스위치)에 연결합니다.

관리자가 목표를 달성합니다. 코어 스위치가 VLAN 1에서 수신하는 각 단일 패킷은 SPAN 포트에서 복제되어 위쪽 허브로 포워딩됩니다. 스�니퍼는 결국 트래픽을 캡처합니다.

유일한 문제는 트래픽이 목적지 SPAN 포트를 통해 코어 2로 재주입된다는 것입니다.

코어 2로 트래픽을 재주입하면 VLAN 1에 브리징 루프가 생성됩니다. 대상 SPAN 포트는 STP를 실행하지 않으며 이러한 루프를 방지할 수 없습니다.



참고: CatOS에 `inpkts(input packets)` 옵션이 도입되었으므로 SPAN 대상 포트는 기본적으로

---

 모든 수신 패킷을 삭제하므로 이 오류 시나리오를 방지할 수 있습니다. 그러나 Catalyst 2900XL/3500XL 시리즈 스위치에서는 여전히 이 문제가 발생할 수 있습니다.

---

 참고: inpkts 옵션이 루프를 방지하는 경우에도 이 섹션에 표시되는 컨피그레이션은 네트워크에 몇 가지 문제를 일으킬 수 있습니다. 목적지 포트에 활성화된 학습과 관련된 MAC 주소 학습 문제 때문에 네트워크 문제가 발생할 수 있습니다.

---

## SPAN이 성능에 영향을 미칩니까?

지정된 Catalyst 플랫폼의 성능 영향에 대한 자세한 내용은 이 문서의 다음 섹션을 참조하십시오.

- [Catalyst 2900XL/3500XL 시리즈](#)
- [Catalyst 4500/4000 시리즈](#)
- [Catalyst 5500/5000 및 6500/6000 시리즈](#)

## EtherChannel 포트에서 SPAN을 설정할 수 있습니까?

번들의 포트 중 하나가 SPAN 목적지 포트라면 EtherChannel이 형성되지 않습니다. 이러한 상황에서 SPAN을 구성하려고 하면 스위치에서 다음 정보를 제공합니다.

```
Channel port cannot be a Monitor Destination Port
Failed to configure span feature
```

EtherChannel 번들의 포트 하나를 SPAN 소스 포트로는 사용할 수 있습니다.

## 여러 SPAN 세션이 동시에 실행될 수 있습니까?

Catalyst 2900XL/3500XL 시리즈 스위치에서는 스위치에서 사용 가능한 목적지 포트의 수가 유일한 SPAN 세션 수 제한 사항입니다.

Catalyst 2950 시리즈 스위치에서는 한 번에 하나의 모니터 포트만 지정할 수 있습니다.

다른 포트를 모니터 포트로는 선택하면, 이전 모니터 포트가 비활성화되고 새로 선택한 포트가 모니터 포트가 됩니다.

Catalyst 4500/4000, 5500/5000, 6500/6000 스위치의 CatOS 5.1 이상에서는 여러 개의 동시 SPAN 세션을 가질 수 있습니다.

이 문서의 [여러 개의 동시 세션 생성 섹션과 기능 요약 및 제한 섹션을 참조하십시오.](#)

## 오류 "% Local Session Limit Has Been Exceeded"

이 메시지는 Supervisor Engine에서 허용된 SPAN 세션 한도를 초과할 때 나타납니다.

% Local Session limit has been exceeded

Supervisor Engine은 SPAN 세션의 제한이 있습니다. 자세한 내용은 로컬 SPAN, RSPAN, ERSPAN 구성의 [로컬 SPAN, RSPAN, ERSPAN 세션 제한](#) 섹션을 참조하십시오.

VPN 서비스 모듈에서 SPAN 세션을 삭제할 수 없습니다. "% Session [Session No:] Used by Service Module" 오류 메시지가 표시됩니다.

이 문제에서는 VPN(Virtual Private Network) 모듈이 새시에 삽입되는데, 여기에는 이미 스위치 패브릭 모듈이 삽입되어 있습니다.

Cisco IOS Software는 멀티캐스트 트래픽을 처리하기 위해 VPN 서비스 모듈에 대한 SPAN 세션을 자동으로 생성합니다.

소프트웨어에서 VPN 서비스 모듈을 위해 생성하는 SPAN 세션을 삭제하려면 이 명령을 실행합니다.

```
<#root>
```

```
Switch(config)#
```

```
no monitor session session_number service-module
```

---

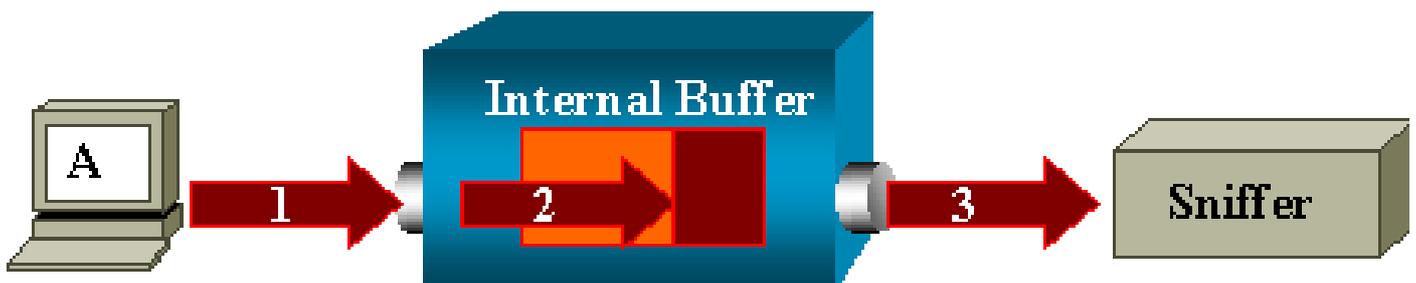
 참고: 세션을 삭제하면 VPN 서비스 모듈에서 멀티캐스트 트래픽을 삭제합니다.

---

### 손상된 패킷을 SPAN으로 캡처할 수 없는 이유는 무엇입니까?

일반적인 스위치 작동 방식 때문에 SPAN으로는 손상된 패킷을 캡처할 수 없습니다. 패킷이 스위치를 통과하면 다음과 같은 이벤트가 발생합니다.

1. 패킷이 인그레스 포트에 도달합니다.
2. 패킷은 하나 이상의 버퍼에 저장됩니다.
3. 패킷은 결국 이그레스 포트에서 다시 전송됩니다.



스위치가 손상된 패킷을 수신하면, 대개 인그레스 포트에서 패킷을 삭제합니다. 따라서 이그레스

포트에 패킷이 나타나지 않습니다.

트래픽 캡처와 관련하여 스위치가 완전한 투명성을 제공하지는 않습니다.

마찬가지로 이 섹션의 시나리오에서 스니퍼에 손상된 패킷이 나타나면, 이그레스 세그먼트에서 3단계에 오류가 발생했음을 알 수 있습니다.

디바이스에서 손상된 패킷을 전송한다고 생각될 경우, 전송 호스트와 스니퍼 디바이스를 허브에 배치하도록 선택할 수 있습니다. 허브는 오류 검사를 수행하지 않습니다.

따라서 스위치와 달리 허브는 패킷을 삭제하지 않습니다. 따라서 패킷을 볼 수 있습니다.

## 오류: 서비스 모듈에서 사용하는 세션 2의 비율(%)

CAT6500에서 FWSM(Firewall Service Module)이 설치되었다면, 이를테면 설치되었다가 나중에 제거되었다면, SPAN 리플렉터 기능이 자동으로 활성화됩니다.

SPAN 리플렉터 기능은 스위치에서 하나의 SPAN 세션을 사용합니다.

더 이상 필요하지 않은 경우, CAT6500의 컨피그레이션 모드에서 no monitor session service module 명령을 입력한 다음 곧바로 원하는 새 SPAN 컨피그레이션을 입력할 수 있습니다.

## 리플렉터 포트에서 패킷 삭제

리플렉터 포트는 모니터링되는 모든 소스 포트에 대해 송수신된 트래픽의 복사본을 수신합니다. 리플렉터 포트가 오버서브스크립션되는 경우 혼잡이 발생할 수 있습니다.

이는 하나 이상의 소스 포트에서 트래픽 포워딩에 영향을 줄 수 있습니다.

리플렉터 포트의 대역폭이 해당 소스 포트의 트래픽 볼륨에 충분하지 않으면 초과 패킷이 삭제됩니다.

10/100 포트는 100Mbps로 리플렉션됩니다. 기가비트 포트는 1Gbps로 리플렉션됩니다.

## Catalyst 6500 Chassis에서는 항상 SPAN 세션을 FWSM과 함께 사용

Cisco Native IOS를 실행하는 새시에서 Supervisor Engine 720을 FWSM과 함께 사용할 경우, 기본적으로 SPAN 세션이 사용됩니다. show monitor 명령으로 미사용 세션을 확인할 경우 session 1을 사용합니다.

```
<#root>
```

```
Cat6K#
```

```
show monitor
```

```
Session 1
```

```
-----
```

```
Type : Service Module Session
```

방화벽 블레이드가 Catalyst 6500 샤페에 있는 경우, FWSM에서 멀티캐스트 스트림을 복제할 수 없기 때문에 이 세션은 하드웨어 멀티캐스트 복제를 지원하기 위해 자동으로 설치됩니다.

FWSM 뒤에서 공급되는 멀티캐스트 스트림이 레이어 3에서 여러 라인 카드에 복제되어야 하는 경우, 자동 세션은 패브릭 채널을 통해 Supervisor에게 트래픽을 복사합니다.

FWSM 뒤에서 멀티캐스트 스트림을 생성하는 멀티캐스트 소스가 있는 경우 SPAN 리플렉터가 필요합니다.

VLAN 외부에 멀티캐스트 소스를 배치하는 경우 SPAN 리플렉터가 필요하지 않습니다. SPAN 리플렉터는 FWSM을 통해 BPDU를 브리징할 때 사용할 수 없습니다.

SPAN 리플렉터를 비활성화하려면 no monitor session service module 명령을 사용합니다.

같은 스위치 내에서 SPAN 세션과 RSPAN 세션의 ID가 같을 수 있습니까?

아니요, 일반 SPAN 세션과 RSPAN 목적지 세션에 동일한 세션 ID를 사용할 수 없습니다. 각 SPAN 및 RSPAN 세션에는 다른 세션 ID가 있어야 합니다.

RSPAN 세션은 서로 다른 여러 VTP 도메인에서 작동할 수 있습니까?

예. 하나의 RSPAN 세션이 서로 다른 여러 VTP 도메인을 포괄할 수 있습니다. 그러나 RSPAN VLAN이 해당 VTP 도메인의 데이터베이스에 있어야 합니다.

또한 세션 소스에서 세션 목적지까지의 경로에 레이어 3 디바이스가 없어야 합니다.

RSPAN 세션은 WAN에서 또는 서로 다른 여러 네트워크에서 작동할 수 있습니까?

아니요. RSPAN은 LAN(레이어 2) 기능이므로 레이어 3 디바이스를 지날 수 없습니다.

WAN 또는 다른 네트워크에서 트래픽을 모니터링하려면 ERSPAN(Encapsulated Remote SwitchPort Analyser)을 사용합니다.

ERSPAN 기능은 다양한 스위치의 소스 포트, 소스 VLAN, 목적지 포트를 지원하므로, 네트워크 전반에 걸쳐 여러 스위치를 원격으로 모니터링할 수 있습니다.

ERSPAN은 ERSPAN 소스 세션, 라우팅 가능한 ERSPAN GRE 캡슐화 트래픽, ERSPAN 목적지 세션으로 구성됩니다.

ERSPAN 소스 세션과 목적지 세션은 서로 다른 스위치에 개별적으로 구성합니다.

현재 ERSPAN 기능은 다음에서 지원됩니다.

- Cisco IOS Software Release 12.2(18)SXE 이상을 실행하는 Supervisor 720(PFC3B 또는 PFC3BXL)
- 하드웨어 버전이 3.2 이상이고 Cisco IOS Software Release 12.2(18)SXE 이상을 실행하는 Supervisor 720(PFC3A)

ERSPAN에 대한 자세한 내용은 [로컬 SPAN, RSPAN\(Remote SPAN\), ERSPAN\(Encapsulated RSPAN\) - Catalyst 6500 Series Cisco IOS Software 컨피그레이션 가이드, 12.2SX 를 참조하십시오.](#)

RSPAN 소스 세션과 목적지 세션이 같은 Catalyst Switch에 있을 수 있습니까?

아니요. RSPAN 소스 세션과 RSPAN 목적지 세션이 같은 스위치에 있을 때는 RSPAN이 작동하지 않습니다.

RSPAN 소스 세션이 특정 RSPAN VLAN으로 설정되었고 해당 RSPAN VLAN에 대한 RSPAN 목적지 세션이 같은 스위치에 설정된 경우, RSPAN 목적지 세션의 목적지 포트는 하드웨어 제한 때문에 RSPAN 소스 세션에서 캡처된 패킷을 전송하지 않습니다. 이는 4500 시리즈 및 3750 시리즈 스위치에서 지원되지 않습니다.

이 문제는 Cisco 버그 ID [CSCeg08870](#)에서 다루고 있습니다(등록된 고객만 이용 가능).

예:

```
monitor session 1 source interface Gi6/44
monitor session 1 destination remote vlan 666
monitor session 2 destination interface Gi6/2
monitor session 2 source remote vlan 666
```

이 문제에 대한 해결 방법은 일반 SPAN을 사용하는 것입니다.

SPAN 목적지 포트에 연결된 네트워크 분석기/보안 디바이스에 연결할 수 없습니다.

SPAN 목적지 포트의 기본 특성은 SPAN 세션에 필요한 트래픽을 제외한 어떤 트래픽도 전송하지 않는다는 것입니다.

SPAN 목적지 포트를 통해 네트워크 분석기/보안 디바이스에 연결해야 하는 경우(IP 연결성), 인그레스 트래픽 포워딩을 활성화해야 합니다.

인그레스를 활성화하면, SPAN 목적지 포트는 수신 패킷(지정된 캡슐화 모드에 따라 태그가 지정될 수 있음)을 받고 정상적으로 스위칭합니다.

SPAN 목적지 포트를 구성할 때, 인그레스 기능의 사용 여부 및 태그가 지정되지 않은 이그레스 패킷을 스위칭하는 데 사용할 VLAN을 지정할 수 있습니다.

ISL 캡슐화가 구성되면 인그레스 VLAN을 지정할 필요 없습니다. 모든 ISL 캡슐화 패킷은 VLAN 태그가 있기 때문입니다.

포트에서 STP 포워딩을 수행하지만 STP에는 참여하지 않으므로, 이 기능을 구성할 때는 네트워크에 스페닝 트리 루프가 생기지 않도록 주의해야 합니다.

SPAN 목적지 포트에 인그레스 및 트렁크 캡슐화가 모두 지정되면, 포트는 모든 활성 VLAN에서 포워딩합니다.

존재하지 않는 VLAN을 이그레스 VLAN으로 구성할 수 없습니다.

```
monitor session session_number destination interface interface [encapsulation {isl | dot1q}]  
ingress [vlan vlan_IDs]
```

이 예에서는 네이티브 VLAN 7을 사용하여 802.1q 캡슐화 및 인그레스 패킷으로 목적지 포트를 구성하는 방법을 보여줍니다.

<#root>

```
Switch(config)#
```

```
monitor session 1 destination interface fastethernet 5/48  
encapsulation dot1q ingress vlan 7
```

이 컨피그레이션에서는 세션 1과 연결된 SPAN 소스의 트래픽이 인터페이스 빠른 이더넷 5/48에서 복사되고 802.1q 캡슐화됩니다.

수신 트래픽을 받아 스위칭하며, 태그가 지정되지 않은 패킷은 VLAN 7으로 분류합니다.

## 관련 정보

- [Cisco IOS Software를 실행하는 Cisco Catalyst 4500 스위치에서 SPAN 및 RSPAN을 구성하는 방법](#)
- [SPAN 목적지 포트는 "연결되지 않음"으로 표시되며, 네트워크의 나머지 부분과 통신하지 않습니다.](#)
- [스위치 제품 지원](#)
- [LAN 스위칭 기술 지원](#)
- [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.