SPAN

1. SPAN(Switch Port Analyzer)이란? Port Mirroring

스위치의 특정 포트에 분석 장비를 접속하고 다른 포트의 트래픽을 분석 장비로 자동 복사해주는 기술

특정 포트를 통해 입출력되는 트래픽을 다른 포트에 접속된 분석 장비를 통해 볼 수 있게 한다.

- Source Port (Monitored Port): Span의 분석 대상이 되는 포트
- Destination Port (Monitoring Port): 분석 장비가 접속되어 있는 포트

○ Span의 종류

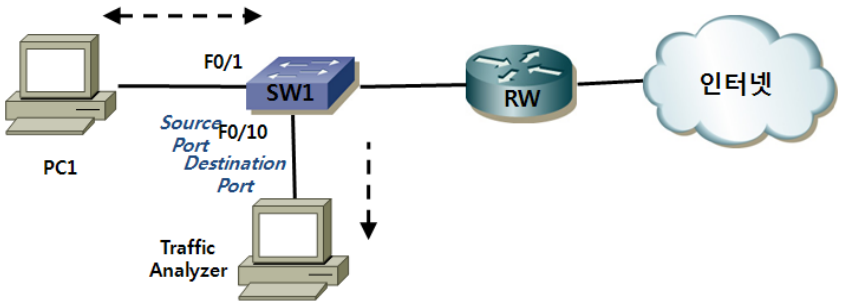
- **Local Span**: 출발지 포트와 목적지 포트가 동일한 스위치에 있는 것
- **Remote Span**: 출발지 포트와 목적지 포트가 서로 다른 스위치에 있는 것
- **ERSPAN**(Encapsulated RSPAN): GRE를 이용하여 L3로 연결된 원격지의 목적지로 SPAN 트래픽을 전송하는 기술로 수퍼바이저 엔진 720/PFC3A 하드웨어 버전 3.2 이상에서만 지원.

2. SPAN 설정

○ 기본적 SPAN 설정

- **monitor session 1 source interface** f0/1
- **monitor session 1 destination interface** f0/10

- Catalyst 3560 스위치에서 사용할 수 있는 세션 번호는 66까지이다. Source를 지정하는 세션은 최대 2개이며 Destination은 64개의 세션까지 지정 가능하다.



○ 확인 명령

- **show monitor (session 번호)**
- **show interface status**

목적지 포트는 SPAN 세션을 위해서 필요한 트래픽이나 IPS를 위해 입력 트래픽 전송이 설정된 경우를 제외하고 자신의 트래픽을 송수신할 수 없다. 즉 SPAN 목적지 포트에 접속된 장비는

인터넷이나 다른 통신기능을 사용할 수 없다. 또 SPAN 목적지 포트에서는 STP, CDP, VTP, PAgP, DTP 등 Layer 2 관련 프로토콜도 동작하지 않는다. SPAN 목적지 포트는 어떤 VLAN에 소속되어 있어도 상관없다.

- **show interface** f0/2

미러링된 트래픽을 분석할 수 있는 것으로는 Sniffer, WireShark 등이 있다. 전용장비도 있고, WireShark와 같이 PC에 설치해서 사용할 수 있는 소프트웨어도 있다. SPAN의 목적지 포트는 show interface ...로 확인해보면 인터페이스 **Status Up, Line Protocol Down(Monitoring)**으로 표시된다.

○ IPS(Intrusion Detection System)가 접속되어 있는 경우

- 공격을 탐지하고 라우터나 방화벽에서 해당 패킷을 차단시키는 명령을 내리려면 SPAN의 목적지 포트를 통해 패킷을 전송할 수 있어야 한다.
- IPS와 연동시 설정
- vlan 999
- **monitor session** 2 **destination interface** f0/10 **ingress vlan** 999

○ SPAN Source Port 지정

- SPAN Source Port 지정시 사용가능한 옵션
- **both** Monitor received and transmitted traffic
- **rx** Monitor received traffic only
- **tx** monitor transmitted traffic only
- 송수신 방향의 기준은 스위치이다.

○ VLAN Mirroring 설정

- VLAN 미러링 설정의 예
- **monitor session** 3 **vlan** 10 , 20 - 22 both

○ Trunk Port 미러링과 VLAN 필터링

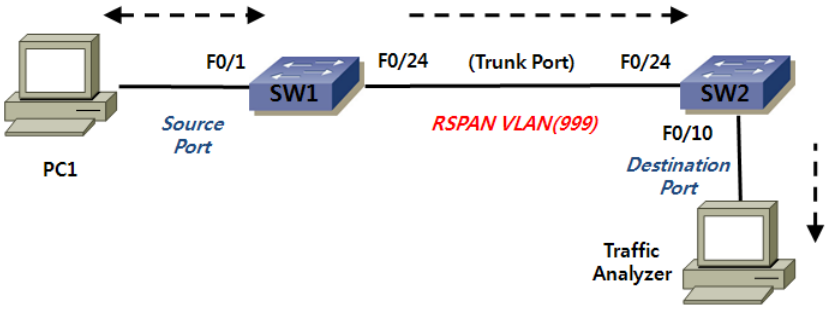
- 스위치의 트렁크 포트를 미러링하면 모니터링 장비에 많은 부하가 걸릴 수 있다.
- 트렁크 포트를 통과하는 트래픽 중에서 특정한 VLAN에 포함되는 것을 제외하면 편리하다.

[설정 Trunk Port 미러링 및 VLAN 필터링]

구분	설정
예	현재까지의 SPAN을 모두 해제한다. 트렁크 포트인 F0/23 - 24를 출발지 포트로, F0/10을 목적지 포트로 설정하되 Vlan 10, 20은 제외한다.
SW1	no monitor session all monitor session 1 source interface f0/23 - 24 both monitor session 1 destination interface f0/10 **monitor session** 1 **filter vlan** 10, 20

3. RSPAN

SPAN의 출발지 포트와 목적지 포트가 서로 다른 스위치에 있는 것



[설정 RSPAN]

구분	설정
예	SW1의 F0/1 포트에서 발생하는 트래픽을 SW2의 F0/10 포트에 접속된 트래픽 분석 장비로 미러링해보자.
SW1	vlan 999 remote-span ! monitor session 1 source interface f0/1 monitor session 1 destination remote vlan 999
SW2	vlan 999 remote-span ! monitor session 1 source remote vlan 999 monitor session 1 destination interface f0/10

- 미러링된 트래픽을 전송할 VLAN을 RSPAN VLAN이라고 한다.
- RSPAN Vlan은 출발지 스위치, 목적지 스위치 및 중간 스위치에 모두 동일하게 정의해주어야 한다.
- RSPAN Vlan이 지나가는 스위치들은 반드시 트렁크로 연결되어야 한다.
- SPAN의 목적지를 remote vlan 옵션을 사용하여 RSPAN Vlan으로 지정한다. **Catalyst 2950이나 3550**에서는 **Reflector Port**라는 중간 포트를 지정하여 미러링 트래픽을 여기로 전송한 다음, 다시 RSPAN Vlan으로 전송하게 한다. **Reflector Port는 출발지 스위치에서 사용하지 않는 임의의 포트를 지정하면 된다.**

○ 확인 명령

- show vlan remote-span

○ RSPAN 중간 스위치가 있는 경우

- 출발지 스위치와 목적지 스위치의 설정은 변함이 없다. 다만 중간 스위치에는 RSPAN을 위한 VLAN만 설정해주면 된다.

○ 모니터링 대상 트래픽 선별

- 트래픽이 많은 네트워크에서는 SPAN을 설정하고 트래픽 분석장비를 가동하는 순간 엄청나게 많은 양의 프레임이 복사되어 원하는 분석이 어렵다.
- 또 RSPAN의 경우 미러링되는 프레임이 대역폭에 영향을 미칠 수 있다.
- 이를 방지하려면 원하는 트래픽만 선별하여 목적지 SPAN 포트로 미러링하면 된다.
- 이를 위해서는 RSPAN과 VACL을 동시에 사용하면 된다.

- 설정 순서

1) RSPAN VLAN 생성
2) Monitor Session 설정
3) ACL 설정
4) VLAN Access-map 설정
5) VLAN Map을 위한 SVI 생성
   Vlan 맵을 지정하기 위해서는 SVI가 있어야 한다.
6) Vlan Filter 설정

[설정 Vlan 맵을 이용하여 미러링 트래픽 선택]

구분	설정
예	SW1의 F0/1로 입출력되는 트래픽 중에서 HTTP 관련 트래픽만 SW2의 F0/10으로 미러링한다.
SW1	vlan 999 remote-span ! monitor session 1 source interface f0/1 monitor session 1 desination remote vlan 999 ! access-list 100 permit tcp any any eq www vlan access-map W-Only match ip address 100 action forward ! interface vlan 999 exit vlan filter W-Only vlan-list 999
SW2	vlan 999 remote-span ! monitor session 1 source remote vlan 999 monitor session 1 destination interface f0/10