Cisco IOS Software를 실행하는 Cisco Catalyst 6000/6500을 통한 세분화된 트래픽 분석을 위한 VACL 캡처

목차

소개

이 문서에서는 네트워크 트래픽 분석을 위해 VACL(VLAN ACL) 캡처 포트 기능을 사용하기 위한 샘플 컨피그레이션을 보다 세부적으로 제공합니다.이 문서에서는 VSPAN(VLAN-based SPAN) 사용과는 달리 VACL 캡처 포트 사용의 이점을 설명합니다.

Catalyst OS 소프트웨어를 실행하는 Cisco Catalyst 6000/6500에서 VACL 캡처 포트 기능을 구성하려면 Cisco Catalyst 6000/6500 Running CatOS Software로 세분화된 트래픽 분석을 위한 VACL 캡처를 참조하십시오.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

- IP 액세스 목록:자세한 내용은 IP 액세스 목록 구성을 참조하십시오.

- 가상 LAN:자세한 내용은 VLAN/VTP(Virtual LAN/VLAN Trunking Protocol) - 소개를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.Cisco IOS® 소프트웨어 릴리스 12.2(18)SXF8을 실행하는 Cisco Catalyst 6506 Series Switch

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

관련 제품

이 구성은 Cisco IOS Software 릴리스 12.1(13)E 이상을 실행하는 Cisco Catalyst 6000/6500 Series 스위치에서도 사용할 수 있습니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참고하십시오.

배경 정보

VLAN 기반 SPAN

SPAN(Switched Port Analyzer)은 분석을 위해 VLAN에 있는 하나 이상의 소스 포트에서 하나 이상의 VLAN에서 대상 포트로 트래픽을 복사합니다.로컬 SPAN은 동일한 Catalyst 6500 Series 스위치에서 소스 포트, 소스 VLAN 및 목적지 포트를 지원합니다.

소스 VLAN은 네트워크 트래픽 분석을 위해 모니터링되는 VLAN입니다.VSPAN(VLAN-based SPAN)은 VLAN을 SPAN 소스로 사용합니다.소스 VLAN의 모든 포트는 소스 포트가 됩니다.소스 포트는 네트워크 트래픽 분석을 위해 모니터링되는 포트입니다.트렁크 포트는 소스 포트로 구성할 수 있으며 트렁크가 아닌 소스 포트와 혼합될 수 있지만 SPAN은 소스 트렁크 포트에서 캡슐화를 복사하지 않습니다.

인그레스(ingress) 및 이그레스(egress)가 모두 구성된 VSPAN 세션의 경우, 패킷이 동일한 VLAN에서 스위칭되는 경우(인그레스 포트의 인그레스 트래픽과 이그레스 포트의 이그레스 트래픽으로 하나씩) 목적지 포트에서 2개의 패킷이 전달됩니다.

VSPAN은 VLAN에서 레이어 2 포트를 나가거나 들어가는 트래픽만 모니터링합니다.

- VLAN을 인그레스 소스로 구성하고 트래픽이 모니터링되는 VLAN으로 라우팅되는 경우, 라우팅된 트래픽은 VLAN에서 레이어 2 포트로 들어가는 인그레스 트래픽으로 나타나지 않으므로 모니터링되지 않습니다.
- VLAN을 이그레스 소스로 구성하고 트래픽이 모니터링되는 VLAN에서 라우팅되는 경우, 라우팅된 트래픽은 VLAN에 레이어 2 포트를 떠나는 이그레스 트래픽으로 나타나지 않으므로 모니터링되지 않습니다.

소스 VLAN에 대한 자세한 내용은 소스 VLAN의 특성을 참조하십시오.

VLAN ACL

VACL은 VLAN 내에 브리징되거나 VLAN 또는 WAN 인터페이스로 라우팅되거나 VACL 캡처를 위한 WAN 인터페이스로 라우팅되는 모든 패킷에 대한 액세스 제어를 제공할 수 있습니다.라우터 인터페이스에만 구성되고 라우팅된 패킷에만 적용되는 일반 Cisco IOS 표준 또는 확장 ACL과 달리 VACL은 모든 패킷에 적용되며 모든 VLAN 또는 WAN 인터페이스에 적용할 수 있습니다.VACL은 하드웨어에서 처리됩니다.VACL은 Cisco IOS ACL을 사용합니다.VACL은 하드웨어에서 지원되지 않는 Cisco IOS ACL 필드를 무시합니다.

IP, IPX 및 MAC 레이어 트래픽에 대한 VACL을 구성할 수 있습니다.WAN 인터페이스에 적용되는 VACL은 VACL 캡처를 위한 IP 트래픽만 지원합니다.

VACL을 구성하고 VLAN에 적용하면 VLAN에 들어오는 모든 패킷이 이 VACL에 대해 점검됩니다.VLAN에 VACL을 적용하고 VLAN의 라우티드 인터페이스에 ACL을 적용하면 VLAN에 들어오는 패킷이 먼저 VACL에 대해 확인되고, 허용된 경우, 라우팅 인터페이스에서 처리하기 전에 입력 ACL에 대해 확인됩니다.패킷이 다른 VLAN으로 라우팅되면 먼저 라우티드 인터페이스에 적용되는 출력 ACL에 대해 확인되며, 허용되는 경우 대상 VLAN에 대해 구성된 VACL이 적용됩니다.패킷 유형에 대해 VACL이 구성되어 있고 해당 유형의 패킷이 VACL과 일치하지 않는 경우 기본 작업은 deny입니다.다음은 VACL의 캡처 옵션에 대한 지침입니다.

- 캡처 포트는 ATM 포트일 수 없습니다.
- 캡처 포트는 VLAN의 스패닝 트리 포워딩 상태에 있어야 합니다.
- 스위치에는 캡처 포트 수가 제한되지 않습니다.
- 캡처 포트는 구성된 ACL에서 허용하는 패킷만 캡처합니다.
- 캡처 포트는 캡처 포트 VLAN에 속하는 트래픽만 전송합니다.많은 VLAN으로 이동하는 트래픽을 캡처하기 위해 필요한 VLAN을 전달하는 트렁크로 캡처 포트를 구성합니다.

주의: ACL의 잘못된 조합은 트래픽 흐름을 방해할 수 있습니다.디바이스에서 ACL을 구성하는 동안 특별히 주의해야 합니다.

참고: VACL은 Catalyst 6000 시리즈 스위치의 IPv6에서 지원되지 않습니다.다시 말해, VLAN ACL 리디렉션과 IPv6는 호환되지 않으므로 ACL을 사용하여 IPv6 트래픽을 확인할 수 없습니다.

VSPAN 사용량에 대한 VACL 사용의 장점

트래픽 분석을 위한 VSPAN 사용에는 몇 가지 제한이 있습니다.

- VLAN에서 흐르는 모든 레이어 2 트래픽이 캡처됩니다.이렇게 하면 분석할 데이터의 양이 늘어납니다.
- Catalyst 6500 Series 스위치에서 구성할 수 있는 SPAN 세션 수는 제한됩니다.자세한 내용은 로컬 SPAN 및 RSPAN 세션 제한을 참조하십시오.
- 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.

VACL 캡처 포트 기능은 이러한 제한 사항을 극복하는 데 도움이 됩니다.VACL은 주로 트래픽을 모니터링하도록 설계되지 않았지만, 트래픽을 분류하는 다양한 기능을 갖춘 Capture Port 기능이 도입되어 네트워크 트래픽 분석이 훨씬 더 간단해질 수 있습니다.다음은 VSPAN을 통한 VACL 캡처 포트 사용의 장점입니다.

- 세분화된 트래픽 분석VACL은 소스 IP 주소, 대상 IP 주소, 레이어 4 프로토콜 유형, 소스 및 목적지 레이어 4 포트 및 기타 정보를 기준으로 매칭할 수 있습니다.이 기능을 통해 VACL은 세분

화된 트래픽 식별 및 필터링에 매우 유용합니다.
- 세션 수VACL은 하드웨어에서 시행됩니다.생성할 수 있는 ACE(Access Control Entries) 수는 스위치에서 사용할 수 있는 TCAM에 따라 다릅니다.
- 대상 포트 오버서브스크립션세분화된 트래픽 식별은 대상 포트로 전달할 프레임 수를 줄여 초과 서브스크립션의 가능성을 최소화합니다.
- 성능VACL은 하드웨어에서 시행됩니다.Cisco Catalyst 6500 Series 스위치의 VLAN에 VACL을 적용하는 경우 성능 저하 없음

구성

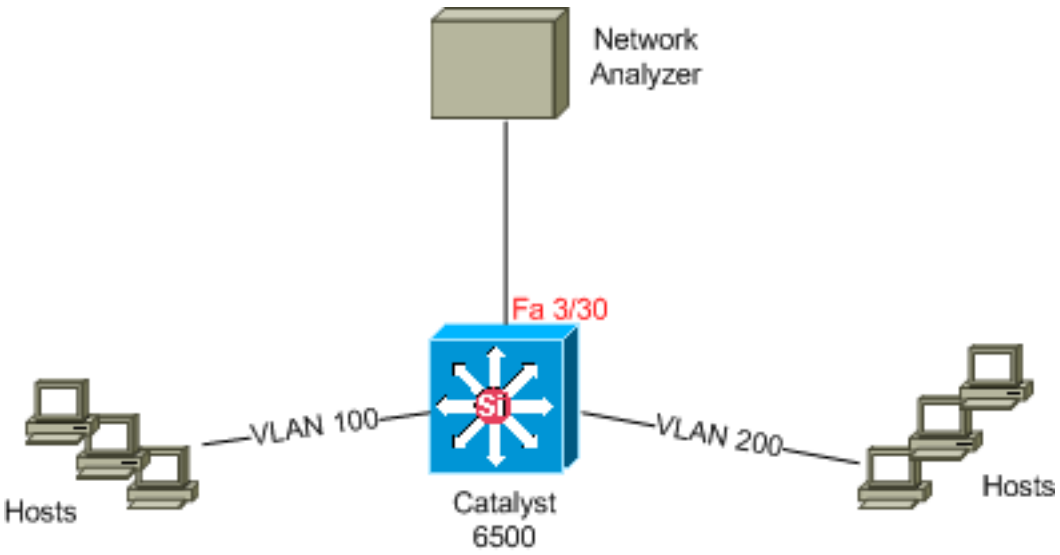
이 섹션에는 이 문서에서 설명하는 기능을 구성하기 위한 정보가 표시됩니다.

- VLAN 기반 SPAN으로 구성
- VACL로 구성

참고: 명령 조회 도구(등록된 고객만 해당)를 사용하여 이 문서에 사용된 명령에 대한 자세한 내용을 확인하십시오.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



VLAN 기반 SPAN을 사용한 컨피그레이션

이 컨피그레이션 예에서는 VLAN 100 및 VLAN 200에서 흐르는 모든 레이어 2 트래픽을 캡처하고 Network Analyzer 디바이스로 전송하는 데 필요한 단계를 나열합니다.

1. 관심 있는 트래픽을 지정합니다.이 예에서는 VLAN 100 및 VLAN 200에서 이동하는 트래픽입니다.

```
Cat6K-IOS#conf t
Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200 ?
  ,     Specify another range of VLANs
  -     Specify a range of VLANs
  both  Monitor received and transmitted traffic
  rx    Monitor received traffic only
  tx    Monitor transmitted traffic only
  <cr>
```

```
!--- Default is to monitor both received and transmitted traffic

Cat6K-IOS(config)#monitor session 50 source vlan 100 , 200
Cat6K-IOS(config)#
```

2. 캡처된 트래픽의 목적지 포트를 지정합니다.

```
Cat6K-IOS(config)#monitor session 50 destination interface Fa3/30
Cat6K-IOS(config)#
```

이를 통해 VLAN 100 및 VLAN 200에 속하는 모든 레이어 2 트래픽이 복사되어 포트 Fa3/30에 전송됩니다. 대상 포트가 트래픽을 모니터링하는 동일한 VLAN의 일부인 경우 대상 포트에서 나가는 트래픽은 캡처되지 않습니다.

show monitor 명령을 사용하여 SPAN 컨피그레이션을 확인합니다.

```
Cat6K-IOS#show monitor detail
Session 50
----------
Type               : Local Session
Source Ports       :
    RX Only        : None
    TX Only        : None
    Both           : None
Source VLANs       :
    RX Only        : None
    TX Only        : None
    Both           : 100,200
Source RSPAN VLAN  : None
Destination Ports  : Fa3/30
Filter VLANs       : None
Dest RSPAN VLAN    : None
```

VACL을 사용한 구성

이 컨피그레이션 예에서는 네트워크 관리자의 여러 요구 사항이 있습니다.

- VLAN 200의 호스트 범위(10.20.20.128/25)에서 VLAN 100의 특정 서버(10.10.10.101)까지 HTTP 트래픽을 캡처해야 합니다.
- 그룹 주소 239.0.0.100으로 향하는 전송 방향의 UDP(Multicast User Datagram Protocol) 트래픽을 VLAN 100에서 캡처해야 합니다.

1. 캡처하여 분석으로 전송할 흥미로운 트래픽을 정의합니다.

```
Cat6K-IOS(config)#ip access-list extended HTTP_UDP_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit tcp 10.20.20.128 0.0.0.127 host 10.10.10.101 eq www
Cat6K-IOS(config-ext-nacl)#permit udp any host 239.0.0.100
Cat6K-IOS(config-ext-nacl)#exit
```

2. 다른 모든 트래픽을 매핑하기 위해 전체 ACL을 정의합니다.

```
Cat6K-IOS(config)#ip access-list extended ALL_TRAFFIC
Cat6K-IOS(config-ext-nacl)#permit ip any any
Cat6K-IOS(config-ext-nacl)#exit
```

3. VLAN 액세스 맵을 정의합니다.

```
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 10
Cat6K-IOS(config-access-map)#match ip address HTTP_UDP_TRAFFIC
Cat6K-IOS(config-access-map)#action forward capture
Cat6K-IOS(config)#vlan access-map HTTP_UDP_MAP 20
Cat6K-IOS(config-access-map)#match ip address ALL_TRAFFIC
Cat6K-IOS(config-access-map)#action forward
Cat6K-IOS(config-access-map)#exit
```

4. 적절한 VLAN에 VLAN 액세스 맵을 적용합니다.

```
Cat6K-IOS(config)#vlan filter HTTP_UDP_MAP vlan-list 100
!--- Here 100 is the ID of VLAN on which the VACL is applied.
```

5. 캡처 포트를 구성합니다.

```
Cat6K-IOS(config)#int fa3/30
Cat6K-IOS(config-if)#switchport capture allowed vlan ?
  WORD    VLAN IDs of the allowed VLANs when this po
  add     add VLANs to the current list
  all     all VLANs
  except  all VLANs except the following
  remove  remove VLANs from the current list

Cat6K-IOS(config-if)#switchport capture allowed vlan 100
Cat6K-IOS(config-if)#switchport capture
Cat6K-IOS(config-if)#exit
```

다음을 확인합니다.

이 섹션을 사용하여 컨피그레이션이 제대로 작동하는지 확인합니다.

Output Interpreter 도구(등록된 고객만 해당)(OIT)는 특정 **show** 명령을 지원합니다.OIT를 사용하여 **show** 명령 출력의 분석을 봅니다.

- **show vlan access-map** — VLAN 액세스 맵의 내용을 표시합니다.

```
Cat6K-IOS#show vlan access-map HTTP_UDP_MAP
Vlan access-map "HTTP_UDP_MAP"  10
        match: ip address HTTP_UDP_TRAFFIC
        action: forward capture
Vlan access-map "HTTP_UDP_MAP"  20
        match: ip address ALL_TRAFFIC
        action: forward
```

- **show vlan filter** — VLAN 필터에 대한 정보를 표시합니다.

```
Cat6K-IOS#show vlan filter
VLAN Map HTTP_UDP_MAP:
        Configured on VLANs:  100
            Active on VLANs:  100
```

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- Cisco Catalyst 6000/6500 Running CatOS Software로 세분화된 트래픽 분석을 위한 VACL 캡처
- Cisco Catalyst 6500 Series 스위치 지원
- LAN 제품 지원
- LAN 스위칭 기술 지원
- 기술 지원 및 문서 – Cisco Systems