Catalyst 4500 Series 스위치 Wireshark 기능 구성 예

목차

소개

이 문서에서는 Cisco Catalyst 4500 Series 스위치용 Wireshark 기능을 구성하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

Wireshark 기능을 사용하려면 다음 조건을 충족해야 합니다.

- 시스템은 Cisco Catalyst 4500 Series 스위치를 사용해야 합니다.
- 스위치는 Supervisor Engine 7-E를 실행해야 합니다(현재 Supervisor Engine 6은 지원되지 않음).
- 이 기능에는 IP Base 및 Enterprise Services 집합이 있어야 합니다(현재 LAN Base는 지원되지 않음).
- Wireshark 기능은 캡처 프로세스에서 CPU 사용량이 많은 특정 패킷과 소프트웨어 스위치를 사용하므로 스위치 CPU의 사용률 상태가 높을 수 없습니다.

사용되는 구성 요소

이 문서의 정보는 Supervisor Engine 7-E를 실행하는 Cisco Catalyst 4500 Series 스위치를 기반으로 합니다.

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.

배경 정보

Supervisor Engine 7-E를 실행하는 Cisco Catalyst 4500 Series 스위치는 Cisco IOS® -XE 버전 3.3(0) / 151.1 이상에서 새로운 내장 기능을 제공합니다.이 내장형 Wireshark 기능은 트러블슈팅 시나리오에서 패킷을 캡처하기 위해 기존의 SPAN(Switch Port Analyzer)을 연결된 PC로 대체하는 방식으로 패킷을 캡처할 수 있습니다.

구성

이 섹션에서는 캡처를 시작하기 위한 빠른 시작 지침으로 사용됩니다.제공된 정보는 매우 일반적이며, 프로덕션 네트워크에서 작업하는 경우 패킷의 과도한 캡처를 제한하려면 필요에 따라 필터 및 버퍼 설정을 구현해야 합니다.

Wireshark 기능을 구성하려면 다음 단계를 완료하십시오.

1. 캡처를 지원하기 위해 조건을 충족하는지 확인합니다.(참조: **요구 사항** 섹션을 참조하십시오.) 다음 명령을 입력하고 출력을 확인합니다.

```
4500TEST#show version

Cisco IOS Software, IOS-XE Software, Catalyst 4500 L3 Switch Software
 (cat4500e-UNIVERSAL-M), Version 03.03.00.SG RELEASE SOFTWARE (fc3)

<output omitted>

License Information for 'WS-X45-SUP7-E'
 License Level: entservices   Type: Permanent
 Next reboot license Level: entservices

cisco WS-C4507R+E (MPC8572) processor (revision 8)
 with 2097152K/20480K bytes of memory.

Processor board ID FOX1512GWG1

MPC8572 CPU at 1.5GHz, Supervisor 7

<output omitted>

4500TEST#show proc cpu history

History information for system:

    8888444442222222222222223333344444222222222222222255555222222
100
 90
 80
 70
 60
 50
 40
 30
```

```
 20
10 ****                                                      ****
0.....5.....1.....1.....2.....2.....3.....3.....4.....4.....5....5
           0     5     0     5     0     5     0     5     0    5

                     CPU% per second (last 60 seconds)
```

2. 포트에서 TX/RX 방향으로 트래픽 캡처 **gig2/26** 이 예제에서는부트 플래시에 캡처 파일 저장 **pcap** 필요한 경우 로컬 PC에서 검토할 파일 형식:**참고:**전역 컨피그레이션 모드가 아닌 **사용자 EXEC** 모드**에서 컨피그레이션을** 수행해야 합니다.

```
4500TEST#monitor capture MYCAP interface g2/26 both
4500TEST#monitor capture file bootflash:MYCAP.pcap
4500TEST#monitor capture MYCAP match any start

*Sep 13 15:24:32.012: %BUFCAP-6-ENABLE: Capture Point MYCAP enabled.
```

3. 포트의 모든 트래픽 인그레스 및 이그레스 캡처 **g2/26**.또한 캡처된 트래픽의 범위를 좁히기 위해 방향을 지정하고 캡처 필터를 적용하지 않는 한, 프로덕션 상황에서 불필요한 트래픽으로 파일을 매우 빠르게 채웁니다.필터를 적용하려면 다음 명령을 입력합니다.

```
4500TEST#monitor capture MYCAP start capture-filter "icmp"
```

참고:이렇게 하면 캡처 파일에서 ICMP(Internet Control Message Protocol) 트래픽만 캡처할 수 있습니다.

4. 캡처 파일이 시간 초과되거나 크기 할당량을 채우면 다음 메시지가 표시됩니다.

```
*Sep 13 15:25:07.933: %BUFCAP-6-DISABLE_ASYNC:
 Capture Point MYCAP disabled. Reason : Wireshark session ended
```

캡처를 수동으로 중지하려면 다음 명령을 입력합니다.

```
4500TEST#monitor capture MYCAP stop
```

5. CLI에서 캡처를 볼 수 있습니다.패킷을 보려면 다음 명령을 입력합니다.

```
4500TEST#show monitor capture file bootflash:MYCAP.pcap

 1   0.000000 44:d3:ca:25:9c:c9 -> 01:00:0c:cc:cc:cc CDP
      Device ID: 4500TEST  Port ID: GigabitEthernet2/26
 2   0.166983 00:19:e7:c1:6a:18 -> 01:80:c2:00:00:00 STP
      Conf. Root = 32768/1/00:19:e7:c1:6a:00  Cost = 0  Port = 0x8018
 3   0.166983 00:19:e7:c1:6a:18 -> 01:00:0c:cc:cc:cd STP
      Conf. Root = 32768/1/00:19:e7:c1:6a:00  Cost = 0  Port = 0x8018
 4   1.067989    14.1.98.2 -> 224.0.0.2    HSRP Hello (state Standby)
 5   2.173987 00:19:e7:c1:6a:18 -> 01:80:c2:00:00:00 STP
      Conf. Root = 32768/1/00:19:e7:c1:6a:00  Cost = 0  Port = 0x8018
```

참고:detail 옵션은 Wireshark 형식으로 패킷을 보려면 마지막에 사용할 수 있습니다.또한 패킷의 16진수 값을 확인하기 위해 덤프 옵션을 사용할 수 있습니다.

6. 캡처를 시작할 때 캡처 필터를 사용하지 않으면 캡처 파일이 어수선해집니다.이 경우 표시에 특정 트래픽을 표시하려면 **display-filter** 옵션을 사용합니다.이전 출력에 표시된 HSRP(Hot Standby Router Protocol), STP(Spanning Tree Protocol) 및 CDP(Cisco Discovery Protocol) 트래픽이 아닌 ICMP 트래픽만 볼 수 있습니다.display**-filter는** Wireshark와 동일한 형식을 사용하므로 온라인에서 필터를 찾을 수 있습니다.

```
4500TEST#show monitor capture file bootflash:MYCAP.pcap display-filter "icmp"

 17   4.936999  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=0/0, ttl=255)
 18   4.936999 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=0/0, ttl=251)
 19   4.938007  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=1/256, ttl=255)
 20   4.938007 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=1/256, ttl=251)
```

```
 21   4.938998  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=2/512, ttl=255)
 22   4.938998 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=2/512, ttl=251)
 23   4.938998  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=3/768, ttl=255)
 24   4.940005 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=3/768, ttl=251)
 25   4.942996  14.1.98.144 -> 172.18.108.26 ICMP Echo
      (ping) request  (id=0x0001, seq(be/le)=4/1024, ttl=255)
 26   4.942996 172.18.108.26 -> 14.1.98.144  ICMP Echo
      (ping) reply    (id=0x0001, seq(be/le)=4/1024, ttl=251)
```

7. 파일을 로컬 시스템으로 전송하고 다른 표준 캡처 파일과 마찬가지로 **pcap** 파일을 확인합니다.전송을 완료하려면 다음 명령 중 하나를 입력합니다.

```
4500TEST#copy bootflash: ftp://Username:Password@
```

```
4500TEST#copy bootflash: tftp:
```

8. 캡처를 정리하려면 다음 명령을 사용하여 컨피그레이션을 제거합니다.

```
4500TEST#no monitor capture MYCAP
4500TEST#show monitor capture MYCAP

<no output>

4500TEST#
```

추가 설정

기본적으로 캡처 파일의 크기 제한은 100개 패킷 또는 선형 파일의 60초입니다.크기 제한을 변경하려면 모니터 캡처 구문에서 **limit** 옵션을 사용합니다.

```
4500TEST#monitor cap MYCAP limit ?

duration       Limit total duration of capture in seconds
packet-length  Limit the packet length to capture
packets        Limit number of packets to capture
```

버퍼 최대 크기는 100MB입니다.이는 순환/선형 버퍼 설정과 함께 다음 명령을 사용하여 조정됩니다.

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
size      Size of buffer
```

내장 Wireshark 기능은 올바르게 사용할 경우 매우 강력한 툴입니다.네트워크 문제를 해결할 때 시간과 리소스를 절약합니다.그러나 이 기능을 사용하면 트래픽이 많은 상황에서 CPU 사용률이 증가할 수 있으므로 주의해야 합니다.도구를 구성하지 않고 무인 상태로 둡니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

하드웨어 제한으로 인해 캡처 파일에서 순서가 잘못된 패킷을 받을 수 있습니다.인그레스 및 이그레스 패킷 캡처에 사용되는 별도의 버퍼가 원인입니다.캡처에서 순서가 잘못된 패킷이 있는 경우 두 버퍼를 모두 인그레스로 **설정합니다**.이렇게 하면 버퍼가 처리될 때 인그레스 패킷이 처리되기 전에 이그레스 패킷이 처리되지 않습니다.

순서가 잘못된 패킷이 표시되는 경우 두 인터페이스에서 컨피그레이션을 **둘 다**에서 **in**으로 변경하는 것이 좋습니다.

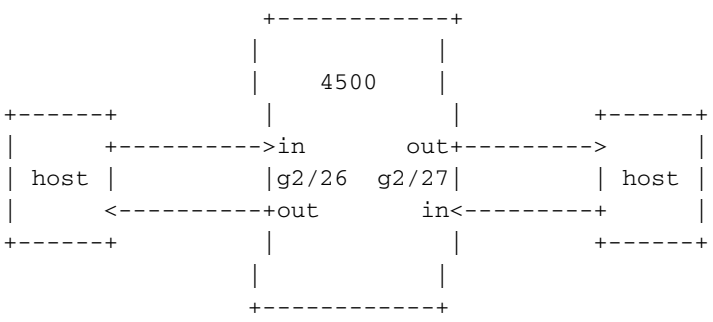
다음은 이전 명령입니다.

```
4500TEST#monitor capture MYCAP interface g2/26 both
```

명령을 다음으로 변경합니다.

```
4500TEST#monitor capture MYCAP interface g2/26 in

4500TEST#monitor capture MYCAP interface g2/27 in
```



관련 정보

- [Catalyst 4500 Series Switch Software 구성 가이드, 릴리스 IOS XE 3.3.0SG 및 IOS 15.1(1)SG - Wireshark 구성]
- [기술 지원 및 문서 – Cisco Systems]