Catalyst 4500 Series switchingvoorbeeld voor configuratie van draadloze functies

Inhoud

Inleiding

Dit document beschrijft hoe u de functie Wireshark voor Cisco Catalyst 4500 Series-switches kunt configureren.

Voorwaarden

Vereisten

U moet aan de volgende voorwaarden voldoen om de functie Wireshark te kunnen gebruiken:

- Het systeem moet gebruik maken van een Cisco Catalyst 4500 Series-switch.
- De schakelaar moet Supervisor Engine 7-E (Supervisor Engine 6 wordt momenteel niet ondersteund) uitvoeren.
- Deze functie moet een ingestelde IP-basis en Enterprise Services hebben (LAN-basis wordt momenteel niet ondersteund).
- De schakelaar CPU kan geen gebruik van een hoge gebruiksconditie hebben, aangezien de functie Wireshark CPU-intensief is en software-schakelaars bepaalde pakketten in het opnameproces veranderen.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Catalyst 4500 Series switches die Supervisor

Engine 7-E uitvoeren.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Cisco Catalyst 4500 Series switches die Supervisor Engine 7-E starten hebben een nieuwe ingebouwde functionaliteit met Cisco IOS?-XE versies 3.3(0)/15.1 of hoger. Deze ingebouwde WinShark-functie heeft de mogelijkheid om pakketten op een manier op te nemen die het traditionele gebruik van Switch Port Analyzer (SPAN) vervangen door een aangesloten pc om pakketten in een scenario voor probleemoplossing op te nemen.

Configureren

Deze sectie fungeert als snelstartgids voor het starten van een opname. De verstrekte informatie is zeer algemeen, en u moet filters en bufferinstellingen zoals nodig uitvoeren om de excessieve vangst van pakketten te beperken als u in een productienetwerk werkt.

Volg deze stappen om de functie Wireshark te configureren:

1. Controleer of u aan de voorwaarden voldoet om de opname te ondersteunen. (referentie de **Vereisten** voor meer informatie .) Voer deze opdrachten in en controleer de uitvoer:

```
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:

    888844444222222222222222333334444422222222222222255555222222
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. Verkeer wordt vanuit poort opgenomen in een TX/RX-richting 02-06-26 in dit voorbeeld . Opslaan van het opnamebestand in een pendop bestandsindeling voor review door een lokale pc, indien nodig:Opmerking: Zorg ervoor dat u de configuratie uitvoert vanuit de EXEC-modus en niet de modus Global Configuration.

```
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. Dit neemt alle ingangen en stress van het verkeer in de poort op g2/26. Het vult het bestand ook zeer snel met nutteloos verkeer in een productiesituatie, tenzij u de richting specificeert en vangfilters toepast om het bereik van het opgenomen verkeer te beperken. Typ deze opdracht om een filter toe te passen:

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

   Opmerking: Dit waarborgt dat u alleen het verkeer Internet Control Message Protocol (ICMP) in uw opnamebestand kunt opnemen.

4. Zodra het opnamebestand is uitgelijnd of het quotum is opgevuld, ontvangt u dit bericht:

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

   Typ deze opdracht om de opname handmatig te stoppen:

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

5. U kunt de opname van de CLI bekijken. Typ deze opdracht om de pakketten te bekijken:

```
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
```

   Opmerking: De detailoptie is aan het einde beschikbaar om het pakket in een Wireless-shark-indeling te bekijken. Bovendien is de optie voor dumpen beschikbaar om de waarde voor Hex van het pakket te zien.

6. Het opnamebestand wordt volledig indien u geen opnamefilter gebruikt wanneer u met de opname begint. Gebruik in dit geval de optie display-filter om het specifieke verkeer in de display weer te geven. U wilt alleen ICMP-verkeer, niet het HSRP-routerprotocol (Hot Standby Router Protocol), Spanning Tree Protocol (STP) en Cisco Discovery Protocol (CDP) bekijken die in de vorige uitvoer worden getoond. Het display-filter gebruikt dezelfde bestandsindeling als Wireshark, zodat u de filters online kunt vinden.

```
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. Breng het bestand over op een lokale machine en kijk naar het pcap-bestand zoals u het andere standaard opnamestation zou bekijken. Voer een van deze opdrachten in om de overdracht te voltooien:

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

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

8. Verwijder de configuratie met deze opdrachten om de opname te reinigen:

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

<no output>

4500TEST#
```

Extra instellingen

De standaardinstelling is dat de grootwetgeving van het opnamebestand 100 pakketten of 60 seconden in een lineair bestand is. Gebruik de **limietoptie** om de grootte te wijzigen in de syntaxis van de monitor-opname:

```
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
```

De maximale buffergrootte is 100 MB. Dit wordt aangepast, evenals de circulaire/lineaire bufferinstelling, met deze opdracht:

```
4500TEST#monitor cap MYCAP buffer ?
```

```
circular  circular buffer
size      Size of buffer
```

De ingebouwde Wireshark optie is een zeer krachtig gereedschap indien correct gebruikt. Het bespaart tijd en middelen wanneer u een netwerk problemen oplossen. Wees echter voorzichtig met het gebruik van de functie, omdat het CPU-gebruik in situaties met veel verkeer kan verhogen. Configureer het gereedschap nooit en laat het los.

Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Vanwege hardwarebeperkingen kunt u out-of-order pakketten in het opnamebestand ontvangen. Dit is te wijten aan de afzonderlijke buffers die gebruikt worden voor het inloggen en strikken van het pakket. Als u niet-bestelde pakketten in uw opname hebt, stel beide buffers dan in op **inslag**. Dit voorkomt dat de pakketten in nood worden verwerkt voordat de ingangspakketten worden verzonden wanneer de buffer wordt verwerkt.

Als u out-of-order pakketten ziet, wordt geadviseerd om uw configuratie van **beide** in op beide interfaces te wijzigen.

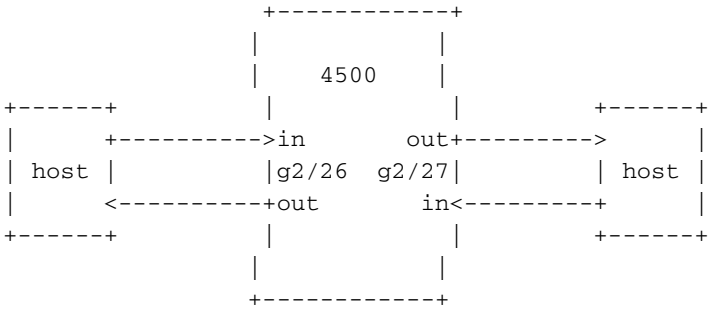
Dit is de vorige opdracht:

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

Wijzig de opdracht in deze:

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

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



Gerelateerde informatie

- [Software voor Catalyst 4500 Series switchinggids, release IOS XE 3.3.0SG en IOS 15.1(1)SG - Wireshark configureren]

- Technische ondersteuning en documentatie – Cisco Systems