Esempio di configurazione degli switch Catalyst serie 4500 Wireshark

Sommario

Introduzione

In questo documento viene descritto come configurare la funzione Wireshark per gli switch Cisco Catalyst serie 4500.

Prerequisiti

Requisiti

Per utilizzare la funzione Wireshark, è necessario che siano soddisfatte le seguenti condizioni:

- Il sistema deve utilizzare uno switch Cisco Catalyst serie 4500.
- Lo switch deve eseguire Supervisor Engine 7-E (al momento Supervisor Engine 6 non è supportato).
- La funzionalità deve disporre di un set IP Base e di servizi aziendali (LAN Base non è attualmente supportata).
- La CPU dello switch non può avere una condizione di utilizzo elevato, in quanto la funzione Wireshark richiede un uso intensivo della CPU e commuta il software su determinati pacchetti nel processo di acquisizione.

Componenti usati

Per la stesura del documento, sono stati usati switch Cisco Catalyst serie 4500 con Supervisor

Engine 7-E.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Gli switch Cisco Catalyst serie 4500 con Supervisor Engine 7-E dispongono di una nuova funzionalità integrata con Cisco IOS?-XE versioni 3.3(0) / 151.1 o successive. Questa funzione Wireshark integrata è in grado di acquisire i pacchetti in modo da sostituire l'uso tradizionale dello Switch Port Analyzer (SPAN) con un PC collegato in modo da acquisire i pacchetti in uno scenario di risoluzione dei problemi.

Configurazione

Questa sezione funge da guida introduttiva per avviare l'acquisizione. Le informazioni fornite sono molto generiche ed è necessario implementare i filtri e le impostazioni del buffer necessarie per limitare l'eccessiva acquisizione dei pacchetti se si opera in una rete di produzione.

Per configurare la funzione Wireshark, completare la procedura seguente:

1. Verificare che siano soddisfatte le condizioni per il supporto dell'acquisizione. (Fare riferimento alla **Requisiti** per ulteriori dettagli.) Immettere questi comandi e verificare l'output:

```
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:

    888844444222222222222223333344444222222222222222255555222222
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. Il traffico viene acquisito in direzione TX/RX dalla porta **gig2/26** in questo esempio. Memorizzare il file di acquisizione su bootflash in una **pcap** formato di file per la revisione da un PC locale, se necessario:**Nota:** Verificare di eseguire la configurazione in modalità di esecuzione **utente**, non in modalità di **configurazione globale**.

```
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. Cattura tutto il traffico in entrata e in uscita sulla porta **g2/26**. Inoltre, riempie il file molto rapidamente con traffico inutile in una situazione di produzione, a meno che non si specifichi la direzione e si applichino i filtri di acquisizione per limitare l'ambito del traffico acquisito. Per applicare un filtro, immettere questo comando:

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

Nota: In questo modo si garantisce di acquisire solo il traffico ICMP (Internet Control Message Protocol) nel file di acquisizione.

4. Una volta scaduto il timeout del file di acquisizione o raggiunta la quota delle dimensioni, viene visualizzato questo messaggio:

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

Immettere questo comando per interrompere manualmente l'acquisizione:

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

5. èpossibile visualizzare l'acquisizione dalla CLI. Immettere questo comando per visualizzare i pacchetti:

```
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
```

Nota: L'opzione detail è disponibile alla fine per visualizzare il pacchetto in formato Wireshark. Inoltre, è possibile usare l'opzione dump per verificare il valore Hex del pacchetto.

6. Se non si utilizza un filtro di acquisizione quando si inizia l'acquisizione, il file di acquisizione diventa irregolare. In questo caso, usare l'opzione **display-filter** per visualizzare il traffico specifico sul display. Si desidera visualizzare solo il traffico ICMP, non il traffico HSRP (Hot Standby Router Protocol), STP (Spanning Tree Protocol) e CDP (Cisco Discovery Protocol), come mostrato nell'output precedente. Il **filtro-visualizzazione** utilizza lo stesso formato di Wireshark, quindi è possibile trovare i filtri online.

```
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. Trasferite il file su un computer locale e osservate il file **pcap** come un qualsiasi altro file di acquisizione standard. Per completare il trasferimento, immettere uno dei seguenti comandi:

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

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

8. Per pulire l'acquisizione, rimuovere la configurazione con questi comandi:

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

<no output>

4500TEST#
```

Impostazioni aggiuntive

Per impostazione predefinita, le dimensioni massime del file di acquisizione sono di 100 pacchetti, ovvero 60 secondi in un file lineare. Per modificare il limite delle dimensioni, utilizzare l'opzione **limit** nella sintassi di acquisizione del monitor:

```
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
```

La dimensione massima del buffer è 100 MB. Questo viene regolato, così come l'impostazione del buffer circolare/lineare, con questo comando:

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

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

La feature Wireshark incorporata è uno strumento molto potente se utilizzato correttamente. Consente di risparmiare tempo e risorse quando si esegue la risoluzione dei problemi di rete. Tuttavia, prestare attenzione quando si utilizza la funzione, in quanto potrebbe aumentare l'utilizzo della CPU in situazioni di traffico elevato. Non configurare mai lo strumento e lasciarlo incustodito.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

A causa delle limitazioni hardware, è possibile che si ricevano pacchetti non ordinati nel file di acquisizione. Ciò è dovuto ai buffer separati utilizzati per le acquisizioni dei pacchetti in entrata e in uscita. Se nell'acquisizione sono presenti pacchetti non ordinati, impostare entrambi i buffer su **In entrata**. In questo modo, i pacchetti in uscita non verranno elaborati prima dei pacchetti in entrata quando il buffer viene elaborato.

Se vengono visualizzati pacchetti non ordinati, si consiglia di modificare la configurazione da **entrambe** a **in** entrambe le interfacce.

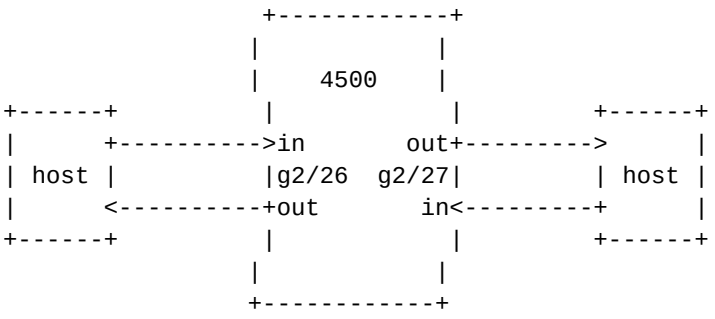
Di seguito è riportato il comando precedente:

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

Modificare il comando come segue:

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

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



Informazioni correlate

- [Guida alla configurazione del software degli switch Catalyst serie 4500, IOS XE 3.3.0SG e

IOS 15.1(1)SG - Configurazione di Wireshark

- Documentazione e supporto tecnico – Cisco Systems