Ejemplo de configuración de la característica de Wireshark de los Catalyst 4500 Series Switch

Contenido

Introducción

Este documento describe cómo configurar la característica de Wireshark para los Cisco Catalyst 4500 Series Switch.

Prerequisites

Requisitos

Para utilizar la característica de Wireshark, usted debe cumplir estas condiciones:

- El sistema debe utilizar un Cisco Catalyst 4500 Series Switch.
- El Switch debe ejecutar el Supervisor Engine 7-E (el Supervisor Engine 6 está sin apoyo ahora).
- La característica debe tener una base IP del conjunto y los Enterprise Service (la base LAN está sin apoyo ahora).
- El Switch CPU no puede tener una condición de la utilización intensa, pues la característica de Wireshark es ciertos paquetes Uso intensivos de la CPU y de los switches del software en el proceso de la captura.

Componentes Utilizados

La información en este documento se basa en los Cisco Catalyst 4500 Series Switch que ejecutan

el Supervisor Engine 7-E.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

¿Los Cisco Catalyst 4500 Series Switch que ejecutan el Supervisor Engine 7-E tienen las nuevas funciones incorporadas con el Cisco IOS? - Versiones XE 3.3(0)/151.1 o más adelante. Esta característica de Wireshark del accesorio tiene la capacidad de capturar los paquetes de una manera que substituya el uso tradicional del (SPAN) del analizador de puertos del switch por un PC asociado para capturar los paquetes en un escenario de Troubleshooting.

Configurar

Esta sección sirve como guía de inicio rápido para comenzar una captura. La información proporcionada es muy general, y usted debe implementar los filtros y las configuraciones del buffer como necesario para limitar la captura excesiva de los paquetes si usted actúa en una red de producción.

Complete estos pasos para configurar la característica de Wireshark:

1. Verifique que usted cumpla las condiciones para soportar la captura. (Refiérase a la sección de los **requisitos** para más detalles.) Ingrese estos comandos y verifique la salida:

```
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. El tráfico se captura en una dirección del TX/RX del puerto **gig2/26** en este ejemplo. Salve el capturar archivo en el bootflash en un formato de archivo del **pcap** para el estudio de a PC local, en caso necesario:**Note**: Asegúrese de que usted realizan la configuración del **modo EXEC de usuario**, no **modo de configuración global**.

```
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. Esto captura todo el ingreso y salida del tráfico en el puerto **g2/26**. También llena el archivo muy rápidamente del tráfico inútil en una situación de producción, a menos que usted especifique la dirección y aplique los filtros de la captura para estrechar el alcance del tráfico se captura que. Ingrese este comando para aplicar un filtro:

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

Note: Esto se asegura de que usted capture solamente el tráfico del Internet Control Message Protocol (ICMP) en su capturar archivo.

4. Una vez que los descansos del capturar archivo, o llenan la cuota del tamaño, usted reciben este mensaje:

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

Ingrese este comando para parar manualmente la captura:

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

5. Usted puede ver la captura del CLI. Ingrese este comando para ver los paquetes:

```
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
```

Note: La opción del detalle está disponible en el extremo para ver el paquete en un formato de Wireshark. También, la opción del volcado está disponible para considerar el valor hex del paquete.

6. El capturar archivo se estorba si usted no utiliza un captura-filtro cuando usted comienza la captura. En este caso, utilice la opción del visualización-**filtro** para mostrar el tráfico específico en la visualización. Usted quiere solamente ver el tráfico ICMP, el tráfico no del Hot Standby Router Protocol (HSRP), del Spanning Tree Protocol (STP), y del Cisco Discovery Protocol (CDP) mostrado en la salida anterior. **El visualización-filtro** utiliza el mismo formato que Wireshark, así que usted puede encontrar el filtersonline.

```
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. Transferencia el archivo a una máquina local, y mirada en el archivo del **pcap** como usted cualquier otro capturar archivo estándar. Ingrese uno de estos comandos para completar la transferencia:

```
4500TEST#copy bootflash: ftp://Username:Password@<ftp server address>
4500TEST#copy bootflash: tftp:
```

8. Para limpiar la captura, quite la configuración con estos comandos:

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

<no output>

4500TEST#
```

Configuraciones adicionales

Por abandono, el límite de tamaño del capturar archivo es 100 paquetes, o 60 segundos en un archivo Lineal. Para cambiar el límite de tamaño, utilice la opción del **límite** en el sintaxis de la captura 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
```

El tamaño máximo del buffer es 100 MB. Se ajusta esto, así como la configuración circular/Lineal del buffer, con este comando:

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
size      Size of buffer
```

La característica de Wireshark del accesorio es una herramienta muy potente si está utilizada correctamente. Guarda el tiempo y los recursos cuando usted resuelve problemas una red. Sin embargo, precaución del ejercicio cuando usted utiliza la característica, porque puede ser que aumente la utilización de la CPU en las situaciones del mucho tráfico. Nunca configure la herramienta y déjela desatendida.

Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

Debido a las limitaciones del hardware, usted puede ser que reciba los paquetes defectuosos en el capturar archivo. Esto es debido a los buffers separados usados para las capturas del ingreso y del paquete de egreso. Si usted tiene paquetes defectuosos en su captura, fije ambos de sus buffers al **ingreso**. Esto evita que los paquetes en la salida procesen antes de los paquetes de ingreso cuando se procesa el buffer.

Si usted ve los paquetes defectuosos, se recomienda que usted cambia su configuración de **ambos** a **adentro** en ambas interfaces.

Aquí está el comando anterior:

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

Cambie el comando a éstos:

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

4500TEST#monitor capture MYCAP interface g2/27 in

4500TEST#monitor capture MYCAP interface g2/26 in

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

Información Relacionada

- IOS XE 3.3.0SG de la guía de configuración de software, de la versión del Catalyst 4500 Series Switch y IOS 15.1(1)SG - configurar Wireshark
- Soporte Técnico y Documentación - Cisco Systems