Ejemplo de Configuración de la Función Wireshark de Catalyst 4500 Series Switches

Contenido

Introducción

Este documento describe cómo configurar la función Wireshark para los switches Catalyst de Cisco serie 4500.

Prerequisites

Requirements

Para utilizar la función Wireshark, debe cumplir estas condiciones:

- El sistema debe utilizar un switch Catalyst de Cisco serie 4500.
- El switch debe ejecutar Supervisor Engine 7-E (el Supervisor Engine 6 no es compatible en este momento).
- La función debe tener un conjunto de servicios empresariales y de base IP (la base LAN no se admite en este momento).
- La CPU del switch no puede tener una condición de alta utilización, ya que la función Wireshark es intensiva en la CPU y el software conmuta ciertos paquetes en el proceso de captura.

Componentes Utilizados

La información de este documento se basa en los switches Catalyst de Cisco serie 4500 que

ejecutan Supervisor Engine 7-E.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

Los switches Catalyst de Cisco serie 4500 que ejecutan Supervisor Engine 7-E tienen una nueva funcionalidad integrada con Cisco IOS?-XE versiones 3.3(0) / 151.1 o posterior. Esta función de Wireshark integrada tiene la capacidad de capturar paquetes de una manera que reemplace el uso tradicional del analizador de puertos de switch (SPAN) por un PC conectado para capturar paquetes en un escenario de solución de problemas.

Configurar

Esta sección sirve como guía de inicio rápido para iniciar una captura. La información proporcionada es muy general, y debe implementar filtros y configuraciones de búfer según sea necesario para limitar la captura excesiva de paquetes si opera en una red de producción.

Complete estos pasos para configurar la función Wireshark:

1. Verifique que cumple con las condiciones para soportar la captura. (Referencia al **Requirements** para obtener más información.) Ingrese estos comandos y verifique el resultado:

```
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. El tráfico se captura en una dirección TX/RX del puerto **gig2/26** en este ejemplo. Almacenar el archivo de captura en bootflash en un **pcap** formato de archivo para su revisión desde un PC local, si es necesario:**Nota:** Asegúrese de realizar la configuración desde el modo **EXEC del usuario, no desde el modo 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 tráfico de entrada y salida en el puerto **g2/26**. También llena el archivo muy rápidamente con tráfico inútil en una situación de producción, a menos que especifique la dirección y aplique filtros de captura para limitar el alcance del tráfico capturado. Ingrese este comando para aplicar un filtro:

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

Nota: Esto garantiza que sólo se captura el tráfico ICMP (Internet Control Message Protocol) en el archivo de captura.

4. Una vez que el archivo de captura se agota o llena la cuota de tamaño, recibe este mensaje:

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

Ingrese este comando para detener manualmente la captura:

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

5. Puede ver la captura desde la 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
```

Nota: La opción de detalle está disponible al final para ver el paquete en un formato Wireshark. Además, la opción de volcado está disponible para ver el valor hexadecimal del paquete.

6. El archivo de captura se agrupará si no utiliza un filtro de captura al iniciar la captura. En este caso, utilice la opción **display-filter** para mostrar tráfico específico en la pantalla. Sólo desea ver el tráfico ICMP, no el tráfico de protocolo de router en espera en caliente (HSRP), el protocolo de árbol de extensión (STP) y el protocolo de detección de Cisco (CDP) que se muestran en la salida anterior. El **filtro-pantalla** utiliza el mismo formato que Wireshark, por lo que puede encontrar la línea de filtro.

```
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. Transfiera el archivo a un equipo local y observe el archivo **pcap** como lo haría con cualquier otro archivo de captura estándar. Ingrese uno de estos comandos para completar la transferencia:

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

```
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#
```

Configuración adicional

De forma predeterminada, el límite de tamaño del archivo de captura es de 100 paquetes, o 60 segundos en un archivo lineal. Para cambiar el límite de tamaño, utilice la opción **limit** en la sintaxis de captura de 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 búfer es de 100 MB. Esto se ajusta, así como la configuración del búfer circular/lineal, con este comando:

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

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

La función Wireshark integrada es una herramienta muy potente si se utiliza correctamente. Ahorra tiempo y recursos al resolver problemas de una red. Sin embargo, tenga cuidado al utilizar la función, ya que podría aumentar la utilización de la CPU en situaciones de tráfico alto. Nunca configure la herramienta y déjela desatendida.

Verificación

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

Troubleshoot

Debido a las limitaciones de hardware, es posible que reciba paquetes despedidos en el archivo de captura. Esto se debe a las memorias intermedias separadas utilizadas para las capturas de paquetes de ingreso y egreso. Si tiene paquetes fuera de servicio en su captura, configure ambos búfers en **ingreso**. Esto evita que los paquetes de salida se procesen antes de los paquetes de ingreso cuando se procesa el búfer.

Si ve paquetes fuera de servicio, se recomienda cambiar la configuración de **ambos** a **dentro** en ambas interfaces.

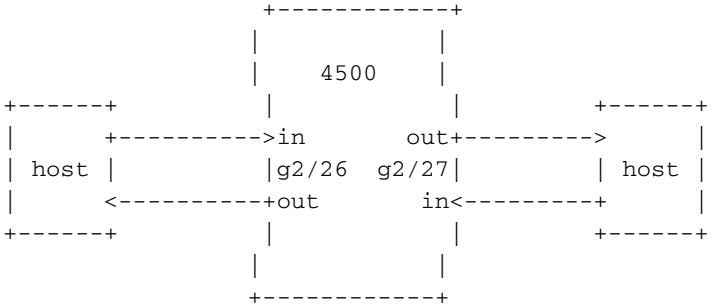
Este es el comando anterior:

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

Cambie el comando a lo siguiente:

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

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



Información Relacionada

- [Guía de Configuración de Catalyst 4500 Series Switch Software, Versión IOS XE 3.3.0SG e IOS 15.1(1)SG - Configuración de Wireshark]

- Soporte Técnico y Documentación - Cisco Systems