Exemplo de configuração da característica de Wireshark dos Catalyst 4500 Series Switch

Índice

Introdução

Este documento descreve como configurar a característica de Wireshark para Cisco Catalyst 4500 Series Switch.

Pré-requisitos

Requisitos

A fim utilizar a característica de Wireshark, você deve estar conformes estas circunstâncias:

- O sistema deve utilizar um Cisco Catalyst 4500 Series Switch.
- O interruptor deve executar o Supervisor Engine 7-E (o Supervisor Engine 6 é unsupported neste tempo).
- A característica deve ter uma base IP do grupo e serviços de empreendimento (a base LAN é unsupported neste tempo).
- O interruptor CPU não pode ter uma condição da utilização elevada, porque a característica de Wireshark é determinados pacotes do processo intensivo de cpu e dos switch de software no processo da captação.

Componentes Utilizados

A informação neste documento é baseada nos Cisco Catalyst 4500 Series Switch que executam o

Supervisor Engine 7-E.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Os Cisco Catalyst 4500 Series Switch que executam o Supervisor Engine 7-E têm uma funcionalidade incorporado nova com Cisco IOS? - Versões 3.3(0) XE/151.1 ou mais atrasado. Esta característica de Wireshark do acessório tem a capacidade para capturar pacotes em uma maneira que substitua o uso tradicional do analisador de porta de switch (PERÍODO) com um PC anexado a fim capturar pacotes em um scenario de Troubleshooting.

Configurar

Esta seção serve como um guia de início rápido a fim começar uma captação. A informação fornecida é muito geral, e você deve executar filtros e ajustes do buffer como necessário a fim limitar a captação excessiva dos pacotes se você se opera em uma rede de produção.

Termine estas etapas a fim configurar a característica de Wireshark:

1. Verifique que você está conformes as circunstâncias a fim apoiar a captação. (Proveja a seção das **exigências** para mais detalhes.) Incorpore estes comandos e verifique a saída:

```
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. O tráfego é capturado em um sentido TX/RX da porta **gig2/26 n**este exemplo. Armazene o arquivo de captura no bootflash em um formato do arquivo do **pcap** para a revisão de um PC local, caso necessário:**Note**: Assegure-se de que você executem a configuração do **modo exec de usuário**, não **modo de configuração 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. Isto captura todo o ingresso e saída do tráfego na porta **g2/26**. Igualmente enche o arquivo muito rapidamente com o tráfego inútil em uma situação de produção, a menos que você especificar o sentido e aplicar filtros da captação a fim reduzir o espaço do tráfego que está capturado. Incorpore este comando a fim aplicar um filtro:

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

Note: Isto assegura-se de que você capture somente o tráfego do Internet Control Message Protocol (ICMP) em seu arquivo de captura.

4. Uma vez que os intervalos do arquivo de captura, ou enchem a quota do tamanho, você recebem esta mensagem:

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

Incorpore este comando a fim parar manualmente a captação:

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

5. Você pode ver a captação do CLI. Incorpore este comando a fim ver os pacotes:

```
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: A opção do detalhe está disponível na extremidade a fim ver o pacote em um formato de Wireshark. Também, a opção da descarga está disponível a fim considerar o valor de HEX do pacote.

6. O arquivo de captura torna-se desordenado se você não usa um captação-filtro quando você começa a captação. Neste caso, utilize a opção do indicador-**filtro** a fim mostrar o tráfego específico no indicador. Você quer somente ver o tráfego ICMP, o tráfego não do Hot Standby Router Protocol (HSRP), do Spanning Tree Protocol (STP), e do Cisco Discovery Protocol (CDP) mostrado na saída precedente. **O indicador-filtro** usa o mesmo formato que Wireshark, assim que você pode encontrar o 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. Transfira o arquivo a uma máquina local, e olhe o arquivo do **pcap** como você todo o outro arquivo de captura padrão. Incorpore um destes comandos a fim terminar transferência:

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

8. A fim limpar a captação, remova a configuração com estes comandos:

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

<no output>

4500TEST#
```

Ajustes adicionais

Àrevelia, o limite de tamanho do arquivo de captura é 100 pacotes, ou 60 segundos em um arquivo Linear. A fim mudar o limite de tamanho, use a opção do **limite na** sintaxe da captação do 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
```

O tamanho máximo do buffer é 100 MB. Isto é ajustado, assim como ajuste circular/Linear do buffer, com este comando:

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
size      Size of buffer
```

A característica de Wireshark do acessório é uma ferramenta muito poderosa se usada corretamente. Salvar o tempo e os recursos quando você pesquisa defeitos uma rede. Contudo,

cuidado do exercício quando você utilizar a característica, porque pôde aumentar a utilização CPU em situações do tráfego elevado. Nunca configurar a ferramenta e deixe-a desacompanhada.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Devido às limitações do hardware, você pôde receber pacotes estragados no arquivo de captura. Isto é devido aos bufferes separados usados para as captações do ingresso e do pacote de saída. Se você tem pacotes estragados em sua captação, ajuste ambos seus bufferes ao **ingresso**. Isto impede que os pacotes na saída processem antes dos pacotes de ingresso quando o buffer é processado.

Se você vê pacotes estragados, recomenda-se que você muda sua configuração de **ambos** a **dentro em** ambas as relações.

Está aqui o comando precedente:

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

Mude o comando a estes:

```
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
```

Informações Relacionadas

- Manual de configuração do software do Catalyst 4500 Series Switch, liberação IO XE 3.3.0SG e IO 15.1(1)SG - configurando Wireshark
- Suporte Técnico e Documentação - Cisco Systems