Exemplo de Configuração do Recurso Wireshark dos Switches Catalyst 4500 Series

Contents

Introduction

Este documento descreve como configurar o recurso Wireshark para os switches Cisco Catalyst 4500 Series.

Prerequisites

Requirements

Para utilizar o recurso Wireshark, você deve atender às seguintes condições:

- O sistema deve utilizar um switch Cisco Catalyst 4500 Series.
- O switch deve executar o Supervisor Engine 7-E (o Supervisor Engine 6 não é suportado neste momento).
- O recurso deve ter uma base IP definida e serviços empresariais (a base LAN não é suportada no momento).
- A CPU do switch não pode ter uma condição de alta utilização, pois o recurso Wireshark é intensivo para a CPU e os switches de software de determinados pacotes no processo de captura.

Componentes Utilizados

As informações neste documento são baseadas nos switches Cisco Catalyst 4500 Series que

executam o 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.

Informações de Apoio

Os switches Cisco Catalyst 4500 Series que executam o Supervisor Engine 7-E têm uma nova funcionalidade integrada com o Cisco IOS?-XE versões 3.3(0) / 151.1 ou posterior. Esse recurso integrado do Wireshark tem a capacidade de capturar pacotes de uma forma que substitui o uso tradicional do Switch Port Analyzer (SPAN) por um PC conectado para capturar pacotes em um cenário de solução de problemas.

Configurar

Esta seção serve como um guia de início rápido para iniciar uma captura. As informações fornecidas são muito gerais e você deve implementar filtros e configurações de buffer conforme necessário para limitar a captura excessiva de pacotes se operar em uma rede de produção.

Conclua estes passos para configurar o recurso Wireshark:

1. Verifique se você atende às condições para suportar a captura. (Consulte o **Requirements** para obter mais detalhes.) Digite 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:

    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. O tráfego é capturado em uma direção TX/RX a partir da porta **gig2/26** neste exemplo. Armazenar o arquivo de captura em flash de inicialização em um **tampa** formato de arquivo para revisão a partir de um PC local, se necessário:**Note**: Certifique-se de executar a configuração no modo **EXEC do usuário**, não no modo **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. Isso captura toda a entrada e saída de tráfego na porta **g2/26**. Ele também preenche o arquivo muito rapidamente com tráfego inútil em uma situação de produção, a menos que você especifique a direção e aplique filtros de captura para restringir o escopo do tráfego capturado. Insira este comando para aplicar um filtro:

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

Note: Isso garante que você capture somente o tráfego do Internet Control Message Protocol (ICMP) em seu arquivo de captura.

4. Quando o tempo limite do arquivo de captura expirar ou preencher a cota de tamanho, você receberá esta mensagem:

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

Insira este comando para interromper manualmente a captura:

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

5. Você pode visualizar a captura da CLI. Insira este comando para visualizar 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 detail está disponível no final para visualizar o pacote em um formato Wireshark. Além disso, a opção de despejo está disponível para ver o valor Hex do pacote.

6. O arquivo de captura ficará desordenado se você não usar um filtro de captura ao iniciar a captura. Nesse caso, utilize a opção **display-filter** para mostrar o tráfego específico na tela. Você só quer ver o tráfego ICMP, não o Hot Standby Router Protocol (HSRP), o Spanning Tree Protocol (STP) e o tráfego do Cisco Discovery Protocol (CDP) mostrado na saída anterior. O **filtro de exibição** usa o mesmo formato que o Wireshark, para que você possa encontrar a linha 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. Transfira o arquivo para uma máquina local e examine o arquivo **pcap** como faria com qualquer outro arquivo de captura padrão. Insira um destes comandos para concluir a transferência:

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

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

8. Para limpar a captura, remova a configuração com estes comandos:

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

<no output>

4500TEST#
```

Configurações adicionais

Por padrão, o limite de tamanho do arquivo de captura é de 100 pacotes, ou 60 segundos em um arquivo linear. Para alterar o limite de tamanho, use a opção **limit** na sintaxe de captura 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. Isso é ajustado, assim como a configuração de buffer circular/linear, com este comando:

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
```

```
size      Size of buffer
```

O recurso Wireshark integrado é uma ferramenta muito poderosa se usada corretamente. Ele economiza tempo e recursos ao solucionar problemas de uma rede. No entanto, tenha cuidado ao utilizar o recurso, pois ele pode aumentar a utilização da CPU em situações de alto tráfego. Nunca configure a ferramenta e deixe-a autônoma.

Verificar

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

Troubleshoot

Devido a limitações de hardware, você pode receber pacotes fora de ordem no arquivo de captura. Isso se deve aos buffers separados usados para as capturas de pacotes de entrada e saída. Se você tiver pacotes fora de ordem na sua captura, defina ambos os buffers como **ingresso**. Isso impede que os pacotes em saída processem antes dos pacotes de entrada quando o buffer é processado.

Se você vir pacotes fora de ordem, é recomendável alterar sua configuração de **ambos** para **dentro** em ambas as interfaces.

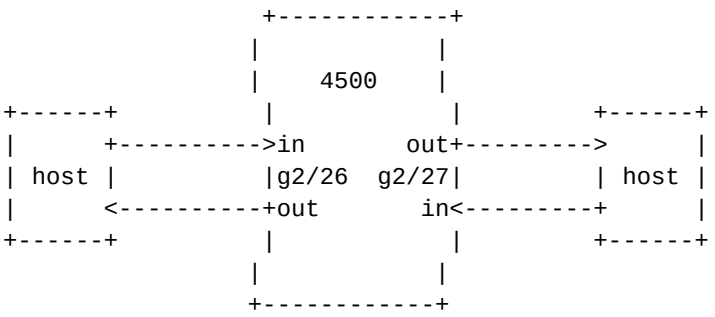
Aqui está o comando anterior:

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

Altere o comando para estes:

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

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



Informações Relacionadas

- [Guia de Configuração do Software do Switch Catalyst 4500 Series, Release IOS XE 3.3.0SG e IOS 15.1(1)SG - Configuração do Wireshark]
- [Suporte Técnico e Documentação - Cisco Systems]