Catalyst 4500系列交换机Wireshark功能配置示例

目录

简介

本文档介绍如何为Cisco Catalyst 4500系列交换机配置Wireshark功能。

先决条件

要求

要使用Wireshark功能，必须满足以下条件：

- 系统必须使用Cisco Catalyst 4500系列交换机。
- 交换机必须运行Supervisor引擎7-E（目前不支持Supervisor引擎6）。
- 该功能必须具有集IP Base和企业服务（目前不支持LAN Base）。
- 交换机CPU不能具有高利用率条件，因为Wireshark功能是CPU密集型功能，并且软件在捕获过程中交换某些数据包。

使用的组件

本文档中的信息基于运行Supervisor引擎7-E的Cisco Catalyst 4500系列交换机。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

运行管理引擎7-E的Cisco Catalyst 4500系列交换机具有Cisco IOS? -XE 3.3(0)/ 151.1或更高版本的新内置功能。此内置的Wireshark功能能够以一种方式捕获数据包，即用连接的PC取代传统的交换机端口分析器(SPAN)，以便在故障排除场景中捕获数据包。

配置

本部分是开始捕获的快速入门指南。提供的信息非常一般，并且必须根据需要实施过滤器和缓冲区设置，以限制在生产网络中运行时对数据包的过度捕获。

要配置Wireshark功能，请完成以下步骤：

1. 验证您是否满足条件以支持捕获。(参考 **要求** 部分了解详细信息。) 输入以下命令并检验输出：

```
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. 从端口以TX/RX方向捕获流量 gig 2/26 在本例中。将捕获文件存储在Bootflash上 PCAP 文件格式，以便从本地PC查看（如果需要）：**注意：**确保从用户执行模式而**不是全**局配置模**式执行**配置。

```
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. 这将捕获端口上的所有流量入口和出口 g 2/26。除非您指定方向并应用捕获过滤器以缩小捕获的流量范围，否则它还会在生产情况下使用无用流量快速填充文件。输入以下命令以应用过滤器：

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

注意：这可确保您仅捕获捕获文件中的互联网控制消息协议(ICMP)流量。

4. 捕获文件超时或填满大小配额后，您将收到以下消息：

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

输入以下命令以手动停止捕获：

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

5. 您可以从CLI查看捕获。输入以下命令以查看数据包：

```
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
```

注意：详细信息选项在结尾处可用，以便以Wireshark格式查看数据包。此外，dump选项也可用，以查看数据包的十六进制值。

6. 如果在开始捕获时不使用捕获过滤器，捕获文件将变得混乱。在这种情况下，请使用**display-filter**选项以在显示中显示特定流量。您只想查看ICMP流量，而不是前面输出中显示的热备份路由器协议(HSRP)、生成树协议(STP)和思科发现协议(CDP)流量。显示**过滤器**使用与Wireshark相同的格式，因此您可以在线查找过滤器。

```
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. 将文件传输到本地计算机，并像查看任何其他标准捕获文件一样查看**pcap文件。**输入以下命令之一以完成传输：

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

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

8. 要清除捕获，请使用以下命令删除配置：

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

<no output>

4500TEST#
```

其他设置

默认情况下，捕获文件的大小限制为100个数据包，或线性文件中的60秒。要更改大小限制，请使用监控器捕获语法中的**limit**选项：

```
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
```

缓冲区最大大小为100 MB。此命令将调整此值以及循环/线性缓冲区设置：

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
size      Size of buffer
```

如果正确使用，内置的Wireshark功能是非常强大的工具。当您排除网络故障时，它可节省时间和资源。但是，在使用该功能时请谨慎，因为它可能会在高流量情况下提高CPU利用率。切勿配置工具并使其无人值守。

验证

当前没有可用于此配置的验证过程。

故障排除

由于硬件限制，您可能会在捕获文件中收到无序数据包。这是由于用于入口和出口数据包捕获的单独缓冲区所致。如果捕获中有无序数据包，请将两个缓冲区设置为**入口**。这可防止在缓冲区处理后，在入口数据包之前处理出口数据包。

如果您看到无序数据包，建议您在两个接口上将配置从**两**者**更改**为in。

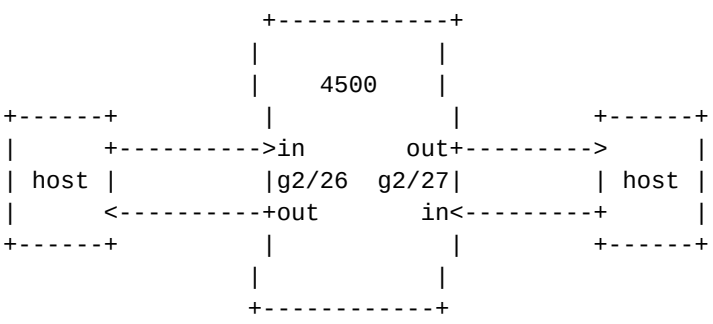
以下是上一个命令：

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

将命令更改为：

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

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



相关信息

- Catalyst 4500系列交换机软件配置指南，版本IOS XE 3.3.0SG和IOS 15.1(1)SG — 配置 Wireshark
- 技术支持和文档 - Cisco Systems