Catalyst 4500系列交换机Wireshark功能配置示例

目录

简介

本文描述如何配置Cisco Catalyst 4500系列交换机的Wireshark功能。

先决条件

要求

为了使用Wireshark功能，您必须符合这些情况：

- 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 (Supervisor引擎6此时是不支持的)。
- 功能必须有集合IP BASE和企业服务(LAN基础此时是不支持的)。
- 因为Wireshark功能是在捕获进程的CPU密集型和软件交换机某些数据包交换机CPU不能有高利用率情况。

使用的组件

本文档中的信息根据运行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Supervisor引擎7-E的Cisco Catalyst 4500系列交换机有与Cisco IOS的一个新的内置的功能？-XE版本3.3(0)/151.1或以上。此内置的Wireshark功能有能力获取数据包用替换传统使用交换机端口分析程序的方法(SPAN)用附加的PC为了获取在故障排除情况的数据包。

配置

此部分担当快速入门指南为了开始捕获。被提供的信息非常一般，并且您必须实现过滤器和缓冲区设置当必要时为了限制数据包额外的捕获，如果在生产网络经营。

完成这些步骤为了配置Wireshark功能：

1. 验证您符合条件为了支持捕获。欲了解更详细的信息(请参考**Requirements部分**。)输入这些命令并且验证输出：

```
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. 流量在从端口**gig2/26的**一个TX/RX方向捕获在本例中。存储在Bootflash的捕获文件在复核的一种**pcap**文件格式从本地PC，如果需要，：**Note**:保证您执行从**用户EXEC模式的**配置，不是**全局配置模式**。

```
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. 这捕获所有流量入口和出口在端口g2/26。它用在生产情况的无用的流量非常迅速也填装文件，除非指定方向并且应用捕获过滤器为了缩小捕获流量的范围。输入此命令为了应用过滤器：

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

Note:这保证您只捕获在您的捕获文件的互联网控制消息协议(ICMP)流量。

4. 一旦捕获文件暂停或者填装大小配额，您收到此消息：

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

输入此命令为了手工终止捕获：

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

5. 您能查看从CLI的捕获。输入此命令为了显示数据包：

```
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
```

Note:详细信息选项是可用在末端为了显示在Wireshark格式的数据包。并且，转储选项是可用为了发现数据包的十六进制值。

6. 捕获文件变得凌乱，如果不使用一个捕获过滤器，当您开始捕获时。在这种情况下，请使用显示**过滤器**选项为了显示在显示的特定的流量。您只要查看ICMP流量，不是热备份路由协议(HSRP)，在上一个输出中显示的生成树协议和思科设备发现协议(CDP)流量。**显示过滤器**使用格式和Wireshark一样，因此您能找到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. 转接文件到本地设备，并且查看pcap文件，您会其他标准的捕获文件。输入这些命令之一为了完成转移：

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

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

8. 为了整理捕获，请删除配置用这些命令：

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

<no output>

4500TEST#
```

另外的设置

默认情况下，捕获文件的大小限制是100数据包或者60秒在一个线性文件。为了更改大小限制，请使用**限制**选项在监视器捕获语法：

```
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
```

缓冲区最大大小是100 MB。这调节，以及圆/线性缓冲区设置，用此命令：

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
size      Size of buffer
```

若被采用内置的Wireshark功能正确地是一个非常强大的工具。当您排除故障网络时，它节约时间和资源。然而，练习小心，当您使用功能，因为也许增加在高数据流情况的CPU利用率。请勿配置工具并且不看管它。

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，您也许收到在捕获文件的无序信息包。这归结于用于入口和出口数据包捕获的独立的缓冲区。如果有无序信息包在您的捕获，设置两个您的缓冲区为**入口**。当缓冲区处理时，这防止在出口的数据包处理在入口数据包前。

如果看到无序信息包，推荐您更改您的从**两个的**配置到在两个接口。

这是前面的命令：

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

更改命令对这些：

```
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
```

相关信息

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