Catalyst 4500系列交換器Wireshark功能設定範例

目錄

簡介

本檔案介紹如何設定Cisco Catalyst 4500系列交換器的Wireshark功能。

必要條件

需求

要使用Wireshark功能，必須滿足以下條件：

- 系統必須使用Cisco Catalyst 4500系列交換機。
- 交換機必須運行Supervisor Engine 7-E（目前不支援Supervisor Engine 6）。
- 該功能必須具有設定的IP Base和企業服務（目前不支援LAN Base）。
- 交換機CPU不能具有高利用率，因為Wireshark功能是CPU密集型，軟體會交換捕獲過程中的某些資料包。

採用元件

本檔案中的資訊是根據執行Supervisor Engine 7-E的Cisco Catalyst 4500系列交換器。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

執行Supervisor Engine 7-E的Cisco Catalyst 4500系列交換器搭載Cisco IOS?-XE 3.3(0)/151.1版或更新版本，具有新的內建功能。此內建Wireshark功能能夠捕獲資料包，取代了連線的電腦使用交換機埠分析器(SPAN)的傳統方式，以便在故障排除場景中捕獲資料包。

設定

本節可作為開始捕獲的快速入門手冊。所提供的資訊非常籠統，如果您在生產網路中操作，必須根據需要實施過濾器和緩衝區設定以限制資料包的過度捕獲。

完成以下步驟以配置Wireshark功能：

1. 驗證是否符合條件以支援捕獲。(請參考 **需求** 一節。) 輸入以下命令並驗證輸出：

```
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. 從埠在TX/RX方向上捕獲流量 **gig2/26** 在本例中。將擷取檔案儲存在bootflash中的 **pcap** 如有必要，從本地PC檢視的檔案格式：**附註**：確保從**使用者EXEC**模式而不是**全域性配置**模式執行配置。

```
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. 這會擷取連線埠上的所有流量輸入和輸出 g2/26.它也會在生產環境中用無用的流量非常快地填充檔案，除非您指定方向並應用捕獲過濾器以便縮小捕獲流量的範圍。輸入以下命令以應用過濾器：

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

附註：這可確保您在擷取檔案中只擷取網際網路控制訊息通訊協定(ICMP)流量。

4. 捕獲檔案超時或填充大小配額後，您將收到以下消息：

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

輸入以下命令可手動停止擷取：

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

5. 您可以從CLI檢視捕獲。輸入以下命令可檢視封包：

```
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
```

附註：為了以Wireshark格式檢視資料包，在末尾提供了詳細資訊選項。此外，dump選項可用於檢視資料包的十六進位制值。

6. 如果在開始捕獲時未使用capture-filter，則捕獲檔案會變得雜亂。在這種情況下，請使用display-filter選項以在顯示中顯示特定流量。您只想檢視ICMP流量，而不想檢視上一輸出中顯示的熱待命路由器協定(HSRP)、生成樹協定(STP)和思科發現協定(CDP)流量。display-filter使用與Wireshark相同的格式，因此您可以線上找到過濾器。

```
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. 將該檔案傳輸到本地電腦，並像檢視任何其他標準捕獲檔案一樣檢視pcap檔案。輸入以下命令之一以完成傳輸：

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

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

8. 為了清理捕獲，請使用以下命令刪除配置：

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

<no output>

4500TEST#
```

其他設定

預設情況下，捕獲檔案的大小限製為100個資料包，或線性檔案中的60秒。若要變更大小限制，請在監控器擷取語法中使用**limit**選項：

```
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
```

緩衝區最大大小為100 MB。使用以下命令可調整此值以及循環/線性緩衝區設定：

```
4500TEST#monitor cap MYCAP buffer ?

circular  circular buffer
size      Size of buffer
```

如果正確使用，內建的Wireshark功能是非常強大的工具。當您對網路進行故障排除時，可以節省時間和資源。但是，使用該功能時請謹慎小心，因為它可能會增加高流量情況下的CPU利用率。切勿配置工具並使其處於無人值守狀態。

驗證

目前沒有適用於此組態的驗證程序。

疑難排解

由於硬體限制，擷取檔案中可能會收到無序的封包。這是因為入口和出口封包擷取使用不同的緩衝區。如果擷取中有無序的封包，請將兩個緩衝區都設定為**輸入**。這可以防止處理緩衝區時，輸出中的封包在輸入封包之前進行處理。

如果您看到無序的封包，建議您兩個介面上的組態都從**both**變更為**in**。

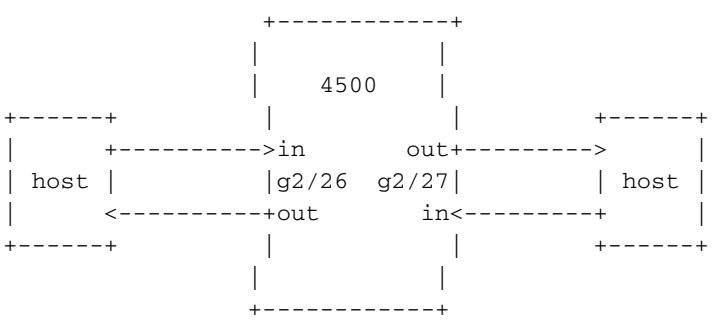
以下是上一個指令：

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

將命令更改為以下內容：

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

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



相關資訊

- Catalyst 4500系列交換器軟體組態設定指南，版本IOS XE 3.3.0SG和IOS 15.1(1)SG — 設定Wireshark
- 技術支援與文件 - Cisco Systems