Catalyst 4500 シリーズ スイッチの Wireshark 機能の設定例

内容

概要

このドキュメントでは、Cisco Catalyst 4500 シリーズ スイッチの Wireshark 機能を設定する方法について説明します。

前提条件

要件

Wireshark 機能を使用するには、次の条件を満たす必要があります。

- システムは Cisco Catalyst 4500 シリーズ スイッチを使用する必要があります。
- スイッチは Supervisor Engine 7-E を実行する必要があります（Supervisor Engine 6 は現在サポートされていません）。
- この機能には、設定済みの IP Base および Enterprise Services が必要です（LAN Base は現在サポートされていません）。
- Wireshark 機能は CPU の負荷が高く、キャプチャ プロセスで特定のパケットをソフトウェアによってスイッチングするため、スイッチを CPU 使用率の高い状態で使用できません。

使用するコンポーネント

このドキュメントの情報は、Supervisor Engine 7-E が稼働する Cisco Catalyst 4500 シリーズ スイッチに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

Supervisor Engine 7-Eを実行するCisco Catalyst 4500シリーズスイッチには、Cisco IOS?-XEバージョン3.3(0) / 151.1以降の新機能が組み込まれています。トラブルシューティングのシナリオでパケットをキャプチャする場合は、接続された PC でスイッチ ポート アナライザ（SPAN）を使用する従来の方法に代わって、この組み込みの Wireshark 機能によってパケットをキャプチャできます。

設定

ここでは、キャプチャを開始するためのクイック スタート ガイドを示します。ここに示す情報は非常に一般的なものであり、実稼働ネットワークで運用する場合は、過剰なパケットのキャプチャを制限するため、必要に応じてフィルタやバッファの設定を実装する必要があります。

Wireshark 機能を設定するには、次の手順を実行します。

1. キャプチャをサポートするための条件を満たしていることを確認します(**要件** を参照してください)。 次のコマンドを入力し、出力を確認します。

```
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. トラフィックはポートからTX/RX方向にキャプチャされます gig2/26 この例の場合は.キャプチャファイルを pcap 必要に応じて、ローカルPCからレビューするためのファイル形式：**注：この設定は、必ずグローバル コンフィギュレーション モードではなくユーザ EXEC モードで実行してください。**

```
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. これにより、ポート上のすべての入力および出力トラフィックがキャプチャされます g2/26.また、実稼働環境では、方向を指定してキャプチャ フィルタを適用することにより、キャプチャされるトラフィックの範囲を制限しない限り、すぐにファイルが無用なトラフィックでいっぱいになります。フィルタを適用するには、次のコマンドを入力します。

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

注：これにより、キャプチャ ファイルにインターネット制御メッセージ プロトコル（ICMP）トラフィックだけがキャプチャされるようになります。

4. キャプチャ ファイルがタイムアウトするか、サイズのクォータに達すると、次のメッセージが表示されます。

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

キャプチャを手動で停止するには、次のコマンドを入力します。

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

5. CLI からキャプチャを確認できます。パケットを表示するには、次のコマンドを入力します。

```
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：パケットを Wireshark 形式で表示するには、末尾に detail オプションを指定します。また、パケットの 16 進値を表示するには、dump オプションを指定します。

6. キャプチャの開始時にキャプチャ フィルタを使用しなかった場合は、キャプチャ ファイルが雑然とした状態になります。このような場合は、**display-filter オプションを使用して特定のトラフィックを表示してください。**上記の出力では、ホット スタンバイ ルータ プロトコル（HSRP）、スパニング ツリー プロトコル（STP）、および Cisco Discovery Protocol（CDP）のトラフィックを表示せずに、ICMP のトラフィックだけを表示する必要があります。**display-filter は Wireshark と同じ形式を使用するため、オンラインで**フィルタを見つけることができます。

```
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. ファイルをローカル マシンに転送し、他の標準キャプチャ ファイルと同様に **pcap ファイルを確認します。**転送を実行するには、次のいずれかのコマンドを入力します。

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

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

8. キャプチャをクリーンアップするには、次のコマンドを使用して設定を削除します。

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

<no output>

4500TEST#
```

その他の設定

デフォルトでは、キャプチャ ファイルのサイズ制限は 100 パケット、またはリニア ファイルでは 60 秒です。サイズ制限を変更するには、monitor capture 構文で **limit オプションを使用します。**

```
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
```

バッファの最大サイズは 100 MB です。このサイズおよび循環/リニア バッファ設定を調整するには、次のコマンドを使用します。

```
4500TEST#monitor cap MYCAP buffer ?
```

```
circular  circular buffer
size      Size of buffer
```
組み込みの Wireshark 機能は、正しく使用すれば非常に強力なツールです。ネットワークのトラブルシューティングにかかる時間とリソースを節約できます。ただし、高トラフィックの状況では CPU 使用率が増加することがあるため、この機能を利用するときは注意が必要です。このツールを設定したまま放置しないでください。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシュート

ハードウェアの制限のため、キャプチャ ファイル内でパケットの順序が正しくなくなる場合があります。これは、入力および出力パケット キャプチャで使用されるバッファが異なることが原因です。キャプチャのパケット順序が正しくない場合は、両方のバッファを ingress に設定してください。これにより、バッファの処理時に入力パケットの前に出力パケットが処理されなくなります。

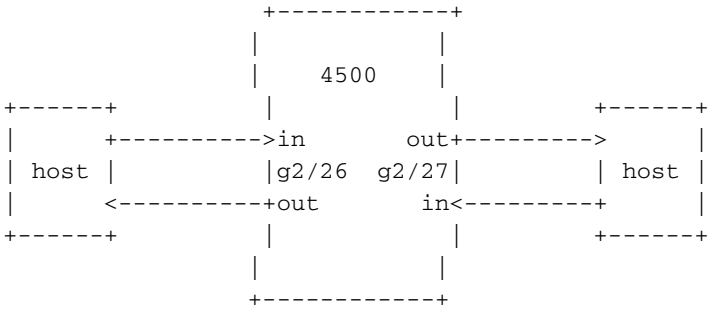
パケットの順序が正しくない場合は、両方のインターフェイスの設定を **both から in に変更することを推奨します。**

以前のコマンドを次に示します。

```
4500TEST#monitor capture MYCAP interface g2/26 both
```
このコマンドを次のように変更します。

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

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



関連情報

- [『Catalyst 4500 シリーズ スイッチ ソフトウェア コンフィギュレーション ガイド リリース IOS XE 3.3.0SG および IOS 15.1(1)SG』の「Wireshark の設定」]

- テクニカル サポートとドキュメント – Cisco Systems