

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

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[その他の設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

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 packets 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。


```

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)

- この例では、ポート **gig2/26** から発信された TX/RX 方向のトラフィックがキャプチャされます。必要に応じて、キャプチャ ファイルを **pcap** ファイル形式でブートフラッシュに保存し、ローカル PC から確認できるようにします。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.

- これにより、ポート **g2/26** 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。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。

- 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。

```

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

```

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

```

- 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。

- 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@<ftp server address>
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。

トラブルシューティング

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
```

```
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](#)