Cisco IOS と IOS XE の組み込みパケット キャプチャの設定例

目次

概要

このドキュメントでは、Cisco IOS® ソフトウェアの組み込みパケット キャプチャ（EPC）の機能について説明します。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS Release 12.4(20)T 以降
- Cisco IOS XE Release 15.2(4)S 3.7.0 以降

このドキュメントの情報は、ラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

背景説明

有効な場合、ルータは送受信されるパケットをキャプチャします。 パケットは DRAM のバッフ

ァ内に格納され、リロード後は保持されません。 データがキャプチャされると、そのデータはルータの要約ビューまたは詳細ビューで調べることができます。 また、データは、さらに調べることができようにパケット キャプチャ（PCAP）ファイルとして エクスポートできます。 ツールはEXEC モードで設定され、一時支援ツールと見なされます。 その結果、ツール設定はルータ設定内に格納されず、システム リロード後には無効になります。

パケットキャプチャ構成ジェネレーターおよびアナライザ ツールはパケットキャプチャの設定、キャプチャおよび抽出を援助して Ciscoカスタマー向けに利用可能です。

Cisco IOS の設定例

基本 EPC 設定

1. キャプチャされたパケットが内部に格納される一時バッファである「キャプチャ バッファ」を定義します。 バッファを定義するときに選択できるさまざまなオプションがあります。 たとえば、サイズ、最大パケット サイズ、円形/線形などです。

   ```
   monitor capture buffer BUF size 2048 max-size 1518 linear
   ```
2. フィルタを適用して、キャプチャするトラフィックを限定できます。 コンフィギュレーション モード内でアクセス コントロール リスト（ACL）を定義し、バッファに対するフィルタを適用します。

   ```
   ip access-list extended BUF-FILTER
   permit ip host 192.168.1.1 host 172.16.1.1
   permit ip host 172.16.1.1 host 192.168.1.1monitor capture buffer BUF filter access-list
   BUF-FILTER
   ```
3. キャプチャが発生する場所を定義する「キャプチャ ポイント」を定義します。 キャプチャポイントは、IPv4 または IPv6 のいずれに対してキャプチャが発生するか、またどのスイッチング パス（プロセス vs CEF）でキャプチャが発生するかも定義します。

   ```
   monitor capture point ip cef POINT fastEthernet 0 both
   ```
4. キャプチャ ポイントにバッファを接続します。

   ```
   monitor capture point associate POINT BUF
   ```
5. キャプチャを開始します。

   ```
   monitor capture point start POINT
   ```
6. これでキャプチャがアクティブになりました。 必要なデータのコレクションを許可します。

7. キャプチャを停止します。

   ```
   monitor capture point stop POINT
   ```
8. 装置でバッファを確認します。

   ```
   show monitor capture buffer BUF dump
   ```
   注: この出力には、パケット キャプチャの 16 進数ダンプのみが表示されます。 見るために人が読み取り可能のそれらはそこに 2 つの方法です。さらに分析するためにルータからバッファをエクスポートします。

   ```
   monitor capture buffer BUF export tftp://10.1.1.1/BUF.pcap
   ```
   ヒント： 機能拡張要求

CSCuw77601 はエクスポートの下でオプション メールに a を追加するためにファイルされました従って電子メール ID にバッファを diretly 電子メールで送ることができます。ただし、ルータへの T/FTP アクセスが必要になるため、上記の方法は常に実用的であるというわけではありません。 そのような状況では、16 進数ダンプのコピーを取り、任意のオンラインの 16 進数パケット キャプチャ コンバータを使用してファイルを表示することができます。

9. 必要なデータが収集されたら、「キャプチャ ポイント」を削除すれば「バッファ」をキャプチャ して下さい: `no monitor capture point ip cef POINT fastEthernet 0 both`
   `no monitor capture buffer BUF`

注：

- Cisco IOS Release 15.0(1)M より前のリリースでは、バッファ サイズは 512 K に限定されていました。
- Cisco IOS Release 15.0(1)M より前のリリースでは、キャプチャ パケット サイズは 1024 バイトに限定されていました。
- パケット バッファは DRAM に格納され、リロード後は保持されません。
- キャプチャ設定は NVRAM には格納されず、リロード後は保持されません。
- CEF またはプロセス スイッチング パスでキャプチャするためにキャプチャ ポイントを定義できます。
- キャプチャ ポイントは、1 つのインターフェイスのみをキャプチャするようにも、全体をキャプチャするようにも定義できます。
- キャプチャ バッファを PCAP 形式でエクスポートする場合は、L2 情報 (イーサネットのカプセル化など) は維持されません。
- SeeBest はこのセクションで使用されるコマンドに関する詳細を得るためにコマンドを検索するために練習します。

Cisco IOS-XE の設定例

組み込みパケット キャプチャ機能は、Cisco IOS XE Release 3.7 15.2(4)S で導入されました。キャプチャの設定は、より多くの機能を追加するため、Cisco IOS とは異なります。

基本 EPC 設定

1. キャプチャが発生する場所を定義します。

   ```
   monitor capture CAP interface GigabitEthernet0/0/1 both
   ```

2. フィルタを関連付けます。 フィルタはインラインに規定 されるかもしれませんまたは ACL か class-map は参照することができます:

   ```
   monitor capture CAP match ipv4 protocol tcp any any
   ```

3. キャプチャを開始します。

   ```
   monitor capture CAP start
   ```

4. これでキャプチャがアクティブになりました。 必要なデータの収集を許可します。

5. キャプチャを停止します。

   ```
   monitor capture CAP stop
   ```

6. サマリー ビューでキャプチャを調べます。

```
show monitor capture CAP buffer brief
```

7. 詳細ビューでキャプチャを調べます。

```
show monitor capture CAP buffer detailed
```

8. また、さらに分析するために PCAP 形式でキャプチャをエクスポートします。

```
monitor capture CAP export ftp://10.0.0.1/CAP.pcap
```

9. 必要なデータが収集されたら、キャプチャを削除します。

```
no monitor capture CAP
```

注：

- キャプチャは、物理インターフェイス、サブインターフェイス、およびトンネル インターフェイスで実行できます。
- クラス マップで **match protocol** コマンドを使用する Network Based Application Recognition（NBAR）ベースのフィルタは、現在サポートされていません。
- コマンドのこのセクションで使用されるコマンドに関する詳細を得るために検索については最良 の 方法を参照して下さい。

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

ここでは、設定のトラブルシューティングに役立つ情報について説明します。

Cisco IOS XE で実行する EPC の場合、このデバッグ コマンドを使用して、EPC が確実に正しく設定されるようにできます。

```
no monitor capture CAP
```

関連情報

- 組み込みパケット キャプチャ - Cisco IOS XE
- 組み込みパケット キャプチャ - Cisco IOS
- テクニカルサポートとドキュメント - Cisco Systems