ソフトウェアでの組み込みパケットの設定とキャプチャ

内容

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特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いています。

- Cisco IOS Release 12.4(20)T 以降
- Cisco IOS XE®リリース15.2(4)S - 3.7.0以降

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

有効にした場合、ルータは送受信されたパケットをキャプチャします。パケットはDRAMのバッファに格納され、リロード後は保持されません。いったんデータがキャプチャされると、ルータの概要ビューまたは詳細ビューで確認できます。

さらに、データをパケットキャプチャ(PCAP)ファイルとしてエクスポートして、さらに詳しく調べることができます。このツールはEXECモードで設定されており、一時的な支援ツールと見なされます。その結果、このツールの設定はルータの設定内に保存されず、システムのリロード後も残りません。

シスコのお客様は、パケットキャプチャの設定、キャプチャ、および抽出を支援するPacket Capture Config Generator and Analyzerツールを使用できます。

Cisco IOS の設定例

基本 EPC 設定

1. 「キャプチャバッファ」を定義します。これは、キャプチャされたパケットが格納される一時バッファです。
2. 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
```

3. フィルタを適用して、キャプチャを目的のトラフィックに制限できます。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 192.168.1.1

monitor capture buffer BUF filter access-list BUF-FILTER
```

4. 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。
5. 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
```

6. 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
```

7. キャプチャを開始します。

```
monitor capture point start POINT
```

8. 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。

9. キャプチャを停止します。

```
monitor capture point stop POINT
```

10. 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。人間が読める形式で表示するには、2つの方法があります。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
```

前の方法は、ルータへのT/FTPアクセスを必要とするため、必ずしも実用的ではありません。このような場合は、16進数ダンプのコピーを取り、オンラインの16進数pcapコンバータを使用してファイルを表示します。

11. 必要なデータを収集したら、「capture point」と「capture buffer」を削除します。

```
no monitor capture point ip cef POINT fastEthernet 0 both
no monitor capture buffer BUF
```

その他のCisco IOS設定情報

- Cisco IOS®リリース15.0(1)Mよりも前のリリースでは、バッファサイズは512Kに制限されていました。
- Cisco IOS®リリース15.0(1)Mよりも前のリリースでは、キャプチャパケットサイズは1024バイトに制限されていました。
- パケットバッファはDRAMに保存され、リロードしても保持されません。
- キャプチャ設定はNVRAMに保存されず、リロードしても保持されません。
- 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。
- このセクションで使用されているコマンドの詳細については、「検索コマンドのベストプラクティス」を参照してください。

基本的なIPトラフィックエクスポート設定

IPトラフィックエクスポートは、複数の同時WANまたはLANインターフェイスで受信したIPパケットをエクスポートする別の方法です。

1.コンフィギュレーションモードでIPトラフィックエクスポートプロファイルを定義します。

```
Device(config)# ip traffic-export profile mypcap mode capture
```

2.プロファイルで双方向トラフィックを設定します。

```
Device(config-rite)# bidirectional
```

3. 終了

4.エクスポートされたトラフィックのインターフェイスを指定します。

```
Device(config-if)# interface GigabitEthernet 0/1
```

5.インターフェイスでIPトラフィックエクスポートを有効にします。

```
Device(config-if)# ip traffic-export apply mypcap size 10000000
```

6.終了

7.キャプチャを開始します。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。

```
Device# traffic-export interface GigabitEthernet 0/1 start
```

8.キャプチャを停止します。

```
Device# traffic-export interface GigabitEthernet 0/1 stop
```

9.キャプチャを外部TFTPサーバにエクスポートします。

```
Device# traffic-export interface GigabitEthernet 0/1 copy tftp://<TFTP_Address>/mypcap.pcap
```

10.必要なデータが収集されたら、プロファイルを削除します。

```
Device(config)# no ip traffic-export profile mypcap
```

IPトラフィックエクスポートの欠点

IPトラフィックエクスポートには、EPC方式と比較して次の短所があります。

- キャプチャされたトラフィックがエクスポートされるインターフェイスは、イーサネットインターフェイスである必要があります。
- IPv6サポートなし。
- レイヤ2の情報はなく、レイヤ3以上の情報だけが含まれます。

Cisco IOS-XE の設定例

Embedded Packet Capture（EPC；組み込みパケットキャプチャ）機能は、Cisco IOS-XE®リリース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で指定するか、ACLまたはクラスマップを参照できます。

```
monitor capture CAP match ipv4 protocol tcp any any limit pps 1000000
```

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工クスポートします。

```
monitor capture CAP export tftp://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
```

追加情報

- 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されます。
- Network Based Application Recognition(NBAR)ベースのフィルタ(**match protocol** コマンド)は現在サポートされていません。
- このセクションで使用されているコマンドの詳細については、「検索コマンドのベストプラクティス」を参照してください。

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

Cisco IOS-XE®で実行されるEPCの場合、EPCが正しく設定されていることを確認するには、次のdebugコマンドを使用します。

```
debug epc provision
debug epc capture-point
```

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

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。