Embedded Packet Capture

Embedded Packet Capture（EPC）は、ネットワーク管理者がデバイスを出入りするかデバイスを通るパケットをキャプチャし、パケットをローカルで分析するか、またはWiresharkのようなツールを使用してオフライン分析を行うために、パケットを保存してエクスポートできるようにするオンボードパケットキャプチャファシリティです。この機能は、デバイスがネットワークの管理と操作にアクティブに参加できるようにすることによって、ネットワーク操作を簡略化します。この機能は、パケットの形式に関する情報を収集することによって、トラブルシューティングを容易にします。また、アプリケーションの分析とセキュリティも容易にします。

- 機能情報の確認，1 ページ
- Embedded Packet Capture の前提条件，2 ページ
- Embedded Packet Capture の制約事項，2 ページ
- Embedded Packet Capture について，2 ページ
- Embedded Packet Capture の実装方法，4 ページ
- Embedded Packet Capture の設定例，8 ページ
- その他の関連資料，10 ページ
- Embedded Packet Capture の機能情報，11 ページ

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の警告および機能情報については、『Bug Search Tool』およびご使用のプラットフォームとソフトウェアリリースに対応したリリースノートを参照してください。このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

Embedded Packet Capture の前提条件

Embedded Packet Capture（EPC）ソフトウェア サブシステムは、その動作で CPU とメモリ リソースを消費します。 さまざまなタイプの操作を行うために十分なシステム リソースを準備する必要があります。 システム リソースの使用のためのガイドラインを次の表に示します。

表 *1*：*EPC* サブシステムのシステム要件

システム リソース	要件
ハードウェア	CPU 利用率の要件は、プラットフォームによって異なります。
メモリ	パケット バッファは DRAM に保存されます。 パケット バッファのサイズは、ユーザが指定します。
ディスクスペース	パケットは外部のデバイスにエクスポートできます。 フラッシュ ディスクでの中間保管は必要ありません。

Embedded Packet Capture の制約事項

- Cisco IOS Release 12.2(33)SRE では、EPC は 7200 プラットフォームでのみサポートされます。
- EPC は入力のマルチキャスト パケットだけをキャプチャし、出力の複製パケットをキャプチャしません。
- 現在、キャプチャ ファイルはデバイスの外部（TFTP または FTP サーバおよびローカル ディスクなど）にだけエクスポートできます。

Embedded Packet Capture について

Embedded Packet Capture の概要

Embedded Packet Capture（EPC）は、パケットのトレースとトラブルシューティングに役立つ組み込みシステム管理機能を提供します。 この機能を使用すると、ネットワーク管理者は、シスコ デバイスを出入りするか通過するデータ パケットをキャプチャできます。 ネットワーク管理者は、キャプチャ バッファ サイズとタイプ（循環またはリニア）およびキャプチャする各パケットの最大バイト数を定義する場合があります。 パケット キャプチャ レートは、詳細な管理制御を使用してスロットリングできます。 たとえば、アクセス コントロール リストを使用してキャプチャ対象パケットをフィルタリングするオプションや、最大パケット キャプチャ レートまたはサンプリング間隔の指定などの詳細な定義を行うオプションが利用できます。

EPC の利点

この機能の利点は次のとおりです。

- シスコ エクスプレス フォワーディング（CEF）パスにある IPv4 および IPv6 パケットをキャプチャする機能
- キャプチャ バッファ パラメータを指定するフレキシブルな方法
- フィルタにキャプチャされたパケット
- さまざまな程度の詳細さでキャプチャされたデータ パケットをデコードする方法
- 外部ツールを使用して、パケット キャプチャを分析に適した PCAP 形式でエクスポートするファシリティ
- パケット キャプチャ ポイントをイネーブルにする拡張可能なインフラストラクチャ

キャプチャ バッファ

キャプチャ バッファは、パケット データを収容するメモリ内の領域です。 バッファの一意の名前、サイズ、およびタイプを指定し、バッファが必要に応じて着信データを処理するように設定できます。

キャプチャ バッファには次のタイプのデータが保存されます。

- パケット データ
- メタデータ

パケット データは datagramstart から開始され、最小の 1 パケットあたりのキャプチャ サイズ（datagramsize）をキャプチャ バッファにコピーします。

メタデータには、パケットデータのセットについての説明情報が含まれています。内容は、次のとおりです。

- バッファに追加される時期のタイムスタンプ
- パケット データが送信される方向（出力または入力）
- キャプチャされたスイッチ パス
- L2 デコーダのデコードを可能にする入力または出力インターフェイスに対応するカプセル化のタイプ

キャプチャ バッファでは、次の作業を実行できます。

- キャプチャ バッファを定義し、キャプチャ ポイントと関連付けます。
- キャプチャ バッファをクリアします。

- オフライン分析用にキャプチャ バッファをエクスポートします。 サポートされたファイル転送オプション（FTP、HTTP、HTTPS、PRAM、RCP、SCP、およびTFTP）のいずれかを使用して、ファイルの書き込みをエクスポートします。
- キャプチャ バッファの内容を表示します。

キャプチャ ポイント

キャプチャポイントは、パケットがキャプチャされ、バッファと関連付けられるトラフィック トランジットポイントです。 一意の名前と異なるパラメータを提供することによって、キャプチャポイントを定義できます。

次のキャプチャ ポイントが使用できます。

- インターフェイス入力および出力がある IPv4 CEF/割り込みスイッチング パス
- インターフェイス入力および出力がある IPv6 CEF/割り込みスイッチング パス

キャプチャ ポイントでは、次の作業を実行できます。

- キャプチャ ポイントをキャプチャ バッファと関連付けるか、関連付けを解除します。 各キャプチャ ポイントは、1 つのキャプチャ バッファとだけ関連付けることができます。
- キャプチャ ポイントを破棄します。
- 特定のインターフェイスのパケット キャプチャ ポイントをアクティブにします。 複数のパケットキャプチャポイントを特定のインターフェイスでアクティブにできます。 たとえば、ボーダー ゲートウェイ プロトコル（BGP）パケットを 1 つのキャプチャ バッファにキャプチャし、Open Shortest Path First（OSPF）パケットを別のキャプチャ バッファにキャプチャできます。
- アクセス コントロール リスト（ACL）をキャプチャ ポイントに適用できます。

Embedded Packet Capture の実装方法

パケット データ キャプチャの開始

この作業を実行し、分析とトラブルシューティングのためのパケット データのキャプチャを開始します。 パケット データをキャプチャするには、キャプチャ バッファとキャプチャ ポイントを定義する必要があります。 次に、キャプチャ ポイントをキャプチャ バッファと関連付ける必要があります。 キャプチャ ポイントをイネーブルにすると、パケット データをキャプチャするプロセスが開始されます。

手順の概要

1. **enable**
2. **monitor capture buffer** *buffer-name* [**clear** | **export** *export-location* | **filter access-list** {*ip-access-list* | *ip-expanded-list* | *access-list-name*} | **limit** {**allow-nth-pak** *nth-packet* | **duration** *seconds* | **packet-count** *total-packets* | **packets-per-sec** *packets*} | [**max-size** *element-size*] [**size** *buffer-size*] [**circular**| **linear**]]
3. **monitor capture point** {**ip**| **ipv6**}{**cef** *capture-point-name interface-name interface-type*{**both** | **in** | **out**}| **process-switched** *capture-point-name* {**both**| **from-us**| **in** | **out**}}
4. **monitor capture point associate** *capture-point-name capture-buffer-name*
5. **monitor capture point start** {*capture-point-name* | **all**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture buffer** *buffer-name* [**clear**	**export** *export-location*	**filter access-list** {*ip-access-list*	*ip-expanded-list*	*access-list-name*}	**limit** {**allow-nth-pak** *nth-packet*	**duration** *seconds*	**packet-count** *total-packets*	**packets-per-sec** *packets*}	[**max-size** *element-size*] [**size** *buffer-size*] [**circular**| **linear**]] 例： `Router# monitor capture buffer pktrace1 size 256 max-size 100 circular`	キャプチャ バッファを指定された名前とパラメータで定義します。 • この例では、pktrace1 という名前で、サイズが 256 バイト、バッファ要素の最大サイズが 100 バイトの循環式キャプチャ バッファが定義されています。
ステップ 3	**monitor capture point** {**ip**	**ipv6**}{**cef** *capture-point-name interface-name interface-type*{**both**	**in**	**out**}	**process-switched** *capture-point-name* {**both**	**from-us**	**in**	**out**}} 例： `Router# monitor capture point ip cef ipceffa0/1 fastEthernet 0/1 both`	キャプチャ ポイントを指定されたパラメータで定義します。 • この例では、ipceffa0/1 という名前で、ファストイーサネット 0/1 インターフェイスが両方向にあるキャプチャ ポイントが定義されています。
ステップ 4	**monitor capture point associate** *capture-point-name capture-buffer-name* 例： `Router# monitor capture point associate ipceffa0/1 pktrace1`	キャプチャ ポイントを指定されたキャプチャ バッファと関連付けます。 • キャプチャ ポイントをキャプチャ バッファと関連付けると、指定されたキャプチャ ポイントからキャ

	コマンドまたはアクション	目的
		プチャされたすべてのパケットが関連付けられたキャプチャ バッファにダンプされます。 • この例では、キャプチャ ポイント ipceffa0/1 がキャプチャ バッファ pktrace1 と関連付けられています。
ステップ 5	**monitor capture point start** {*capture-point-name* | **all**} 例： `Router# monitor capture point start ipceffa0/1`	キャプチャ ポイントでのパケット データのキャプチャの開始をイネーブルにします。 • この例では、キャプチャ ポイント ipceffa0/1 がイネーブルになっています。

パケット データ キャプチャの停止

パケット データのキャプチャを停止するには、次の作業を実行します。

手順の概要

1. **enable**
2. **monitor capture point stop** {*capture-point-name* | **all**}

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture point stop** {*capture-point-name* | **all**} 例： `Router# monitor capture point stop ipceffa0/1`	キャプチャ ポイントをディセーブルにし、パケット データ キャプチャ プロセスを停止します。 • この例では、キャプチャ ポイント ipceffa0/1 がディセーブルになっています。

分析のためのパケット データのエクスポート

外部ツールを使用して、分析のためにパケット データをエクスポートするには、次の作業を実行します。

手順の概要

1. **enable**
2. **monitor capture buffer** *buffer-name* **export** *export-location*

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**monitor capture buffer** *buffer-name* **export** *export-location* 例： `Router# monitor capture buffer pktrace1 export tftp://10.1.88.9/pktrace1`	分析のためにデータをエクスポートします。 • この例では、キャプチャ バッファ pktrace1 からのデータは、TFTP プロトコルを使用してエクスポートされます。

キャプチャされたデータのモニタリングとメンテナンス

キャプチャされたパケット データのモニタリングとメンテナンスを行うには、次の作業を実行します。 キャプチャ バッファの詳細とキャプチャ ポイントの詳細を表示できます。

手順の概要

1. **enable**
2. **show monitor capture** {**buffer** {*capture-buffer-name* [**parameters**] | **all parameters** | **merged** *capture-buffer-name1 capture-buffer-name2*}[**dump**] [**filter** *filter-parameters*]} | **point** {**all** | *capture-point-name*}}
3. **debug packet-capture**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Router> enable`	特権 EXEC モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	**show monitor capture** {**buffer** {*capture-buffer-name* [**parameters**] | **all parameters** | **merged** *capture-buffer-name1 capture-buffer-name2*}[**dump**] [**filter** *filter-parameters*]} | **point** {**all** | *capture-point-name*}} 例： `Router# show monitor capture buffer pktrace1 dump`	キャプチャされたデータを表示します。 • この例では、キャプチャ バッファ pktrace1 からのデータが表示されています。
ステップ 3	**debug packet-capture** 例： `Router# debug packet-capture`	パケット キャプチャ インフラ デバッグをイネーブルにします。

Embedded Packet Capture の設定例

パケット データ キャプチャの開始の例

次に、ファスト イーサネット 0/1 インターフェイスから、またはファスト イーサネット 0/1 インターフェイスにパケットをキャプチャする例を示します。

```
Router> enable
Router# monitor capture buffer pktrace1 ip cef ipceffa0/1 fastEthernet 0/1 both
Router# monitor capture point associate ipceffa0/1 pktrace1
Router# monitor capture point start ipceffa0/1
Mar 21 11:13:34.023: %BUFCAP-6-ENABLE: Capture Point ipceffa0/1 enabled.
Router# show monitor capture point all
Status Information for Capture Point ipceffa0/1
IPv4 CEF
Switch Path: IPv4 CEF            , Capture Buffer: pktrace1
Status : Inactive
Configuration:
monitor capture point ip cef ipceffa0/1 FastEthernet0/1 both
Router# show monitor capture buffer all
Capture buffer pktrace1 (circular buffer)
Buffer Size : 262144 bytes, Max Element Size : 256 bytes, Packets : 31
Allow-nth-pak : 0, Duration : 0 (seconds), Max packets : 0, pps : 0
```

```
Associated Capture Points:
Name : ipceffa0/1, Status : Active
Configuration:
monitor capture buffer pktrace1 size 256 max-size 256 circular
monitor capture point associate ipceffa0/1 pktrace1
```

パケット データ キャプチャの停止の例

次に、パケット データのキャプチャを停止する例を示します。

```
Router> enable
Router# monitor capture point stop ipceffa0/1
Mar 21 11:14:20.152: %BUFCAP-6-DISABLE: Capture Point ipceffa0/1 disabled.
```

パケット データのエクスポートの例

次に、外部ツールを使用して分析のためにデータをエクスポートする例を示します。

```
Router> enable
Router# monitor capture buffer pktrace1 export tftp://10.1.88.9/pktrace1
```

キャプチャされたデータのモニタリングとメンテナンスの例

EPC 機能を使用すると、パケットを ASCII でダンプできます。 次の例は、1 つのホストから別のホストへの IPv4 ICMP エコー応答パケットを示します。

```
<timestamp>: IPv4 packet received on Ethernet0/0 in the IPv4 CEF LES switch path
029E28E0: AABBCC01 2D00AABB CC013000 08004500  *;L.-.*;L.0...E.
029E28F0: 00640001 0000FE01 A8950A00 00020A00  .d....~.(.......
029E2900: 00010000 D5C80001 00000000 00000000  ....UH..........
029E2910: B080ABCD ABCDABCD ABCDABCD ABCDABCD  0.+M+M+M+M+M+M+M
029E2920: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
029E2930: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
029E2940: ABCDABCD ABCDABCD ABCDABCD ABCDABCD  +M+M+M+M+M+M+M+M
029E2950: ABCD
```

次に、キャプチャ バッファ pktrace1 の内容を表示する例を示します。 この出力は、**show monitor capture buffer** *capture-buffer-name* **dump** コマンドを使用して表示されます。 このコマンドは、デフォルトモードとダンプモードの2つのモードをサポートしています。ダンプモードでは、キャプチャされたパケットの 16 進数でのダンプも表示されます。

```
Router> enable
Router# show monitor capture buffer pktrace1 dump

11:13:00.593 EDT Mar 21 2007 : IPv4 Turbo      : Fa2/1 Fa0/1
65B6F500: 080020A2 44D90009 E94F8406 08004500  .. "DY..iO....E.
65B6F510: 00400F00 0000FE01 92AF5801 13025801  .@....~../X...X.
65B6F520: 58090800 4D1A1169 00000000 0005326C  X...M..i......2l
65B6F530: 01CCABCD ABCDABCD ABCDABCD ABCDABCD  .L+M+M+M+M+M+M+M
65B6F540: ABCDABCD ABCDABCD ABCDABCD ABCD00    +M+M+M+M+M+M+M.
11:13:20.593 EDT Mar 21 2007 : IPv4 Turbo      : Fa2/1 Fa0/1

65B6F500: 080020A2 44D90009 E94F8406 08004500  .. "DY..iO....E.
65B6F510: 00400F02 0000FE01 92AD5801 13025801  .@....~..-X...X.
65B6F520: 58090800 FEF91169 00000000 0005326C  X...~y.i......2l
65B6F530: 4FECABCD ABCDABCD ABCDABCD ABCDABCD  Ol+M+M+M+M+M+M+M
65B6F540: ABCDABCD ABCDABCD ABCDABCD ABCDFF    +M+M+M+M+M+M+M
```

次に、パケット キャプチャ インフラ デバッグをイネーブルにする例を示します。

```
Router> enable
Router# debug packet-capture
Buffer Capture Infrastructure debugging is on
```

その他の関連資料

関連資料

関連項目	参照先
Cisco IOS コマンド	『Cisco IOS Master Commands List, All Releases』
ネットワーク管理コマンド（EEMコマンドを含む）：コマンド構文の詳細、デフォルト設定、コマンドモード、コマンド履歴、使用上のガイドライン、および例	『*Cisco IOS Network Management Command Reference*』

標準

標準	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。 この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

Embedded Packet Capture の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。 この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。 その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。 Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。 Cisco.com のアカウントは必要ありません。

表 *2* : ***Embedded Packet Capture*** の機能情報

機能名	リリース	機能情報
Embedded Packet Capture	12.2(33)SRE 12.4(20)T	

機能名	リリース	機能情報
		Cisco IOS Embedded Packet Capture（EPC）は、ネットワーク管理者がデバイスを出入りするかデバイスを通るパケットをキャプチャし、パケットをローカルで分析するか、または Wireshark のようなツールを使用してオフライン分析を行うために、パケットを保存してエクスポートできるようにするオンボード パケット キャプチャ ファシリティです。 この機能は、デバイスがネットワークの管理と操作にアクティブに参加できるようにすることによって、操作を簡略化します。 この機能は、パケットの形式に関する情報を収集することによって、よりよいトラブルシューティングを容易にします。 また、アプリケーションの分析とセキュリティも容易にします。 この機能は Cisco IOS Release 12.4(20)T で導入され、Cisco IOS Release 12.2(33)SRE に統合されました。 （注） Cisco IOS Release 12.2(33)SRE では、EPC は 7200 プラットフォームでのみサポートされます。 次のコマンドが導入または変更されました。 **debug packet-capture**、**monitor capture buffer**、**monitor capture point**、**monitor capture point associate**、**monitor capture point disassociate**、**monitor capture point start**、**monitor capture point stop**、**show monitor capture**。