

Catalyst 1200および1300スイッチでのオンボードパケットキャプチャ

目的

この記事の目的は、Catalyst 1200および1300スイッチのファームウェアバージョン4.1.3.36における新しいオンボードパケットキャプチャ(OPC)機能を説明することです。このファームウェアでは、コマンドラインインターフェイス(CLI)を使用してのみOPCを設定できます。

適用可能なデバイス | [Software Version]

- Catalyst 1200 スイッチ | 4.1.3.36
- Catalyst 1300 スイッチ | 4.1.3.36

はじめに

Catalyst 1200および1300スイッチのファームウェアバージョン4.1.3.36では、オンボードパケット機能(OPC)と呼ばれる新機能が導入されています。有効にすると、OPCはパケットデータのキャプチャに最大20 MBのメモリを割り当てます。この機能には、OPCインスタンスの動作を定義するキャプチャポイントの設定が必要です。キャプチャポイントは、OPCインスタンスに関連付けられたすべての設定を定義するために使用されます。OPC機能は、デバイスのトラブルシューティング機能を拡張します。

このファームウェアでは、CLIを使用してのみOPCを設定できます。キャプチャポイントは特権EXECモードで設定され、スイッチのコンフィギュレーションファイルにも、スイッチのリポート後に保存された設定にも保存されません。

スイッチには最大4つのキャプチャポイントを設定できますが、一度にアクティブにできるキャプチャポイントは1つだけです。パケットキャプチャは、コントロールプレーン(CPU)インターフェイスでサポートされています。メモリに取り込まれたデータは、オンボードフラッシュ(空き容量がある場合)またはUSBフラッシュドライブなどの接続されたUSBデバイスに保存できます。OPCは大量のCPUリソースを消費する可能性があるため、必要な場合にのみ使用することをお勧めします。

目次

- [キャプチャポイントを設定するためのコマンド](#)
- [バッファ設定](#)

- [送信元インターフェイスの設定](#)
- [キャプチャフィルタ設定](#)
- [キャプチャの開始と停止](#)
- [パケットキャプチャデータの保存](#)

キャプチャポイントを設定するためのコマンド

手順 1

キャプチャポイントを作成するには、コマンド `monitor capture {capture-name}` を使用します。

```
monitor capture cap1
```

上記の例では、cap1 という名前のキャプチャポイントが作成されています。

手順 2

設定されたキャプチャポイントの詳細を表示するには、コマンド `show monitor capture {capture-name}` を入力します。

```
show monitor capture cap1
```

Note:

キャプチャ名を指定せずに `show monitor capture` コマンドを使用すると、現在設定されているすべてのキャプチャポイントを表示できます。

```
switch4ac12e#monitor capture cap1
switch4ac12e#show monitor capture

Status Information for Capture cap1
  Target Type:
  Interface: None, Direction: NONE
  Status : Inactive
  Filter Details:
    None
  Buffer Details:
    Buffer Type: LINEAR (default)
    Buffer size (in MB): 5 (default)
```

手順 3

キャプチャポイントを削除するには、no monitor capture {capture-name}コマンドを使用します。

```
no monitor capture cap1
```

```
Buffer size (in MB): 5 (default)
switch4ac12e#no monitor capture cap1
switch4ac12e#show monitor capture
No capture exist
switch4ac12e#
```

バッファ設定

キャプチャポイントで使用するバッファ設定、具体的にはバッファのサイズとバッファモードをカスタマイズできます。

- 最小バッファサイズは1MBで、最大バッファサイズは20MBです。
- バッファサイズを指定しない場合は、5 MBのデフォルトサイズが使用されます。

- すべてのキャプチャポイントに最大20 MBのメモリを割り当てることができます。20 MBを割り当てられた単一のキャプチャポイントを使用できますが、20 MBを使用するように4つのキャプチャポイントを設定することはできません。合計20 MBが、設定されているすべてのキャプチャポイントに分割されます。
- バッファモードには、リニアとサーキュラの2つがあります。
- リニアモードがデフォルトモードです。リニアモードでは、アクティブなパケットキャプチャは、設定されたバッファがいっぱいになるまでデータを収集し、その後キャプチャは停止します。また、リニアロギングを使用していて、バッファがすでに満杯の場合は、パケットキャプチャを再開できません。この場合、最初にバッファをクリアする必要があります。
- 循環バッファモードでは、バッファがいっぱいになると、先入れ先出し(FIFO)を使用して以前にキャプチャしたデータが上書きされます。循環バッファモードを使用するキャプチャは、手動で停止する必要があります。

手順 1

バッファ設定を手動で設定するコマンドは、`monitor capture {capture-name} buffer {circular [size buffer-size] | size buffer-size}`を使用します。

```
monitor capture cap1 buffer size 2 circular
```

この例では、2 MBのバッファサイズがcap1キャプチャポイント用に設定され、バッファモードは循環モードです。

```
switch4acl2e#monitor capture cap1 buffer size 2 circular
switch4acl2e#show monitor capture cap1

Status Information for Capture cap1
  Target Type:
  Interface: None, Direction: NONE
  Status : Inactive
  Filter Details:
  None
  Buffer Details:
  Buffer Type: CIRCULAR
  Buffer size (in MB): 2
switch4acl2e#
```

手順 2

コマンド`no monitor capture {capture-name} buffer {circular [size buffer-size]}`を使用します。| size buffer-size} は、バッファモードをデフォルトのリニアモードに戻します。

。

```
no monitor capture cap1 buffer size 2 circular
```

Note:

[circular]オプションと[size]オプションを指定せずに「no」コマンドを使用すると、バッファモードとサイズがデフォルト設定のリニアモードと5 MBバッファサイズに設定されます。

手順 3

バッファを空にするには、`monitor capture {capture-name} clear`コマンドを使用します。

```
monitor capture cap1 clear
```

この例では、cap1のバッファは256 KBを使用しています。clearコマンドを発行すると、バッファは0 KBになります。

```
switch4acl2e#show monitor capture cap1 buffer
buffer size (KB)           : 5120
buffer used (KB)           : 256
packets in buf             : 841
packets dropped            : 0
Packet rate per second    : 0
switch4acl2e#monitor capture cap1 clear
Captured data will be deleted [clear]? (Y/N) [Y] Y
Cleared capture point : cap1
switch4acl2e#show monitor capture cap1 buffer
buffer size (KB)           : 5120
buffer used (KB)           : 0
packets in buf             : 0
packets dropped            : 0
Packet rate per second    : 0
switch4acl2e#
```

送信元インターフェイスの設定

キャプチャポイントが作成されたら、キャプチャの送信元インターフェイスを設定する必要があります。キャプチャを開始するには、送信元インターフェイスの設定が必須です。

- 現在、サポートされているソースタイプはコントロールプレーンだけです。

- 方向を設定するには、in、out、またはbothのいずれかのオプションを選択します。
- In：スイッチへの着信パケットをキャプチャします。
- Out：スイッチからの発信パケットをキャプチャします。
- Both：着信および発信パケットをキャプチャします。

手順 1

コマンド `monitor capture {capture-name} control-plane {in | out | both}` を使用して、送信元インターフェイスの設定を行います。

```
monitor capture cap1 control-plane both
```

```
switch4ac12e#monitor capture cap1 control-plane both
switch4ac12e#show monitor capture cap1

Status Information for Capture cap1
  Target Type:
  Interface: Control Plane, Direction: BOTH
  Status : Inactive
  Filter Details:
  None
  Buffer Details:
  Buffer Type: CIRCULAR
  Buffer size (in MB): 2
switch4ac12e#
```

手順 2

`no monitor capture {capture-name} control-plane {in | out | both}` コマンドを発行して、送信元インターフェイスの設定を削除します。

```
no monitor capture cap1 control-plane both
```

キャプチャフィルタ設定

キャプチャフィルタは、パケットキャプチャ用に設定する必要がある必須設定です。現在、ファームウェア4.1.3.36ではフィルタ操作はサポートされていません。送信元インターフェイス（コントロールプレーン）上のすべてのパケットがキャプチャされます。ただし、「any」オプションを使用してこのパラメータを設定する必要があります。

キャプチャフィルタ設定を設定するには、コマンド `monitor capture {capture-name}`

match anyを使用します。

```
monitor capture cap1 match any
```

この例では、キャプチャポイントcap1は、すべてのパケットと一致するように設定されています。

```
switch4ac12e#monitor capture cap1 match any
switch4ac12e#show monitor capture cap1

Status Information for Capture cap1
  Target Type:
  Interface: Control Plane, Direction: BOTH
  Status : Inactive
  Filter Details:
    Capture all packets
  Buffer Details:
    Buffer Type: LINEAR (default)
    Buffer size (in MB): 5 (default)
switch4ac12e#
```

キャプチャの開始と停止

キャプチャを開始する前に、次のことを確認します。

- 送信元インターフェイスとキャプチャフィルタを設定します。
- 開始する前にCPU使用率を確認することをお勧めします。

一度にアクティブにできるキャプチャセッションは1つだけであることに注意してください。キャプチャが停止した後に再開された場合、新しいパケットはバッファに追加されます。ただし、バッファがいっぱいになり、モードがlinearに設定されている場合は、キャプチャを再開できません。

手順 1

キャプチャを開始するには、コマンドmonitor capture {capture-name} startを使用します。

```
monitor capture cap1 start
```

手順 2

キャプチャを停止するには、`monitor capture {capture-name} stop`コマンドを使用します。

```
monitor capture cap1 stop
```

```
switch4ac12e#monitor capture cap1 start
Started capture point : cap1
switch4ac12e#monitor capture cap1 stop
Stopped capture point : cap1
switch4ac12e#
```

パケットキャプチャデータの保存

パケットキャプチャが完了したら、バッファ内のデータ(RAM)を保存する必要があります。データを保存する場合は、次の2つのインスタンスがあります。

- ユーザがCLIコマンドを使用してトリガーしたとき
- 致命的なエラーが発生した場合に自動的に実行されます。

パケットキャプチャは、スイッチのオンボードフラッシュに空きがある場合は、スイッチのオンボードフラッシュに保存するか、またはフラッシュドライブなどの接続されたUSBデバイスに保存できます。パケットキャプチャ中に致命的なエラーが発生した場合、データはフラッシュのメインディレクトリに自動的に保存されます。

パケットキャプチャをエクスポートするには、コマンドを使用して`monitor capture {capture-name} export {destination/filename}`

```
monitor capture cap1 export flash: cap1.pcap
```

```
monitor capture cap1 export usb: cap1.pcap
```

```
switch4acl2e#monitor capture capl export flash:capl.pcap
Copy: 270862 bytes copied in 00:00:01 [hh:mm:ss]
switch4acl2e#monitor capture capl export usb:capl.pcap
Copy: 270862 bytes copied in 00:00:01 [hh:mm:ss]
switch4acl2e#
```

キャプチャがフラッシュに保存されている場合は、CLIコマンドcopy {filename} usb:/を使用して、USBフラッシュドライブにコピーできます。

C1200およびC1300スイッチは、FATおよびFAT32でフォーマットされたUSBドライブをサポートします。FATまたはFAT32 USBドライブがない場合は、TFTPを使用してスイッチからファイルをコピーする必要があります。

TFTPを使用してスイッチのファイルをコピーするには、次の手順を実行します。

- TFTPサーバの設定 (TFTP64またはその他のサービスを使用)
- スwitchのCLIから次のコマンドを使用します。copy flash: {pcap file name} tftp://{tftp server ip}/{pcap file name}

結論

これで、Catalyst 1200および1300スイッチのオンボードパケットキャプチャ機能と、設定を行うためのCLIコマンドについて完全に理解できました。

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。