

두 인터페이스의 동시 임베디드 패킷 캡처 컨피그레이션 예

목차

[소개](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[구성](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[관련 정보](#)

소개

이 문서에서는 GigabitEthernet 0/0 및 GigabitEthernet 0/1 인터페이스에서 10메가바이트의 순환 캡처 버퍼에서 최대 1550바이트의 프레임을 캡처하는 EPC(Embedded Packet Capture) 컨피그레이션의 예를 설명합니다.

EPC는 네트워크 관리자가 디바이스로 또는 디바이스에서 송수신되는 패킷을 캡처하여 로컬에서 분석하거나(Wireshark와 같은 툴)을 저장하여 오프라인 분석을 위해 내보낼 수 있도록 해주는 온보드 패킷 캡처 기능입니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS[®] Software Release 15.x를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

구성

참고: 이 [섹션](#)에 사용된 명령에 대한 자세한 내용을 보려면 [Command Lookup Tool](#)([등록된 고객만 해당](#))을 사용합니다.

이 컨피그레이션에서는 GigabitEthernet 0/0 및 GigabitEthernet 0/1 인터페이스에서 10MB의 순환 캡처 버퍼에서 최대 1550바이트의 프레임을 캡처합니다.

!-- Define a capture buffer.

```
monitor capture buffer pcap-buffer1 size 10000 max-size 1550
```

!-- Define a capture point.

```
monitor capture point ip cef pcap-point1 g0/0 both
monitor capture point ip process-switched pcap-point2 both
```

**!-- Associates the capture point with the capture buffer
!-- so that packets captured from the specified capture
!-- point can be dumped to the associated capture buffer.**

```
monitor capture point associate pcap-point1 pcap-buffer1
monitor capture point associate pcap-point2 pcap-buffer1
```

!-- Repeat the same steps for second interface.

```
monitor capture buffer pcap-bufferA size 10000 max-size 1550
monitor capture point ip cef pcap-pointA g0/1 both
monitor capture point ip process-switched pcap-pointB both
monitor capture point associate pcap-pointA pcap-bufferA
monitor capture point associate pcap-pointB pcap-bufferA
```

**!-- Optionally you can specify an access-list in order to capture
!-- only interesting traffic as defined by access-lists 110 and 120.**

```
monitor capture buffer pcap-buffer1 filter access-list 110
monitor capture buffer pcap-bufferA filter access-list 120
```

!-- Enable the capture point in order to start packet data capture.

```
monitor capture point start pcap-point1
monitor capture point start pcap-point2
monitor capture point start pcap-pointA
monitor capture point start pcap-pointB
```

!-- Verify the configuration.

```
show monitor capture point all
show monitor capture buffer all
```

```
!-- Disable the capture point, and stop the packet data capture process.
```

```
monitor capture point stop pcap-point1  
monitor capture point stop pcap-point2  
monitor capture point stop pcap-pointA  
monitor capture point stop pcap-pointB
```

```
!-- Export the data for analysis.
```

```
monitor capture buffer pcap-buffer1 export tftp://192.0.2.100/1.cap  
monitor capture buffer pcap-bufferA export tftp://192.0.2.100/A.cap
```

참고: 이 기능은 Cisco IOS Software 릴리스 12.4(20)T에서 도입되었습니다. 버전 12.4 코드는 패킷의 처음 512바이트만 캡처하므로 버전 15.x를 사용하는 것이 좋습니다.

다음을 확인합니다.

현재 이 구성에 대해 사용 가능한 확인 절차가 없습니다.

문제 해결

현재 이 컨피그레이션에 사용할 수 있는 특정 문제 해결 정보가 없습니다.

관련 정보

- [임베디드 패킷 캡처](#)
- [기술 지원 및 문서 - Cisco Systems](#)