Nexus 7000의 Ethanalyzer 문제 해결 가이드 사용

목차

소개

이 문서에서는 Wireshark 기반 제어 패킷을 위한 Cisco NX-OS 통합 패킷 캡처 툴인 Ethanalyzer에 대해 설명합니다.

배경 정보

Wireshark는 여러 산업과 교육 기관에서 널리 사용되는 오픈 소스 네트워크 프로토콜 분석기입니다. 패킷 캡처 라이브러리인 libpcap에서 캡처한 패킷을 디코딩합니다. Cisco NX-OS는 패킷 캡처를 지원하기 위해 libpcap 라이브러리를 사용하는 Linux 커널에서 실행됩니다.

Ethanalyzer를 사용하면 다음을 수행할 수 있습니다.

- 수퍼바이저가 보내거나 받은 패킷을 캡처합니다.
- 캡처할 패킷 수를 설정합니다.
- 캡처할 패킷의 길이를 설정합니다.
- 요약 또는 자세한 프로토콜 정보와 함께 패킷을 표시합니다.
- 캡처된 패킷 데이터를 열고 저장합니다.
- 여러 조건에서 캡처된 패킷을 필터링합니다.
- 여러 기준에 표시할 패킷을 필터링합니다.
- 제어 패킷의 내부 7000 헤더를 디코딩합니다.

Ethanalyzer는 다음을 수행할 수 없습니다.

- 네트워크에 문제가 발생할 경우 경고합니다. 그러나 Ethanalyzer를 사용하면 문제의 원인을 파악할 수 있습니다.
- 하드웨어에서 전달되는 데이터 플레인 트래픽을 캡처합니다.
- 인터페이스별 캡처 지원

출력 옵션

이것은 ethanalyzer local interface inband 명령의 **출력**에 대한 요약 보기입니다. '?' 옵션에 도움말이 표시됩니다.

```
DC# ethanalyzer local interface inband ?
  <CR>
  >                     Redirect it to a file
  >>                    Redirect it to a file in append mode
  autostop              Capture autostop condition
  capture-filter        Filter on ethanalyzer capture
  capture-ring-buffer   Capture ring buffer option
  decode-internal       Include internal system header decoding
  detail                Display detailed protocol information
  display-filter        Display filter on frames captured
  limit-captured-frames Maximum number of frames to be captured (default is
                        10)
  limit-frame-size      Capture only a subset of a frame
  raw                   Hex/Ascii dump the packet with possibly one line
                        summary
  write                 Filename to save capture to
  |                     Pipe command output to filter

DC# ethanalyzer local interface inband
Capturing on inband
2013-02-10 22:58:09.660171 00:23:33:74:47:05 -> 01:80:c2:00:00:00 STP Conf. Root = 32768/1/00:23:33:74:47:00  Cost = 0
    Port = 0x8006
2013-02-10 22:58:09.696505   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 22:58:09.697311   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 22:58:10.018963   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 22:58:10.086445 00:26:99:c7:f0:c3 -> 01:00:0c:cc:cc:cd STP RST. Root = 32768/96/00:23:04:ee:be:01  Cost = 0
    Port = 0x905e
2013-02-10 22:58:10.086608 00:26:99:c7:f0:c3 -> 01:00:0c:cc:cc:cd STP RST. Root = 32768/96/00:23:04:ee:be:01  Cost = 0
    Port = 0x905e
2013-02-10 22:58:10.086667 88:43:e1:c7:4d:b8 -> 01:80:c2:00:00:00 STP RST. Root = 32768/0/00:0d:ec:a3:96:3c  Cost = 3
    Port = 0x9000
```

자세한 프로토콜 정보를 보려면 'detail' 옵션을 사용하십시오. 필요한 경우 ^C를 사용하여 중단한 후 캡처 중간에 스위치 프롬프트를 다시 가져올 수 있습니다.

```
DC# ethanalyzer local interface inband detail
Capturing on inband
Frame 1 (106 bytes on wire, 74 bytes captured)
    Arrival Time: Feb 10, 2013 23:00:24.253088000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 106 bytes
    Capture Length: 74 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:eigrp]
Ethernet II, Src: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44), Dst: 01:00:5e:00:00:0a
(01:00:5e:00:00:0a)
    Destination: 01:00:5e:00:00:0a (01:00:5e:00:00:0a)
        Address: 01:00:5e:00:00:0a (01:00:5e:00:00:0a)
        .... ...1 .... .... .... .... = IG bit: Group address (multicast/broadca
st)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Source: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44)
        Address: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Type: IP (0x0800)
Internet Protocol, Src: 10.10.18.6 (10.10.18.6), Dst: 224.0.0.10 (224.0.0.10)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
        1100 00.. = Differentiated Services Codepoint: Class Selector 6 (0x30)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    ----------------------------------------SNIP----------------------------------------
```

필터 옵션

캡처 필터

캡처 중에 어떤 패킷을 표시하거나 디스크에 저장할지 선택하려면 'capture-filter' 옵션을 사용합니다. 캡처 필터는 필터링하는 동안 높은 캡처 속도를 유지합니다. 패킷에 대해 전체 해부가 수행되지 않았으므로 필터 필드가 미리 정의되어 있으며 제한됩니다.

디스플레이 필터

캡처 파일(tmp 파일)의 보기를 변경하려면 'display-filter' 옵션을 사용하십시오. 디스플레이 필터는 완전히 구분된 패킷을 사용하므로, 네트워크 추적 파일을 분석할 때 매우 복잡하고 고급 필터링을 수행할 수 있습니다. 그러나 tmp 파일은 모든 패킷을 먼저 캡처한 다음 원하는 패킷만 표시하므로 빠르게 채울 수 있습니다.

이 예에서는 'limit-captured-frames'가 5로 설정됩니다. 'capture-filter' 옵션을 사용하면 Ethanalyzer는 'host 10.10.10.2' 필터와 일치하는 5개의 패킷을 표시합니다. 'display-filter' 옵션을 사용하면 Ethanalyzer는 먼저 5개의 패킷을 캡처한 다음 'ip.addr==10.10.10.2' 필터와 일치하는 패킷만 표시합니다.

```
DC# ethanalyzer local interface inband capture-filter "host 10.10.10.2" limit-captured-frames 5
Capturing on inband
2013-02-10 12:51:52.150404   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:51:52.150480   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:51:52.496447   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:51:52.497201   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:51:53.149831   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
5 packets captured

DC# ethanalyzer local interface inband display-filter "ip.addr==10.10.10.2" limit-captured-frames 5
Capturing on inband
2013-02-10 12:53:54.217462   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 12:53:54.217819   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2 packets captured
```

쓰기 옵션

쓰기

'write' 옵션을 사용하면 나중에 분석할 수 있도록 캡처 데이터를 Cisco Nexus 7000 Series Switch의 스토리지 디바이스(예: boothflash 또는 logflash) 중 하나에 있는 파일에 쓸 수 있습니다. 캡처 파일 크기는 10MB로 제한됩니다.

'write' 옵션이 있는 Ethanalyzer 명령의 예로는 **ethanalyzer 로컬 인터페이스 인밴드 write bootflash:capture**_*file_name이 있습니다*. 'capture-filter'와 출력 파일 이름이 'first-capture'인 'write' 옵션의 예는 다음과 같습니다.

```
DC# ethanalyzer local interface inband capture-filter "host 10.10.10.2" limit-captured-frames 5 write ?
  bootflash:  Filename
  logflash:   Filename
  slot0:      Filename
  usb1:       Filename
  usb2:       Filename
  volatile:   Filename
DC# ethanalyzer local interface inband capture-filter "host 10.10.10.2" limit-captured-frames 5 write
    bootflash:first-capture
```

캡처 데이터를 파일에 저장하면 캡처된 패킷은 기본적으로 터미널 창에 표시되지 않습니다. 'display' 옵션은 캡처 데이터를 파일에 저장하는 동안 Cisco NX-OS가 패킷을 표시하도록 강제합니다.

캡처-링-버퍼

'capture-ring-buffer' 옵션은 지정된 시간(초), 지정된 파일 수 또는 지정된 파일 크기 이후에 여러 파일을 만듭니다. 이 스크린샷에는 이러한 옵션에 대한 정의가 나와 있습니다.

```
DC# ethanalyzer local interface inband capture-ring-buffer ?
  duration  Stop writing to the file or switch to the next file after value
            seconds have elapsed
  files     Stop writing to capture files after value number of files were
            written or begin again with the first file after value number of
            files were written (form a ring buffer)
  filesize  Stop writing to a capture file or switch to the next file after it
            reaches a size of value kilobytes
```

읽기 옵션

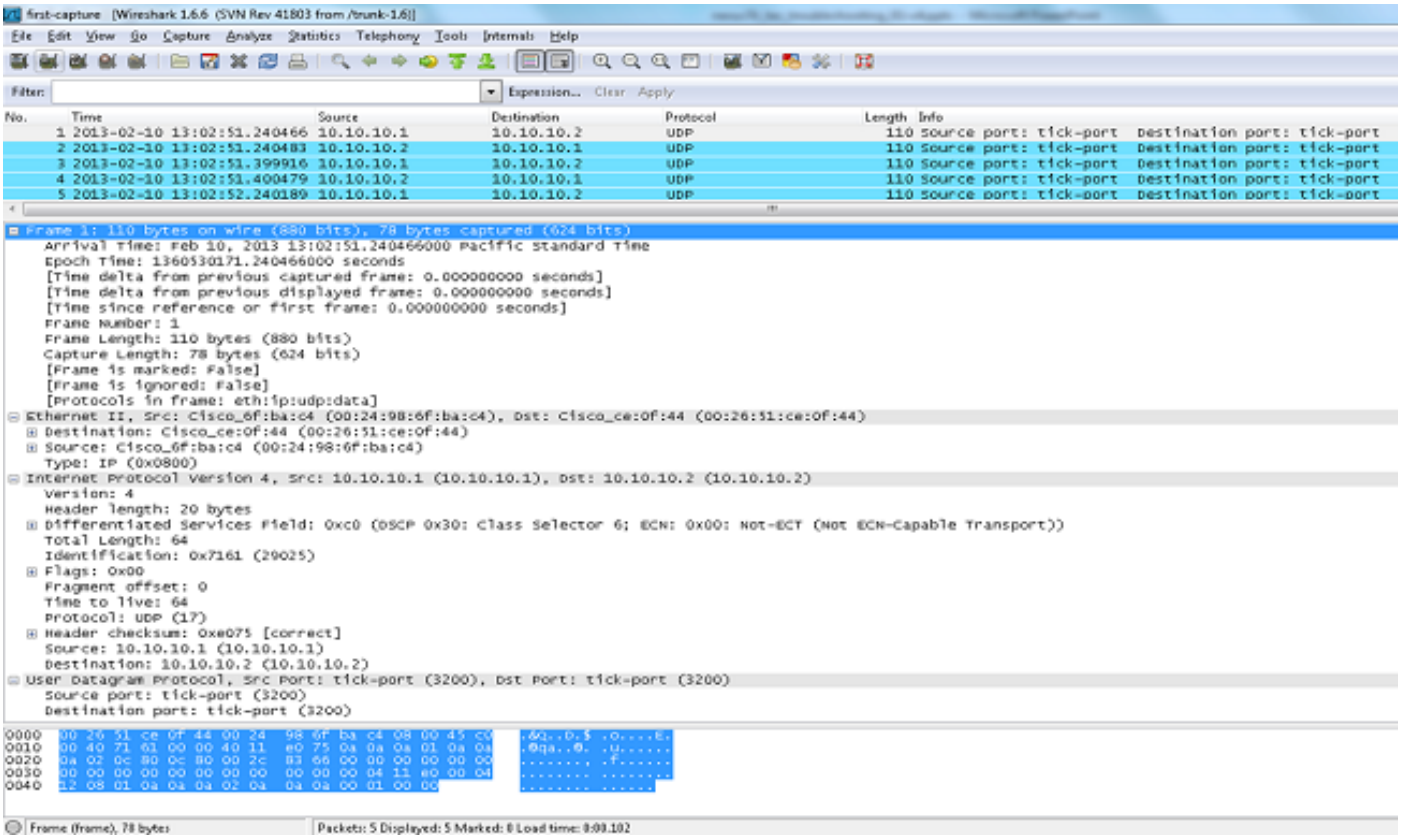
'읽기' 옵션을 사용하면 디바이스 자체에 저장된 파일을 읽을 수 있습니다.

```
DC# ethanalyzer local read bootflash:first-capture
2013-02-10 13:02:51.240466   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 13:02:51.240483   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 13:02:51.399916   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200
2013-02-10 13:02:51.400479   10.10.10.2 -> 10.10.10.1   UDP Source port: 3200  Destination port: 3200
2013-02-10 13:02:52.240189   10.10.10.1 -> 10.10.10.2   UDP Source port: 3200  Destination port: 3200

DC# ethanalyzer local read bootflash:first-capture detail
Frame 1 (110 bytes on wire, 78 bytes captured)
--------------------------SNIP-------------------------------------------------
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:24:98:6f:ba:c4 (00:24:98:6f:ba:c4), Dst: 00:26:51:ce:0f:44
(00:26:51:ce:0f:44)
    Destination: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44)
        Address: 00:26:51:ce:0f:44 (00:26:51:ce:0f:44)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Source: 00:24:98:6f:ba:c4 (00:24:98:6f:ba:c4)
        Address: 00:24:98:6f:ba:c4 (00:24:98:6f:ba:c4)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Type: IP (0x0800)
Internet Protocol, Src: 10.10.10.1 (10.10.10.1), Dst: 10.10.10.2 (10.10.10.2)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0xc0 (DSCP 0x30: Class Selector 6; ECN: 0x00)
-----------------------------------SNIP-------------------------------------
```

서버나 PC로 파일을 전송하고 Wireshark 또는 cap 또는 pcap 파일을 읽을 수 있는 다른 응용 프로그램으로 파일을 읽을 수도 있습니다.

```
DC# copy bootflash:first-capture tftp:
Enter vrf (If no input, current vrf 'default' is considered): management
Enter hostname for the tftp server: 192.168.21.22
Trying to connect to tftp server......
Connection to Server Established.
TFTP put operation was successful
Copy complete.
```



디코드-내부 및 세부 정보 옵션

'decode-internal' 옵션은 Nexus 7000에서 패킷을 전달하는 방법에 대한 내부 정보를 보고합니다. 이 정보는 CPU를 통한 패킷 흐름을 이해하고 문제를 해결하는 데 도움이 됩니다.

```
DC# ethanalyzer local interface inband decode-internal capture-filter "host 10.10.10.2" limit-captured-frames 5
detail
Capturing on inband
NXOS Protocol
    NXOS VLAN: 0====================➔VLAN in decimal=0=L3 interface
    NXOS SOURCE INDEX: 1024 ========================➔PIXM LTL source index in decimal=400=SUP inband
    NXOS DEST INDEX: 2569=========================➔PIXM LTL destination index in decimal=0xa09=e1/25
Frame 1 (78 bytes on wire, 78 bytes captured)
    Arrival Time: Feb 10, 2013 22:40:02.216492000
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 78 bytes
    Capture Length: 78 bytes
    [Frame is marked: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:26:51:ce:0f:43 (00:26:51:ce:0f:43), Dst: 00:24:98:6f:ba:c3
(00:24:98:6f:ba:c3)
    Destination: 00:24:98:6f:ba:c3 (00:24:98:6f:ba:c3)
        Address: 00:24:98:6f:ba:c3 (00:24:98:6f:ba:c3)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory
 default)
    Source: 00:26:51:ce:0f:43 (00:26:51:ce:0f:43)
----------------------------------------------SNIP-----------------------------------------
```

NX-OS 인덱스를 16진수로 변환한 다음 **show system internal pixm info ltl x 명령**을 사용하여 로컬 대상 논리(LTL) 인덱스를 물리적 또는 논리적 인터페이스에 매핑합니다.

Capture-filter 값의 예

IP 호스트로 또는 IP 호스트로부터 트래픽 캡처

```
host 10.1.1.1
```

IP 주소 범위에서 트래픽 캡처

```
net 172.16.7.0/24
net 172.16.7.0 mask 255.255.255.0
```

IP 주소 범위에서 트래픽 캡처

```
src net 172.16.7.0/24
src net 172.16.7.0 mask 255.255.255.0
```

IP 주소 범위로 트래픽 캡처

```
dst net 172.16.7.0/24
dst net 172.16.7.0 mask 255.255.255.0
```

특정 프로토콜에서만 트래픽 캡처 - DNS 트래픽만 캡처

DNS는 Domain Name System Protocol입니다.

```
port 53
```

특정 프로토콜에서만 트래픽 캡처 - DHCP 트래픽만 캡처

DHCP는 Dynamic Host Configuration Protocol입니다.

```
port 67 or port 68
```

특정 프로토콜이 아닌 트래픽 캡처 - HTTP 또는 SMTP 트래픽 제외

SMTP는 Simple Mail Transfer Protocol입니다.

```
host 172.16.7.3 and not port 80 and not port 25
```

특정 프로토콜이 아닌 트래픽 캡처 - ARP 및 DNS 트래픽 제외

ARP는 Address Resolution Protocol입니다.

```
port not 53 and not arp
```

IP 트래픽만 캡처 - ARP 및 STP와 같은 하위 레이어 프로토콜 제외

STP는 스패닝 트리 프로토콜입니다.

```
ip
```

유니캐스트 트래픽만 캡처 - 브로드캐스트 및 멀티캐스트 알림 제외

```
not broadcast and not multicast
```

레이어 4 포트 범위 내에서 트래픽 캡처

```
tcp portrange 1501-1549
```

이더넷 유형 기반 트래픽 캡처 - EAPOL 트래픽 캡처

EAPOL은 LAN을 통한 확장 가능 인증 프로토콜입니다.

```
ether proto 0x888e
```

IPv6 캡처 해결 방법

```
ether proto 0x86dd
```

IP 프로토콜 유형 기반 트래픽 캡처

```
ip proto 89
```

Reject Ethernet Frames Based on MAC Address(MAC 주소 기반 이더넷 프레임 거부) - LLDP 멀티캐스트 그룹에 속하는 트래픽을 제외합니다.

LLDP는 Link Layer Discovery Protocol입니다.

```
not ether dst 01:80:c2:00:00:0e
```

UDLD, VTP 또는 CDP 트래픽 캡처

UDLD는 단방향 링크 감지, VTP는 VLAN 트렁킹 프로토콜, CDP는 Cisco Discovery Protocol입니다
.

```
ether host 01:00:0c:cc:cc:cc
```

MAC 주소로 또는 MAC 주소로부터 트래픽 캡처

```
ether host 00:01:02:03:04:05
```

> **참고:**
> 및 = &&
> 또는 = ||
> not = !
> MAC 주소 형식: xx:xx:xx:xx:xx

공통 컨트롤 플레인 프로토콜

- UDLD: DMAC(Destination Media Access Controller) = 01-00-0C-CC-CC 및 EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02, EthType = 0x8809. LACP는 Link Aggregation Control Protocol의 약자입니다.
- STP: DMAC = 01:80:C2:00:00:00 및 EthType = 0x4242 - 또는 - DMAC = 01:00:0C:CC:CC:CD 및 EthType = 0x010B
- CDP: DMAC = 01-00-0C-CC-CC-CC, EthType = 0x2000
- LLDP: DMAC = 01:80:C2:00:00:0E 또는 01:80:C2:00:00:03 또는 01:80:C2:00:00:00 및 EthType = 0x88CC
- DOT1X: DMAC = 01:80:C2:00:00:03 및 EthType = 0x888E. DOT1X는 IEEE 802.1x를 나타냅니다.
- IPv6: 이더넷 유형 = 0x86DD
- UDP 및 TCP 포트 번호 목록

알려진 문제

Cisco 버그 ID CSCue48854: Ethanalyzer capture-filter는 SUP2의 CPU에서 트래픽을 캡처하지 않습니다.

Cisco 버그 ID CSCtx79409: decode-internal과 함께 캡처 필터를 사용할 수 없습니다.

Cisco 버그 ID CSCvi02546: SUP3에서 생성된 패킷에 FCS가 있을 수 있습니다. 이는 정상적인 동작입니다.

관련 정보

- Wireshark: 캡처필터
- Wireshark: 디스플레이필터
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.