使用Nexus 7000上的Ethanalyzer故障排除指南

目錄

簡介

本文檔介紹Ethanalyzer，它是Cisco NX-OS整合資料包捕獲工具，用於基於Wireshark控制資料包。

背景資訊

Wireshark是一種開源網路協定分析器，廣泛用於許多行業和教育機構。它對libpcap（資料包捕獲庫）捕獲的資料包進行解碼。Cisco NX-OS在Linux核心上運行，該核心使用libpcap庫來支援資料包捕獲。

使用Ethanalyzer，您可以：

- 捕獲Supervisor傳送或接收的資料包。
- 設定要捕獲的資料包數。
- 設定要捕獲的資料包的長度。
- 顯示包含摘要或詳細協定資訊的資料包。
- 開啟並儲存捕獲的資料包資料。
- 過濾根據許多條件捕獲的資料包。
- 過濾要在多個標準上顯示的資料包。
- 解碼控制資料包的內部7000報頭。

Ethanalyzer無法：

- 當您的網路遇到問題時發出警告。但是，Ethanalyzer可以幫助您確定問題的原因。
- 捕獲在硬體中轉發的資料平面流量。
- 支援特定於介面的捕獲。

輸出選項

這是**ethanalyzer local interface inband**命令**輸出的摘要視**圖。「？」選項顯示幫助。

```
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
```

使用「detail」選項可獲得詳細的協定資訊。^C可用於中止並在擷取過程中傳回交換器提示（如需要）。

```
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----------------------------------------
```

篩選選項

Capture-filter

使用「capture-filter」選項可以選擇在捕獲期間顯示或儲存到磁碟的資料包。捕獲過濾器在過濾時保持高捕獲率。由於尚未對資料包進行完全解除，因此過濾器欄位是預定義並受限制的。

Display-filter

使用「display-filter」選項可更改捕獲檔案（tmp檔案）的檢視。顯示過濾器使用完全剖析的資料包，因此可以在分析網路跟蹤檔案時執行非常複雜和高級的過濾。但是，tmp檔案可以快速填充，因為它首先捕獲所有資料包，然後僅顯示所需資料包。

在此示例中，「limit-captured-frames」設定為5。使用「capture-filter」選項，Ethanalyzer向您顯示五個與過濾器「host 10.10.10.2」匹配的資料包。使用「display-filter」選項，Ethanalyzer首先捕獲五個資料包，然後僅顯示與過濾器「ip.addr==10.10.10.2」匹配的資料包。

```
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
```

寫入選項

寫入

使用「write」選項，可以將捕獲資料寫入到Cisco Nexus 7000系列交換機上某個儲存裝置（如bootflash或logflash）中的檔案，供以後分析。捕獲檔案大小限製為10 MB。

帶有「write」選項的Ethanalyzer命令示例**是ethanalyzer local interface inband write bootflash***:capture_file_name*。以下是具有「capture-filter」的「write」選項和輸出檔名「first-capture」的示例：

```
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
```

將捕獲資料儲存到檔案時，捕獲的資料包預設不會顯示在終端視窗中。「display」（顯示）選項強制思科NX-OS在將捕獲資料儲存到檔案的同時顯示資料包。

Capture-ring-buffer

「capture-ring-buffer」選項在指定的秒數、指定的檔案數或指定的檔案大小後建立多個檔案。這些選項的定義位於此螢幕抓圖中：

```
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
```

讀取選項

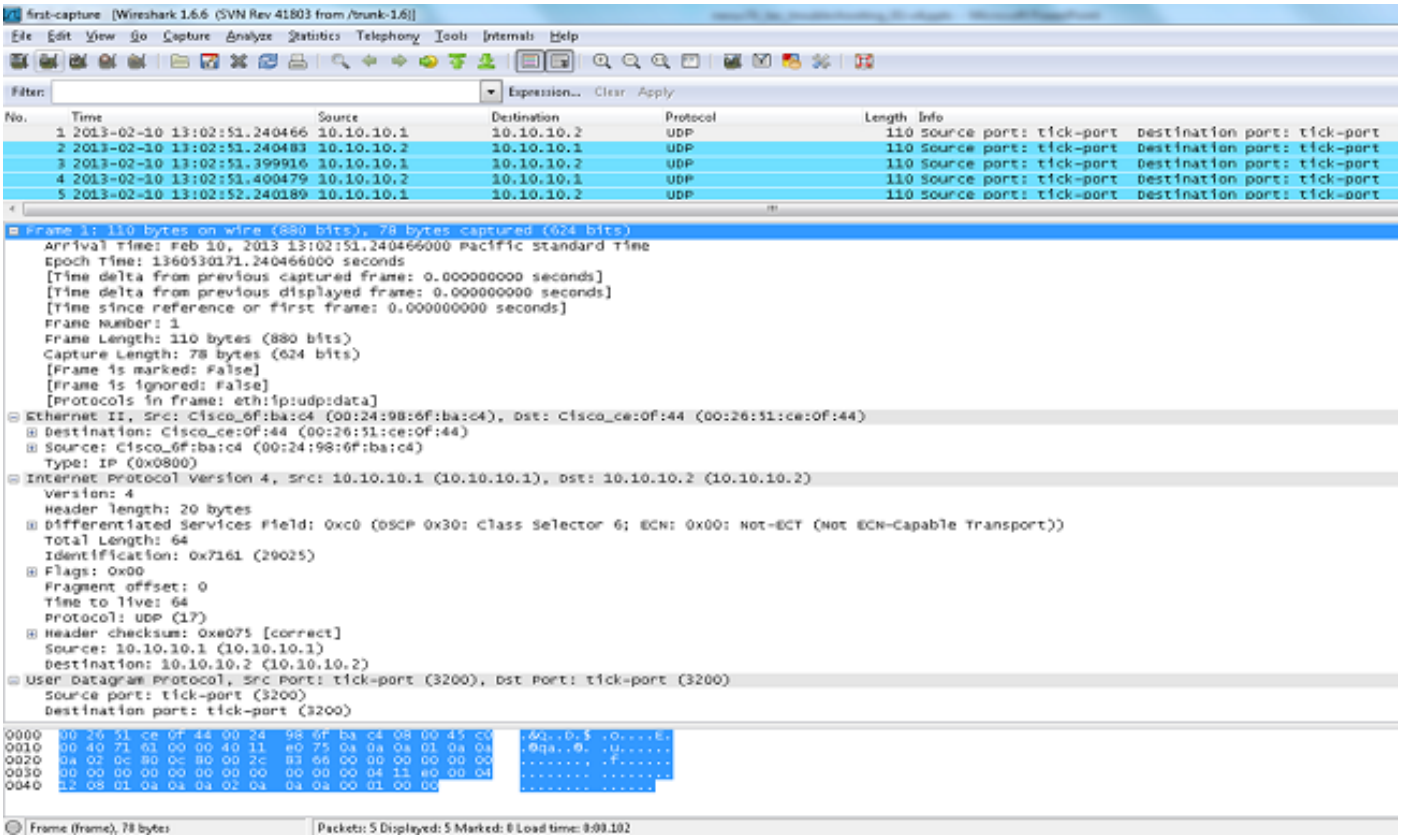
通過「讀取」選項可以讀取裝置本身上儲存的檔案。

```
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-----------------------------------------
```

您也可以將檔案傳輸到伺服器或PC，並使用Wireshark或任何其它可以讀取cap或pcap檔案的應用程式讀取該檔案。

```
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.
```



Decode-internal with Detail選項

「decode-internal」選項報告有關Nexus 7000如何轉發資料包的內部資訊。此資訊有助於您瞭解通過CPU的資料包流並對其進行故障排除。

```
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-----------------------------------------
```

將NX-OS索引轉換為十六進位制，然後使用**show system internal pixm info ltl x**命令將本地目標邏輯(LTL)索引對映到物理或邏輯介面。

Capture-filter值示例

擷取IP主機之間的流量

```
host 10.1.1.1
```

捕獲來往於某個IP地址範圍的流量

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

從一系列IP位址擷取流量

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

擷取到一系列IP位址的流量

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

僅捕獲特定協定上的流量 — 僅捕獲DNS流量

DNS是域名系統協定。

```
port 53
```

僅捕獲特定協定上的流量 — 僅捕獲DHCP流量

DHCP是動態主機配置協定。

```
port 67 or port 68
```

捕獲未使用特定協定的流量 — 排除HTTP或SMTP流量

SMTP是一種簡單郵件傳輸協定。

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

捕獲未使用特定協定的流量 — 排除ARP和DNS流量

ARP是位址解析通訊協定。

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

僅捕獲IP流量 — 排除ARP和STP等低層協定

STP是生成樹協定。

```
ip
```

僅捕獲單播流量 — 排除廣播和組播通告

```
not broadcast and not multicast
```

擷取第4層連線埠範圍內的流量

```
tcp portrange 1501-1549
```

根據乙太網路型別擷取流量 — 擷取EAPOL流量

EAPOL是LAN上的可擴充驗證通訊協定。

```
ether proto 0x888e
```

IPv6捕獲解決方法

```
ether proto 0x86dd
```

根據IP通訊協定型別擷取流量

```
ip proto 89
```

根據MAC地址拒絕乙太網幀 — 排除屬於LLDP組播組的流量

LLDP是鏈路層發現協定。

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

捕獲UDLD、VTP或CDP流量

UDLD是單向鏈路檢測，VTP是VLAN中繼協定，CDP是Cisco發現協定。

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

捕獲來往於MAC地址的流量

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

> **附註**：
> 和= &&
> 或= ||
> 不是= !
> MAC地址格式： xx:xx:xx:xx:xx:xx

通用控制平面通訊協定

- UDLD：目標媒體訪問控制器(DMAC)= 01-00-0C-CC-CC-CC，乙太網型別= 0x0111

- LACP:DMAC = 01:80:C2:00:00:02和EthType = 0x8809。LACP代錶鏈路聚合控制協定。
- STP:DMAC = 01:80:C2:00:00:00和EthType = 0x4242 — 或 — DMAC = 01:00:0C:CC:CC:CD和EthType = 0x010B
- CDP:DMAC = 01-00-0C-CC-CC-CC，乙太網型別= 0x2000
- LLDP: DMAC = 01:80:C2:00:00:0E或01:80:C2:00:00:03或01:80:C2:00:00:00和EthType = 0x88CC
- DOT1X: DMAC = 01:80:C2:00:00:03和EthType = 0x888E。DOT1X代表IEEE 802.1x。
- IPv6：乙太網型別= 0x86DD
- UDP和TCP埠號清單

已知的問題

思科錯誤ID CSCue48854: Ethanalyzer capture-filter不捕獲SUP2上CPU的流量。

思科錯誤ID CSCtx79409: 不能將捕獲篩選器與decode-internal一起使用。

思科錯誤ID CSCvi02546: SUP3生成的資料包可以具有FCS，這是預期行為。

相關資訊

- **Wireshark：捕獲過濾器**
- **Wireshark:DisplayFilters**
- **技術支援與文件 - Cisco Systems**

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。