使用Nexus 7000上Ethanalyzer的故障排除指南

目录

简介

本文档介绍Ethanalyzer，这是一款基于Wireshark的控制数据包的Cisco NX-OS集成数据包捕获工具。

背景信息

Wireshark是一种开源网络协议分析器，广泛应用于许多行业和教育机构。它解码数据包捕获库libpcap捕获的数据包。Cisco NX-OS在Linux内核上运行，该内核使用libpcap库来支持数据包捕获。

使用Ethanalyzer，您可以：

- 捕获主控引擎发送或接收的数据包。
- 设置要捕获的数据包数量。
- 设置要捕获的数据包的长度。
- 显示包含摘要或详细协议信息的数据包。
- 打开并保存捕获的数据包数据。
- 过滤根据许多条件捕获的数据包。
- 过滤要在多个条件中显示的数据包。
- 解码控制数据包的内部7000报头。

Ethanalyzer无法：

- 网络出现问题时发出警告。但是，Ethanalyzer可以帮助您确定问题的原因。
- 捕获在硬件中转发的数据平面流量。
- 支持特定于接口的捕获。

输出选项

这是**ethanalyzer local interface inband**命令输出的摘要视图。“？”选项显示帮助。

```
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”选项可获得详细的协议信息。^C可用于中止并在捕获过程中重新获得交换机提示（如果需要）。

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

过滤器选项

捕获过滤器

使用“capture-filter”选项可选择在捕获期间显示或保存到磁盘的数据包。捕获过滤器在过滤时保持高捕获率。由于尚未对数据包进行完全解剖，因此过滤器字段是预定义并受限制的。

Display-filter

使用“display-filter”选项更改捕获文件（tmp文件）的视图。显示过滤器使用完全分离的数据包，因此您可以在分析网络跟踪文件时执行非常复杂和高级的过滤。但是，tmp文件可以快速填充，因为它首先捕获所有数据包，然后仅显示所需数据包。

在本示例中，“limit-captured-frames”设置为5。使用“capture-filter”（捕获过滤器）选项，Ethanalyzer将显示五个与过滤器“host 10.10.10.2”匹配的数据包。使用“display-filter”选项，Ethanalyzer首先捕获五个数据包，然后仅显示与过滤器“ip.addr==10.10.10.2”匹配的数据包。

```
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
```

写入选项

写入

通过“write”选项，您可以将捕获数据写入Cisco Nexus 7000系列交换机上某个存储设备（如bootflash或logflash）中的文件，以便稍后进行分析。捕获文件大小限制为10 MB。

带有“write”选项的Ethanalyzer命令示例**是ethanalyzer local interface inband write bootflash:***capture_file_name*。带有“capture-filter”的“write”选项和输出文件名为“first-capture”的示例如下：

```
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
```

将捕获数据保存到文件时，捕获的数据包默认不会显示在终端窗口中。“display”（显示）选项强制Cisco NX-OS在将捕获数据保存到文件的同时显示数据包。

Capture-ring-buffer

“capture-ring-buffer”选项在指定的秒数、指定的文件数或指定的文件大小后创建多个文件。以下屏幕截图显示了这些选项的定义：

```
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
```

读取选项

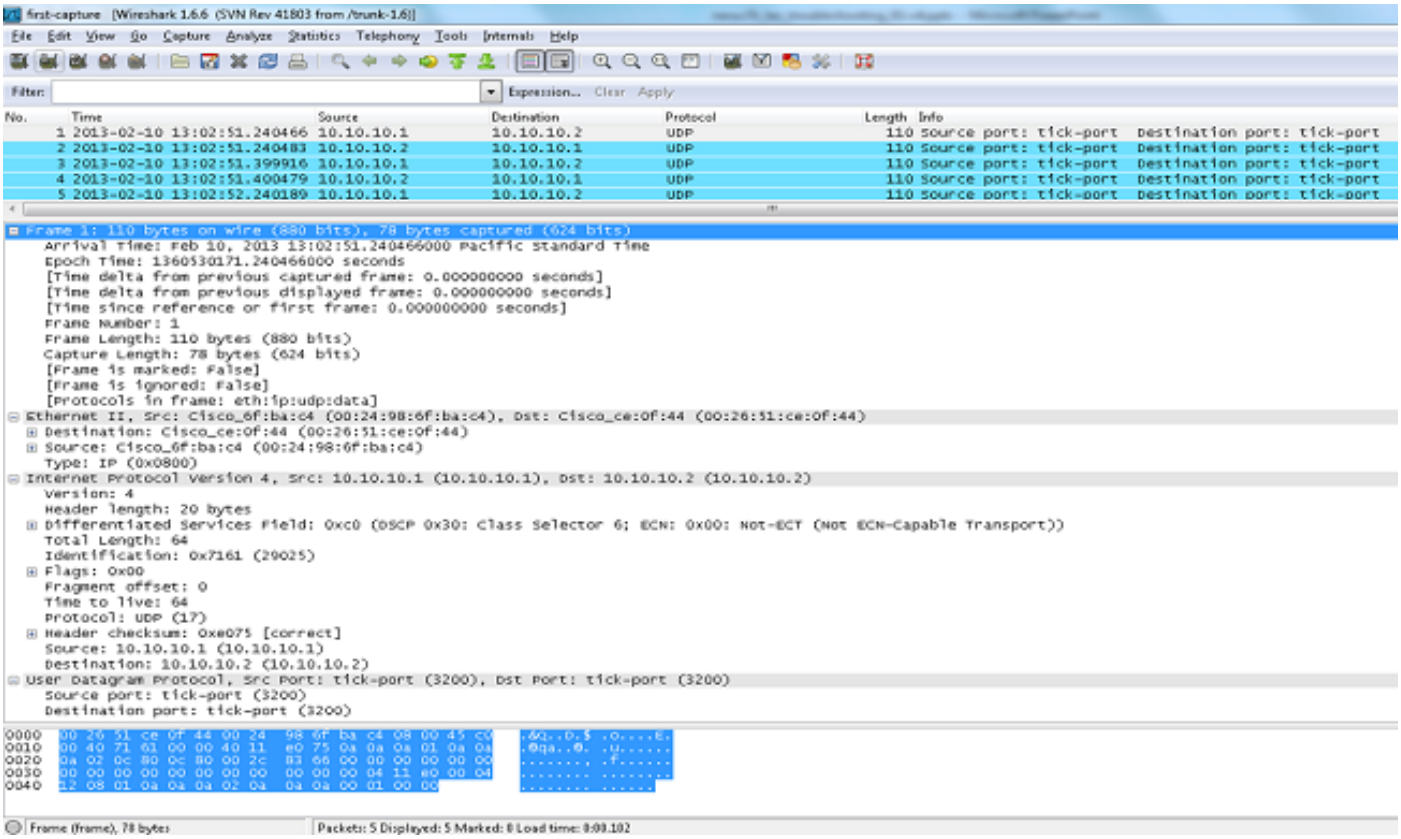
通过“read”选项，您可以读取设备本身上保存的文件。

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

您也可以将文件传输到服务器或PC，并使用Wireshark或任何其它可以读取cap或pcap文件的应用程序读取该文件。

```
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选项

“decode-internal”选项报告有关Nexus 7000如何转发数据包的内部信息。此信息有助于您了解数据包通过CPU的流程并对其进行故障排除。

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

将NX-OS索引转换为十六进制，然后使用**show system internal pixm info ltl x**命令将本地目标逻辑(LTL)索引映射到物理或逻辑接口。

Capture-filter值的示例

捕获流向IP主机或流向IP主机的流量

```
host 10.1.1.1
```

捕获来往于某个IP地址范围的流量

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

捕获来自一系列IP地址的流量

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

捕获流向一系列IP地址的流量

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

仅捕获特定协议上的流量 — 仅捕获DNS流量

DNS是域名系统协议。

```
port 53
```

仅捕获特定协议上的流量 — 仅捕获DHCP流量

DHCP是动态主机配置协议。

```
port 67 or port 68
```

捕获未使用特定协议的流量 — 排除HTTP或SMTP流量

SMTP是简单邮件传输协议。

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

捕获未使用特定协议的流量 — 排除ARP和DNS流量

ARP是地址解析协议。

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

仅捕获IP流量 — 排除ARP和STP等下层协议

STP是生成树协议。

```
ip
```

仅捕获单播流量 — 排除广播和组播通告

```
not broadcast and not multicast
```

捕获第4层端口范围内的流量

```
tcp portrange 1501-1549
```

根据以太网类型捕获流量 — 捕获EAPOL流量

EAPOL是LAN上的可扩展身份验证协议。

```
ether proto 0x888e
```

IPv6捕获解决方法

```
ether proto 0x86dd
```

根据IP协议类型捕获流量

```
ip proto 89
```

根据MAC地址拒绝以太网帧 — 排除属于LLDP组播组的流量

LLDP是链路层发现协议。

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

捕获UDLD、VTP或CDP流量

UDLD是单向链路检测，VTP是VLAN中继协议，CDP是Cisco发现协议。

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

捕获流入或流出MAC地址的流量

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

> **注意：**
> 和= &&
> 或= ||
> not = !
> MAC地址格式：xx:xx:xx:xx:xx:xx

通用控制平面协议

- UDLD：目标媒体访问控制器(DMAC)= 01-00-0C-CC-CC-CC，以太网类型= 0x0111

- LACP:DMAC = 01:80:C2:00:00:02，以太网类型= 0x8809。LACP代表链路汇聚控制协议。
- 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，以太网类型= 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：以太网类型= 0x86DD
- UDP和TCP端口号列表

已知问题

Cisco bug ID CSCue48854:Ethanalyzer capture-filter不捕获来自SUP2上CPU的流量。

Cisco Bug ID CSCtx79409：不能将捕获过滤器与decode-internal一起使用。

Cisco Bug ID CSCvi02546: SUP3生成的数据包可以有FCS，这是预期行为。

相关信息

- **Wireshark：捕获过滤器**
- **Wireshark:DisplayFilters**
- **技术支持和文档 - Cisco Systems**

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。