在连结7000故障排除指南的Ethanalyzer

目录

简介

本文描述Ethanalyzer，控制数据包的一个Cisco NX-OS集成的数据包捕获工具根据Wireshark。

Wireshark是开放原始码的软体、网络协议分析器用途广泛在许多行业间和教育机构。它解码libpcap捕获的数据包，数据包捕获库。Cisco NX-OS运行在它上面Linux内核，使用libpcap库为了支持数据包捕获。

使用Ethanalyzer，您能：

- 捕获发送的数据包或接收由Supervisor。
- 设置将捕获的数据包数量。
- 设置将捕获的数据包的长度。
- 显示有摘要或详细的协议信息的数据包。
- 打开并且保存捕获的数据包数据。
- 过滤在许多标准捕获的数据包。
- 过滤在许多标准将显示的数据包。
- 解码控制数据包的内部7000报头。

Ethanalyzer不能：

- 当您的网络遇到问题时，请警告您。然而， Ethanalyzer也许帮助您确定问题的原因。
- 捕获在硬件方面转发的数据层面流量。
- 支持特定接口的捕获。

输出选项

这是输出一张概略的视图从**ethanalyzer本地接口带内**命令的。‘？’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
```

请使用‘详细信息’选项详细的协议信息。^C可以用于在捕获中间如果必须中止和获得交换机提示符上一步。

```
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

请使用显示或保存的数据包对磁盘在捕获期间的‘捕获过滤器’选项为了选择。当过滤时，捕获过滤器保持捕获高速率。由于全双工解剖不是完成在数据包，过滤器领域预定义并且被限制。

显示过滤器

请使用‘显示过滤器’选项为了更改捕获文件(tmp文件)的视图。显示过滤器使用充分地被解剖的数据包，因此您能执行非常复杂和先进的过滤，当您分析tracefile时的网络。然而，因为首先获取所有信息包然后显示仅所需的信息包， tmp文件能迅速填装。

在本例中，‘限制捕捉帧的设置到5。使用‘捕获过滤器’选项， Ethanalyzer显示您五数据包哪匹配过滤器‘主机10.10.10.2'。使用‘显示过滤器’选项， Ethanalyzer首先获取五数据包然后显示匹配过滤器'ip.addr==10.10.10.2.的仅数据包

```
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

写道

‘请写入’选项让您写捕获数据到一个文件在其中一存储设备中(例如boothflash或logflash)在后续分析的Cisco连结7000系列交换机。捕获文件大小对10 MB被限制。

示例命令与‘写入’选项的Ethanalyzer是**带内ethanalyzer的本地接口写入Bootflash**：*capture_file_name*。示例‘写入’选项用‘捕获过滤器’，并且‘最初捕获’输出文件名是：

```
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
```

当捕获数据保存到文件时，默认情况下，获取数据包在终端窗口没有显示。当保存捕获数据到文件时，‘显示’选项强制Cisco NX-OS显示数据包。

捕获RING缓冲区

‘捕获RING缓冲区’选项在秒钟指定的编号，文件指定的编号或者指定的文件大小以后创建多个文件。那些选项的定义在此屏幕画面：

```
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
```

读选项

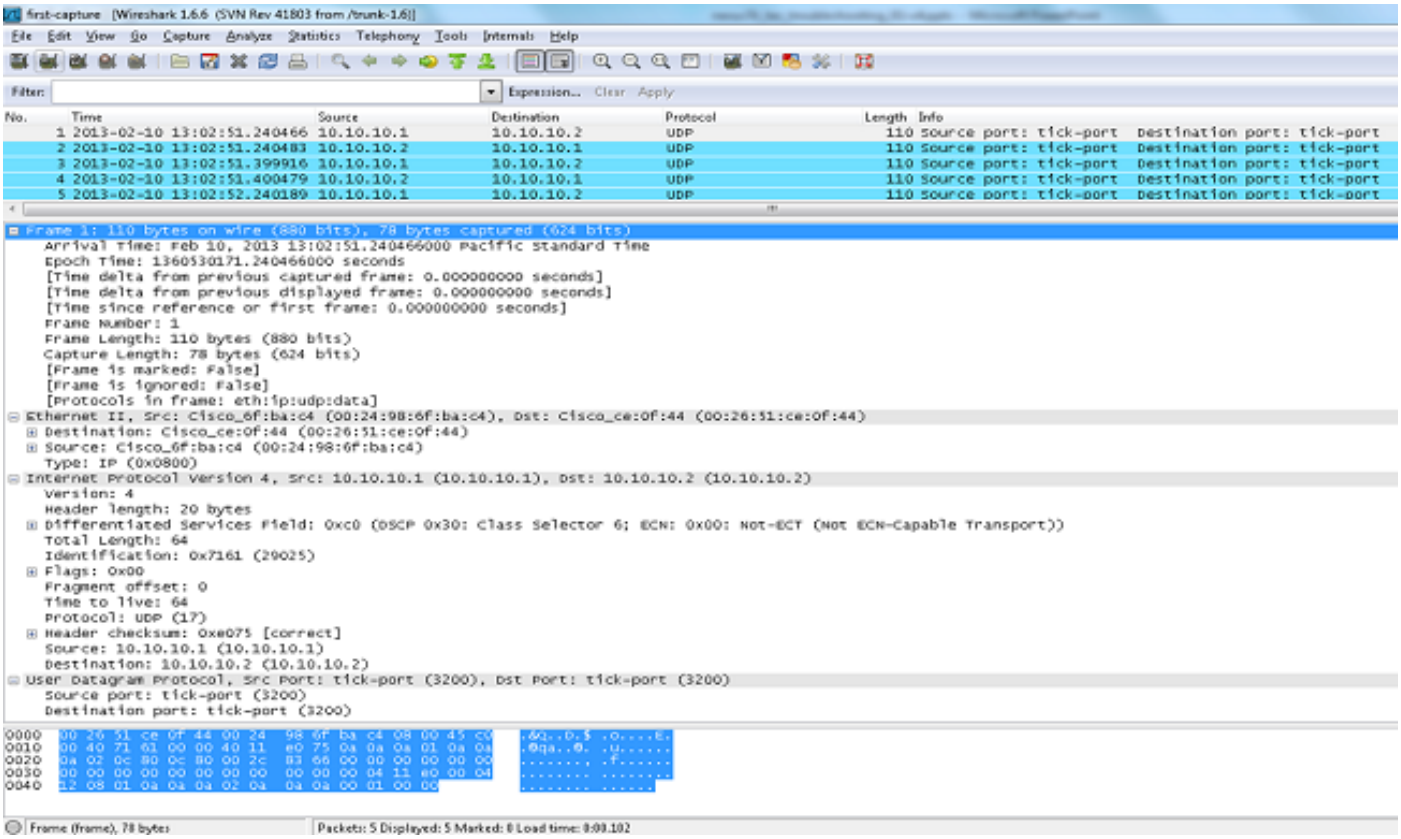
‘读的’选项在设备让您读保存的文件。

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

您能也转接文件到服务器或PC和读它与能读盖帽或pcap文件的Wireshark或其他应用程序。

```
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.
```



解码内部与详细信息选项

‘解码内部’选项报告关于连结7000如何的内部信息转发数据包。此信息帮助您了解和排除故障数据包流通过CPU。

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

转换NX-OS索引对十六进制，然后请使用**x命令show system内部pixm信息的ltl**为了映射Local Target Logic (LTL)索引到物理或逻辑接口。

捕获过滤器值示例

到/从IP主机的捕获流量

```
host 1.1.1.1
```

到/从IP地址范围的捕获流量

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

从IP地址范围的捕获流量

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

对IP地址范围的捕获流量

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

捕获仅流量在有些协议-捕获仅DNS流量

DNS是域名系统协议。

```
port 53
```

捕获仅流量在有些协议-仅捕获DHCP流量

DHCP是动态主机配置协议。

```
port 67 or port 68
```

捕获流量不在有些协议-请排除HTTP或SMTP流量

SMTP是简单邮件转发协议。

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

捕获流量不在有些协议-请排除ARP和DNS流量

ARP是地址解析协议。

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

仅捕获IP数据流-排除较低层协议类似ARP和STP

STP是生成树协议。

```
ip
```

仅捕获单播流量-排除广播并且组播通告

```
not broadcast and not multicast
```

捕获在范围的流量Layer4端口内

```
tcp portrange 1501-1549
```

捕获根据以太网类型的流量-捕获EAPOL流量

EAPOL是LAN上的可扩展认证协议。

```
ether proto 0x888e
```

IPv6捕获应急方案

```
ether proto 0x86dd
```

根据IP协议类型的捕获流量

```
ip proto 89
```

根据MAC地址的拒绝以太网帧-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或者CDP数据流

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

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

到/从MAC地址的捕获流量

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

> **注意**：
> 并且= &&
> 或者=||
> 没有=!
> MAC地址格式：xx ： xx ： xx ： xx ： xx ： xx

普通控制平面协议

- UDLD ：目的地媒介访问控制器(DMAC) = 01-00-0C-CC-CC-CC和EthType = 0x0111
- LACP ：DMAC = 01:80:C2:00:00:02和EthType = 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和EthType = 0x2000
- LLDP ：DMAC = 01:80:C2:00:00:0E或者01:80:C2:00:00:03或者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 ：EthType = 0x86DD
- UDP和TCP端口编号列表

已知问题

请参阅Cisco Bug ID CSCue48854 ：Ethanalyzer捕获过滤器不捕获从CPU的流量在SUP2。并且请参阅Cisco Bug ID CSCtx79409 ： 不能以解码内部使用捕获过滤器。

相关信息

- Wireshark ：CaptureFilters
- Wireshark ：DisplayFilters
- 技术支持和文档 - Cisco Systems