Nexus 3000/5000/7000使用Ethanalyzer工具

目錄

簡介

本文檔介紹如何在Nexus 3000/5000/7000交換機上使用內建資料包捕獲工具Ethanalyzer。

必要條件

需求

本文件沒有特定需求。

採用元件

本文檔中的資訊基於Nexus 3000、Nexus 5000和Nexus 7000交換機。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

Ethanalyzer

Ethanalyzer是排查控制平面和發往交換機CPU的流量的有用工具。Mgmt是用來對到達mgmt0介面的資料包進行故障排除的介面。入站 — 低(eth3)用於低優先順序（ping、telnet、安全外殼）CPU繫結流量，入站 — 高(eth4)用於高優先順序(生成樹協定(STP)、網橋協定資料單元、FIP)CPU繫結流量。

> **附註**：您可以使用顯示過濾器或捕獲過濾器作為選項。在Nexus 5000上首選顯示篩選器選項，在Nexus 3000和Nexus 7000上首選捕獲篩選器。

常用的顯示過濾器可在Wireshark中找到

常用的捕獲過濾器位於Wireshark

附註：由於Nexus 5000使用內部VLAN轉發幀，因此Ethanlyzer具有內部VLAN。Nexus 5000根據內部VLAN轉發幀，Ethanalyzer顯示內部VLAN。使用Ethanalyzer進行故障排除時，VLAN ID可能會造成困難。但是，可以使用**show system internal fcfwd fwcvidmap cvid**命令來確定對映。以下提供範例。

```
Nexus# ethanalyzer local interface inbound-low detail display-filter icmp
Capturing on eth3
Frame 16 (102 bytes on wire, 102 bytes captured)
     Arrival Time: Sep 7, 2011 15:42:37.081178000
     [Time delta from previous captured frame: 0.642560000 seconds]
     [Time delta from previous displayed frame: 1315424557.081178000 seconds]
     [Time since reference or first frame: 1315424557.081178000 seconds]
     Frame Number: 16
     Frame Length: 102 bytes
     Capture Length: 102 bytes
     [Frame is marked: False]
     [Protocols in frame: eth:vlan:ip:icmp:data]
Ethernet II, Src: 00:0d:ec:a3:81:bc (00:0d:ec:a3:81:bc),
Dst: 00:05:73:ce:3c:7c (00:05:73:ce:3c:7c)
     Destination: 00:05:73:ce:3c:7c (00:05:73:ce:3c:7c)
        Address: 00:05:73:ce:3c:7c (00:05:73:ce:3c:7c)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address(factory default)
     Source: 00:0d:ec:a3:81:bc (00:0d:ec:a3:81:bc)
        Address: 00:0d:ec:a3:81:bc (00:0d:ec:a3:81:bc)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address(factory default)
     Type: 802.1Q Virtual LAN (0x8100)
802.1Q Virtual LAN
     000. .... .... .... = Priority: 0
     ...0 .... .... .... = CFI: 0
     .... 0000 0011 1001 = ID: 57 <<----------
     Type: IP (0x0800)
Internet Protocol, Src: 144.1.1.63 (144.1.1.63), Dst: 144.1.1.41 (144.1.1.41)
     Version: 4
     Header length: 20 bytes
     Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
     Total Length: 84
     Identification: 0x1118 (4376)
<snip>
```

您可以看到，Ethanalyzer表示在VLAN 57（即內部VLAN）上收到資料包。但是，VLAN 57不是實際VLAN，因為57不是十六進位制。十六進位制中的57是0x0039。此命令確定十六進位制中的實際VLAN。

```
Nexus# show system internal fcfwd fwcvidmap cvid | grep 0x0039
0x0039 enet 0x01 0x0090 0100.0000.080a 0100.0000.0809
0x0039 fc 0x01 0x0090 0100.0000.0007 0100.0000.0006
```

0x0090是以十六進位制表示的實際VLAN。然後，您必須將數字轉換為十進位制，即144。此計算說明了上一幀中的實際VLAN是VLAN 144，儘管Ethanalyzer指示其為57。

以下是使用VLAN的顯示過濾器捕獲FIP幀的示例。(==.0x8914)

```
Nexus# ethanalyzer local interface inbound-hi display-filter vlan.etype==0x8914
Capturing on eth4
2011-10-18 13:36:47.047492 00:c0:dd:15:d4:41 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 56
2011-10-18 13:36:48.313531 00:c0:dd:15:d0:95 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 56
2011-10-18 13:36:49.373483 00:0d:ec:a3:81:80 -> 01:10:18:01:00:01 0x8914
PRI: 3 CFI: 0 ID: 56
2011-10-18 13:36:49.373868 00:0d:ec:a3:81:80 -> 01:10:18:01:00:01 0x8914
PRI: 3 CFI: 0 ID: 56
2011-10-18 13:36:49.374131 00:0d:ec:a3:81:80 -> 01:10:18:01:00:01 0x8914
PRI: 3 CFI: 0 ID: 56
2011-10-18 13:36:49.374378 00:0d:ec:a3:81:80 -> 01:10:18:01:00:01 0x8914
PRI: 3 CFI: 0 ID: 56
2011-10-18 13:36:49.374618 00:0d:ec:a3:81:80 -> 01:10:18:01:00:01 0x8914
PRI: 3 CFI: 0 ID: 56
2011-10-18 13:36:49.374859 00:0d:ec:a3:81:80 -> 01:10:18:01:00:01 0x8914
PRI: 3 CFI: 0 ID: 56
2011-10-18 13:36:49.375098 00:0d:ec:a3:81:80 -> 01:10:18:01:00:01 0x8914
PRI: 3 CFI: 0 ID: 56
2011-10-18 13:36:49.375338 00:0d:ec:a3:81:80 -> 01:10:18:01:00:01 0x8914
PRI: 3 CFI: 0 ID: 56
10 packets captured
Program exited with status 0.
Nexus#
```

以下範例從特定CNA（與Po1311連結的vFC1311）擷取FKA訊框。 此配置會使Ethanalyzer每8秒檢視主機的FKA（即FKA計時器）。

```
Nexus# show flogi database
--------------------------------------------------------------------------------
INTERFACE VSAN FCID PORT NAME NODE NAME
--------------------------------------------------------------------------------
vfc15 200 0x1e0000 50:0a:09:81:89:4b:84:32 50:0a:09:80:89:4b:84:32
vfc16 200 0x1e0003 50:0a:09:81:99:4b:84:32 50:0a:09:80:89:4b:84:32
vfc17 200 0x1e0002 21:00:00:c0:dd:12:b9:b7 20:00:00:c0:dd:12:b9:b7
vfc18 200 0x1e0006 21:00:00:c0:dd:14:6a:73 20:00:00:c0:dd:14:6a:73
vfc19 200 0x1e0001 21:00:00:c0:dd:11:00:49 20:00:00:c0:dd:11:00:49
vfc20 200 0x1e0007 21:00:00:c0:dd:12:0e:37 20:00:00:c0:dd:12:0e:37
vfc23 200 0x1e0004 10:00:00:00:c9:85:2d:e5 20:00:00:00:c9:85:2d:e5
vfc1311 200 0x1e0008 10:00:00:00:c9:9d:23:73 20:00:00:00:c9:9d:23:73

Total number of flogi = 8.

Nexus# ethanalyzer local interface inbound-hi display-filter "eth.addr==
00:00:c9:9d:23:73 && vlan.etype==0x8914 && frame.len==60"limit-captured-frames 0
Capturing on eth4
2011-10-22 11:06:11.352329 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:06:19.352116 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:06:27.351897 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:06:35.351674 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:06:43.351455 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:06:51.351238 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:06:59.351016 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:07:07.350790 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
```

```
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:07:15.350571 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:07:23.350345 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:07:31.350116 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:07:39.349899 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:07:47.349674 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:07:55.349481 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:08:03.349181 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:08:11.348965 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:08:19.348706 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:08:27.348451 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
2011-10-22 11:08:35.348188 00:00:c9:9d:23:73 -> 00:0d:ec:a3:81:80 0x8914
PRI: 3 CFI: 0 ID: 24
52 packets dropped

Nexus# 19 packets captured
```

上一個捕獲僅顯示標頭。您也可以列印詳細封包；但是，當您使用detail選項時，最好將捕獲寫入檔案，然後使用Wireshark開啟檔案。

```
Nexus# ethanalyzer local interface inbound-hi detail display-filter
vlan.etype==0x8914 write bootflash:flogi.pcap ?
     <CR>
     >Redirect it to a file
     >>Redirect it to a file in append mode
     display Display packets even when writing to a file
     | Pipe command output to filter
```

以下是捕獲LACP幀的示例：

```
Nexus# ethanalyzer local interface inbound-hi display-filter slow
Capturing on eth42011-12-05 12:00:08.472289 00:0d:ec:a3:81:92 -> 01:80:c2:00:00:02 LACP Link
Aggregation Control ProtocolVersion 1. Actor Port = 16651 Partner Port = 283
2011-12-05 12:00:16.944912 00:1d:a2:00:02:99 -> 01:80:c2:00:00:02 LACP Link
Aggregation Control ProtocolVersion 1. Actor Port = 283 Partner Port = 16651
2011-12-05 12:00:25.038588 00:22:55:77:e3:ad -> 01:80:c2:00:00:02 LACP Link
Aggregation Control ProtocolVersion 1. Actor Port = 16666 Partner Port = 16643
2011-12-05 12:00:25.394222 00:1b:54:c1:94:99 -> 01:80:c2:00:00:02 LACP Link
Aggregation Control ProtocolVersion 1. Actor Port = 282 Partner Port = 16644
2011-12-05 12:00:26.613525 00:0d:ec:8f:c9:ee -> 01:80:c2:00:00:02 LACP Link
Aggregation Control ProtocolVersion 1. Actor Port = 295 Partner Port = 295
2011-12-05 12:00:26.613623 00:0d:ec:8f:c9:ef -> 01:80:c2:00:00:02 LACP Link
Aggregation Control ProtocolVersion 1. Actor Port = 296 Partner Port = 296
```

以下範例擷取來源為MAC位址00:26:f0（萬用字元過濾器）的所有訊框。

```
Nexus# ethanalyzer local interface inbound-hi display-filter
"eth.src[0:3]==00:26:f0" limit-captured-frames 0
Capturing on eth4
2012-06-20 16:37:22.721291 00:26:f0:05:00:00 -> 01:80:c2:00:00:00 STP Conf.
Root = 8192/d0:57:4c:b7:dc:00 Cost = 200 Port = 0x9004
```

```
2012-06-20 16:37:22.721340 00:26:f0:05:00:00 -> 01:00:0c:cc:cc:cd STP Conf.
Root = 8192/d0:57:4c:b7:dc:00 Cost = 200 Port = 0x9004
2012-06-20 16:37:22.721344 00:26:f0:05:00:00 -> 01:00:0c:cc:cc:cd STP Conf.
Root = 8192/d0:57:4c:b7:dc:00 Cost = 200 Port = 0x9004
2012-06-20 16:37:22.721348 00:26:f0:05:00:00 -> 01:00:0c:cc:cc:cd STP Conf.
Root = 8192/d0:57:4c:b7:dc:00 Cost = 200 Port = 0x9004
19 packets dropped
Nexus# 4 packets captured
```

附註：在先前的輸出中，您看到「19 Packets dropped」。 這些資料包實際上不會被丟棄，但不會被Ethanalyzer捕獲。

確保選擇適當的CPU隊列（入站hi、入站lo或管理）。

以下是常見的流量型別和隊列：

- 入站低 — SUP-low(eth3)(地址解析協定(ARP)/交換機虛擬介面上的IP、網際網路組管理協定監聽)
- 入站高 — SUP-high(eth4)(STP、FIP、乙太網光纖通道(FCoE)、FC、思科發現協定、鏈路層發現協定/資料中心橋接功能交換協定、鏈路聚合控制協定、單向鏈路檢測)
- Mgmt — 帶外（通過mgmt0介面的任何內容）
- FIP（交換矩陣登入、清除虛擬鏈路、FKA）：VLAN.etype==0x8914
- FCoE（埠登入、域名系統）：VLAN.etype==0x8906

以下是捕獲FIP和FCoE的示例：

```
ethanalyzer local interface inbound-hi display-filter "vlan.etype==0x8914
|| vlan.etype==0x8906"
```

以下是一些ARP過濾器：

```
Nexus# ethanalyzer local interface inbound-low display-filter
arp.src.hw_mac==0013.8066.8ac2
Capturing on eth3
2012-07-12 21:23:54.643346 00:13:80:66:8a:c2 ->
ff:ff:ff:ff:ff:ff ARP Who has 172.18.121.59?  Tell 172.18.121.1

NexusF340.24.10-5548-2# 1 packets captured

Nexus# ethanalyzer local interface inbound-low display-filter
arp.src.proto_ipv4==172.18.121.4
Capturing on eth3
2012-07-12 21:25:38.767772 00:05:73:ab:29:fc ->
ff:ff:ff:ff:ff:ff ARP Who has 172.18.121.1?  Tell 172.18.121.4
```