Nexus 3000/5000/7000 Uso da ferramenta Ethanalyzer

Contents

Introduction

Este documento descreve como usar a ferramenta incorporada de captura de pacotes, o Ethanalyzer, nos switches Nexus 3000/5000/7000.

Prerequisites

Requirements

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nos switches Nexus 3000, Nexus 5000 e Nexus 7000.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Ethanalyzer

O Ethanalyzer é uma ferramenta útil para solucionar problemas de plano de controle e tráfego destinado à CPU do switch. Mgmt é a interface para solucionar problemas de pacotes que acessam a interface mgmt0. Entrada-baixa (eth3) é para tráfego vinculado à CPU de baixa prioridade (ping, telnet, Secure Shell) e entrada-hi (eth4) é para tráfego associado à CPU de alta prioridade (Spanning Tree Protocol (STP), Bridge Protocol Data Units, FIP).

Os filtros de exibição mais usados podem ser encontrados no [Wireshark](#)

Os filtros de captura mais usados podem ser encontrados no [Wireshark](#)

```
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>
```

Como você pode ver, o Ethanalyzer indica que o pacote foi recebido na VLAN 57, que é a VLAN interna. No entanto, a VLAN 57 não é a VLAN real, porque 57 não está em hexadecimal. 57 em hex é 0x0039. Esse comando determina a VLAN real em hexadecimal.

```
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 é a VLAN real em hexadecimal. Você deve converter o número em decimal, que é 144. Esse cálculo ilustra que a VLAN real no quadro anterior era a VLAN 144, embora o Ethanalyzer indique que ela era 57.

Aqui está um exemplo que captura quadros FIP com o Filtro de Exibição da VLAN.(tipo==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#
```

Aqui está um exemplo que captura quadros FKA de um CNA específico (vFC1311 ligado ao Po1311). Essa configuração faz com que o Ethanalyzer veja o FKA do host a cada oito segundos, que é o temporizador FKA.

```
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
```

A captura anterior exibe apenas cabeçalhos. Você também pode imprimir um pacote detalhado; mas, quando você usa a opção detail, é melhor gravar a captura em um arquivo e depois abrir o arquivo com o Wireshark.

```
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
```

Aqui está um exemplo para capturar quadros LACP:

```
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
```

Aqui está um exemplo para capturar todos os quadros originados com um endereço MAC de 00:26:f0 (um filtro curinga).

```
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
```

> **Note**: Na saída anterior, você vê "19 pacotes descartados". Esses pacotes não são descartados na verdade, mas não são capturados pelo Ethanalyzer.

Certifique-se de selecionar a Fila da CPU apropriada (Inbound-hi, inbound-lo ou mgmt).

Aqui estão tipos de tráfego e filas comuns:

- Entrada-baixa - SUP-baixa (eth3) (Address Resolution Protocol (ARP)/IP sobre a interface virtual do switch, Internet Group Management Protocol Snooping)
- Entrada alta - SUP-alta (eth4) (STP, FIP, Fibre Channel over Ethernet (FCoE), FC, Cisco Discovery Protocol, Link Layer Discovery Protocol/Data Center Bridging Capabilities Exchange Protocol, Link Aggregation Control Protocol, Unidirectional Link Detection)
- Gerenciamento - Fora da banda (qualquer coisa através da interface mgmt0)
- FIP (Fabric Login, Clear Virtual Link, FKA): VLAN.etype==0x8914
- FCoE (Port Login, Domain Name System): VLAN.etype==0x8906

Aqui está um exemplo de FIP e FCoE de captura:

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

Aqui estão alguns filtros ARP:

```
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
```