

Nexus 3000/5000/7000 Gebruik van het Ethanalyzer-gereedschap

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Ethanalyzer](#)

Inleiding

In dit document wordt beschreven hoe u het ingebouwde pakketopnamegereedschap, Ethanalyzer, kunt gebruiken op de Nexus 3000/5000/7000 switches.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Nexus 3000, Nexus 5000 en Nexus 7000 switches.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Ethanalyzer

Ethanalyzer is een handig gereedschap om een besturingsplane voor de probleemoplossing te definiëren en verkeer dat is bedoeld om naar een CPU te overschakelen. Mgmt is de interface naar probleemoplossing pakketten die op de GMT0-interface worden geraakt. Inbound-low (eth3) is voor verkeer met lage prioriteit (ping, telnet, Secure Shell) met CPU's en inkomende-hi (eth4) is voor verkeer met hoge prioriteit (Spanning Tree Protocol (STP), Bridge Protocol Data Units (FIP)

met CPU's.

Opmerking: U kunt het display filter of het Capture Filter als een optie gebruiken. De optie Filter tonen heeft de voorkeur op Nexus 5000 en de voorkeur voor het Capture Filter op Nexus 3000 en Nexus 7000.

Vaak gebruikte weergavefilters zijn te vinden bij [Wireshark](#)

Vaak gebruikte Capture Filters zijn te vinden op [Wireshark](#)

Opmerking: Aangezien Nexus 5000 interne VLAN's gebruikt om frames door te sturen, heeft Ethanalyzer interne VLAN's. Nexus 5000 voorwaartse frames gebaseerd op interne VLAN's en Ethernet-analyzer geeft het interne VLAN weer. Wanneer u problemen oplost met de Ethanalyzer, kan VLAN ID problemen veroorzaken. U kunt echter wel de opdracht **tonen systeem interne fcwd fwcvidmap cvid** om de afbeelding te bepalen. Hierna volgt een voorbeeld.

```
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>
```

Zoals u kunt zien, geeft Ethanalyzer aan dat het pakket op VLAN 57 is ontvangen, wat het interne

VLAN is. Maar VLAN 57 is niet het eigenlijke VLAN, omdat 57 niet in hex is. 57 in hex is 0x0039. Deze opdracht bepaalt het eigenlijke VLAN in hex.

```
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 is het eigenlijke VLAN in hex. U moet het getal vervolgens converteren naar decimaal, dat 144 is. Deze berekening illustreert dat het eigenlijke VLAN in het vorige frame VLAN 144 was, alhoewel de Ethalyzer aangeeft dat het 57 was.

Hier is een voorbeeld dat FIP-frames opneemt met de Display Filter van VLAN.(type==0x8914)

```
Nexus# ethalyzer 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#
```

Hier is een voorbeeld dat FKA-frames vastlegt van een bepaalde CNA (vFC1311 gekoppeld aan Po1311). Deze configuratie zorgt ervoor dat Ethalyzer elke acht seconden FKA van de host ziet, wat de FKA-timer is.

```
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# ethalyzer 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
```

De vorige opname geeft alleen kopregels weer. U kunt ook een detailpakket afdrukken. Maar als u de optie Details gebruikt, is het beter om de opname naar een bestand te schrijven en het bestand vervolgens met Wireshark te openen.

```
Nexus# ethalyzer 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
```

Hier volgt een voorbeeld van LACP-frames:

```
Nexus# ethalyzer 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

```

Hier is een voorbeeld om alle frames vast te leggen die zijn gebaseerd op een MAC-adres van 00:26:f0 (een wild kaartfilter).

```

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

```

Opmerking: In de vorige uitvoer, ziet u "19 gevallen pakketten". Deze pakketten worden niet laten vallen, maar worden niet opgenomen door Ethanalyzer.

Zorg ervoor dat u de juiste CPU-wachtrij selecteert (inkomende in-hi, inkomende in-lo of inkomende in-mt).

Dit zijn veel verkeerstypen en wachtrijen:

- Inkomend-low - SUP-low (eth3) (Address Resolutie Protocol (ARP)/IP over switch virtuele interface, Internet Group Management Protocol Snooping)
- Inbound-hi - SUP-high (eth4) (STP, FIP, Fibre Channel over Ethernet (FCoE), FC, Cisco Discovery Protocol, Link Layer Discovery Protocol/Data Center Bridging Capability Exchange Protocol, Link Aggregation Control Protocol, Unidirectional Link Detection)
- Mgmt - Out-of-Band (alles via GMT0-interface)
- FIP (Fabric Login, Clear Virtual Link, FKA): VLAN.type==0x8914
- FCoE (Port Login, Domain Name System): VLAN.type==0x8906

Hier is een voorbeeld van een opname FIP en FCoE:

```

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

```

Hier zijn een paar ARP-filters:

```

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# **ethalyzer 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