

# Nexus 3000/5000/7000 での Ethalyzer ツールの使用

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[Ethalyzer](#)

## 概要

このドキュメントでは、Nexus 3000/5000/7000 スイッチで組み込みパケット キャプチャ ツール Ethalyzer を使用する方法を説明します。

## 前提条件

### 要件

このドキュメントに特有の要件はありません。

### 使用するコンポーネント

このドキュメントの情報は、Nexus 3000、Nexus 5000、および Nexus 7000 スイッチに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## Ethalyzer

Ethalyzer は、コントロールプレーンとスイッチ CPU 宛のトラフィックのトラブルシューティングを行うのに便利なツールです。Mgmt は、mgmt0 インターフェイスにヒットするパケットのトラブルシューティングを行うためのインターフェイスです。Inbound-low ( eth3 ) は CPU に送られる優先順位の低い ( ping、telnet、セキュア シェル ) トラフィック用であり、inbound-

hi ( eth4 ) は CPU に送られる優先順位の高い ( スパニング ツリー プロトコル ( STP )、ブリッジ プロトコル データ ユニット、FIP ) トラフィック用です。

注 : オプションとして表示フィルタまたはキャプチャ フィルタを使用できます。Nexus 5000 では表示フィルタ オプションが、Nexus 3000 および Nexus 7000 ではキャプチャ フィルタ オプションがそれぞれ推奨されます。

[Wireshark には、一般的に使用される表示フィルタがあります。](#)

[Wireshark には、一般的に使用されるキャプチャ フィルタがあります。](#)

注 : Nexus 5000 は内部 VLAN を使用してフレームを転送するため、Ethanalyzer には内部 VLAN があります。Nexus 5000 は内部 VLAN に基づいてフレームを転送し、Ethanalyzer はその内部 VLAN を表示します。Ethanalyzer でトラブルシューティングを行う場合、VLAN ID のためにトラブルシューティングが難しくなることがあります。ただし、マッピングを決定するために、コマンド `show system internal fcfwd fwcvidmap cvid` を使用できません。次に例を示します。

```
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>
```

出力例からわかるように、Ethanalyzer は、内部 VLAN である VLAN 57 でパケットが受信されたことを示しています。ただし、57 は 16 進数表記ではないため、VLAN 57 は実際の VLAN ではありません。16 進数の 57 は 0x0039 です。このコマンドは、16 進数の実際の VLAN を決定します。

```
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
```

16 進数表記の実際の VLAN は 0x0090 です。次に、数値を 144 の 10 進数に変換する必要があります。この計算は、Ethanalyzer が 57 であることを示していますが、前のフレームの実際の VLAN が VLAN 144 であることを示しています。

次に、VLAN.(etype==0x8914) の表示フィルタで FIP フレームをキャプチャした例を示します。

```
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#

次に、特定の CNA から FKA フレームをキャプチャした例を示します (vFC1311 は Po1311 に関連付けられています)。この設定により、Ethanalyzer では、ホストからの FKA が 8 秒 (FKA タイマー) ごとに確認されます。

```
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
```

上記のキャプチャでは、ヘッダーだけが表示されています。詳細なパケットを印刷することもできます。ただし、詳細オプションを使用する場合、キャプチャをファイルに書き込んでから、Wireshark で開くことが最適です。

```
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
```

次に、LACP フレームをキャプチャする例を示します。

```
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
```

次に、MAC アドレス 00:26:f0 ( ワイルドカードフィルタ ) を送信元とするすべてのフレームをキャプチャする例を示します。

```
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
```

注：上記の出力には、「19 Packets dropped」と表示されています。これらのパケットは実際に廃棄されませんが、Ethanalyzerによってキャプチャされていません。

適切な CPU キュー ( Inbound-hi、inbound-lo、または mgmt ) を選択してください。

次に、一般的なトラフィックタイプとキューを示します。

- Inbound-low : SUP-low ( eth3 ) ( アドレス解決プロトコル ( ARP ) /スイッチ仮想インターフェイス IP、Internet Group Management Protocol のスヌーピング )
- Inbound-hi : SUP-high ( eth4 ) ( STP、FIP、Fibre Channel over Ethernet ( FCoE )、FC、Cisco Discovery Protocol、Link Layer Discovery Protocol/Data Center Bridging Capabilities Exchange Protocol、リンク集約制御プロトコル、単方向リンク検出 )
- Mgmt : アウトオブバンド ( mgmt0 インターフェイスを通過するものすべて )
- FIP ( ファブリック ログイン、クリア仮想リンク、FKA ) : VLAN.etype==0x8914
- FCoE ( ポート ログイン、ドメイン ネーム システム ) : VLAN.etype==0x8906

次に、キャプチャした FIP と FCoE の例を示します。

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

次に、一部の ARP フィルタの例を示します。

```
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