

Nexus 7000 での Ethalyzer トラブルシューティング ガイド

目次

[概要](#)

[出力オプション](#)

[フィルタ オプション](#)

[capture-filter](#)

[display-filter](#)

[書き込みオプション](#)

[write](#)

[capture-ring-buffer](#)

[読み取りオプション](#)

[詳細オプションでの decode-internal](#)

[capture-filter 値の例](#)

[IP ホスト間のトラフィックのキャプチャ](#)

[IP アドレスの範囲間のトラフィックのキャプチャ](#)

[IP アドレスの範囲からのトラフィックのキャプチャ](#)

[IP アドレスの範囲へのトラフィックのキャプチャ](#)

[特定のプロトコル上のみのトラフィックのキャプチャ - DNS トラフィックのみのキャプチャ](#)

[特定のプロトコル上のみのトラフィックのキャプチャ - DHCP トラフィックのみのキャプチャ](#)

[特定のプロトコル上以外のトラフィックのキャプチャ - HTTP または SMTP トラフィックの除外](#)

[特定のプロトコル上以外のトラフィックのキャプチャ - ARP または DNS トラフィックの除外](#)

[IP トラフィックのみのキャプチャ - ARP、STP などの下位レイヤのプロトコルの除外](#)

[ユニキャスト トラフィックのみのキャプチャ - ブロードキャストおよびマルチキャストのアナウンスメントの除外](#)

[レイヤ 4 ポートの範囲内のトラフィックのキャプチャ](#)

[イーサネット タイプに基づいたトラフィックのキャプチャ - EAPOL トラフィックのキャプチャ](#)

[IPv6 キャプチャの回避策](#)

[IP プロトコル タイプに基づいたトラフィックのキャプチャ](#)

[MAC アドレスに基づいたイーサネット フレームの拒否 - LLDP マルチキャスト グループに属するトラフィックの除外](#)

[UDLD、VTP、または CDP トラフィックのキャプチャ](#)

[MAC アドレス間のトラフィックのキャプチャ](#)

[共通のコントロールプレーン プロトコル](#)

[既知の問題](#)

[関連情報](#)

概要

このドキュメントでは、Wireshark に基づいてパケットを制御するための Cisco NX-OS 統合パケット キャプチャ ツールである Ethalyzer について説明します。

Wireshark はオープンソース、多くの企業を渡って広く利用されたネットワークプロトコルアナライザおよび教育機関です。これは、パケットキャプチャライブラリ libpcap でキャプチャされたパケットをデコードします。Cisco NX-OS はパケットキャプチャをサポートするために libpcap ライブラリを使用する Linuxカーネルの上を動作します。

Ethalyzer を使用すると、次のことができます。

- スーパーバイザがパケットキャプチャを送受信する。
- キャプチャされるパケット数を設定する。
- キャプチャされるパケット長を設定する。
- プロトコル情報の要約または詳細を含めてパケットを表示する。
- キャプチャされたパケットデータを開き、保存する。
- キャプチャされたパケットを多くの条件を使用してフィルタリングする。
- 表示されるパケットを多くの条件を使用してフィルタリングする。
- 制御パケットの内部 7000 ヘッダーをデコードする。

Ethalyzer は、次のことを行うことはできません。

- ネットワークで問題が発生したときに警告する。ただし、Ethalyzer は、問題の原因を特定するのに役立つ場合があります。
- ハードウェアで転送されるデータプレーントラフィックをキャプチャする。
- インターフェイス固有のキャプチャをサポートする。

出力オプション

ethalyzer local interface inband コマンドによる出力のサマリービューを次に示します。「？」オプションはヘルプを表示します。

```
DC# ethalyzer 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 ethalyzer 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# ethalyzer 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 = 0x9006
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
```

詳細なプロトコル情報を表示するには、「detail」オプションを使用します。^Cが必要であればキャプチャの真中でスイッチプロンプトを打ち切り、表示されるのに使用することができます。

```
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:igrp]
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/broadcast)
  .... 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-----
```

フィルタ オプション

capture-filter

キャプチャ中に表示するか、あるいはディスクに保存するパケットを選択するには、「capture-filter」オプションを使用します。キャプチャフィルタでは、フィルタリング中にキャプチャの割合を高く維持します。パケットで完全な分割が行われていないため、フィルタフィールドは事前に定義され、制限されます。

display-filter

キャプチャファイル (tmp ファイル) のビューを変更するには、「display-filter」オプションを使用します。ディスプレイフィルタでは、完全に分割されたパケットを使用するため、ネットワークトレースファイルを分析する際に非常に複雑かつ高度なフィルタリングを実行できます。ただし、tmp ファイルは、まずすべてのパケットをキャプチャしてから、目的のパケットのみを表示するため、すぐにいっぱいになります。

この例では、「limit-captured-frames」が 5 に設定されています。「capture-filter」オプションを使用すると、Ethanalyzer では、フィルタ「host 10.10.10.2」に一致する 5 つのパケットを表示します。「display-filter」オプションを使用すると、Ethanalyzer では、まず 5 つのパケットをキャプチャし、フィルタ「ip.addr==10.10.10.2」に一致するパケットのみを表示します。

```
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
```

書き込みオプション

write

「write」オプションを使用して、後で分析するために Cisco Nexus 7000 シリーズ スイッチ上のストレージ デバイスの 1 つ (bootflash、logflash など) にあるファイルにキャプチャ データを書き込むことができます。キャプチャ ファイルのサイズは 10 MB に制限されます。

「write」オプションを使用した Ethanalyzer のコマンド例は、**ethanalyzer local interface inband write bootflash:capture_file_name** です。「capture-filter」を使用した「write」オプションの例と「first-capture」の出力ファイル名を次に示します。

```
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
```

キャプチャ データをファイルに保存すると、デフォルトでは、キャプチャされたパケットはターミナル ウィンドウに表示されません。「display」オプションを使用すると、Cisco NX-OS では、キャプチャ データをファイルに保存しながら、パケットを表示します。

capture-ring-buffer

「capture-ring-buffer」オプションを使用すると、指定した秒数、指定したファイル数、または指定したファイルのサイズの後には複数のファイルが作成されます。これらのオプションの定義次のスクリーンショットに示します。

```
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
```

読み取りオプション

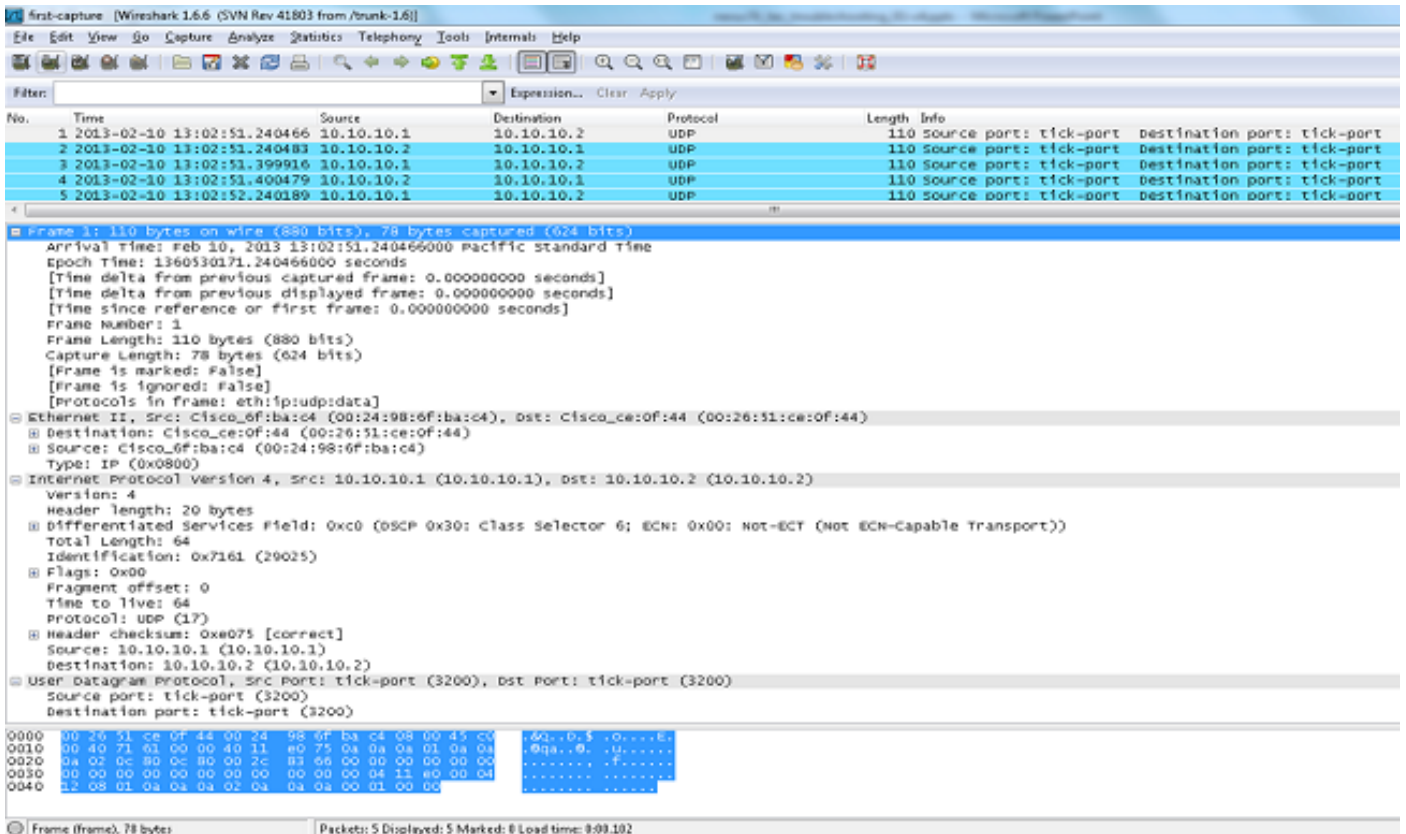
「read」オプションを使用すると、デバイス自体に保存されたファイルを読み取ることができます。

```
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-----
```

サーバまたは PC にファイルを転送し、cap ファイルまたは pcap ファイルを読み取ることができる Wireshark や他のアプリケーションでそのファイルを読み取ることもできます。

```
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.
```



詳細オプションでの decode-internal

「decode-internal」オプションは、Nexus 7000 のパケット転送方法に関する内部情報を報告します。この情報は、CPU 経由のパケット フローの理解とトラブルシューティングに役立ちます。

```
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-----
```

NX-OS インデックスを 16 進数に変換してから、Local Target Logic (LTL) インデックスを物理または論理インターフェイスにマップするためにできます。show system internal pixm info ltl x コマンドを使用します。

capture-filter 値の例

IP ホスト間のトラフィックのキャプチャ

```
host 1.1.1.1
```

IP アドレスの範囲間のトラフィックのキャプチャ

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

IP アドレスの範囲からのトラフィックのキャプチャ

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

IP アドレスの範囲へのトラフィックのキャプチャ

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

特定のプロトコル上のみのトラフィックのキャプチャ - DNS トラフィックのみのキャプチャ

DNS はドメイン ネーム システム プロトコルです。

```
port 53
```

特定のプロトコル上のみのトラフィックのキャプチャ - DHCP トラフィックのみのキャプチャ

DHCP は Dynamic Host Configuration Protocol です。

```
port 67 or port 68
```

特定のプロトコル上以外のトラフィックのキャプチャ - HTTP または SMTP トラフィックの除外

SMTP は Simple Mail Transfer Protocol です。

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

特定のプロトコル上以外のトラフィックのキャプチャ - ARP または DNS トラフィックの除外

ARP はアドレス解決プロトコルです。

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

IP トラフィックのみのキャプチャ - ARP、STP などの下位レイヤのプロトコルの除外

STP はスパンニング ツリー プロトコルです。

```
ip
```

ユニキャスト トラフィックのみのキャプチャ - ブロードキャストおよびマルチキャスト

ストのアナウンスメントの除外

```
not broadcast and not multicast
```

レイヤ 4 ポートの範囲内のトラフィックのキャプチャ

```
tcp portrange 1501-1549
```

イーサネット タイプに基づいたトラフィックのキャプチャ - EAPOL トラフィックのキャプチャ

EAPOL は Extensible Authentication Protocol over LAN です。

```
ether proto 0x888e
```

IPv6 キャプチャの回避策

```
ether proto 0x86dd
```

IP プロトコル タイプに基づいたトラフィックのキャプチャ

```
ip proto 89
```

MAC アドレスに基づいたイーサネット フレームの拒否 - LLDP マルチキャスト グループに属するトラフィックの除外

LLDP はリンク層検出プロトコルです。

```
not ether dst 01:80:c2:00:00:0e
```

UDLD、VTP、または CDP トラフィックのキャプチャ

UDLD は単方向リンク検出であり、VTP は VLAN トランキンング プロトコルであり、CDP は Cisco Discovery Protocol です。

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

MAC アドレス間のトラフィックのキャプチャ

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

注:

and = &&

or = ||

not = !

MAC アドレス形式 : xx: xx: xx: xx: xx: xx

共通のコントロール プレーン プロトコル

- UDLD : 宛先 Media Access Controller (DMAC) = 01-00-0C-CC-CC-CC およびイーサネット タイプ = 0x0111
- LACP : DMAC = 01:80:C2:00:00:02 およびイーサネット タイプ = 0x8809。 LACP は Link Aggregation Control Protocol の略語です。
- STP : DMAC = 01:80:C2:00:00:00 およびイーサネット タイプ = 0x4242 または DMAC = 01:00:0C:CC:CC:CD およびイーサネット タイプ = 0x010B
- CDP : DMAC = 01-00-0C-CC-CC-CC およびイーサネット タイプ = 0x2000
- LLDP : DMAC = 01:80:C2:00:00:0E、01:80:C2:00:00:03、または 01:80:C2:00:00:00 および

イーサネット タイプ = 0x88CC

- DOT1X : DMAC = 01:80:C2:00:00:03 およびイーサネット タイプ = 0x888E。DOT1X は IEEE 802.1x を意味します。
- IPv6 : イーサネット タイプ = 0x86DD
- [UDP および TCP ポート番号のリスト](#)

既知の問題

Cisco Bug ID [CSCue48854](#): 「Ethanalyzer の capture-filter によって SUP2 上の CPU からトラフィックがキャプチャされない」を参照してください。また、Cisco Bug ID [CSCtx79409](#): 「decode-internal によるキャプチャフィルタを使用できない」も参照してください。

関連情報

- [Wireshark: CaptureFilters](#)
- [Wireshark: DisplayFilters](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)