Nexus 7000でのEthanalyzerのトラブルシューティングガイドの使用

内容

概要

このドキュメントでは、Ethanalyzer について説明します。これは、Wireshark に基づいてパケットを制御するための Cisco NX-OS の組み込みパケット キャプチャ ツールです。

背景説明

Wiresharkは、多くの業界や教育機関で広く使用されているオープンソースのネットワークプロトコルアナライザです。パケット キャプチャ ライブラリである libpcap によってキャプチャされたパケットをデコードします。Cisco NX-OSはLinuxカーネル上で動作し、パケットキャプチャをサポートするためにlibpcapライブラリを使用します。

Ethanalyzer では以下のことが可能です。

- スーパバイザが送受信するパケットをキャプチャします。
- キャプチャするパケットの数を設定します。
- キャプチャするパケットの長さを設定します。
- プロトコルの概要または詳細な情報と共にパケットを表示します。
- キャプチャされたパケット データを開き、保存します。
- キャプチャされたパケットを多くの条件でフィルタ処理します。
- 表示されるパケットを多くの条件でフィルタ処理します。
- 制御パケットの内部 7000 ヘッダーをデコードします。

Ethanalyzer には次の機能はありません。

- ネットワークで問題が発生したときに警告する。ただし、Ethanalyzerは問題の原因の特定に役立ちます。
- 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

次に示すのは、**ethanalyzer local interface inband コマンドからの出力の概要です。**「?」オプションを指定すると、ヘルプが表示されます。

```
DC# ethanalyzer 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 ethanalyzer 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# ethanalyzer 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 = 0x8006
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
```

プロトコルの詳細な情報を表示するには、「detail」オプションを使用します。^Cを使用して中断し、必要に応じてキャプチャの途中でスイッチのプロンプトを戻すことができます。

```
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:eigrp]
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/broadca
st)
        .... ..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

キャプチャの間に表示するパケットまた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 フィルタは、フィルタ処理中に高率のキャプチャを維持します。パケットの完全な分析は行われていないので、フィルタ フィールドはあらかじめ決められており、限定されています。

display-filter

キャプチャ ファイル（tmp ファイル）の表示を変更するには、「display-filter」オプションを使用します。表示フィルタは完全に分離されたパケットを使用するので、ネットワーク トレースファイルを分析するときは、非常に複雑で高度なフィルタリングを行うことができます。ただし、tmp ファイルは、最初に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、急速にいっぱいになる可能性があります。

この例では、「limit-captured-frames」は 5 に設定されています。「capture-filter」オプションを指定すると、Ethanalyzer はフィルタ「host 10.10.10.2」に一致する 5 個のパケットを表示します。「display-filter」オプションを指定すると、Ethanalyzer は最初に 5 個のパケットをキャプチャ

した後、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」オプションを使用すると、後で分析するために、Cisco Nexus 7000 シリーズ スイッチのストレージ デバイス (ブートフラッシュ、LogFlash など) の 1 つの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コマンドの例は、**ethanalyzer local interface inband write bootflash:***capture_file_name*です。「capture-filter」と出力ファイル名「first-capture」を指定した「write」オプションの例を次に示します。

```
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 データがファイルに保存されるとき、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」オプションは、キャプチャ データをファイルに保存するときにパケットを表示するよう Cisco NX-OS に強制します。

capture-ring-buffer

「capture-ring-buffer」オプションは、指定された秒数、指定されたファイル数、または指定されたファイル サイズごとに、複数のファイルを作成します。これらのオプションの定義は、次のスクリーン ショットを参照してください。

```
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

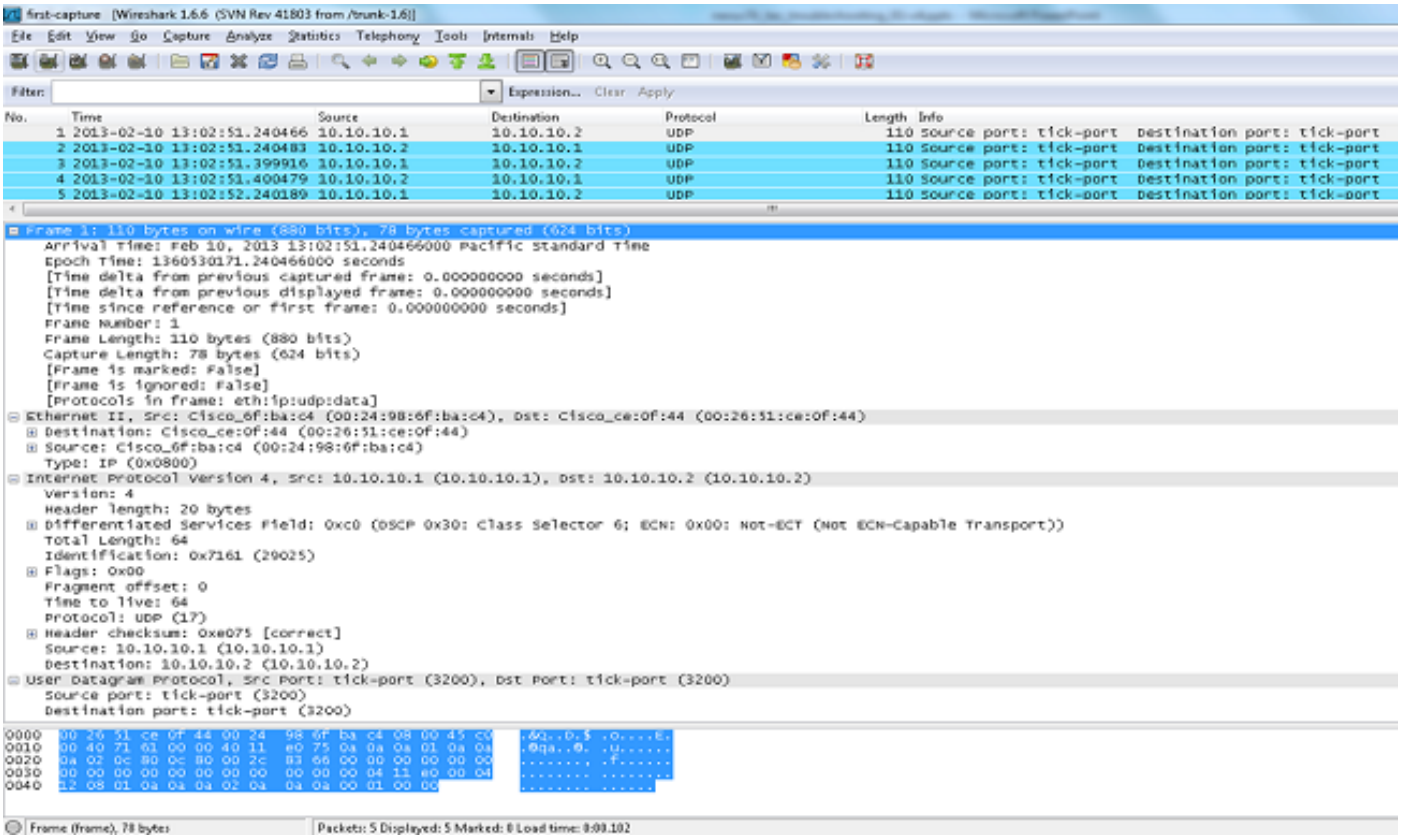
「read」オプションを使用すると、デバイス自体に保存されているファイルを読み取ることができます。

```
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-----------------------------------------
```

また、ファイルをサーバまたは PC に転送し、Wireshark、あるいは cap または pcap ファイルを読み取ることができる他のアプリケーションで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 によるパケットの転送方法についての内部情報をレポートします。この情報は、CPU を通過するパケットのフローを理解し、トラブルシューティングするのに役立ちます。

```
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 進数に変換した後、**show system internal pixm info ltl x コマンドを使用してローカル ターゲット ロジック (LTL) インデックスを物理インターフェイスまたは論理イ**

ンターフェイスにマップします。

capture-filter の値の例

1 つの IP ホストとの間でやり取りされるトラフィックのキャプチャ

```
host 10.1.1.1
```

IP アドレスの範囲との間でやり取りされる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
```

特定のプロトコルのトラフィックのみのキャプチャ - 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
```

特定のプロトコルのトラフィックのみのキャプチャ - 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
```

特定のプロトコル以外のトラフィックのキャプチャ - HTTP または SMTP の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
```

特定のプロトコル以外のトラフィックのキャプチャ - ARP および DNS のトラフィックの除外

ARP は Address Resolution Protocol です。

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

IP トラフィックのみのキャプチャ - ARP や STP などの下層プロトコルの除外

STP はスパニング 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 - ブロードキャストとマルチキャストの通知の除外

```
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 タイプに基づく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 のキャプチャの回避策

```
ether proto 0x86dd
```

IP プロトコル タイプに基づくトラフィックのキャプチャ

```
ip proto 89
```

MAC アドレスに基づくイーサネット 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 Link Layer Discovery Protocol です。

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

UDLD、VTP、CDP のトラフィックのキャプチャ

UDLD は 単方向リンク検出、VTP は VLAN Trunking Protocol、CDP は Cisco Discovery Protocol です。

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

MAC アドレスとの間でやり取りされる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アドレスの形式：xx:xx:xx:xx:xx:xx

一般的なコントロール プレーン プロトコル

- UDLD:Destination Media Access Controller(DMAC) = 01-00-0C-CC-CC-CCおよびEthType = 0x0111
- LACP:DMAC = 01:80:C2:00:00:02およびEthType = 0x8809。LACP は Link Aggregation Control Protocol を意味します。
- STP:DMAC = 01:80:C2:00:00:00およびEthType = 0x4242 – または – DMAC = 01:00:0C:CC:CC:CDおよびEthType = 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または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 と TCP のポート番号のリスト

既知の問題

Cisco Bug ID CSCue48854:Ethanalyzer capture-filterがSUP2のCPUからのトラフィックをキャプチャしない。

Cisco Bug ID CSCtx79409:decode-internalでキャプチャフィルタを使用できません。

Cisco Bug ID CSCvi02546:SUP3で生成されたパケットにFCSが発生する可能性があります。これは正常な動作です。

関連情報

- Wireshark:CaptureFilter
- Wireshark:DisplayFilters
- テクニカル サポートとドキュメント – Cisco Systems

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。