Gebruik de handleiding voor probleemoplossing voor Ethanalyzer op Nexus 7000

Inhoud

Inleiding

Dit document beschrijft de Ethanalyzer, een Cisco NX-OS geïntegreerd pakketopnamegereedschap voor controlepakketten die zijn gebaseerd op Wireshark.

Achtergrondinformatie

Wireshark is een open-source, netwerk protocol analyzer die veel wordt gebruikt in vele industrieën en onderwijsinstellingen. Het decodeert pakketten die zijn opgenomen door libpcap, de pakketopnamebibliotheek. Cisco NX-OS draait bovenop de Linux-kernel, die de libpcap-bibliotheek gebruikt om pakketopname te ondersteunen.

Met Ethanalyzer kunt u:

- Leg pakketten vast die door de supervisor zijn verzonden of ontvangen.
- Stel het aantal pakketten in dat moet worden opgenomen.
- Stel de lengte in van de pakketten die moeten worden opgenomen.
- Vertoon pakketten met summiere of gedetailleerde protocolinformatie.
- Open en bewaar pakketgegevens die zijn opgenomen.
- Filterpakketten die op vele criteria zijn opgenomen.
- Filterpakketten die op vele criteria moeten worden weergegeven.
- Decodeer de interne 7000 header van het besturingspakket.

Ethanalyzer kan niet:

- Waarschuw u wanneer uw netwerk problemen ervaart. Ethanalyzer kan u echter helpen bij het bepalen van de oorzaak van het probleem.
- Leg dataplatformverkeer vast dat doorgestuurd wordt in de hardware.
- Ondersteuning van interfacespecifieke opname.

Uitloopopties

Dit is een overzichtsweergave van de uitvoer van de **ethanalyzer lokale interface inband** opdracht. De "?" optie geeft help weer.

```
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
```

Gebruik de optie 'detail' voor gedetailleerde protocolinformatie. ^C kan worden gebruikt om de switch-prompt te annuleren en indien nodig terug te krijgen in het midden van een opname.

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

Filteropties

Opname-filter

Gebruik de optie 'Opname-filter' om te selecteren welke pakketten moeten worden weergegeven of tijdens de opname op de harde schijf moeten worden opgeslagen. Een opnamefilter behoudt een hoge opnamesnelheid terwijl het filtert. Omdat volledige dissectie niet is gedaan op de pakketten, zijn de filtervelden vooraf gedefinieerd en beperkt.

Display filter

Gebruik de optie 'display-filter' om de weergave van een opnamebestand (tmp-bestand) te wijzigen. Een weergavefilter maakt gebruik van volledig ontlede pakketten, zodat u zeer complexe en geavanceerde filtering kunt uitvoeren wanneer u een netwerk tracefile analyseert. Het tmp-bestand kan echter snel worden gevuld, omdat het eerst alle pakketten opneemt en vervolgens alleen de gewenste pakketten weergeeft.

In dit voorbeeld wordt 'limit-captured-frames' ingesteld op 5. Met de optie 'Capture-filter' toont Ethanalyzer u vijf pakketten die overeenkomen met het filter 'host 10.10.10.2'. Met de 'display-filter' optie, neemt Ethanalyzer eerst vijf pakketten op en toont dan alleen de pakketten die

overeenkomen met het filter 'ip.addr==10.10.10.2'.

```
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
```

Schrijfopties

Schrijven

Met de optie 'schrijven' kunt u de opnamegegevens schrijven naar een bestand in een van de opslagapparaten (zoals boothflash of logflash) op de Cisco Nexus 7000 Series Switch voor latere analyse. De grootte van het opnamebestand is beperkt tot 10 MB.

Een voorbeeld Ethanalyzer commando met een 'schrijf' optie is **ethanalyzer lokale interface in band schrijven bootflash:***capture_file_name*. Een voorbeeld van een 'schrijf'-optie met 'opname-filter' en een uitvoerbestandsnaam van 'eerste opname' is:

```
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
```

Wanneer de opnamegegevens in een bestand worden opgeslagen, worden de opgenomen pakketten standaard niet weergegeven in het terminalvenster. De 'weergave' optie dwingt Cisco NX-OS de pakketten weer te geven terwijl de opnamegegevens in een bestand worden opgeslagen.

Capture-ring-buffer

De optie 'Capture-ring-buffer' maakt meerdere bestanden na een bepaald aantal seconden, een bepaald aantal bestanden of een bepaalde bestandsgrootte. De definities van deze opties zijn in deze schermopname:

```
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
```

Leesopties

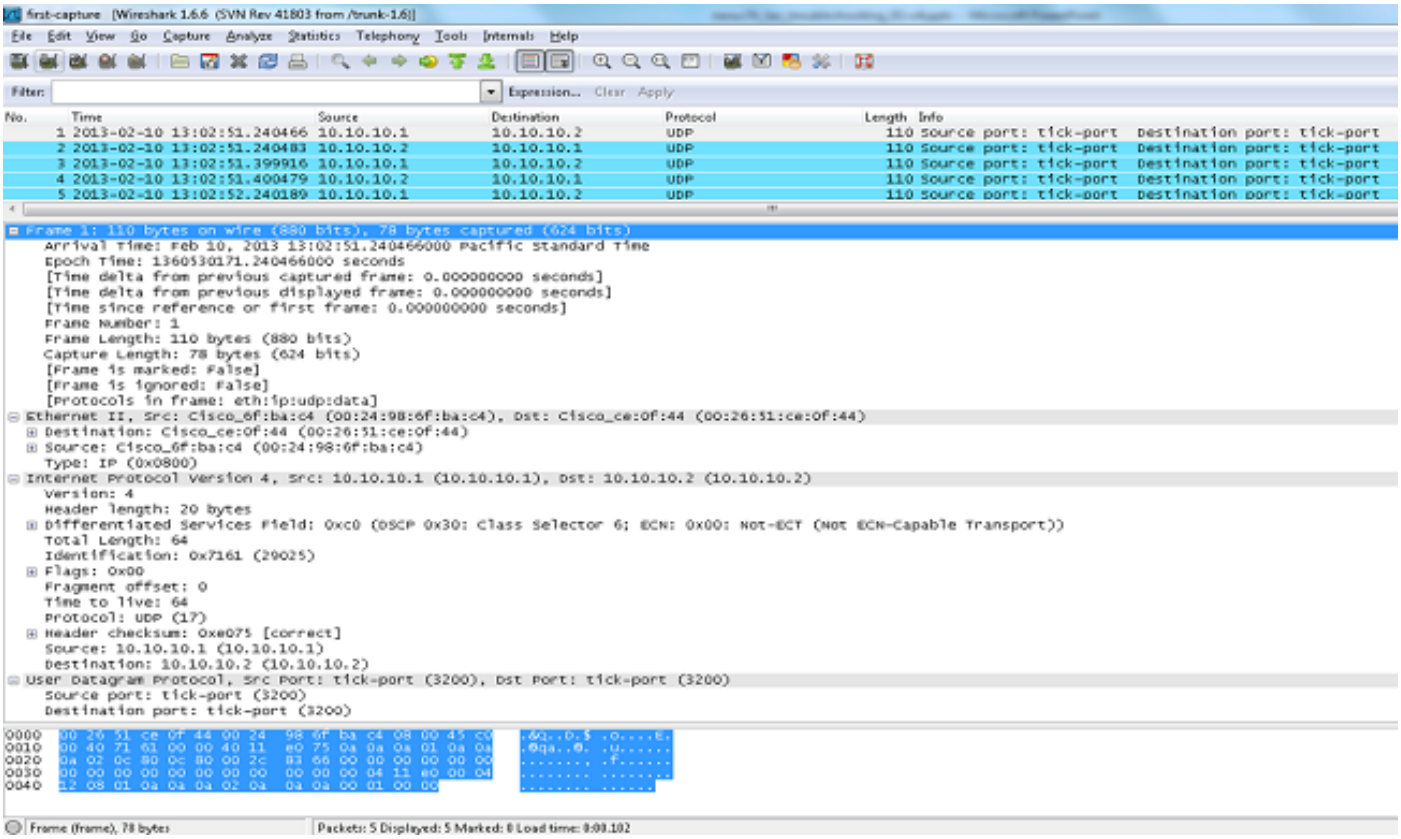
Met de optie 'lezen' kunt u het opgeslagen bestand op het apparaat zelf lezen.

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

U kunt het bestand ook overdragen naar een server of een pc en het lezen met Wireshark of een andere toepassing die cap-bestanden of pcap-bestanden kan lezen.

```
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.
```



Decodeer intern met Detail-optie

De 'decodeer-interne' optie meldt interne informatie over hoe de Nexus 7000 het pakket doorstuurt. Deze informatie helpt u de stroom van pakketten via de CPU te begrijpen en problemen op te lossen.

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

Converteer de NX-OS index naar hexadecimaal en gebruik vervolgens de **show system interne pixm info ltl x** commando om de lokale target logic (LTL) index naar een fysieke of logische

interface te koppelen.

Voorbeelden van opnamefilterwaarden

Opname van verkeer naar of van een IP-host

```
host 10.1.1.1
```

Leg verkeer naar of van een reeks IP-adressen vast

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

Leg verkeer vanaf een reeks IP-adressen vast

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

Leg verkeer op een bereik van IP-adressen vast

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

Leg verkeer alleen op een bepaald protocol vast - alleen DNS-verkeer opnemen

DNS is het Domain Name System Protocol.

```
port 53
```

Leg verkeer alleen op een bepaald protocol vast - alleen DHCP-verkeer opnemen

DHCP is het Dynamic Host Configuration Protocol.

```
port 67 or port 68
```

Leg verkeer niet op een bepaald protocol vast - sluit HTTP- of SMTP-verkeer uit

SMTP is het Simple Mail Transfer Protocol.

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

Leg verkeer niet op een bepaald protocol vast - sluit ARP- en DNS-verkeer uit

ARP is het Protocol voor adresoplossing.

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

Alleen IP-verkeer vastleggen - protocollen op lagere laag, zoals ARP en STP, uitsluiten

STP is het Spanning Tree Protocol.

```
ip
```

Alleen Unicast-verkeer vastleggen - uitzending en multicast-aankondigingen uitsluiten

```
not broadcast and not multicast
```

Capture Traffic binnen een bereik van Layer 4-poorten

```
tcp portrange 1501-1549
```

Capture Traffic op basis van Ethernet-type - Capture Ethernet-verkeer

EAPOL is het verlengbare verificatieprotocol via LAN.

```
ether proto 0x888e
```

IPv6-opnametijdelijke oplossing

```
ether proto 0x86dd
```

Capture Traffic op basis van IP-protocoltype

```
ip proto 89
```

Ethernet-frames afwijzen op basis van MAC-adres - verkeer uitsluiten dat tot de LLDP-multicastgroep behoort

LLDP is het Link Layer Discovery Protocol.

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

Leg UDLD-, VTP- of CDP-verkeer vast

UDLD is Unidirectionele linkdetectie, VTP is het VLAN-trunkingprotocol en CDP is het Cisco-detectieprotocol.

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

Opname van verkeer naar of van een MAC-adres

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

> **Opmerking:**
> en = &
> of = ||
> niet = !

MAC-adresindeling: xx:xx:xx:xx:xx:xx

Protocollen van gemeenschappelijke controlevliegtuigen

- UDLD: Bestemmingsmedia-toegangscontroller (DMAC) = 10-00-0C-CC-CC en EthType = 0x011
- LACP: DMAC = 01:80:C2:00:00:02 en EthType = 0x809. LACP staat voor Link Aggregation Control Protocol.
- STP: DMAC = 01:80:C2:00:00 en EthType = 0x4242 - of - DMAC = 01:00:0C:CC:CD en EthType = 0x010B
- CDP: DMAC = 01-00-0C-CC-CC en EthType = 0x2000
- LLDP: DMAC = 01:80:C2:00:00:0E of 01:80:C2:00:00:03 of 01:80:C2:00:00:00 en EthType = 0x88CC
- DOT1X: DMAC = 01:80:C2:00:00:03 en EthType = 0x88E. DOT1X staat voor IEEE 802.1x.
- IPv6: EthType = 0x86DD
- Lijst met UDP- en TCP-poortnummers

Bekende problemen

Cisco bug-id CSCue4854: het Ethanalyzer Capture-filter neemt geen verkeer van CPU op SUP2 op.

Cisco bug-id CSCtx79409: kan opnamefilter niet gebruiken met een decoder-intern.

Cisco bug-id CSCvi02546: SUP3-gegenereerd pakket kan FCS hebben, dit is verwacht gedrag.

Gerelateerde informatie

- Wireshark: CaptureFilters
- Wireshark: DisplayFilters
- Technische ondersteuning en documentatie – Cisco Systems

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.