Verwendung des Troubleshoot Guide für Ethanalyzer auf Nexus 7000

Inhalt

Einleitung

In diesem Dokument wird der Ethanalyzer beschrieben, ein integriertes Tool zur Paketerfassung in Cisco NX-OS für Steuerungspakete auf Basis von Wireshark.

Hintergrundinformationen

Wireshark ist ein Open-Source-Netzwerkprotokoll-Analysator, der in vielen Branchen und Bildungseinrichtungen eingesetzt wird. Es dekodiert Pakete, die von libpcap, der Paketerfassungsbibliothek, erfasst wurden. Cisco NX-OS läuft auf dem Linux-Kernel, der die libpcap-Bibliothek verwendet, um die Paketerfassung zu unterstützen.

Mit Ethanalyzer können Sie:

- Erfassen Sie vom Supervisor gesendete oder empfangene Pakete.
- Legen Sie die Anzahl der zu erfassenden Pakete fest.
- Legen Sie die Länge der zu erfassenden Pakete fest.
- Zeigt Pakete mit zusammengefassten oder detaillierten Protokollinformationen an.
- Öffnen und Speichern der erfassten Paketdaten
- Filtern von Paketen, die anhand zahlreicher Kriterien erfasst wurden
- Pakete filtern, die nach vielen Kriterien angezeigt werden sollen.
- Decodieren Sie den internen 7000-Header des Steuerungspakets.

Ethanalyzer kann nicht:

- Warnung anzeigen, wenn in Ihrem Netzwerk Probleme auftreten Ethanalyzer kann Ihnen jedoch dabei helfen, die Ursache des Problems zu ermitteln.
- Erfassen Sie Datenverkehr auf Datenebene, der an die Hardware weitergeleitet wird.
- Unterstützung der schnittstellenspezifischen Erfassung.

Ausgabeoptionen

Dies ist eine zusammenfassende Ansicht der Ausgabe des Befehls **ethanalyzer local interface inband**. Die Option? zeigt Hilfe an.

```
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
```

Verwenden Sie die Option 'detail' für detaillierte Protokollinformationen. ^C kann verwendet werden, um den Vorgang abzubrechen und die Switch-Eingabeaufforderung bei Bedarf während einer Erfassung erneut abzurufen.

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

Filteroptionen

Erfassungsfilter

Verwenden Sie die Option 'capture-filter', um auszuwählen, welche Pakete während der Erfassung angezeigt oder auf der Festplatte gespeichert werden sollen. Ein Erfassungsfilter behält eine hohe Erfassungsrate bei, während er filtert. Da die Pakete nicht vollständig zerlegt wurden, sind die Filterfelder vordefiniert und eingeschränkt.

Anzeigefilter

Verwenden Sie die Option 'display-filter', um die Ansicht einer Erfassungsdatei (TMP-Datei) zu ändern. Ein Anzeigefilter verwendet vollständig sezierte Pakete, sodass Sie bei der Analyse einer Netzwerk-Ablaufverfolgungsdatei sehr komplexe und erweiterte Filter durchführen können. Die TMP-Datei kann jedoch schnell gefüllt werden, da sie zunächst alle Pakete erfasst und dann nur die gewünschten Pakete anzeigt.

In diesem Beispiel wird 'limit-captured-frames' auf 5 gesetzt. Mit der Option 'capture-filter' zeigt Ihnen Ethanalyzer fünf Pakete an, die mit dem Filter 'host 10.10.10.2' übereinstimmen. Mit der Option 'display-filter' erfasst Ethanalyzer zunächst fünf Pakete und zeigt dann nur die Pakete an,

die mit dem Filter 'ip.addr==10.10.10.2' übereinstimmen.

```
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
```

Schreiboptionen

Schreiben

Mit der Schreiboption können Sie die Erfassungsdaten in eine Datei auf einem der Speichergeräte (z. B. boothflash oder logflash) des Cisco Nexus Switches der Serie 7000 schreiben, um sie später zu analysieren. Die Größe der Erfassungsdatei ist auf 10 MB beschränkt.

Ein Beispiel für einen Ethanalyzer-Befehl mit einer 'write'-Option ist **ethanalyzer local interface inband write bootflash:***capture_file_name*. Ein Beispiel für eine 'write'-Option mit 'capture-filter' und dem Namen der Ausgabedatei 'first-capture' ist:

```
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
```

Wenn die erfassten Daten in einer Datei gespeichert werden, werden die erfassten Pakete standardmäßig nicht im Terminalfenster angezeigt. Die Anzeigeoption erzwingt die Anzeige der Pakete in Cisco NX-OS, während die Erfassungsdaten in einer Datei gespeichert werden.

Capture-Ring-Puffer

Die Option 'capture-ring-buffer' erstellt mehrere Dateien nach einer bestimmten Anzahl von Sekunden, einer bestimmten Anzahl von Dateien oder einer bestimmten Dateigröße. Definitionen dieser Optionen finden Sie in diesem Screenshot:

```
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
```

Leseoptionen

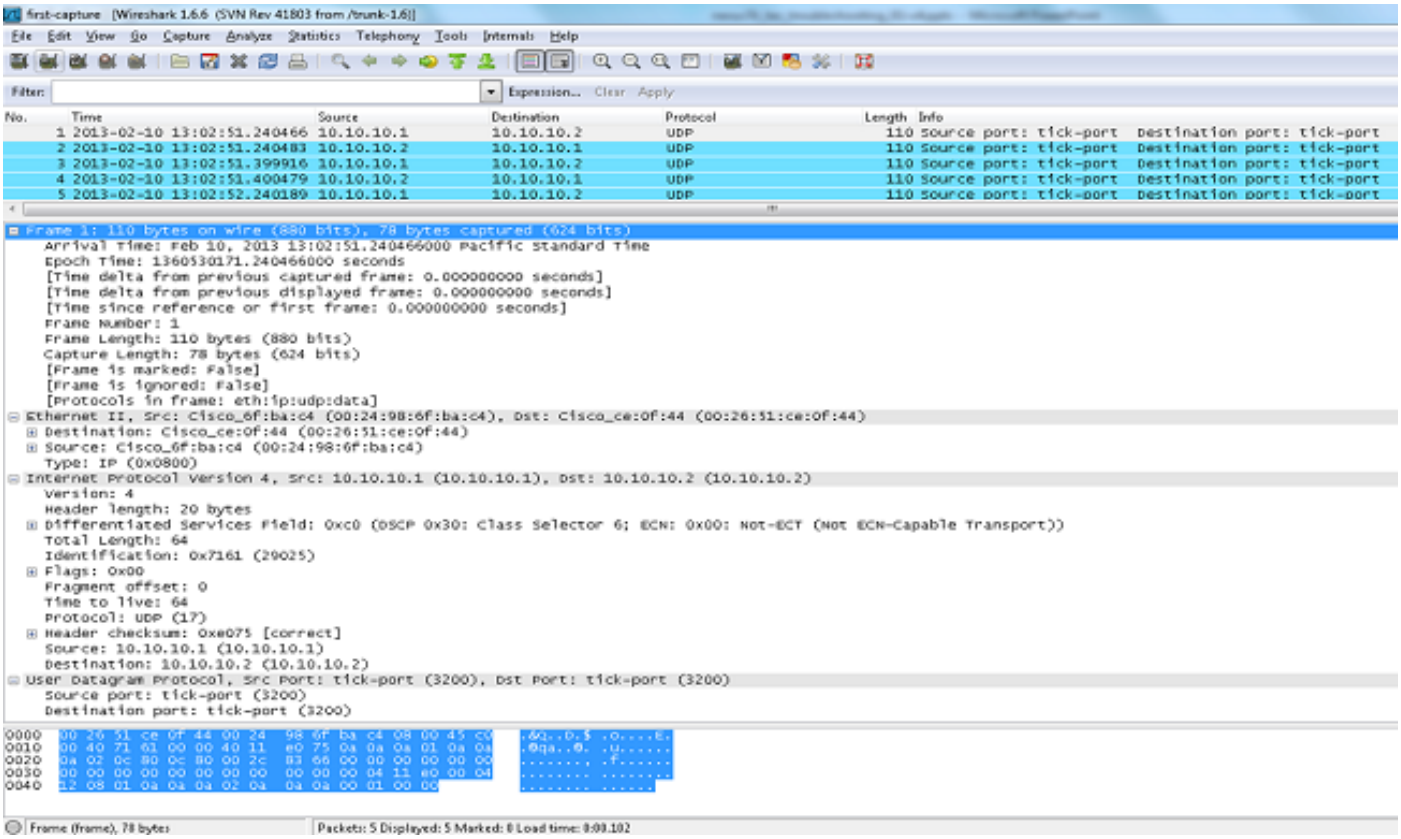
Mit der Leseoption können Sie die gespeicherte Datei auf dem Gerät selbst lesen.

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

Sie können die Datei auch auf einen Server oder einen PC übertragen und mit Wireshark oder einer anderen Anwendung lesen, die Cap- oder PCAP-Dateien lesen kann.

```
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.
```



Decodierungsintern mit Detail-Option

Die Option "decode-internal" gibt interne Informationen darüber aus, wie der Nexus 7000 das Paket weiterleitet. Diese Informationen helfen Ihnen, den Fluss von Paketen durch die CPU zu verstehen und Fehler zu beheben.

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

Konvertieren Sie den NX-OS-Index in hexadezimale Zahlen. Verwenden Sie dann den Befehl **show system internal pixm info ltl x,** um den LTL-Index (Local Target Logic) einer physischen oder

logischen Schnittstelle zuzuordnen.

Beispiele für Erfassungsfilterwerte

Erfassen von Datenverkehr zu oder von einem IP-Host

```
host 10.1.1.1
```

Erfassen von Datenverkehr zu oder von einem Bereich von IP-Adressen

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

Erfassen von Datenverkehr von einem IP-Adressbereich

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

Erfassen von Datenverkehr an einen IP-Adressbereich

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

Nur Datenverkehr über ein bestimmtes Protokoll erfassen - Nur DNS-Datenverkehr erfassen

DNS ist das Domain Name System Protocol.

```
port 53
```

Erfassung von Datenverkehr nur über ein bestimmtes Protokoll - Erfassung von DHCP-Datenverkehr

DHCP ist das Dynamic Host Configuration Protocol.

```
port 67 or port 68
```

Erfassen von Datenverkehr außerhalb eines bestimmten Protokolls - Ausschließen von HTTP- oder SMTP-Datenverkehr

SMTP ist das Simple Mail Transfer Protocol.

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

Erfassen von Datenverkehr außerhalb eines bestimmten Protokolls - Ausschließen von ARP- und DNS-Datenverkehr

ARP ist das Address Resolution Protocol.

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

Nur IP-Datenverkehr erfassen - Protokolle der unteren Ebene wie ARP und STP ausschließen

STP ist das Spanning Tree Protocol.

```
ip
```

Nur Unicast-Datenverkehr erfassen - Broadcast- und Multicast-Ankündigungen ausschließen

```
not broadcast and not multicast
```

Erfassung von Datenverkehr innerhalb eines Bereichs von Layer-4-Ports

```
tcp portrange 1501-1549
```

Erfassung von Datenverkehr auf Basis des Ethernet-Typs - Erfassung von EAPOL-Datenverkehr

EAPOL ist das Extensible Authentication Protocol over LAN.

```
ether proto 0x888e
```

IPv6-Workaround für die Erfassung

```
ether proto 0x86dd
```

Erfassung von Datenverkehr basierend auf IP-Protokolltyp

```
ip proto 89
```

Ablehnen von Ethernet-Frames basierend auf der MAC-Adresse - Ausschließen von Datenverkehr, der zur LLDP-Multicast-Gruppe gehört

LLDP ist das Link Layer Discovery Protocol.

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

Erfassung von UDLD-, VTP- oder CDP-Datenverkehr

UDLD steht für Unidirectional Link Detection, VTP für das VLAN Trunking Protocol und CDP für das Cisco Discovery Protocol.

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

Erfassen von Datenverkehr zu oder von einer MAC-Adresse

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

Anmerkung:
und
oder = ||
nicht = !
MAC-Adressformat: xx:xx:xx:xx:xx:xx

Gemeinsame Kontrollebenenprotokolle

- UDLD: Destination Media Access Controller (DMAC) = 01-00-0C-CC-CC-CC und EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02 und EthType = 0x8809. LACP steht für Link Aggregation Control Protocol.
- STP: DMAC = 01:80:C2:00:00:00 und EthType = 0x4242 - oder - DMAC = 01:00:0C:CC:CC:CD und EthType = 0x010B
- CDP: DMAC = 01-00-0C-CC-CC-CC und EthType = 0x2000
- LLDP: DMAC = 01:80:C2:00:00:0E oder 01:80:C2:00:00:03 oder 01:80:C2:00:00:00 und EthType = 0x88CC
- DOT1X: DMAC = 01:80:C2:00:00:03 und EthType = 0x888E. DOT1X steht für IEEE 802.1x.
- IPv6: EthType = 0x86DD
- Liste der UDP- und TCP-Portnummern

Bekannte Probleme

Cisco Bug-ID CSCue4854: Der Ethianalyzer-Erfassungsfilter erfasst keinen Datenverkehr von der CPU auf SUP2.

Cisco Bug-ID CSCtx79409: Capture-Filter kann nicht mit decode-intern verwendet werden.

Cisco Bug-ID CSCvi02546: SUP3-generiertes Paket kann FCS haben, dies ist erwartetes Verhalten.

Zugehörige Informationen

- Wireshark: Erfassungsfilter
- Wireshark: Anzeigefilter
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.