Utilizzare la Guida alla risoluzione dei problemi per Ethanalyzer su Nexus 7000

Sommario

Introduzione

Questo documento descrive Ethanalyzer, uno strumento di acquisizione pacchetti integrato Cisco NX-OS per pacchetti di controllo basati su Wireshark.

Premesse

Wireshark è un analizzatore di protocolli di rete open-source ampiamente utilizzato in molti settori e istituzioni educative. Decodifica i pacchetti acquisiti da libpcap, la libreria di acquisizione dei pacchetti. Cisco NX-OS viene eseguito sul kernel Linux, che utilizza la libreria libpcap per supportare l'acquisizione dei pacchetti.

Con Ethanalyzer puoi:

- Acquisire i pacchetti inviati o ricevuti dal Supervisor.
- Impostare il numero di pacchetti da acquisire.
- Impostare la lunghezza dei pacchetti da acquisire.
- Visualizza i pacchetti con informazioni di protocollo riepilogative o dettagliate.
- Aprire e salvare i dati del pacchetto acquisiti.
- Filtra i pacchetti acquisiti in base a molti criteri.
- Filtrare i pacchetti da visualizzare in base a molti criteri.
- Decodificare l'intestazione interna 7000 del pacchetto di controllo.

Ethanalyzer non può:

- Avvisa in caso di problemi di rete. Tuttavia, Ethanalyzer può aiutarti a determinare la causa del problema.
- Acquisire il traffico del piano dati inoltrato nell'hardware.
- Supportare l'acquisizione specifica dell'interfaccia.

Opzioni di output

Questa è una visualizzazione di riepilogo dell'output del comando in banda dell'interfaccia locale di ethanalyzer. L'opzione ? visualizza la Guida.

```
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
```

Utilizzare l'opzione detail per ottenere informazioni dettagliate sul protocollo. Se necessario, ^C può essere utilizzato per interrompere e visualizzare di nuovo il prompt dello switch durante un'acquisizione.

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

Opzioni filtro

Capture-Filter

Usare l'opzione capture-filter per selezionare i pacchetti da visualizzare o salvare su disco durante la cattura. Un filtro di acquisizione mantiene un'elevata velocità di acquisizione mentre filtra. Poiché non è stata eseguita la dissezione completa sui pacchetti, i campi filtro sono predefiniti e limitati.

Display-Filter

Usare l'opzione display-filter per modificare la visualizzazione di un file di acquisizione (file tmp). Un filtro di visualizzazione utilizza pacchetti completamente dissezionati, pertanto è possibile eseguire operazioni di filtraggio molto complesse e avanzate quando si analizza un file di traccia di rete. Tuttavia, il file tmp può riempirsi rapidamente poiché cattura prima tutti i pacchetti e quindi visualizza solo i pacchetti desiderati.

In questo esempio, limit-capture-frames è impostato su 5. Con l'opzione capture-filter, Ethanalyzer mostra cinque pacchetti che corrispondono all'host filtro 10.10.10.2. Con l'opzione display-filter, Ethanalyzer acquisisce prima cinque pacchetti, quindi visualizza solo i pacchetti che corrispondono al filtro 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
```

Opzioni di scrittura

Scrittura

L'opzione write consente di scrivere i dati di acquisizione su un file in uno dei dispositivi di archiviazione (ad esempio bootflash o logflash) sullo switch Cisco Nexus serie 7000 per un'analisi successiva. Le dimensioni del file di acquisizione sono limitate a 10 MB.

Un esempio di comando Ethanalyzer con un'opzione write è ethanalyzer local interface inband write bootflash: capture_file_name. Di seguito è riportato un esempio di opzione write con capture-filter e il nome del file di output first-capture:

```
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
```

Quando i dati di acquisizione vengono salvati in un file, per impostazione predefinita i pacchetti acquisiti non vengono visualizzati nella finestra del terminale. L'opzione display forza Cisco NX-OS a visualizzare i pacchetti mentre salva i dati di acquisizione in un file.

Capture-Ring-Buffer

L'opzione capture-ring-buffer consente di creare più file dopo un numero di secondi specificato, un numero di file specificato o una dimensione di file specificata. Le definizioni di tali opzioni sono riportate nella seguente schermata:

```
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
```

Opzioni di lettura

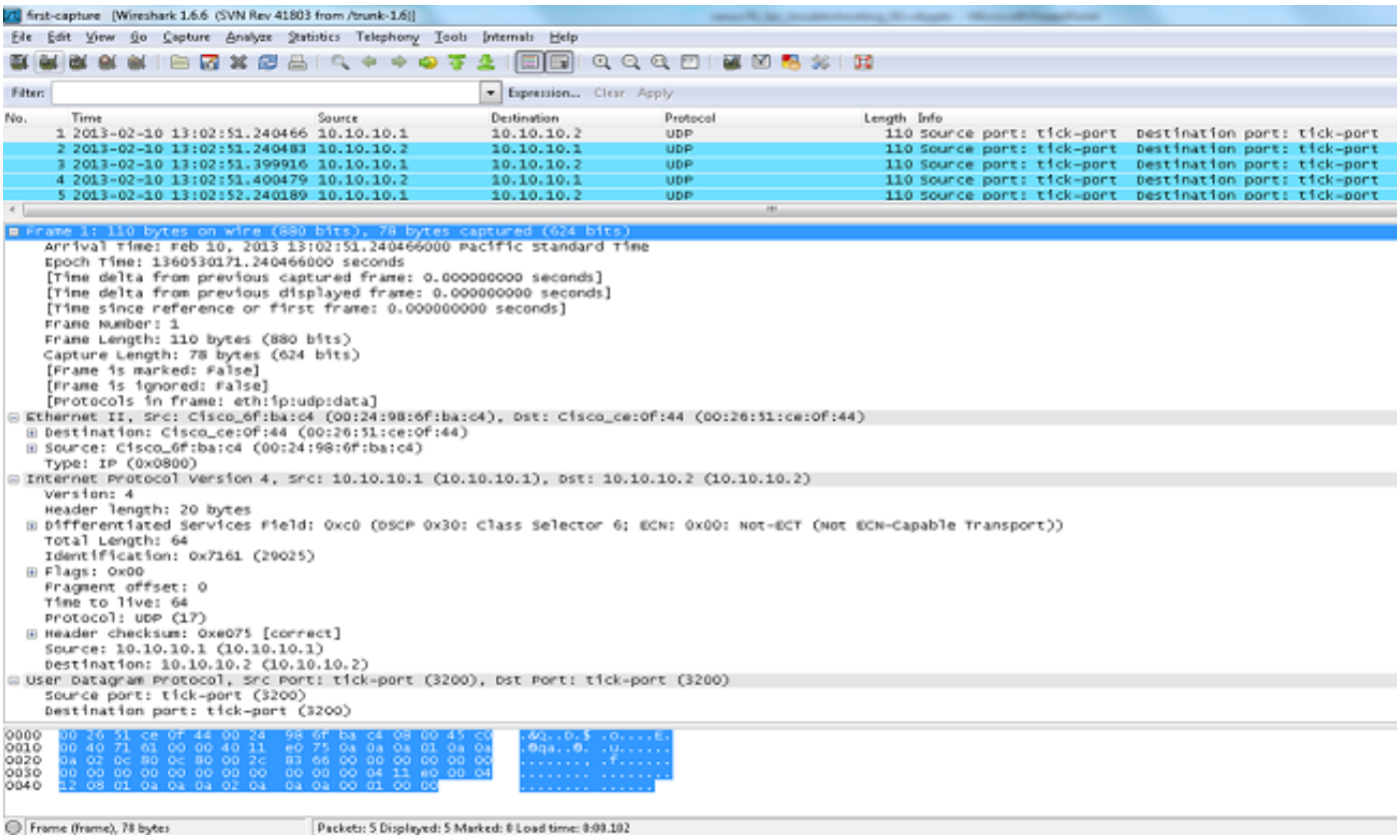
L'opzione di lettura consente di leggere il file salvato sul dispositivo stesso.

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

È inoltre possibile trasferire il file su un server o un PC e leggerlo con Wireshark o con qualsiasi altra applicazione in grado di leggere i file cap o cap.

```
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.
```



Decodifica interna con opzione Detail

L'opzione decode-internal riporta informazioni interne sul modo in cui Nexus 7000 inoltra il pacchetto. Queste informazioni aiutano a comprendere e risolvere i problemi relativi al flusso di pacchetti attraverso la CPU.

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

Convertire l'indice NX-OS in esadecimale, quindi utilizzare il comando show system internal pixm info ltl x per mappare l'indice LTL (Local Target Logic) a un'interfaccia fisica o logica.

Esempi di valori di filtro di acquisizione

Acquisire il traffico da o verso un host IP

```
host 10.1.1.1
```

Acquisire il traffico da o verso un intervallo di indirizzi IP

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

Acquisisci traffico da un intervallo di indirizzi IP

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

Acquisire il traffico su un intervallo di indirizzi IP

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

Acquisisci traffico solo su un determinato protocollo - Acquisisci solo traffico DNS

DNS è il protocollo Domain Name System.

```
port 53
```

Acquisisci traffico solo su un determinato protocollo - Acquisisci solo traffico DHCP

DHCP è il protocollo di configurazione host dinamico.

```
port 67 or port 68
```

Acquisisci traffico non su un determinato protocollo - Escludi traffico HTTP o SMTP

SMTP è il protocollo per il trasferimento di posta semplice.

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

Acquisisci traffico non su un determinato protocollo - Escludi traffico ARP e DNS

ARP è il protocollo di risoluzione degli indirizzi.

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

Acquisisci solo traffico IP - Escludi protocolli di livello inferiore come ARP e STP

STP è lo Spanning Tree Protocol.

```
ip
```

Acquisisci solo traffico unicast - Escludi annunci broadcast e multicast

```
not broadcast and not multicast
```

Acquisire il traffico all'interno di un intervallo di porte di livello 4

```
tcp portrange 1501-1549
```

Acquisire il traffico in base al tipo Ethernet - Acquisire il traffico EAPOL

EAPOL è il protocollo di autenticazione estendibile su LAN.

```
ether proto 0x888e
```

Soluzione di acquisizione IPv6

```
ether proto 0x86dd
```

Acquisisci traffico in base al tipo di protocollo IP

```
ip proto 89
```

Rifiuta frame Ethernet in base all'indirizzo MAC - Esclude il traffico che appartiene al gruppo multicast LLDP

LLDP è il protocollo di rilevamento del livello di collegamento.

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

Acquisire il traffico UDLD, VTP o CDP

Il protocollo UDLD è Unidirectional Link Detection, il protocollo VTP è il protocollo VLAN Trunking e il protocollo CDP è Cisco Discovery Protocol.

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

Acquisire il traffico da o verso un indirizzo MAC

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

Nota:
e = &&

---

o = ||
non = !
Formato indirizzo MAC : xx:xx:xx:xx:xx:xx

Protocolli Control Plane comuni

- UDLD: Destination Media Access Controller (DMAC) = 01-00-0C-CC-CC e EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02 e EthType = 0x8809. LACP è l'acronimo di Link Aggregation Control Protocol.
- STP: DMAC = 01:80:C2:00:00:00 e EthType = 0x4242 - o - DMAC = 01:00:0C:CC:CD e EthType = 0x010B
- CDP: DMAC = 01-00-0C-CC-CC-CC e EthType = 0x2000
- LLDP: DMAC = 01:80:C2:00:00:0E o 01:80:C2:00:00:03 o 01:80:C2:00:00 e EthType = 0x88CC
- DOT1X: DMAC = 01:80:C2:00:00:03 e EthType = 0x888E. DOT1X è l'acronimo di IEEE 802.1x.
- IPv6: EthType = 0x86DD
- Elenco di numeri di porta UDP e TCP

Problemi noti

ID bug Cisco CSCue48854: il filtro di acquisizione Ethanalyzer non acquisisce il traffico dalla CPU sul pacchetto SUP2.

ID bug Cisco CSCtx79409: impossibile utilizzare il filtro di acquisizione con decode-internal.

ID bug Cisco CSCvi02546: il pacchetto generato con SUP3 può avere FCS, questo è il comportamento previsto.

Informazioni correlate

- Wireshark: filtri di acquisizione
- Wireshark: filtri di visualizzazione
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).