Use o Guia de solução de problemas do Ethanalyzer no Nexus 7000

Contents

Introdução

Este documento descreve o Ethanalyzer, uma ferramenta integrada de captura de pacotes do Cisco NX-OS para controlar pacotes com base no Wireshark.

Informações de Apoio

O Wireshark é um analisador de protocolo de rede de código aberto amplamente usado em muitos setores e instituições educacionais. Ele decodifica pacotes capturados pela libpcap, a biblioteca de captura de pacotes. O Cisco NX-OS é executado sobre o kernel do Linux, que usa a biblioteca libpcap para suportar a captura de pacotes.

Com o Ethanalyzer, você pode:

- Capturar pacotes enviados ou recebidos pelo Supervisor.
- Defina o número de pacotes a serem capturados.
- Defina o comprimento dos pacotes a serem capturados.
- Exiba pacotes com informações resumidas ou detalhadas do protocolo.
- Abra e salve os dados do pacote capturados.
- Filtrar pacotes capturados com muitos critérios.
- Filtrar pacotes a serem exibidos com base em vários critérios.
- Decodifique o cabeçalho interno 7000 do pacote de controle.

O etanalyzer não pode:

- Avisá-lo quando sua rede tiver problemas. No entanto, o Ethanalyzer pode ajudá-lo a determinar a causa do problema.
- Capturar o tráfego do plano de dados que é encaminhado no hardware.
- Suportar captura específica de interface.

Opções de saída

Esta é uma visão resumida da saída do comando ethanalyzer local interface inband. A opção ? exibe a ajuda.

```
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
```

Use a opção detail para obter informações detalhadas sobre o protocolo. ^C pode ser usado para anular e obter o prompt do switch de volta no meio de uma captura, se necessário.

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

Opções de filtro

Capture-Filter

Use a opção capture-filter para selecionar quais pacotes exibir ou salvar em disco durante a captura. Um filtro de captura mantém uma alta taxa de captura enquanto filtra. Como a dissecação completa não foi feita nos pacotes, os campos de filtro são predefinidos e limitados.

Filtro de exibição

Use a opção display-filter para alterar a exibição de um arquivo de captura (arquivo tmp). Um filtro de exibição usa pacotes totalmente dissecados, de modo que você pode fazer uma filtragem muito complexa e avançada ao analisar um arquivo de rastreamento de rede. No entanto, o arquivo tmp pode ser preenchido rapidamente, pois primeiro captura todos os pacotes e depois exibe apenas os pacotes desejados.

Neste exemplo, limit-capture-frames é definido como 5. Com a opção capture-filter, o Ethanalyzer

mostra cinco pacotes que correspondem ao host de filtro 10.10.10.2. Com a opção display-filter, o Ethanalyzer primeiro captura cinco pacotes e, em seguida, exibe apenas os pacotes que correspondem ao 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
```

Opções de gravação

Gravar

A opção de gravação permite gravar os dados de captura em um arquivo em um dos dispositivos de armazenamento (como bootflash ou logflash) no switch Cisco Nexus 7000 Series para análise posterior. O tamanho do arquivo de captura é limitado a 10 MB.

Um exemplo de comando do Ethanalyzer com uma opção de gravação é ethanalyzer local interface inband write bootflash: capture_file_name. Um exemplo de uma opção de gravação com capture-filter e um nome de arquivo de saída first-capture é:

```
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 os dados de captura são salvos em um arquivo, os pacotes capturados não são, por padrão, exibidos na janela do terminal. A opção de exibição força o Cisco NX-OS a exibir os pacotes enquanto salva os dados de captura em um arquivo.

Capture-Ring-Buffer

A opção capture-ring-buffer cria vários arquivos após um número especificado de segundos, um número especificado de arquivos ou um tamanho de arquivo especificado. As definições dessas opções estão nesta captura de tela:

```
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
```

Opções de leitura

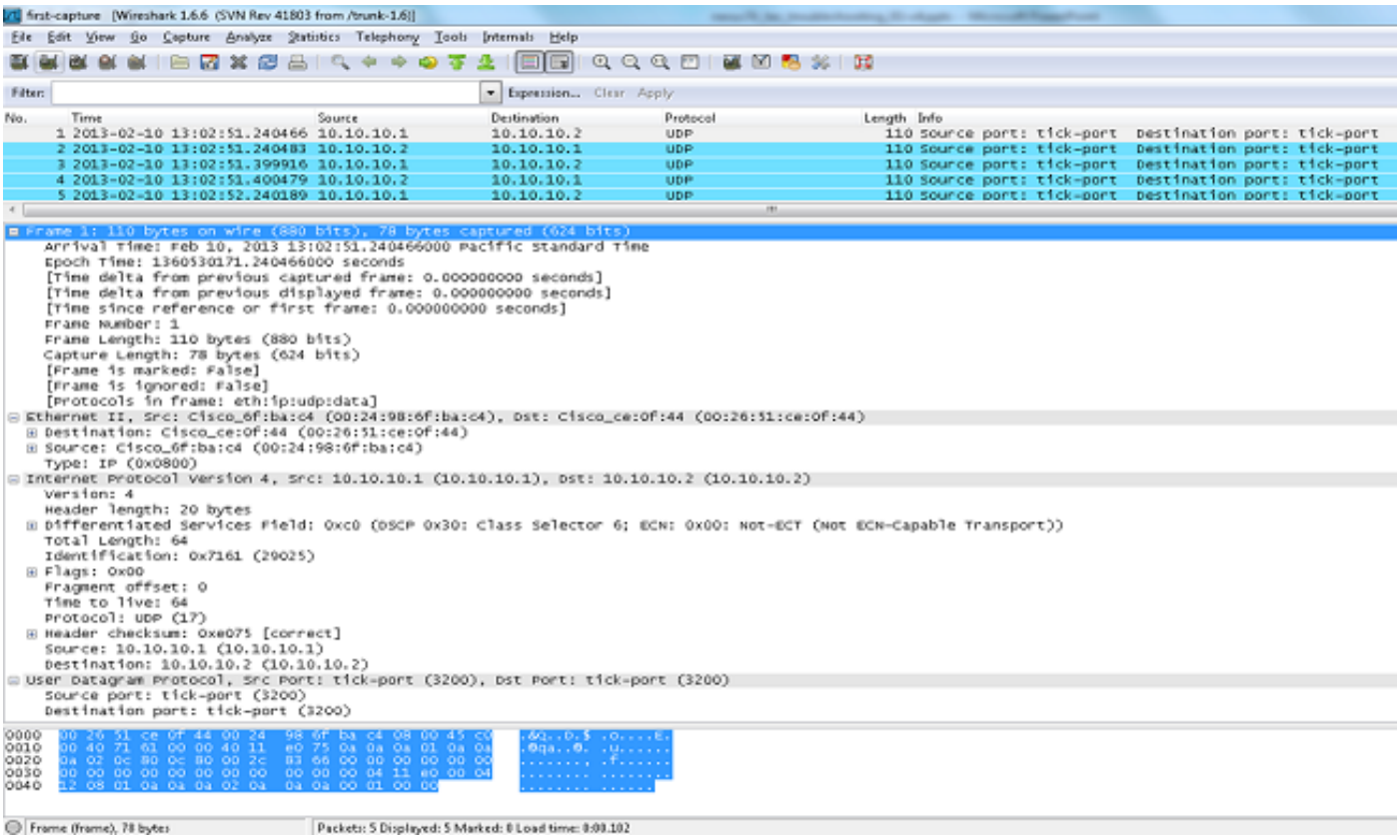
A opção de leitura permite ler o arquivo salvo no próprio dispositivo.

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

Você também pode transferir o arquivo para um servidor ou PC e lê-lo com o Wireshark ou qualquer outro aplicativo que possa ler arquivos cap ou pcap.

```
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.
```



Decodificar-Interno com Opção de Detalhe

A opção decode-internal relata informações internas sobre como o Nexus 7000 encaminha o pacote. Essas informações o ajudam a entender e solucionar problemas do fluxo de pacotes através da 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-----------------------------------------
```

Converta o índice do NX-OS em hexadecimal e use o comando show system internal pixm info ltl x para mapear o índice de lógica de destino local (LTL) para uma interface física ou lógica.

Exemplos de valores do filtro de captura

Capturar tráfego de ou para um host IP

```
host 10.1.1.1
```

Capturar tráfego de ou para um intervalo de endereços IP

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

Capturar o tráfego de um intervalo de endereços IP

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

Capturar o tráfego para um intervalo de endereços IP

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

Capturar apenas o tráfego em um determinado protocolo - Capturar apenas o tráfego DNS

O DNS é o Protocolo do Sistema de Nomes de Domínio.

```
port 53
```

Capturar apenas o tráfego em um determinado protocolo - Capturar apenas o

tráfego DHCP

O DHCP é o Dynamic Host Configuration Protocol.

```
port 67 or port 68
```

Capturar tráfego fora de um determinado protocolo - Excluir tráfego HTTP ou SMTP

O SMTP é o Simple Mail Transfer Protocol (protocolo de transferência de correspondência simples).

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

Capturar tráfego fora de um determinado protocolo - Excluir tráfego ARP e DNS

O ARP é o Address Resolution Protocol (Protocolo de Resolução de Endereços).

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

Capturar apenas tráfego IP - Excluir protocolos de camada inferior como ARP e STP

O STP é o Spanning Tree Protocol.

```
ip
```

Capturar apenas tráfego unicast - Excluir anúncios de broadcast e multicast

```
not broadcast and not multicast
```

Capturar o tráfego dentro de uma faixa de portas da camada 4

```
tcp portrange 1501-1549
```

Capturar tráfego com base no tipo de Ethernet - Capturar tráfego EAPOL

EAPOL é o Extensible Authentication Protocol over LAN.

```
ether proto 0x888e
```

Solução alternativa de captura IPv6

```
ether proto 0x86dd
```

Capturar tráfego com base no tipo de protocolo IP

```
ip proto 89
```

Rejeitar quadros Ethernet com base no endereço MAC - Excluir o tráfego que pertence ao grupo de multicast LLDP

O LLDP é o Link Layer Discovery Protocol .

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

Capturar tráfego UDLD, VTP ou CDP

O UDLD é detecção de enlace unidirecional, o VTP é o protocolo de entroncamento de VLAN e o CDP é o protocolo de descoberta Cisco.

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

Capturar tráfego de ou para um endereço MAC

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

Note:
e = &&
ou = ||
não = !
Formato do endereço MAC : xx:xx:xx:xx:xx:xx

Protocolos de plano de controle comum

- UDLD: DMAC (Media Access Controller, Controlador de acesso à mídia de destino) = 01-00-0C-CC-CC-CC e EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02 e EthType = 0x809. LACP significa Link Aggregation Control Protocol (protocolo de controle de agregação de link).
- STP: DMAC = 01:80:C2:00:00:00 e EthType = 0x4242 - ou - DMAC = 01:00:0C:CC:CD e EthType = 0x010B
- CDP: DMAC = 01-00-0C-CC-CC e EthType = 0x2000
- LLDP: DMAC = 01:80:C2:00:00:0E ou 01:80:C2:00:00:03 ou 01:80:C2:00:00:00 e EthType = 0x88CC
- DOT1X: DMAC = 01:80:C2:00:00:03 e EthType = 0x88E. DOT1X significa IEEE 802.1x.
- IPv6: EthType = 0x86DD
- Lista de números de porta UDP e TCP

Problemas conhecidos

ID de bug Cisco CSCue4854: O filtro de captura do Ethanalyzer não captura o tráfego da CPU no SUP2.

ID de bug Cisco CSCtx79409: Não é possível usar o filtro de captura com decode-internal.

ID de bug da Cisco CSCvi02546: O pacote gerado pelo SUP3 pode ter FCS; esse é o comportamento esperado.

Informações Relacionadas

- Wireshark: Filtros de Captura
- Wireshark: filtros de exibição
- Suporte Técnico e Documentação - Cisco Systems

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.