Índice

Introdução

Este documento descreve o Ethanalyzer, uma ferramenta integrada Cisco NX-OS da captura de pacote de informação para os pacotes de controle baseados em Wireshark.

Wireshark é aberta, analisador do protocolo de rede amplamente utilizado através de muitas indústrias e instituições educacionais. Descodifica os pacotes capturados pelo libpcap, a biblioteca da captura de pacote de informação. O Cisco NX-OS é executado sobre o kernel

(centro) de Linux, que usa a biblioteca do libpcap para apoiar a captura de pacote de informação.

Com Ethanalyzer, você pode:

- Capture os pacotes enviados ou recebidos pelo supervisor.
- Ajuste o número de pacotes a ser capturados.
- Ajuste o comprimento dos pacotes a ser capturados.
- Indique pacotes com informação de protocolo sumária ou detalhada.
- Abra e salvar os dados do pacote capturados.
- Filtre os pacotes capturados em muitos critérios.
- Filtre os pacotes a ser indicados em muitos critérios.
- Descodifique o encabeçamento 7000 interno do pacote de controle.

Ethanalyzer não pode:

- Advirta-o quando sua rede experimenta problemas. Contudo, Ethanalyzer pôde ajudá-lo a determinar a causa do problema.
- Capture o tráfego plano dos dados que é enviado no hardware.
- Apoie a captação relação-específica.

Opções de saída

Esta é uma ideia sumária da saída do comando **inband da interface local do ethanalyzer**. “?” ajuda dos indicadores da opção.

```
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 do “detalhe” para informação de protocolo detalhada.

```
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

captação-filtro

Use a opção do “captação-filtro” a fim selecionar que os pacotes a indicar ou salvar ao disco durante a captação. Um filtro da captação mantém uma taxa alta da captação quando filtrar. Porque a disseção completa não foi feita nos pacotes, os campos do filtro são predefinidos e limitados.

indicador-filtro

Use a opção do “indicador-filtro” a fim mudar a ideia de um arquivo de captura (arquivo de tmp). Um filtro do indicador usa pacotes inteiramente dissecados, assim que você pode fazer a filtração muito complexa e avançada quando você analisa uma rede tracefile. Contudo, o arquivo de tmp pode encher-se rapidamente, desde que captura primeiramente todos os pacotes e indica então somente os pacotes desejados.

Neste exemplo, os “limite-capturar-quadros” são ajustados ao 5. Com o “captação-filtro” a opção, Ethanalyzer mostra-lhe cinco pacotes que fósforo o host 10.10.10.2' do filtro '. Com a opção do “indicador-filtro”, Ethanalyzer primeiramente captura cinco pacotes a seguir indica somente os pacotes que combinam o 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
```

Escreva opções

escreva

“Escreva” a opção deixa-o redigir os dados da captação a um arquivo em um dos dispositivos de armazenamento (tais como o boothflash ou o logflash) no 7000 Series Switch do nexo de Cisco para a análise posterior. O tamanho de arquivo de captura é limitado ao 10 MB.

Um comando de Ethanalyzer do exemplo com “escreve” a opção é **interface local do ethanalyzer inband escreve o bootflash:** *capture_file_name*. Um exemplo do “escreve” a opção com o “captação-filtro” e um nome de arquivo da saída da “primeiro-captação” 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 da captação salvar a um arquivo, os pacotes capturados, não estão indicados à revelia na janela terminal. A opção do “indicador” força o Cisco NX-OS para indicar os pacotes quando salvar os dados da captação a um arquivo.

captação-anel-buffer

A opção do “captação-anel-buffer” cria arquivos múltiplos após um número especificado de segundos, um número especificado de arquivos, ou um tamanho do arquivo especificado. As definições daquelas opções estão neste screen shot:

```
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
```

Leia opções

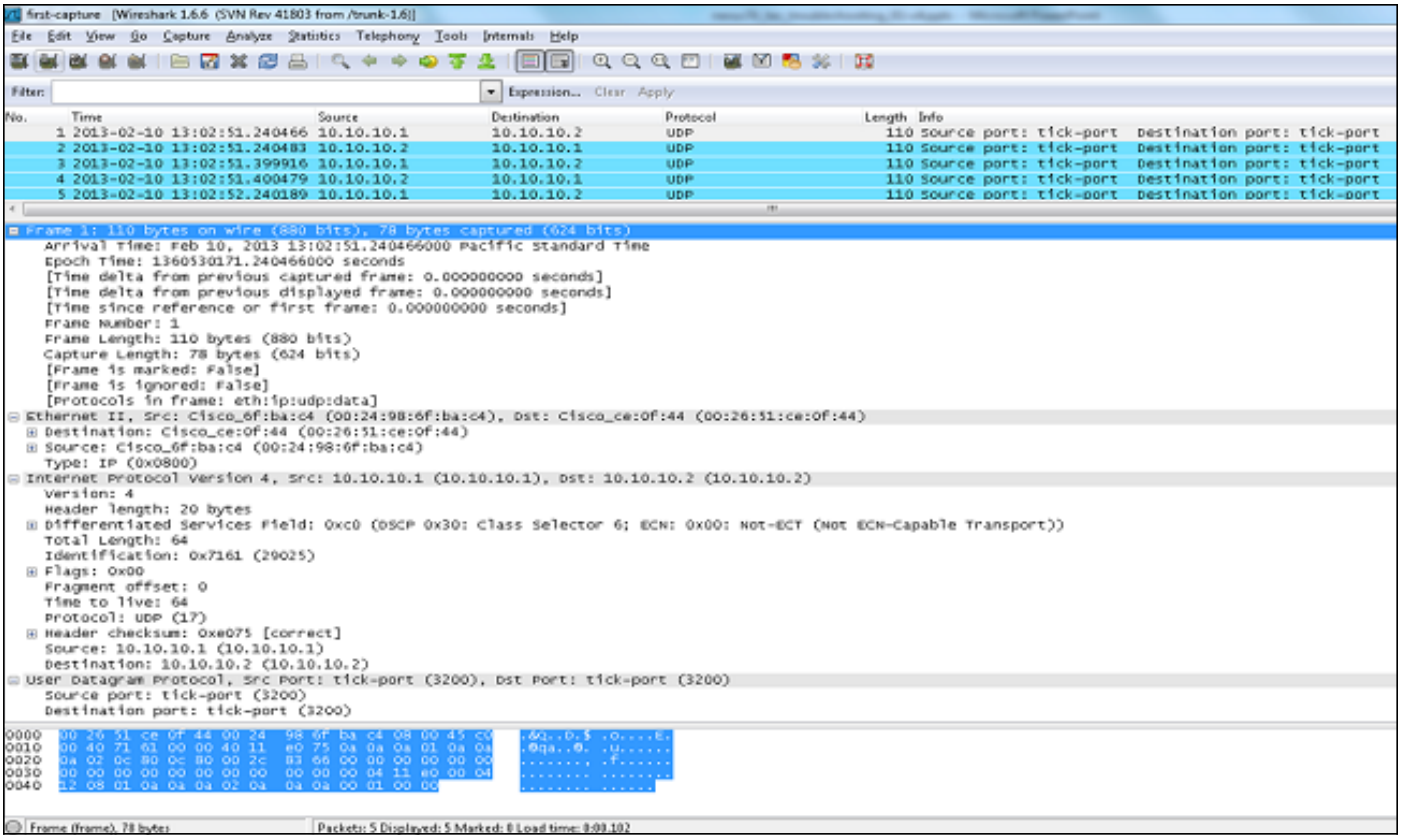
A opção “lida” deixa-o ler o arquivo salvo no dispositivo próprio.

```
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 pode igualmente transferir o arquivo a um server ou a um PC e lê-lo com Wireshark ou todo o outro aplicativo que puderem ler arquivos do tampão ou do 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.
```



descodificar-interno com opção do detalhe

A opção “descodificar-interna” relata a informação interna em como o nexo 7000 para a frente o pacote. Esta informação ajuda-o a compreender e pesquisar defeitos o fluxo dos pacotes com o 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 deslocamento predeterminado NX-OS ao hexadecimal, a seguir use o **comando x**

interno LTL da informação do pixm do sistema da mostra a fim traçar o deslocamento predeterminado da lógica de alvo local (LTL) a um exame ou a uma interface lógica.

Exemplos de valores do captação-filtro

Tráfego da captação a ou de um Host IP

Tráfego da captação a ou de uma escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT

Tráfego da captação de uma escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT

Tráfego da captação a uma escala dos endereços IP de Um ou Mais Servidores Cisco ICM NT

Tráfego da captação somente em algum protocolo - tráfego da captação somente DNS

O DNS é o protocolo do Domain Name System.

Tráfego da captação somente em algum protocolo - tráfego da captação somente DHCP

O DHCP é o protocolo de configuração dinâmica host.

Tráfego da captação não em algum protocolo - exclua o tráfego HTTP ou S TP

O S TP é o protocolo simple mail transfer.

Tráfego da captação não em algum protocolo - exclua o tráfego ARP e DNS

O ARP é o protocolo Protocolo de resolución de la dirección (ARP).

Tráfego IP da captação somente - Exclua protocolos da camada mais baixa como o ARP e o STP

O STP é o Spanning Tree Protocol.

Tráfego de unicast da captação somente - Exclua anúncios da transmissão e do Multicast

Capture o tráfego dentro de uma escala de portas da camada 4

Capture o tráfego baseado no tipo de Ethernet - Capture o tráfego EAPOL

O EAPOL é o protocolo extensible authentication sobre o LAN.

Workaround da captação do IPv6

Tráfego da captação baseado no tipo de protocolo IP

Frames da Ethernet da rejeição baseados no MAC address - Exclua o tráfego que pertence ao grupo de transmissão múltipla LLDP

LLDP é o protocolo de descoberta da camada de enlace.

Captação UDLD, VTP, ou tráfego de CDP

O UDLD é detecção de enlace unidirecional, o VTP é o protocolo VLAN trunking, e o CDP é o protocolo cisco discovery.

Tráfego da captação a ou de um MAC address

> Nota:
> e = &&
> ou = ||
> não =!
> Formato do MAC address: xx: xx: xx: xx: xx: xx

Protocolos planos do controle comum

- UDLD: Controlador do acesso da mídia de destino (DMAC) = 01-00-0C-CC-CC-CC e EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02 e EthType = 0x8809. O LACP representa o protocolo link aggregation control.
- STP: DMAC = 01:80:C2:00:00:00 e EthType = 0x4242 - ou - DMAC = 01:00:0C:CC:CC:CD e EthType = 0x010B

- CDP: DMAC = 01-00-0C-CC-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 = 0x888E. O DOT1X representa o IEEE 802.1X.
- IPv6: EthType = 0x86DD
- Lista de UDP e de números de porta de TCP

Problemas conhecidos

Veja a identificação de bug Cisco CSCue48854: O captação-filtro de Ethanalyzer não captura o tráfego do CPU no SUP2. Igualmente veja a identificação de bug Cisco CSCtx79409: Não pode usar o filtro da captação com descodificar-interno.

Informações Relacionadas

- Wireshark: CaptureFilters
- Wireshark: DisplayFilters
- Suporte Técnico e Documentação - Cisco Systems