Contenido

Introducción

Este documento describe el Ethanalyzer, una herramienta integrada Cisco NX-OS de la captura de paquetes para los paquetes de control basados sobre Wireshark.

Wireshark es analizador de fuente abierta, del Network Protocol ampliamente utilizado a través de muchas industrias y instituciones educativas. Decodifica los paquetes capturados por el libpcap, la biblioteca de la captura de paquetes. El Cisco NX-OS se ejecuta encima del núcleo de Linux,

que utiliza la biblioteca del libpcap para apoyar a la captura de paquetes.

Con Ethanalyzer, usted puede:

- Capture los paquetes enviados o recibidos por el supervisor.
- Fije el número de paquetes que se capturarán.
- Fije la longitud de los paquetes que se capturarán.
- Visualice los paquetes con la información sobre protocolo sumaria o detallada.
- Abra y salve los datos del paquete capturados.
- Filtre los paquetes capturados en muchos criterios.
- Filtre los paquetes que se visualizarán en muchos criterios.
- Decodifique la encabezado interna 7000 del paquete de control.

Ethanalyzer no puede:

- Adviértale cuando su red experimenta los problemas. Sin embargo, Ethanalyzer pudo ayudarle a determinar la causa del problema.
- Capture el tráfico del plano de los datos que se remite en hardware.
- Soporte la captura interfaz-específica.

Opciones de resultado

Ésta es una vista sumaria de la salida del comando **inband de la interfaz local del ethanalyzer**. “?” ayuda de las visualizaciones de la opción.

```
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
```

Utilice la opción del “detalle” para la información sobre protocolo detallada.

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

Opciones de filtro

captura-filtro

Utilice la opción del “captura-filtro” para seleccionar que los paquetes a visualizar o a salvar al disco durante la captura. Un filtro de la captura mantiene una alta velocidad de la captura mientras que filtra. Porque la disección completa no se ha hecho en los paquetes, se predefinen y se limitan los campos del filtro.

visualización-filtro

Utilice la opción del “visualización-filtro” para cambiar la vista de un capturar archivo (archivo de tmp). Un filtro de la visualización utiliza los paquetes completamente disecados, así que usted puede hacer la filtración muy compleja y avanzada cuando usted analiza una red tracefile. Sin embargo, el archivo de tmp puede llenar rápidamente, puesto que primero captura todos los paquetes y en seguida visualiza solamente los paquetes deseados.

En este ejemplo, las “límite-capturar-tramas” se fijan a 5. Con el “captura-filtro” la opción, Ethanalyzer le muestra cinco paquetes qué coincidencia host 10.10.10.2' del filtro el '. Con la opción del “visualización-filtro”, Ethanalyzer primero captura cinco paquetes después visualiza solamente los paquetes que hacen juego el 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
```

Escriba las opciones

escriba

“Escriba” la opción le deja escribir los datos de la captura a un archivo en uno de los dispositivos de almacenamiento (tales como boothflash o logflash) en el 7000 Series Switch del nexo de Cisco para la análisis posterior. El tamaño del capturar archivo se limita al 10 MB.

Un comando de Ethanalyzer del ejemplo con “escribe” la opción es **interfaz local del ethanalyzer inband escribe el bootflash:** *capture_file_name*. Un ejemplo del “escribe” la opción con el “captura-filtro” y un nombre del archivo de la salida de la “primero-captura” es:

```
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
```

Cuando los datos de la captura se guardan a un archivo, los paquetes capturados, por abandono, no se visualizan en la ventana de terminal. La opción de la “visualización” fuerza el Cisco NX-OS para visualizar los paquetes mientras que guarda los datos de la captura a un archivo.

captura-timbre-buffer

La opción del “captura-timbre-buffer” crea los Archivos múltiples después de un número especificado de segundos, de un número especificado de archivos, o de un tamaño del archivo especificado. Las definiciones de esas opciones están en esta captura de pantalla:

```
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
```

Lea las opciones

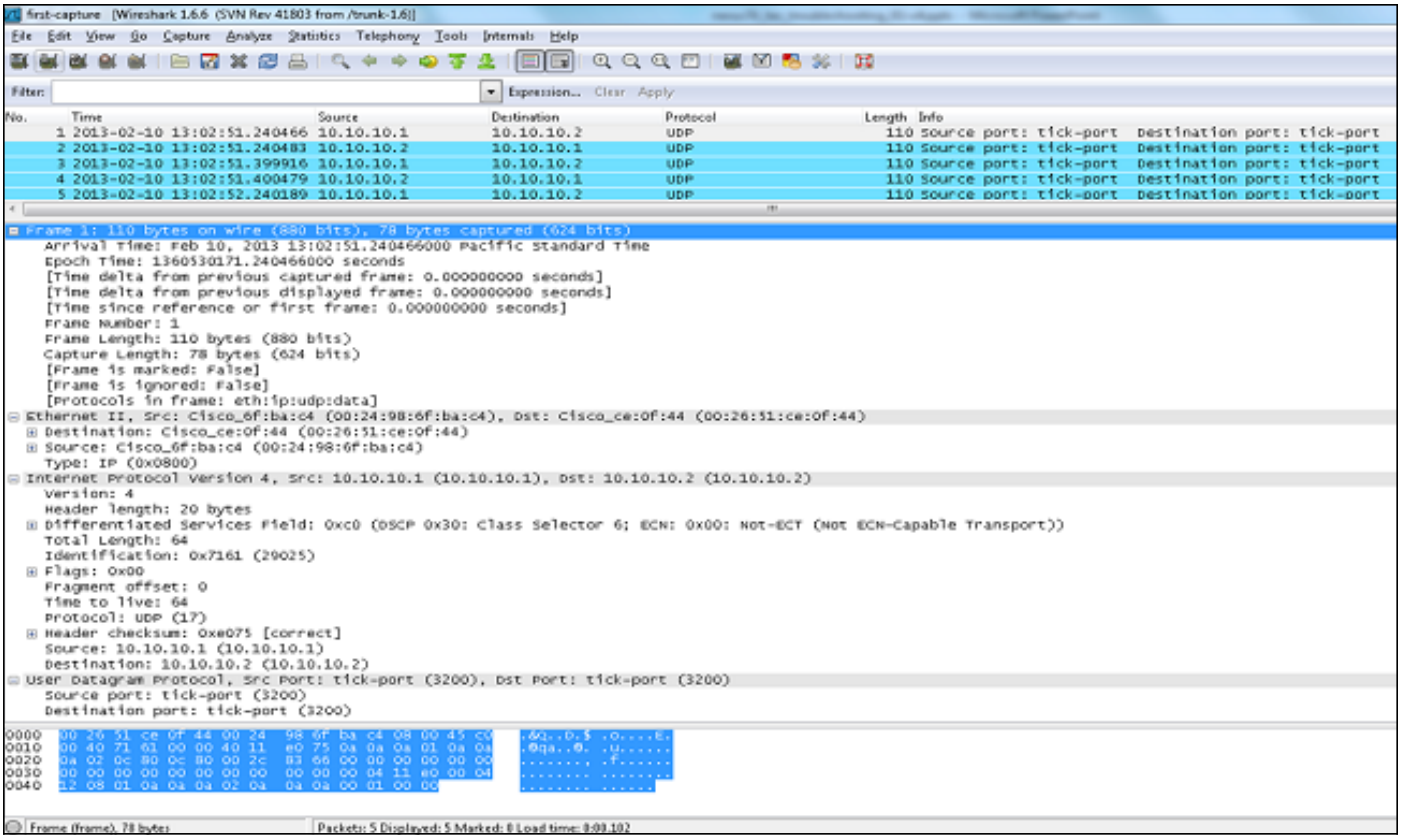
La opción “leída” le deja leer el archivo guardado en el dispositivo sí mismo.

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

Usted puede también transferir el archivo a un servidor o a un PC y leerlo con Wireshark o cualquier otra aplicación que puedan leer los archivos del casquillo o del 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 con la opción del detalle

La opción “decodificar-interna” señala la información interna en cómo el nexo 7000 adelante el paquete. Esta información le ayuda a entender y a resolver problemas el flujo de paquetes con el 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-----------------------------------------
```

Convierta el índice NX-OS al hexadecimal, después utilice el **comando x interno LTL de la**

información del pixm del sistema de la demostración para asociar el índice de la lógica de destino local (LTL) a una comprobación o a una interfaz lógica.

Ejemplos de los valores del captura-filtro

Tráfico de la captura a o desde un host IP

Tráfico de la captura a o desde un rango de los IP Addresses

Tráfico de la captura de un rango de los IP Addresses

Tráfico de la captura a un rango de los IP Addresses

Tráfico de la captura solamente en cierto protocolo - tráfico de la captura solamente DNS

El DNS es el protocolo del Sistema de nombres de dominio (DNS).

Tráfico de la captura solamente en cierto protocolo - tráfico del DHCP de la captura solamente

El DHCP es el protocolo DHCP.

Tráfico de la captura no en cierto protocolo - excluya el tráfico HTTP o S TP

El S TP es el protocolo simple mail transfer.

Tráfico de la captura no en cierto protocolo - excluya el tráfico ARP y DNS

El ARP es el protocolo Protocolo de resolución de la dirección (ARP).

Tráfico IP de la captura solamente - Excluya los protocolos de la capa inferior como el ARP y el STP

El STP es el Spanning Tree Protocol.

Tráfico de unidifusión de la captura solamente - Excluya los avisos del broadcast y

del Multicast

Capture el tráfico dentro de un rango de los puertos de la capa 4

Capture el tráfico basado en el tipo Ethernet - Capture el tráfico EAPOL

El EAPOL es el protocolo extensible authentication sobre el LAN.

Workaround de la captura del IPv6

Tráfico de la captura basado en el tipo de protocolo IP

Tramas Ethernet del rechazo basadas en la dirección MAC - Excluya el tráfico que pertenece al grupo de multidifusión LLDP

LLDP es el Discovery Protocol de la capa de link.

Captura UDLD, VTP, o tráfico CDP

El UDLD es detección de link unidireccional, el VTP es el protocolo VLAN trunking, y el CDP es el protocolo cisco discovery.

Tráfico de la captura a o desde una dirección MAC

> Nota:
> y = &&
> o = ||
> ¡no =!
> Formato de la dirección MAC: xx: xx: xx: xx: xx: xx

Protocolos planos del control común

- UDLD: Regulador del acceso de los medios de destino (DMAC) = 01-00-0C-CC-CC-CC y EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02 y EthType = 0x8809. Protocolo link aggregation control de la significa LACP.
- STP: DMAC = 01:80:C2:00:00:00 y EthType = 0x4242 - o - DMAC = 01:00:0C:CC:CC:CD y EthType = 0x010B
- CDP: DMAC = 01-00-0C-CC-CC-CC y EthType = 0x2000
- LLDP: DMAC = 01:80:C2:00:00:0E o 01:80:C2:00:00:03 o 01:80:C2:00:00:00 y EthType =

0x88CC
- DOT1X: DMAC = 01:80:C2:00:00:03 y EthType = 0x888E. IEEE 802.1X de la significa del DOT1X.
- IPv6: EthType = 0x86DD
- Lista de UDP y de números del puerto TCP

Problemas conocidos

Vea el Id. de bug Cisco CSCue48854: El captura-filtro de Ethanalyzer no captura el tráfico del CPU en el SUP2. También vea el Id. de bug Cisco CSCtx79409: No puede utilizar el filtro de la captura con decodificar-interno.

Información Relacionada

- Wireshark: CaptureFilters
- Wireshark: DisplayFilters
- Soporte Técnico y Documentación - Cisco Systems