Utilice la guía de solución de problemas de Ethanalyzer en Nexus 7000

Contenido

Introducción

Este documento describe Ethanalyzer, una herramienta integrada de captura de paquetes de Cisco NX-OS para controlar paquetes basados en Wireshark.

Antecedentes

Wireshark es un analizador de protocolos de red de código abierto ampliamente utilizado en muchos sectores e instituciones educativas. Descodifica los paquetes capturados por libpcap, la biblioteca de captura de paquetes. Cisco NX-OS se ejecuta sobre el kernel de Linux, que utiliza la biblioteca libpcap para soportar la captura de paquetes.

Con Ethanalyzer, puede:

- Capturar los paquetes enviados o recibidos por el supervisor.
- Establezca el número de paquetes que se van a capturar.
- Establezca la longitud de los paquetes que se van a capturar.
- Mostrar paquetes con información de protocolo resumida o detallada.
- Abra y guarde los datos de paquetes capturados.
- Filtrar paquetes capturados según muchos criterios.
- Filtrar paquetes para mostrarlos según muchos criterios.
- Decodificar el encabezado interno 7000 del paquete de control.

Ethanalyzer no puede:

- Advertirle cuando su red experimente problemas. Sin embargo, Ethanalyzer puede ayudarle a determinar la causa del problema.
- Capture el tráfico del plano de datos que se reenvía en el hardware.
- Admita la captura específica de interfaz.

Opciones de salida

Esta es una vista de resumen del resultado del comando **ethanalyzer local interface inband**. La opción '?' muestra la ayuda.

```
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 'detail' para obtener información detallada sobre el protocolo. ^C se puede utilizar para anular y recuperar el mensaje del switch en medio de una captura si es necesario.

```
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

Capturar-filtrar

Utilice la opción 'capture-filter' para seleccionar qué paquetes mostrar o guardar en el disco durante la captura. Un filtro de captura mantiene una alta tasa de captura mientras filtra. Debido a que no se ha realizado una disección completa de los paquetes, los campos de filtro están predefinidos y limitados.

Display-filter

Utilice la opción 'display-filter' para cambiar la vista de un archivo de captura (archivo tmp). Un filtro de visualización utiliza paquetes completamente diseccionados, por lo que puede realizar un filtrado muy complejo y avanzado cuando analiza un archivo de seguimiento de red. Sin embargo, el archivo tmp puede llenarse rápidamente, ya que primero captura todos los paquetes y luego muestra sólo los paquetes deseados.

En este ejemplo, 'limit-capture-frames' se establece en 5. Con la opción 'capture-filter', Ethanalyzer muestra cinco paquetes que coinciden con el filtro 'host 10.10.10.2'. Con la opción 'display-filter', Ethanalyzer primero captura cinco paquetes y luego muestra solamente los

paquetes que coinciden con 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
```

Opciones de escritura

Escritura

La opción de "escritura" le permite escribir los datos de captura en un archivo de uno de los dispositivos de almacenamiento (como bothflash o logflash) en el switch Nexus de Cisco serie 7000 para su análisis posterior. El tamaño del archivo de captura está limitado a 10 MB.

Un ejemplo del comando Ethanalyzer con una opción 'write' es **ethanalyzer local interface inband write bootflash:***capture_file_name*. Un ejemplo de una opción 'write' con 'capture-filter' y un nombre de archivo de salida de 'first-capture' 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 captura se guardan en un archivo, los paquetes capturados no se muestran, de forma predeterminada, en la ventana de terminal. La opción 'display' obliga a Cisco NX-OS a mostrar los paquetes mientras guarda los datos de captura en un archivo.

Capture-ring-buffer

La opción 'capture-ring-buffer' crea varios archivos después de un número de segundos especificado, un número de archivos especificado o un tamaño de archivo especificado. Las definiciones de estas opciones se encuentran 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
```

Opciones de lectura

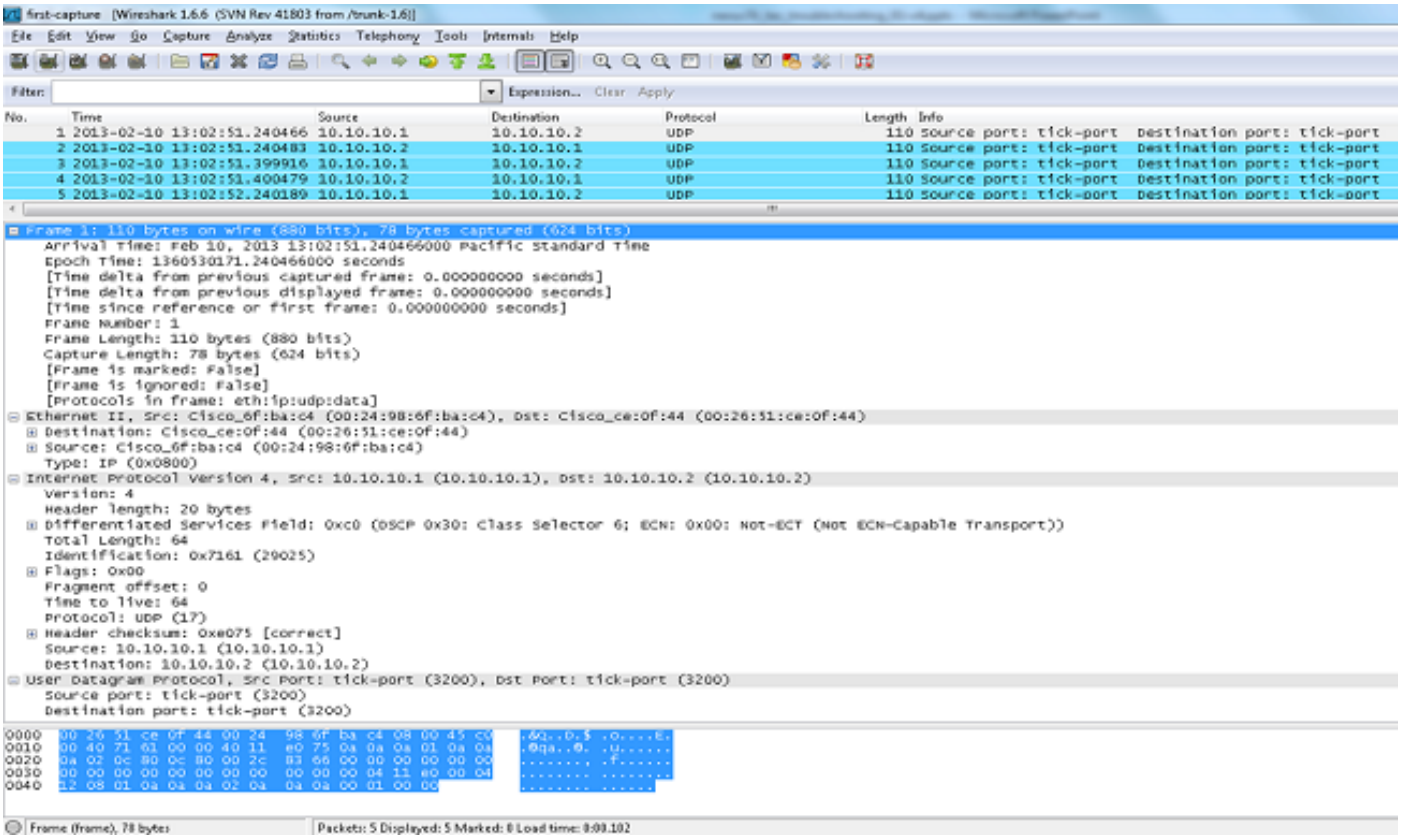
La opción 'read' le permite leer el archivo guardado en el propio dispositivo.

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

También puede transferir el archivo a un servidor o un PC y leerlo con Wireshark o cualquier otra aplicación que pueda leer archivos cap o 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.
```



Decodificación interna con opción de detalle

La opción 'decode-internal' informa de información interna sobre cómo Nexus 7000 reenvía el paquete. Esta información le ayuda a entender y resolver problemas del flujo de paquetes a través de 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-----------------------------------------
```

Convierta el índice NX-OS a hexadecimal y, a continuación, utilice el comando **show system internal pixm info ltl x** para asignar el índice de lógica de destino local (LTL) a una interfaz física o

lógica.

Ejemplos de Valores de Capture-filter

Capturar tráfico hacia o desde un host IP

```
host 10.1.1.1
```

Capturar tráfico hacia o desde un rango de direcciones IP

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

Capturar tráfico desde un rango de direcciones IP

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

Capturar tráfico a un rango de direcciones IP

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

Capturar tráfico sólo en un protocolo determinado - Capturar sólo tráfico DNS

DNS es el protocolo del sistema de nombres de dominio.

```
port 53
```

Capturar tráfico sólo en un protocolo determinado - Capturar sólo tráfico DHCP

DHCP es el protocolo de configuración dinámica de host.

```
port 67 or port 68
```

Capturar tráfico que no está en un protocolo determinado - Excluir tráfico HTTP o SMTP

SMTP es el protocolo simple de transferencia de correo.

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

Capturar tráfico que no está en un protocolo determinado - Excluir tráfico ARP y DNS

ARP es el protocolo de resolución de direcciones.

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

Capturar sólo tráfico IP - Excluir protocolos de capa inferior como ARP y STP

STP es el protocolo de árbol de extensión.

```
ip
```

Capturar sólo tráfico unidifusión - Excluir anuncios de difusión y multidifusión

```
not broadcast and not multicast
```

Captura de tráfico dentro de un rango de puertos de capa 4

```
tcp portrange 1501-1549
```

Capturar tráfico basado en el tipo de Ethernet: Capturar tráfico EAPOL

EAPOL es el protocolo de autenticación extensible sobre LAN.

```
ether proto 0x888e
```

Solución alternativa de captura IPv6

```
ether proto 0x86dd
```

Capturar tráfico basado en el tipo de protocolo IP

```
ip proto 89
```

Rechazar Tramas Ethernet Basadas en la Dirección MAC - Excluya el Tráfico que Pertenece al Grupo Multicast LLDP

LLDP es el protocolo de descubrimiento de la capa de link.

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

Capturar tráfico UDLD, VTP o CDP

UDLD es Detección de Link Unidireccional, VTP es el VLAN Trunking Protocol y CDP es el Cisco Discovery Protocol.

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

Capturar tráfico hacia o desde una dirección MAC

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

> **Nota:**
> y = &&
> o = ||

not = !
Formato de dirección MAC: xx:xx:xx:xx:xx:xx

Protocolos comunes del plano de control

- UDLD: controlador de acceso a medios de destino (DMAC) = 01-00-0C-CC-CC-CC y EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02 y EthType = 0x809. LACP significa protocolo de control de agregación de enlaces.
- 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 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 = 0x88E. DOT1X significa IEEE 802.1x.
- IPv6: EthType = 0x86DD
- Lista de números de puerto UDP y TCP

Problemas conocidos

ID de bug de Cisco CSCue48854: El filtro de captura de Ethanalyzer no captura el tráfico de la CPU en SUP2.

Id. de error de Cisco CSCtx79409: No se puede utilizar el filtro de captura con decode-internal.

Id. de error de Cisco CSCvi02546: el paquete generado por el SUP3 puede tener FCS; se trata de un comportamiento esperado.

Información Relacionada

- Wireshark: Capturar filtros
- Wireshark: filtros de visualización
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).