Contenu

[Introduction](#)
[Options de sortie](#)
[Options de filtre](#)
[capture-filtre](#)
[affichage-filtre](#)
[Écrivez les options](#)
[écrivez](#)
[capture-sonnerie-mémoire tampon](#)
[Lisez les options](#)
[décoder-interne avec l'option de détail](#)
[Exemples des valeurs de capture-filtre](#)
[Le trafic de capture à ou d'un hôte IP](#)
[Le trafic de capture à ou d'une plage des adresses IP](#)
[Le trafic de capture d'une plage des adresses IP](#)
[Le trafic de capture à une plage des adresses IP](#)
[Le trafic de capture seulement sur certain Protocol - le trafic DNS de capture seulement](#)
[Le trafic de capture seulement sur certain Protocol - le trafic DHCP de capture seulement](#)
[Le trafic de capture pas sur certain Protocol - excluez le trafic de HTTP ou de SMTP](#)
[Le trafic de capture pas sur certain Protocol - excluez l'ARP et le trafic DNS](#)
[Le trafic IP de capture seulement - Excluez les protocoles de couche inférieure comme l'ARP et le STP](#)
[Le trafic unicast de capture seulement - Excluez les annonces d'émission et de Multidiffusion](#)
[Le trafic de capture dans une marge des ports de la couche 4](#)
[Le trafic de capture basé sur le type d'Ethernets - Le trafic de la capture EAPOL](#)
[Contournement de capture d'IPv6](#)
[Le trafic de capture basé sur le type de protocole IP](#)
[Trames Ethernet d'anomalie basées sur l'adresse MAC - Excluez le trafic qui appartient au groupe de multidiffusion de LLDP](#)
[Capture UDLD, VTP, ou trafic CDP](#)
[Le trafic de capture à ou d'une adresse MAC](#)
[Protocoles d'avion de contrôle commun](#)
[Problèmes identifiés](#)
[Informations connexes](#)

Introduction

Ce document décrit l'Ethanalyzer, un outil de capture de paquet intégré par Cisco NX-OS pour des paquets de contrôle basés sur Wireshark.

Wireshark est open-source, analyseur de protocole réseau très utilisé à travers beaucoup de secteurs et établissements d'enseignement. Il décode des paquets capturés par le libpcap, la bibliothèque de capture de paquet. Le Cisco NX-OS fonctionne sur le kernel Linux, qui emploie la

bibliothèque de libpcap pour prendre en charge la capture de paquet.

Avec Ethanalyzer, vous pouvez :

- Capturez les paquets envoyés ou reçus par le superviseur.
- Placez le nombre de paquets à capturer.
- Placez la longueur des paquets à capturer.
- Affichez les paquets avec les informations récapitulatives ou détaillées de protocole.
- Ouvrez et sauvegardez les données de paquets capturées.
- Paquets de filtre capturés sur beaucoup de critères.
- Filtrez les paquets à afficher sur beaucoup de critères.
- Décodez l'en-tête 7000 interne du paquet de contrôle.

Ethanalyzer ne peut pas :

- Avertissez-vous quand vos problèmes d'expériences réseau. Cependant, Ethanalyzer pourrait vous aider à déterminer la cause du problème.
- Le trafic de plan de données de capture qui est expédié dans le matériel.
- Capture d'interface-particularité de support.

Options de sortie

C'est une vue récapitulative de sortie de la commande **intrabande d'ethanalyzer local interface**. « ? » aide d'affichages d'option.

```
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
```

Utilisez l'option de « détail » pour les informations détaillées de protocole.

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

Options de filtre

capture-filtre

Employez l'option de « capture-filtre » afin de sélectionner qui des paquets à afficher ou sauvegarder au disque pendant la capture. Un filtre de capture met à jour un haut débit de capture tandis qu'il filtre. Puisque la pleine dissection n'a pas été faite sur les paquets, les champs de filtre sont prédéfinis et limités.

affichage-filtre

Employez l'option de « affichage-filtre » afin de changer la vue d'un fichier de capture (fichier de tmp). Un filtre d'affichage utilise les paquets entièrement disséqués, ainsi vous pouvez faire le filtrage très complexe et avancé quand vous analysez un réseau tracefile. Cependant, le fichier de tmp peut remplir rapidement, puisqu'il capture d'abord tous les paquets et affiche ensuite seulement les paquets désirés.

Dans cet exemple, des « limite-capturer-trames » est placées à 5. Avec le « capture-filtre » l'option, Ethanalyzer t'affiche cinq paquets quelle correspondance hôte 10.10.10.2'du filtre le '. Avec l'option de « affichage-filtre », Ethanalyzer d'abord capture cinq paquets puis affiche seulement les paquets qui apparient le filtre '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
```

Écrivez les options

écrivez

« Écrivez » l'option vous permet d'écrire les données de saisie à un fichier dans un des périphériques de stockage (tels que le boothflash ou le logflash) sur la gamme 7000 de Cisco Nexus commutent pour l'analyse postérieure. La taille de fichier de capture est limitée à 10 Mo.

Une commande d'Ethanalyzer d'exemple avec « écrivent » l'option est **ethanalyzer local interface intrabande écrivent le bootflash :** *capture_file_name*. Un exemple d'« écrivent » l'option avec le « capture-filtre » et un nom du fichier de sortie de « premier-capture » est :

```
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
```

Quand les données de capture sont enregistrées à un fichier, les paquets capturés, par défaut, ne sont pas affichés dans le terminal window. L'option de « affichage » force le Cisco NX-OS pour afficher les paquets tandis qu'elle enregistre les données de capture à un fichier.

capture-sonnerie-mémoire tampon

L'option de « capture-sonnerie-mémoire tampon » crée des plusieurs fichiers après qu'un nombre spécifié de secondes, un nombre spécifié de fichiers, ou un volume de fichier spécifié. Les définitions de ces options sont dans cette copie d'écran :

```
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
```

Lisez les options

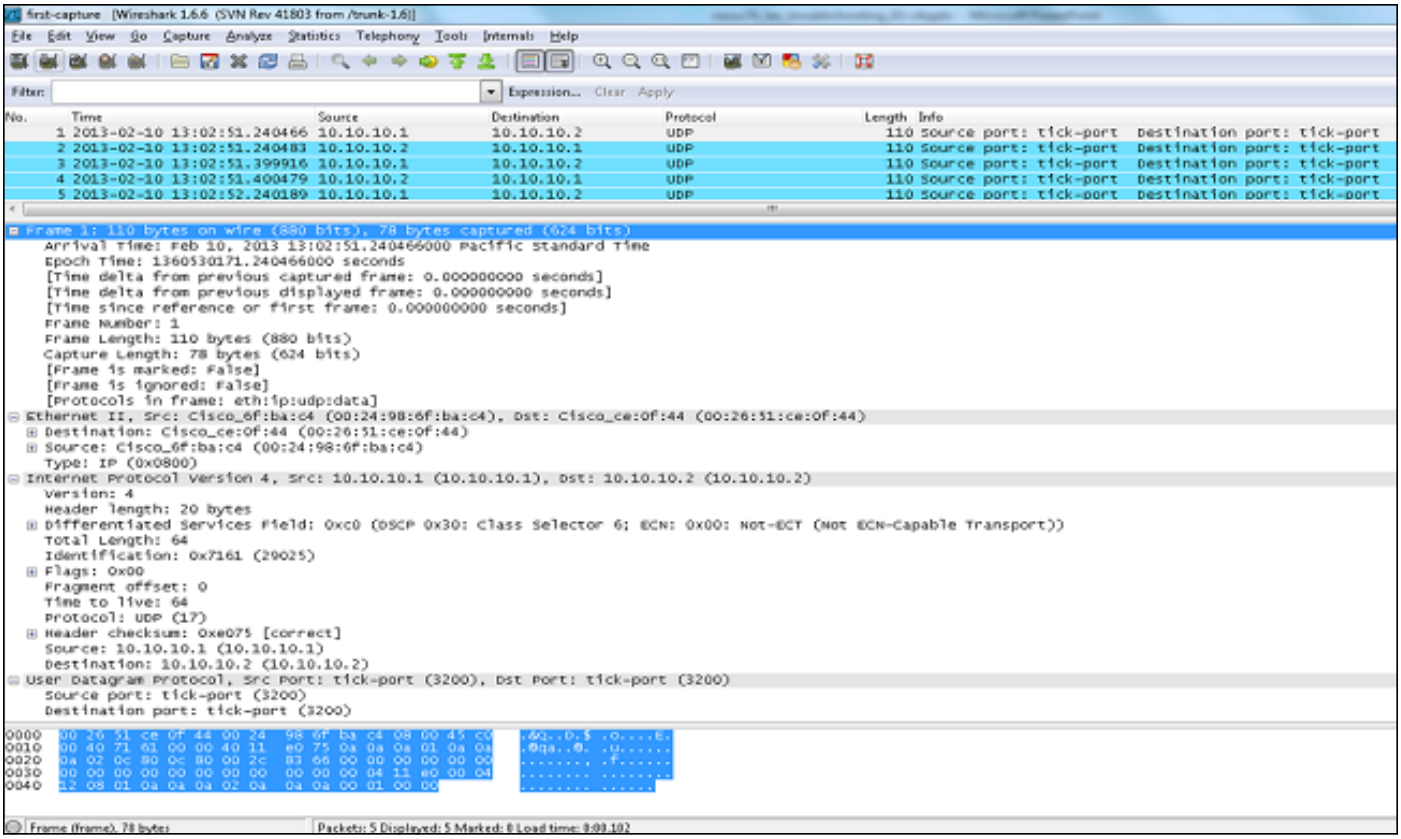
L'option « lue » vous permet de lire le fichier sauvegardé sur le périphérique lui-même.

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

Vous pouvez également transférer le fichier vers un serveur ou un PC et le lire avec Wireshark ou n'importe quelle autre application qui peuvent lire des fichiers de CAP ou de 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.
```



décoder-interne avec l'option de détail

L'option « décoder-interne » signale les informations internes sur la façon dont le Nexus 7000 en avant le paquet. Ces informations vous aident à comprendre et dépanner l'écoulement des paquets par 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-----------------------------------------
```

Convertissez l'index NX-OS en hexadécimal, puis employez la commande **interne LTL X de**

l'information de pixm de show system afin de tracer l'index local de la logique de cible (LTL) à un examen médical ou à une interface logique.

Exemples des valeurs de capture-filtre

Le trafic de capture à ou d'un hôte IP

Le trafic de capture à ou d'une plage des adresses IP

Le trafic de capture d'une plage des adresses IP

Le trafic de capture à une plage des adresses IP

Le trafic de capture seulement sur certain Protocol - le trafic DNS de capture seulement

Les DN est le système de noms de domaine Protocol.

Le trafic de capture seulement sur certain Protocol - le trafic DHCP de capture seulement

Le DHCP est le protocole DHCP.

Le trafic de capture pas sur certain Protocol - excluez le trafic de HTTP ou de SMTP

Le SMTP est le Simple Mail Transfer Protocol.

Le trafic de capture pas sur certain Protocol - excluez l'ARP et le trafic DNS

L'ARP est Address Resolution Protocol.

Le trafic IP de capture seulement - Excluez les protocoles de couche inférieure comme l'ARP et le STP

STP est le Protocole Spanning Tree.

Le trafic unicast de capture seulement - Excluez les annonces d'émission et de

Multidiffusion

Le trafic de capture dans une marge des ports de la couche 4

Le trafic de capture basé sur le type d'Ethernets - Le trafic de la capture EAPOL

EAPOL est Extensible Authentication Protocol au-dessus de RÉSEAU LOCAL.

Contournement de capture d'IPv6

Le trafic de capture basé sur le type de protocole IP

Trames Ethernet d'anomalie basées sur l'adresse MAC - Excluez le trafic qui appartient au groupe de multidiffusion de LLDP

Le LLDP est le Discovery Protocol de couche de liaison.

Capture UDLD, VTP, ou trafic CDP

UDLD est détection unidirectionnelle de lien, le VTP est le VLAN trunking protocol, et le CDP est le Cisco Discovery Protocol.

Le trafic de capture à ou d'une adresse MAC

> Remarque:
> et = &&
> ou = ||
> pas = !
> Format d'adresse MAC : xx : xx : xx : xx : xx : xx

Protocoles d'avion de contrôle commun

- UDLD : Contrôleur d'accès au support de destination (DMAC) = 01-00-0C-CC-CC-CC et EthType = 0x0111
- LACP : DMAC = 01:80:C2:00:00:02 et EthType = 0x8809. Le LACP signifie le Control Protocol d'agrégation de liaisons.
- STP : DMAC = 01:80:C2:00:00:00 et EthType = 0x4242 - ou - DMAC = 01:00:0C:CC:CC:CD et EthType = 0x010B
- CDP : DMAC = 01-00-0C-CC-CC-CC et EthType = 0x2000
- LLDP : DMAC = 01:80:C2:00:00:0E ou 01:80:C2:00:00:03 ou 01:80:C2:00:00:00 et EthType =

0x88CC
- DOT1X : DMAC = 01:80:C2:00:00:03 et EthType = 0x888E. Le DOT1X signifie le 802.1x d'IEEE.
- IPv6 : EthType = 0x86DD
- Liste de nombres d'UDP et de port TCP

Problèmes identifiés

Voir l'ID de bogue Cisco CSCue48854 : Le capture-filtre d'Ethanalyzer ne capture pas le trafic de la CPU sur SUP2. Voir également l'ID de bogue Cisco CSCtx79409 : Ne peut pas utiliser le filtre de capture avec décoder-interne.

Informations connexes

- Wireshark : CaptureFilters
- Wireshark : DisplayFilters
- Support et documentation techniques - Cisco Systems