Utilisation du guide de dépannage d'Ethanalyzer sur Nexus 7000

Table des matières

Introduction

Ce document décrit l'Ethanalyzer, un outil de capture de paquets intégré à Cisco NX-OS pour contrôler les paquets basés sur Wireshark.

Informations générales

Wireshark est un analyseur de protocole réseau open source largement utilisé dans de nombreux secteurs et établissements d'enseignement. Il décode les paquets capturés par libpcap, la bibliothèque de capture de paquets. Cisco NX-OS s'exécute sur le noyau Linux, qui utilise la bibliothèque libpcap afin de prendre en charge la capture de paquets.

Avec Ethanalyzer, vous pouvez :

- Capturez les paquets envoyés ou reçus par le superviseur.
- Définissez le nombre de paquets à capturer.
- Définissez la longueur des paquets à capturer.
- Affichez les paquets avec des informations récapitulatives ou détaillées sur le protocole.
- Ouvrez et enregistrez les données de paquet capturées.
- Filtrez les paquets capturés selon de nombreux critères.
- Filtrer les paquets à afficher selon plusieurs critères.
- Décodez l'en-tête 7000 interne du paquet de contrôle.

Ethanalyzer ne peut pas :

- Vous avertir en cas de problème sur votre réseau. Cependant, Ethanalyzer peut vous aider à déterminer la cause du problème.
- Capturez le trafic du plan de données transféré dans le matériel.
- Prise en charge de la capture spécifique aux interfaces.

Options de sortie

Il s'agit d'une vue récapitulative du résultat de la commande ethanalyzer local interface inband. L'option ? affiche l'aide.

```
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 detail pour obtenir des informations détaillées sur le protocole. ^C peut être utilisé pour abandonner et récupérer l'invite du commutateur au milieu d'une capture, si nécessaire.

```
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

Filtre-Capture

Utilisez l'option capture-filter afin de sélectionner les paquets à afficher ou enregistrer sur le disque pendant la capture. Un filtre de capture conserve un taux élevé de capture pendant qu'il filtre. Étant donné que la dissection complète n'a pas été effectuée sur les paquets, les champs de filtre sont prédéfinis et limités.

Filtre-Écran

Utilisez l'option display-filter afin de changer l'affichage d'un fichier de capture (fichier tmp). Un filtre d'affichage utilise des paquets entièrement disséqués, ce qui vous permet d'effectuer un filtrage très complexe et avancé lorsque vous analysez un fichier de trace réseau. Cependant, le fichier tmp peut se remplir rapidement puisqu'il capture d'abord tous les paquets, puis affiche uniquement les paquets souhaités.

Dans cet exemple, limit-capture-frames est défini sur 5. Avec l'option capture-filter, Ethanalyzer affiche cinq paquets qui correspondent à l'hôte de filtrage 10.10.10.2. Avec l'option display-filter, Ethanalyzer capture d'abord cinq paquets, puis affiche uniquement les paquets correspondant au 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
```

Options d'écriture

Écrire

L'option d'écriture vous permet d'écrire les données de capture dans un fichier dans l'un des périphériques de stockage (tels que bootflash ou logflash) sur le commutateur Cisco Nexus 7000 pour une analyse ultérieure. La taille du fichier de capture est limitée à 10 Mo.

Un exemple de commande Ethanalyzer avec une option write est ethanalyzer local interface inband write bootflash: capture_file_name. Voici un exemple d'option d'écriture avec capture-filter et le nom de fichier de sortie first-capture :

```
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
```

Lorsque les données de capture sont enregistrées dans un fichier, les paquets capturés ne sont pas affichés par défaut dans la fenêtre du terminal. L'option d'affichage force Cisco NX-OS à afficher les paquets pendant qu'il enregistre les données de capture dans un fichier.

Capture-Ring-Buffer

L'option capture-ring-buffer crée plusieurs fichiers après un nombre de secondes spécifié, un nombre de fichiers spécifié ou une taille de fichier spécifiée. Les définitions de ces options sont dans cette capture 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
```

Options de lecture

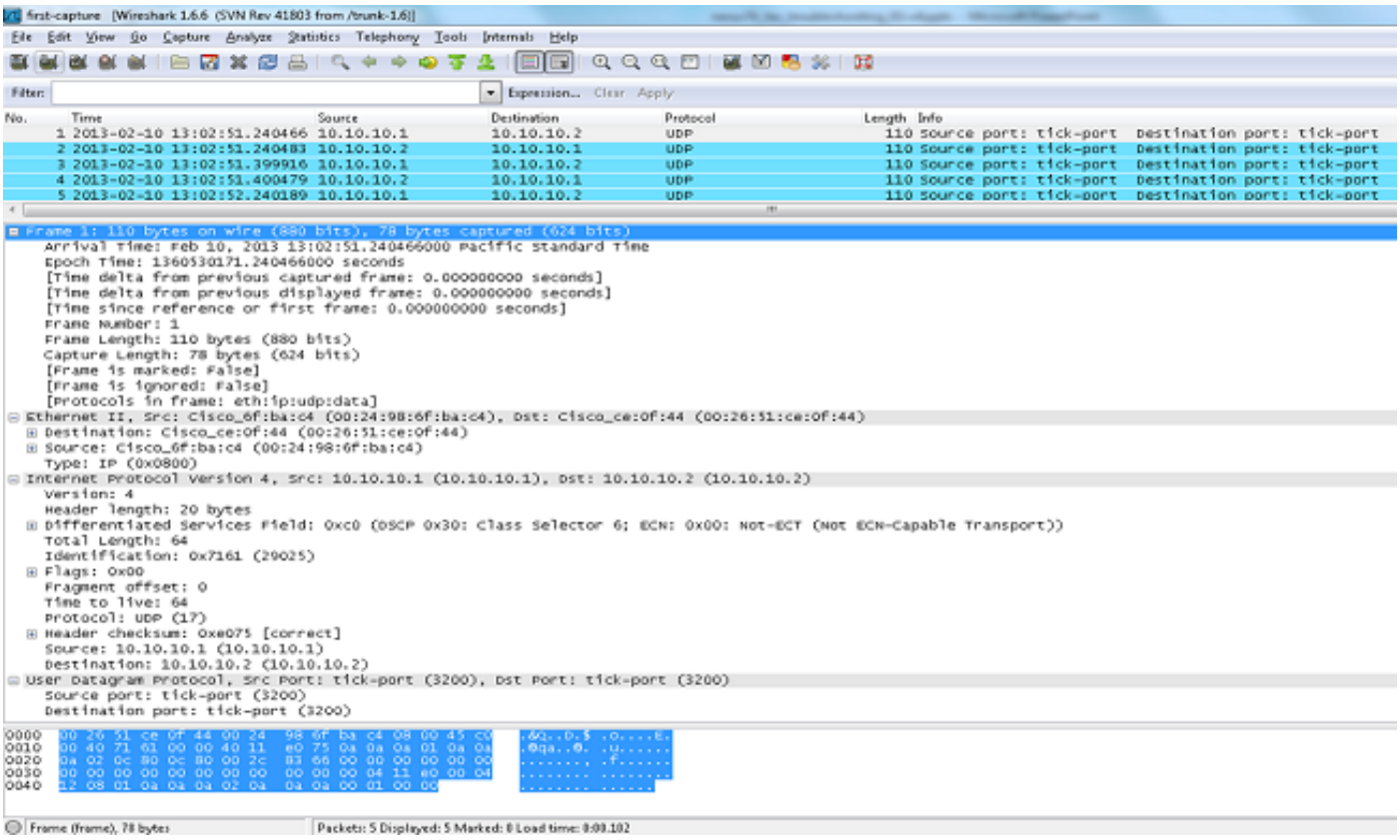
L'option de lecture vous permet de lire le fichier enregistré sur le périphérique lui-même.

```
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 à l'aide de Wireshark ou de toute autre application capable de lire des fichiers 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.
```



Décodage interne avec option de détail

L'option decode-internal fournit des informations internes sur la façon dont le Nexus 7000 transfère le paquet. Ces informations vous aident à comprendre et à dépanner le flux de paquets à travers le processeur.

```
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 utilisez la commande show system internal pixm info ltl x afin de mapper l'index LTL (Local Target Logic) à une interface physique ou logique.

Exemples de valeurs Capture-Filter

Capturer le trafic vers ou depuis un hôte IP

```
host 10.1.1.1
```

Capturer le trafic en provenance ou à destination d'une plage d'adresses IP

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

Capturer le trafic d’une plage d’adresses IP

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

Capturer le trafic vers une plage d'adresses IP

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

Capture du trafic uniquement sur un certain protocole - Capture du trafic DNS uniquement

DNS est le protocole DNS.

```
port 53
```

Capture du trafic uniquement sur un certain protocole - Capture du trafic DHCP

uniquement

DHCP est le protocole DHCP (Dynamic Host Configuration Protocol).

```
port 67 or port 68
```

Capturer le trafic ne se trouvant pas sur un certain protocole - Exclure le trafic HTTP ou SMTP

SMTP est le protocole SMTP (Simple Mail Transfer Protocol).

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

Capturer le trafic ne se trouvant pas sur un certain protocole - Exclure le trafic ARP et DNS

ARP est le protocole de résolution d'adresse.

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

Capture uniquement le trafic IP : excluez les protocoles de couche inférieure tels que ARP et STP

STP est le protocole Spanning Tree.

```
ip
```

Capturer uniquement le trafic de monodiffusion - Exclure les annonces de diffusion et de multidiffusion

```
not broadcast and not multicast
```

Capturer le trafic dans une plage de ports de couche 4

```
tcp portrange 1501-1549
```

Capturer le trafic en fonction du type Ethernet - Capturer le trafic EAPOL

EAPOL est le protocole d'authentification extensible sur LAN.

```
ether proto 0x888e
```

Solution de contournement de capture IPv6

```
ether proto 0x86dd
```

Capturer le trafic en fonction du type de protocole IP

```
ip proto 89
```

Refuser les trames Ethernet en fonction de l'adresse MAC : exclure le trafic appartenant au groupe de multidiffusion LLDP

LLDP est le protocole de découverte de la couche liaison.

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

Capturer le trafic UDLD, VTP ou CDP

UDLD est la détection de liaison unidirectionnelle, VTP est le protocole d'agrégation VLAN et CDP est le protocole de découverte Cisco.

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

Capturer le trafic vers ou depuis une adresse MAC

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

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

Protocoles de plan de contrôle communs

- UDLD : DMAC (Destination Media Access Controller) = 01-00-0C-CC-CC et EthType = 0x0111
- LACP : DMAC = 01:80:C2:00:00:02 et EthType = 0x809. LACP est l'acronyme de Link Aggregation Control Protocol.
- STP : DMAC = 01:80:C2:00:00:00 et EthType = 0x4242 - ou - DMAC = 01:00:0C:CC:CD et EthType = 0x010B
- CDP : DMAC = 01-00-0C-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 = 0x88E. DOT1X signifie IEEE 802.1x.
- IPv6 : EthType = 0x86DD
- Liste des numéros de port UDP et TCP

Problèmes identifiés

Bogue Cisco ayant l'ID CSCue4854 : le filtre de capture d'Ethanalyzer ne capture pas le trafic provenant du CPU sur SUP2.

ID de bogue Cisco CSCtx79409 : impossible d'utiliser le filtre de capture avec decode-internal.

ID de bogue Cisco CSCvi02546 : le paquet généré par SUP3 peut avoir FCS, ce comportement est attendu.

Informations connexes

- Wireshark : CaptureFilters
- Wireshark : filtres d'affichage
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.