

# Ethalyzer на руководстве по поиску и устранению проблем Nexus 7000

## Содержание

[Введение](#)

[Выходные параметры](#)

[Параметры фильтрации](#)

[фильтр перехвата](#)

[фильтр дисплейного отображения](#)

[Опции Write](#)

[write](#)

[кольцевой буфер перехвата](#)

[Считайте опции](#)

[декодируйте - внутренний с Подробной Опцией](#)

[Примеры Значений фильтра перехвата](#)

[Трафик перехвата к или от IP-узла](#)

[Трафик перехвата к или из диапазона IP-адресов](#)

[Трафик перехвата из диапазона IP-адресов](#)

[Трафик перехвата к диапазону IP-адресов](#)

[Трафик перехвата только на определенном протоколе - перехватывает только трафик DNS](#)

[Трафик перехвата только на определенном протоколе - перехватывает только трафик DHCP](#)

[Трафик перехвата не на определенном протоколе - исключает трафик HTTP или трафик SMTP](#)

[Трафик перехвата не на определенном протоколе - исключает трафик DNS и ARP](#)

[Перехватите Только IP - трафик - Исключают Протоколы нижнего уровня как ARP и STP](#)

[Перехватите только трафик с конкретным адресом - исключают объявления широковещания и групповой адресации](#)

[Трафик перехвата в диапазоне портов уровня 4](#)

[Трафик перехвата На основе Типа ethernet - Трафик EAPOL Перехвата](#)

[Обходной путь перехвата IPv6](#)

[Трафик перехвата на основе типа IP - протокола](#)

[Фреймы Ethernet отклонения на основе MAC-адреса - исключают трафик, который принадлежит группе многоадресной рассылки LLDP](#)

[UDLD перехвата, VTP или трафик CDP](#)

[Трафик перехвата к или от MAC-адреса](#)

[Протоколы плоскости обычного управления](#)

[Типичные ошибки](#)

[Дополнительные сведения](#)

## Введение

Этот документ описывает Ethalyzer, Cisco NX-OS интегрировал программное средство

захвата пакета для управляющих пакетов, основанных на Wireshark.

Wireshark является открытым исходным кодом, сетевой протокол анализатор, широко используемый через многие отрасли и образовательные учреждения. Это декодирует пакеты, перехваченные libpcap, библиотекой захвата пакета. Cisco NX-OS выполняется поверх Ядра Linux, которое пользуется libpcap библиотекой для поддержки захвата пакета.

С Ethalyzer вы можете:

- Пакеты перехвата, переданные или полученные Супервизором.
- Определите номер пакетов, которые будут перехвачены.
- Заставьте длину пакетов быть перехваченной.
- Пакеты показа с информацией об итоговом или подробном протоколе.
- Откройте и сохраните перехваченные данные пакета.
- Пакеты фильтра перехвачены на многих критериях.
- Пакеты фильтра, которые будут отображены на многих критериях.
- Декодируйте внутренние 7000 заголовков управляющего пакета.

Ethalyzer не может:

- Предупредите вас, когда ваша сеть испытывает проблемы. Однако Ethalyzer мог бы помочь вам определять причину проблемы.
- Перехватите трафик плоскости данных, который передан в аппаратных средствах.
- Поддержите интерфейсно-специфичный перехват.

## Выходные параметры

Это - итоговое представление выходных данных от **ethalyzer local interface** **внутриполосная** команда. '?' опция отображает справку.

```

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

```

Используйте 'подробную' опцию для получения информации о подробном протоколе. ^C может использоваться, чтобы прерваться и вернуть приглашение коммутатора посреди перехвата при необходимости.

```

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:igrp]
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/broadcast)
  .... ..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-----

```

## Параметры фильтрации

### фильтр перехвата

Используйте опцию 'фильтра перехвата' для выбора который пакеты отобразить или сохранить на диск во время перехвата. Фильтр перехвата поддерживает высокую скорость перехвата, в то время как это фильтрует. Поскольку полное рассечение не было сделано на пакетах, поля фильтра predeterminedены и ограничены.

### фильтр дисплейного отображения

Используйте опцию 'фильтра дисплейного отображения' для изменения представления перехвата файла (файл tnr). Фильтр дисплейного отображения использует полностью разделенные пакеты, таким образом, можно сделать очень сложную и усовершенствованную фильтрацию при анализе сетевого файла трассировки. Однако файл tnr может заполниться быстро, так как он сначала перехватывает все пакеты и затем отображает только необходимые пакеты.

В данном примере 'limit-captured-frames' установлен в 5. С опцией 'фильтра перехвата' Ethalyzer показывает вам пять пакетов, которые совпадают с фильтром 'хост 10.10.10.2'.

С опцией 'фильтра дисплейного отображения' Ethalyzer сначала перехватывает пять пакетов, тогда отображает только пакеты, которые совпадают с фильтром 'ip.addr == 10.10.10.2'.

```
DC# ethalyzer 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# ethalyzer 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
```

## Опции Write

### write

Опция 'записи' позволяет вам записать данные перехвата в файл в одном из устройств хранения (таких как bootflash или logflash) на коммутаторе Cisco Nexus серии 7000 для последующего анализа. Размер перехвата файла ограничен 10 МБ.

Команда Ethalyzer в качестве примера с опцией 'записи' является **ethalyzer local interface внутриволновая запись bootflash:capture\_file\_name**. Пример опции 'записи' с 'фильтром перехвата' и названием выходного файла 'первого перехвата':

```
DC# ethalyzer 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# ethalyzer local interface inband capture-filter "host 10.10.10.2" limit-captured-frames 5 write
bootflash:first-capture
```

Когда данные перехвата сохранены в файл, захваченные пакеты, по умолчанию, не отображены в окне терминала. Опция 'показа' вынуждает Cisco NX-OS отобразить пакеты, в то время как это сохраняет данные перехвата в файл.

### кольцевой буфер перехвата

'Кольцевая буферная перехватом' опция создает множественные файлы после заданного номера секунд, заданного номера файлов или указанного размера файла. Определения тех опций находятся в этом снимке экрана:

```
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
```

## Считайте опции

Опция 'чтения' позволяет вам считать сохраненный файл на самом устройстве.

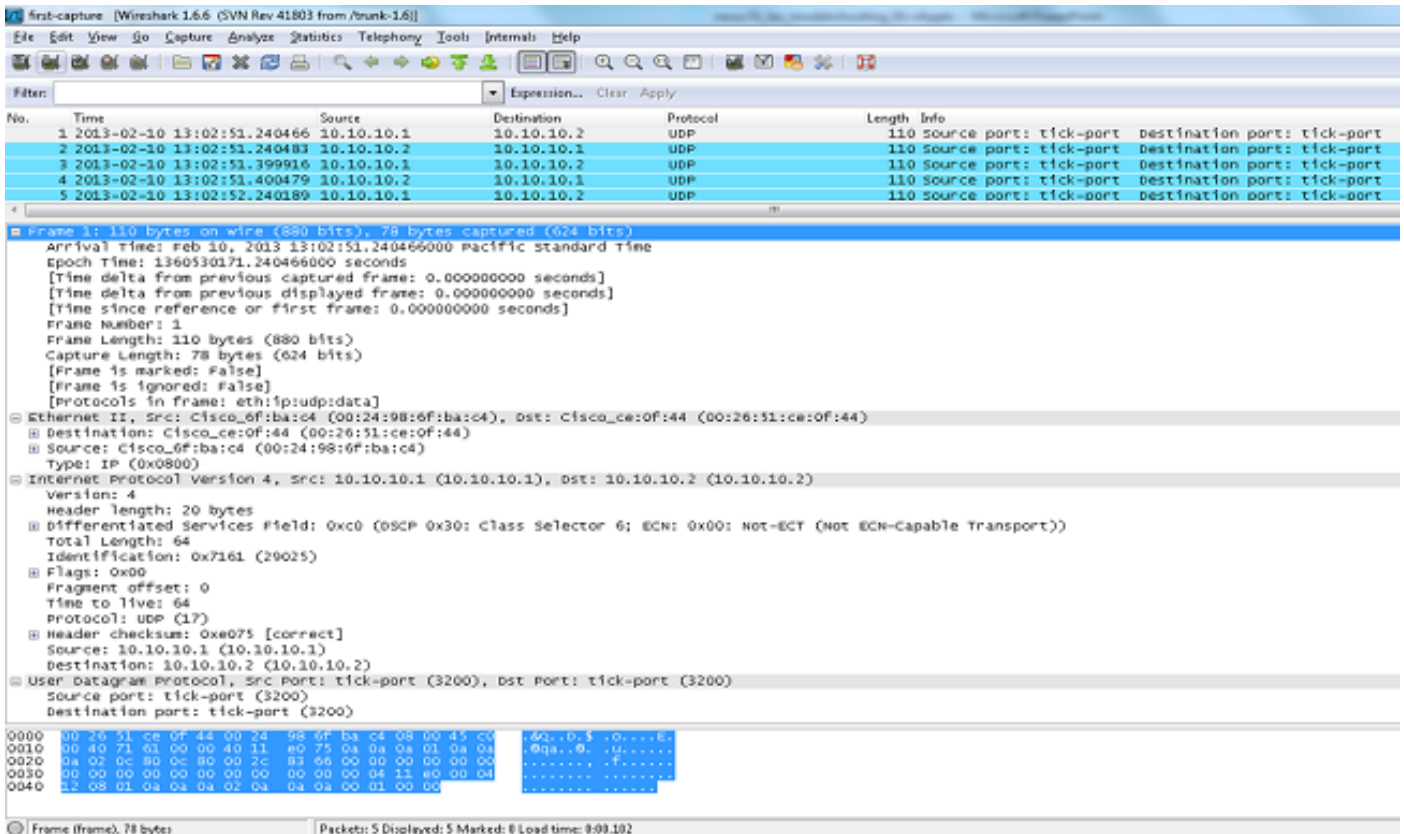
```
DC# ethanalyzer local read bootflash:first-capture
2013-02-10 13:02:51.240466 10.10.10.1 -> 10.10.10.2 UDP Source port: 3200 Destination port: 3200
2013-02-10 13:02:51.240483 10.10.10.2 -> 10.10.10.1 UDP Source port: 3200 Destination port: 3200
2013-02-10 13:02:51.399916 10.10.10.1 -> 10.10.10.2 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-----
```

Можно также передать файл серверу или ПК и считать его с Wireshark или любым другим приложением, которое может считать колпачок или pcap файлы.

```
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.
```





## декодируйте - внутренний с Подробной Опцией

'Декодируют - внутренняя' внутренняя информация отчётов об опции о том, как Nexus 7000 передает пакет. Эта информация помогает вам понимать и устранять неполадки потока пакетов через ЦП.

```

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=SVP 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-----

```

Преобразуйте индекс NX-OS в шестнадцатеричный, затем используйте **show system внутренняя pixm** информация ltl x команда для сопоставления индекса логики локальной

цели (LTL) с медосмотром или логическим интерфейсом.

## Примеры Значений фильтра перехвата

### Трафик перехвата к или от IP-узла

```
host 1.1.1.1
```

### Трафик перехвата к или из диапазона IP-адресов

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

### Трафик перехвата из диапазона IP-адресов

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

### Трафик перехвата к диапазону IP-адресов

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

### Трафик перехвата только на определенном протоколе - перехватывает только трафик DNS

DNS является Протоколом Системы доменных имен.

```
port 53
```

### Трафик перехвата только на определенном протоколе - перехватывает только трафик DHCP

DHCP является протоколом динамической конфигурации хоста.

```
port 67 or port 68
```

### Трафик перехвата не на определенном протоколе - исключает трафик HTTP или трафик SMTP

SMTP является Простой протокол передачи почты.

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

### Трафик перехвата не на определенном протоколе - исключает трафик DNS и ARP

ARP является протоколом разрешения адресов.

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

### Перехватите Только IP - трафик - Исключают Протоколы нижнего уровня как ARP и STP

STP является Протокол STP.



ip

**Перехватите только трафик с конкретным адресом - исключают объявления широковещания и групповой адресации**

not broadcast and not multicast

**Трафик перехвата в диапазоне портов уровня 4**

tcp portrange 1501-1549

**Трафик перехвата На основе Типа ethernet - Трафик EAPOL Перехвата**

EAPOL является Расширяемый протокол аутентификации по LAN.

ether proto 0x888e

**Обходной путь перехвата IPv6**

ether proto 0x86dd

**Трафик перехвата на основе типа IP - протокола**

ip proto 89

**Фреймы Ethernet отклонения на основе MAC-адреса - исключают трафик, который принадлежит группе многоадресной рассылки LLDP**

LLDP является Протоколом обнаружения Уровня соединения.

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

**UDLD перехвата, VTP или трафик CDP**

UDLD является Поддержка соединений с однонаправленным обменом, VTP является Протокол магистральных каналов VLAN, и CDP является протоколом обнаружения Cisco.

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

**Трафик перехвата к или от MAC-адреса**

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

**Примечание:**

и = &&

или = ||

не = !

Формат MAC-адреса : xx:xx:xx:xx:xx:xx

**Протоколы плоскости обычного управления**

- UDLD: Контроллер доступа интерфейса назначения (DMAC) = 01-00-0C-CC-CC-CC и EthType = 0x0111
- LACP: DMAC = 01:80:C2:00:00:02 и EthType = 0x8809. LACP обозначает Протокол управления агрегацией каналов.
- STP: DMAC = 01:80:C2:00:00:00 и EthType = 0x4242 - или - DMAC = 01:00:0C:CC:CC:CD и EthType = 0x010B
- CDP: DMAC = 01-00-0C-CC-CC-CC и EthType = 0x2000

- LLDP: DMAC = 01:80:C2:00:00:0E или 01:80:C2:00:00:03 или 01:80:C2:00:00:00 и EthType = 0x88CC
- DOT1X: DMAC = 01:80:C2:00:00:03 и EthType = 0x888E. DOT1X обозначает IEEE 802.1x.
- IPv6: EthType = 0x86DD
- [Список UDP и номеров порта TCP](#)

## Типичные ошибки

Посмотрите идентификатор ошибки Cisco [CSCue48854](#): фильтр перехвата Ethalyzer не перехватывает трафик от ЦП на SUP2. Также посмотрите идентификатор ошибки Cisco [CSCtx79409](#): не Может использовать фильтр перехвата с декодированием - внутренний.

## Дополнительные сведения

- [Wireshark: CaptureFilters](#)
- [Wireshark: DisplayFilters](#)
- [Cisco Systems – техническая поддержка и документация](#)