Содержание

Введение

Этот документ описывает использование команды CLI **tcpdump** для получения необходимых пакетов от сервера Главной инфраструктуры (PI) Cisco.

Используйте Команду tcpdump

Этот раздел предоставляет примеры, которые иллюстрируют путь, которым используется **команда tcpdump**.

```
nms-pi/admin# tech dumptcp ?
<0-3> Gigabit Ethernet interface number
```

Выходные данные **команды show interface** предоставляют точную информацию об имени интерфейса и номере, который используется в настоящее время.

```
nms-pi/admin# tech dumptcp 0 ?
count Specify a max package count, default is continuous (no limit)
<cr> Carriage return.
```

> **Примечание:** Банка можно указать на определенное количество пакета в предыдущей команде. Если вы не указываете на определенное количество пакета, непрерывный перехват выполнен без предела.

```
nms-pi/admin# tech dumptcp 0 | ?
Output modifier commands:
begin Begin with line that matches
count Count the number of lines in the output
end End with line that matches
exclude Exclude lines that match
include Include lines that match
last Display last few lines of the outputnms-pi/admin# tech dumptcp 0 > test-capture.pcap
```

> **Примечание:** Является самым легким сохранить файл, и затем рассмотреть его. В данном примере сервер сохранил файл в root структуры каталогов. Для просмотра файлов введите **команду dir**.

Скопируйте перехваченные файлы к внешнему местоположению

Вот два примера, которые иллюстрируют способ, которым перехваченные файлы

скопированы к местоположению, которое является за пределами сервера:

- В данном примере перехват файла скопирован к серверу FTP с IP-адресом **1.2.3.4**:
  `copy disk:/test-capture.pcap ftp://1.2.3.4/`
- В данном примере перехват файла скопирован к серверу TFTP с IP-адресом **5.6.7.8**:
  `copy disk:/test-capture.pcap tftp://5.6.7.8/`

Пакеты перехвата как пользователь маршрута

Если вы желаете больших гранулированных перехватов, входите в CLI как *пользователь маршрута* после регистрации как *пользователь с правами администратора*.

```
test$ ssh admin@12.13.14.15
Password:
nms-pi/admin#
nms-pi/admin# root
Enter root password :
Starting root bash shell ...
ade # su -
[root@nms-pi~]#
```

Перехваты пользователя маршрута в качестве примера

Вот три примера перехватов, которые взяты пользователем маршрута:

- В данном примере перехвачены все пакеты, которые предназначены к **порту 162** на сервере PI:
  `[root@nms-pi~]# tcpdump -i eth0 -s0 -n dst port 162`
- В данном примере все пакеты, которые предназначены к **порту 9991**, перехвачены и записаны в файл, названный **test.pcap** в**/localdisk/ftp/**каталоге:
  `[root@nms-pi~]# tcpdump -w /localdisk/ftp/test.pcap -s0 -n dst port 9991`
- В данном примере перехвачены любые пакеты с IP - адресом источника **1.1.1.1**:
  `[root@nms-pi~]# tcpdump -n src host 1.1.1.1`