Телекоммуникационные системы и технологии

Лабораторная работа №3

Мониторинг сетевого трафика на хосте на примере работы с утилитами диагностики и мониторинга сетевых соединений в Linux

Выполнил: Птицын Владислав
Группа: М3301
Преподаватель: Береснев А.Д.

Санкт-Петербург, 2024

Цель работы: получить практические навыки по работе с анализаторами сетевого трафика. На практике ознакомиться с различиями в принципах работы активного сетевого оборудования. Уяснить особенности взаимодействия сетевого и канального уровней на примере стека TCP/IP. Выяснить отличия форматов кадров Ethernet. Познакомиться с консольными утилитами диагностики и анализа сетевых соединений.

Часть 2

На машине c7-2 напишите команду ping, которая (!) интервалом 10 секунд отправляет 5 пакетов размером 1500 байт на машину c7-1

```
ping -i 10 -c 5 -s 1500 10.0.2.6 > 21.text
```

```
PING 10.0.2.6 (10.0.2.6) 1500(1528) bytes of data.
1508 bytes from 10.0.2.6: icmp_seq=1 ttl=64 time=0.037 ms
1508 bytes from 10.0.2.6: icmp_seq=2 ttl=64 time=0.047 ms
1508 bytes from 10.0.2.6: icmp_seq=3 ttl=64 time=0.077 ms
1508 bytes from 10.0.2.6: icmp_seq=4 ttl=64 time=0.093 ms
1508 bytes from 10.0.2.6: icmp_seq=5 ttl=64 time=0.080 ms

--- 10.0.2.6 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 40843ms
rtt min/avg/max/mdev = 0.037/0.066/0.093/0.021 ms
```

Напишите команду, которая сохранит в файл расширенную статистику работы mtr при отправке 40 пакетов (!).

```
mtr -c 40 -w www.itmo.ru > 2.text
```

```
Start: 2024-10-02T15:07:26+0300
HOST: d12                          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- 10.0.2.1                    0.0%    40    0.2   0.7   0.1   1.8   0.3
  2.|-- 172.28.16.1                 2.5%    40    3.2  14.3   2.0 183.0  34.8
  3.|-- 77.234.199.66                0.0%    40    4.8  27.3   3.2 538.3  88.0
  4.|-- 87.248.228.102.pool.sknt.ru  0.0%    40   11.4  23.2   3.7 479.1  76.2
  5.|-- yacloud.spb.piter-ix.net     0.0%    40   50.0  26.8  11.7 427.9  65.4
  6.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
  7.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
  8.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
  9.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
 10.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
 11.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
 12.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
 13.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
 14.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
 15.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
 16.|-- ???                        100.0    40    0.0   0.0   0.0   0.0   0.0
 17.|-- 51.250.54.78                2.5%    40   21.3  33.8  19.9 318.2  49.9
```

Часть 3

Узел с максимальной активностью (по объему переданных данных)

Address A	Address B	Packets	Bytes
dc:21:48:50:29:68	c4:ad:34:22:f3:7e	62,556	61 MB
d0:37:45:67:ce:28	dc:21:48:50:29:68	1,942	2 MB
42:73:0b:42:dc:74	dc:21:48:50:29:68	1,833	2 MB

Используя инструментарий статистики, определите Узел, осуществивший наибольшее количество широковещательных рассылок

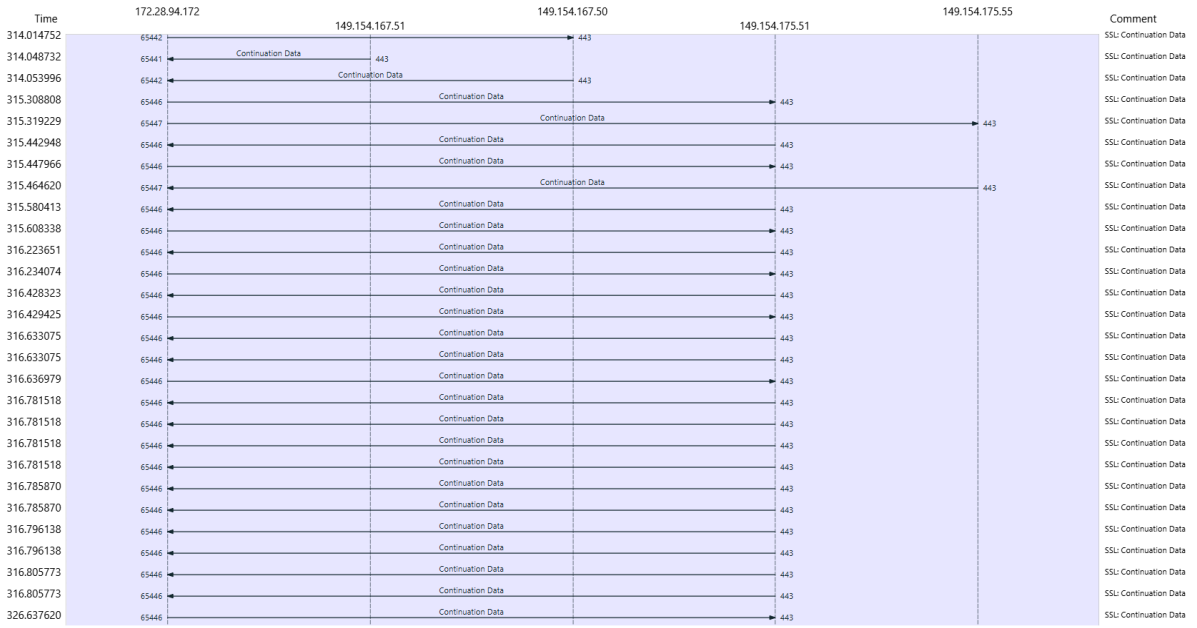
Address A	Address B	Packets	Bytes	Stream ID	Total Packets
c4:ad:34:22:f3:7e	ff:ff:ff:ff:ff:ff	2,876	161 kB	9	2,876
d2:b6:13:81:38:43	ff:ff:ff:ff:ff:ff	154	9 kB	67	154

Самый активный TCP-порт на хосте (по количеству переданных пакетов)

Address A	Port A	Address B	Port B	Packets
172.28.94.172	50169	199.232.42.172	80	5,180

Постройте на одной координатной сетке постройте графики интенсивности TCP и UDP трафика (пункт Io Graphs)

Постройте диаграмму связей только для пакетов, содержащих сообщения протокола HTTPS (пункт Flow Graph)




```
Отбирающие сообщения протокола DNS (53 порт udp и tcp) относящиеся только к взаимодействию DNS клиента на хосте и внешних серверов.
((ip.dst == 192.168.1.41) && (_ws.col.info matches "Standard query response*")) || ((ip.dst == 192.168.1.1) && (_ws.col.info matches "Standard query 0x*"))

Все кадры Ethernet, отправленные с сетевого интерфейса хоста
(arp or icmp) && ip.host

Напишите фильтр, отбирающий только широковещательные сообщения. Определите
назначение 3-х широковещательных рассылок разных протоколов (или тех, которые удалось
обнаружить).
eth.dst == ff:ff:ff:ff:ff:ff
```

Определите назначение 3-х широковещательных рассылок разных протоколов

Arp

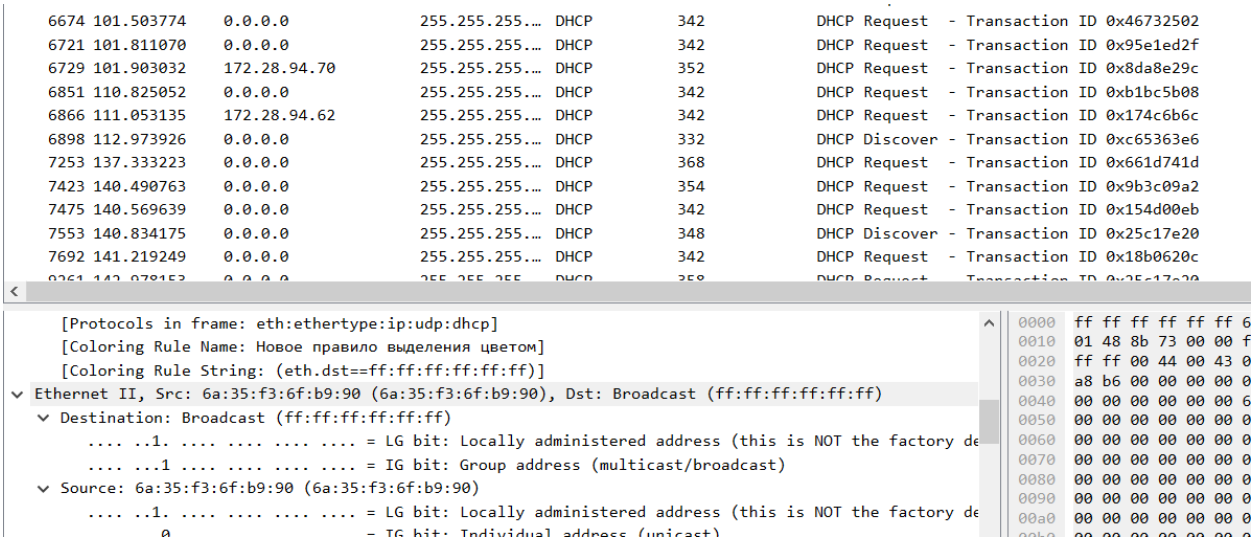
3518	54.846106	0.0.0.0	255.255.255.…	DHCP	338	DHCP Request - Transaction ID 0xce759108
3519	54.860046	Routerboardc_22:f3:…	Broadcast	ARP	56	Who has 172.28.93.0? Tell 172.28.64.1
3520	54.870969	Routerboardc_22:f3:…	Broadcast	ARP	56	Who has 172.28.100.166? Tell 172.28.64.1
3521	54.870969	Routerboardc_22:f3:…	Broadcast	ARP	56	Who has 172.28.85.209? Tell 172.28.64.1
3523	54.871575	172.28.93.235	172.28.127.2…	DTLS	445	Continuation Data

```
Encapsulation type: Ethernet (1)
Arrival Time: Oct 10, 2024 08:56:45.715688000 RTZ 2 (зима)
```

```
0000  ff ff ff ff ff ff
0010  08 00 06 04 00 01
```

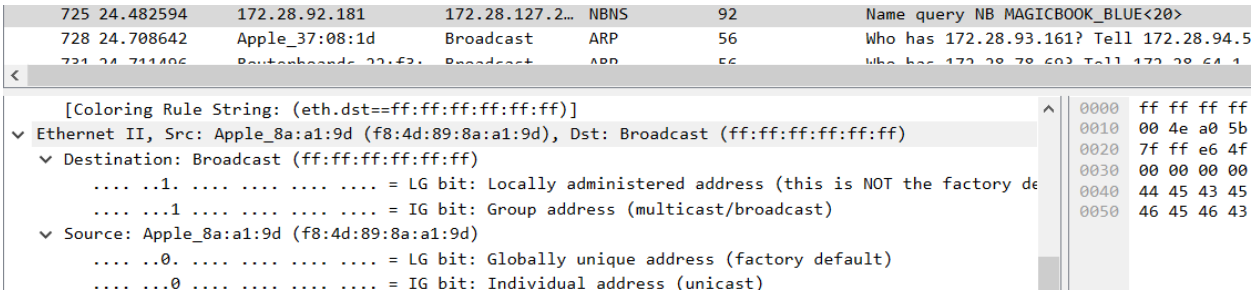
ARP – мапим ip адреса на mac

DHCP



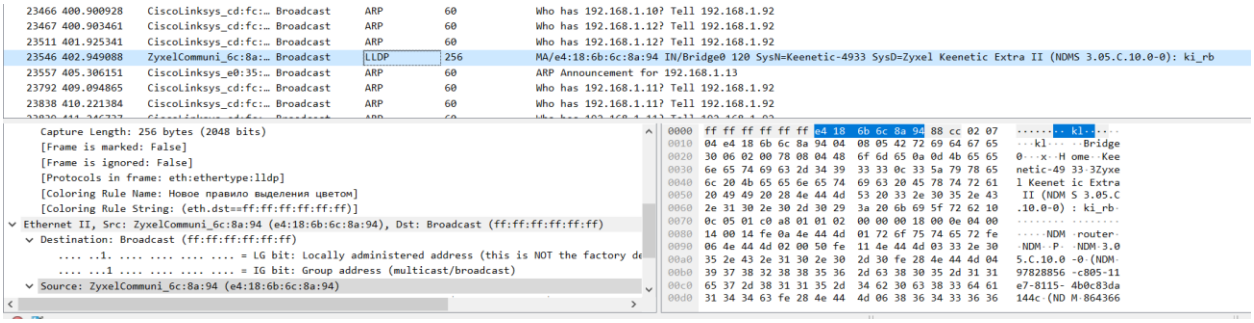
DHCP – получаем конфигурацию
Discover – обнаруживаем dhcp серверы
Offer – получаем предложение конфигурации со всех dhcp
Request – выбираем 1 dhcp сервер
Acknowledgement – получаем подтверждение с выбранного

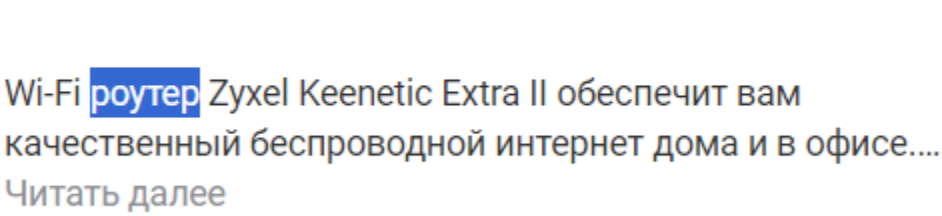
NBNS



NBNS – разрешаем имена как DNS но внутри локалки

На основании анализа адресов отправителя и получателя в перехваченных пакетах, их вида и распределения, определите к какому типу коммутационного оборудования подключен используемый компьютер (концентратор, коммутатор или маршрутизатор).





Часть 4

На машине c7-1 напишите команды traceroute, которые (!): определяют маршрут до хоста 8.8.8.8 с помощью ICMP, UDP, TCP, а также позволяют определить используется ли по маршруту фрагментация IPv4

```
traceroute -I 8.8.8.8
traceroute -U 8.8.8.8
traceroute -T 8.8.8.8
traceroute -I 8.8.8.8
traceroute -I 8.8.8.8 -F
```

Часть 5

На хосте c7-1 последовательно с помощью утилиты bmon или ее аналогов получите данные о загрузке интерфейса, на который отправляет трафик хост c7-2

Скрипт на c7-2

```
ping -f 10.0.2.5
```

Скрипт на c7-1

```
bmon -p enp0s3 -o ascii >> 5.text
```

Форматирование файла на c7-1

```
cat 5.text | sed '/Interf/d' > 52.text
cat 52.text > 5.text
rm 52.text
```

```
enp0s3                                0          0                0          0
enp0s3                           63.45KiB      662           63.45KiB      662
enp0s3                          269.21KiB     2.81K          269.21KiB     2.81K
enp0s3                          309.99KiB     3.24K          309.99KiB     3.24K
enp0s3                          337.84KiB     3.53K          337.84KiB     3.53K
enp0s3                          329.80KiB     3.45K          329.73KiB     3.44K
enp0s3                          340.03KiB     3.55K          340.01KiB     3.55K
enp0s3                          335.43KiB     3.50K          335.50KiB     3.50K
enp0s3                          331.76KiB     3.47K          331.78KiB     3.47K
enp0s3                          327.11KiB     3.42K          327.04KiB     3.42K
enp0s3                          332.25KiB     3.47K          332.30KiB     3.47K
enp0s3                          338.78KiB     3.54K          338.80KiB     3.54K
enp0s3                          341.55KiB     3.57K          341.48KiB     3.57K
enp0s3                          344.66KiB     3.60K          344.65KiB     3.60K
enp0s3                          344.66KiB     3.60K          343.98KiB     3.59K
enp0s3                          347.24KiB     3.63K          347.07KiB     3.63K
enp0s3                          343.18KiB     3.58K          343.14KiB     3.58K
enp0s3                          331.28KiB     3.46K          331.34KiB     3.46K
enp0s3                          343.77KiB     3.59K          343.78KiB     3.59K
enp0s3                          338.48KiB     3.54K          338.49KiB     3.54K
enp0s3                          342.39KiB     3.58K          342.39KiB     3.58K
enp0s3                          346.30KiB     3.62K          346.30KiB     3.62K
enp0s3                          344.31KiB     3.60K          344.24KiB     3.60K
```

Изменяйте размер пакета, передаваемой утилитой ping пакета от 100 до 60100 с шагом 10000. Определите, как меняется загрузка на сетевом интерфейсе

```
i=100
while [[ $i -lt 60100 ]];
do
    let i=$i+10000
    timeout 5s ping -f 10.0.2.5 -s "$i"
done
```

```
enp0s3                                  0          0                0          0
enp0s3                                  0          0                0          0
enp0s3                           13.96MiB     9.90K          13.96MiB     9.90K
enp0s3                           14.83MiB    10.52K          14.83MiB    10.52K
enp0s3                           15.37MiB    10.90K          15.36MiB    10.90K
enp0s3                           15.50MiB    11.00K          15.50MiB    11.00K
enp0s3                           15.91MiB    11.28K          15.91MiB    11.28K
enp0s3                           19.29MiB    13.74K          19.28MiB    13.73K
enp0s3                           20.32MiB    14.49K          20.33MiB    14.49K
enp0s3                           20.40MiB    14.55K          20.39MiB    14.54K
enp0s3                           20.74MiB    14.79K          20.74MiB    14.79K
enp0s3                           20.14MiB    14.36K          20.14MiB    14.36K
enp0s3                           22.80MiB    16.28K          22.79MiB    16.28K
enp0s3                           23.79MiB    17.00K          23.81MiB    17.01K
enp0s3                           24.50MiB    17.50K          24.49MiB    17.50K
enp0s3                           23.86MiB    17.04K          23.85MiB    17.04K
enp0s3                           23.83MiB    17.03K          23.84MiB    17.03K
enp0s3                           25.91MiB    18.52K          25.89MiB    18.51K
enp0s3                           27.59MiB    19.73K          27.61MiB    19.74K
enp0s3                           27.74MiB    19.83K          27.72MiB    19.82K
enp0s3                           26.87MiB    19.21K          26.87MiB    19.21K
enp0s3                           26.87MiB    19.21K          26.87MiB    19.21K
enp0s3                           26.17MiB    18.37K          26.20MiB    18.39K
enp0s3                           26.71MiB    18.62K          26.68MiB    18.59K
enp0s3                           26.02MiB    18.11K          26.04MiB    18.12K
enp0s3                           26.93MiB    18.73K          26.94MiB    18.74K
enp0s3                           26.64MiB    18.53K          26.62MiB    18.51K
enp0s3                           27.66MiB    19.30K          27.64MiB    19.29K
enp0s3                           27.39MiB    19.14K          27.40MiB    19.14K
enp0s3                           28.72MiB    20.07K          28.75MiB    20.09K
enp0s3                           28.84MiB    20.16K          28.85MiB    20.17K
enp0s3                           28.53MiB    19.94K          28.48MiB    19.91K
enp0s3                            9.64MiB     6.74K           9.67MiB     6.76K
enp0s3                            2.41MiB     1.68K           2.42MiB     1.69K
enp0s3                          616.90KiB      421         619.04KiB      422
```

Часть 6

```
vnstat -i enp0s3 -l >> 6.text
```

```
Database updated: 2024-10-13 22:10:00

   enp0s3 since 2024-10-13

          rx:  51,86 KiB      tx:  48,74 KiB      total:  100,60 KiB

   monthly
                     rx      |     tx      |    total    |   avg. rate
     ------------------------+-------------+-------------+---------------
       2024-10     51,86 KiB |   48,74 KiB |  100,60 KiB |    3,10 kbit/s
     ------------------------+-------------+-------------+---------------
     estimated    296,45 MiB |  278,57 MiB |  575,03 MiB |

   daily
                     rx      |     tx      |    total    |   avg. rate
     ------------------------+-------------+-------------+---------------
       today      51,86 KiB |   48,74 KiB |  100,60 KiB |    3,10 kbit/s
     ------------------------+-------------+-------------+---------------
     estimated        55 KiB |      52 KiB |     107 KiB |
```

Часть 7

Используя утилиту netstat или lsof на c7-1 вывести все активные (прослушиваемые) порты

```
netstat -ltun
```

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp6       0      0 :::22                   :::*                    LISTEN
```

Используя утилиту netstat или ss все установленные соединения

```
ss -ntl
```

```
State Recv-Q Send-Q Local Address:Port Peer Address:Port Process
ESTAB 0      0          10.0.2.5:ssh      10.0.2.7:41964
ESTAB 0      0          10.0.2.5:ssh      10.0.2.7:45946
ESTAB 0      0          10.0.2.5:ssh      10.0.2.7:57448
```

Напишите скрипт, которой выводит список IP-адресов и количество подключений с них к нашему хосту через порт, задаваемый параметрами скрипта (значение по умолчанию 22). Список упорядочить по количеству соединений с IP адреса

```
temp="$1"
if [[ "$temp" == "" ]]; then
    temp=22
fi
ss -nt | tr ':' ' ' | awk -v var="$temp" '{ if ($5 == var) print $6}' | sort | uniq -c
```

```
  1 10.0.2.15
  1 10.0.2.2
  3 10.0.2.7
```

На хосте c7-1 с помощью утилиты nethogs определите: Среднюю скорость передачи данных до sshd и PID процесса sshd.

```
timeout 5s nethogs -t | tail -3 > temp.txt
echo -e pid "\t\t" send "\t\t" recieved
cat temp.txt | tr "\/" " " | grep sshd | awk '{print $4, "\t\t", $6, "\t", $7}'
```

```
pid             send        recieved
2711            2.40352     0.445312
```

Часть 8

На машине c7-1 на отдельной консоли запустите tcpdump для сбора всего трафика с портов 9999 и 4444, так, чтобы на консоль выводилось содержимое сообщения, а не только информация из служебных заголовков

```
tcpdump -i any -vv port 9999 or port 4444 -w tcpdumpfile.pcap
```

Используя утилиту nc на обоих машинах передайте текстовый файл с произвольным текстовым содержимым (не мнее 20 слов) принимая файл на порту tcp 9999

```
nc -v 10.0.2.15 9999 < file_for_netcat_test.txt
```

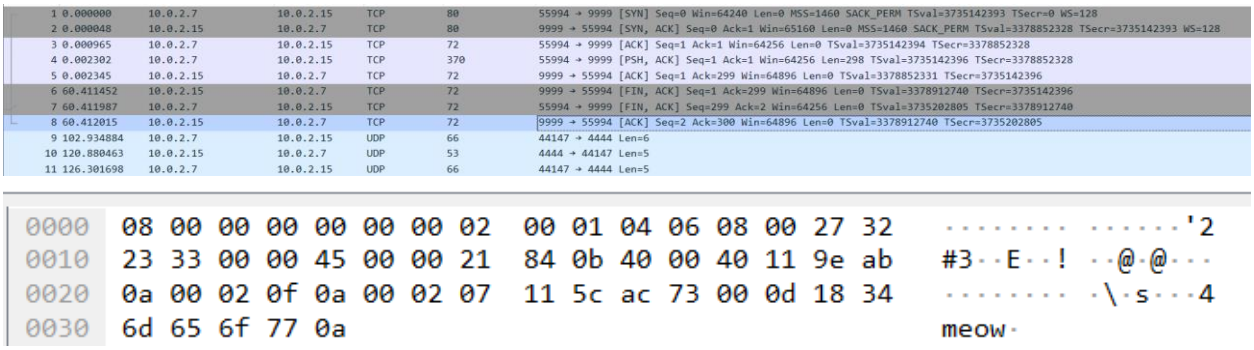
```
nc -lvp 9999 > file_test_for_netcat.txt
```

Используя утилиту nc на обоих машинах организовать текстовый чат между машинами через порт udp 4444.

```
nc -uv 10.0.2.15 4444
```

```
nc -luvp 4444
```

Остановите работу tcpdump, проанализируйте перехваченные сообщения. Какие выводы можно сделать?



1	0.000000	10.0.2.7	10.0.2.15	TCP	80	55994 → 9999 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSval=3735142393 TSecr=0 WS=128
2	0.000048	10.0.2.15	10.0.2.7	TCP	80	9999 → 55994 [SYN, ACK] Seq=0 Ack=1 Win=65160 Len=0 MSS=1460 SACK_PERM TSval=3378852328 TSecr=3735142393 WS=128
3	0.000965	10.0.2.7	10.0.2.15	TCP	72	55994 → 9999 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3735142394 TSecr=3378852328
4	0.002302	10.0.2.7	10.0.2.15	TCP	370	55994 → 9999 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=298 TSval=3735142396 TSecr=3378852328
5	0.002345	10.0.2.15	10.0.2.7	TCP	72	9999 → 55994 [ACK] Seq=1 Ack=299 Win=64896 Len=0 TSval=3378852331 TSecr=3735142396
6	60.411452	10.0.2.15	10.0.2.7	TCP	72	9999 → 55994 [FIN, ACK] Seq=1 Ack=299 Win=64896 Len=0 TSval=3378912740 TSecr=3735142396
7	60.411987	10.0.2.7	10.0.2.15	TCP	72	55994 → 9999 [FIN, ACK] Seq=299 Ack=2 Win=64256 Len=0 TSval=3735202805 TSecr=3378912740
8	60.412015	10.0.2.15	10.0.2.7	TCP	72	9999 → 55994 [ACK] Seq=2 Ack=300 Win=64896 Len=0 TSval=3378912740 TSecr=3735202805
9	102.934884	10.0.2.7	10.0.2.15	UDP	66	44147 → 4444 Len=6
10	120.880463	10.0.2.15	10.0.2.7	UDP	53	4444 → 44147 Len=5
11	126.301698	10.0.2.7	10.0.2.15	UDP	66	44147 → 4444 Len=5

```
0000  08 00 00 00 00 00 00 02  00 01 04 06 08 00 27 32   ........ ......'2
0010  23 33 00 00 45 00 00 21  84 0b 40 00 40 11 9e ab   #3··E··! ··@·@···
0020  0a 00 02 0f 0a 00 02 07  11 5c ac 73 00 0d 18 34   ........ ·\·s···4
0030  6d 65 6f 77 0a                                    meow·
```

Ответы на вопросы и задания

1) По какому протоколу работает утилита mtr? Как это можно определить?

По умолчанию – ICMP, возможна работа с UDP и TCP
Чтобы определить текущий рабочий протокол – можно посмотреть на трафик в tcpdump или Wireshark

2) Опишите значения столбцов статистики, выводимой утилитой mtr. Какие еще статистики доступны в mtr кроме основных?

Host — Имя или IP-адрес узла (хоста) на маршруте.
Loss% — Процент потерянных пакетов.
Snt — Общее количество отправленных пакетов.
Last — Время отклика последнего пакета
Avg — Среднее время отклика
Best — Минимальное время отклика
Wrst — Максимальное время отклика
StDev — Стандартное отклонение времени отклика.

-e – детализация пакетов
-T использовать TCP
-u host:port – трассировка до конкретного порта с UDP
-4 -6 – ipv4 или ipv6
-n – показывать ip адрес
-s – размер пакета
-m – максимальное число переходов

3) Какие типы кадров Ethernet бывают, в чем их отличия?

Формат Ethernet II

Ethernet II является наиболее распространенным и широко поддерживаемым форматом ethernet frame. Он был определен стандартом IEEE 802.3 и также известен как DIX или Ethernet SNAP. Фреймы Ethernet II имеют фиксированный размер заголовка в 14 байт и переменный размер полезной нагрузки до 1500 байт. Заголовок состоит из шести байт для адреса назначения, шести байт для адреса источника и двух байт для поля типа. Поле "Тип" определяет протокол полезной нагрузки, такой как IPv4, IPv6 или ARP.

Формат IEEE 802.3

IEEE 802.3 - это оригинальный формат фрейма Ethernet, который был определен стандартом IEEE 802.3. Он также известен как Ethernet RAW или Ethernet 802.3. Фреймы стандарта IEEE 802.3 имеют фиксированный размер заголовка в 14 байт и переменный размер полезной нагрузки до 1492 байт. Заголовок состоит из шести байт для адреса назначения, шести байт для адреса источника и двух байт для поля длины. В поле длина указывается размер полезной нагрузки в байтах. За полезной нагрузкой следует четырехбайтовый трейлер, содержащий циклическую проверку избыточности (CRC) для обнаружения ошибок.

Формат IEEE 802.2

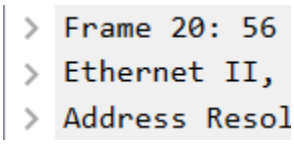
IEEE 802.2 является расширением формата IEEE 802.3, которое добавляет заголовок подуровня к полезной нагрузке. Он был определен стандартом IEEE 802.2 и также известен как Ethernet LLC или Ethernet 802.2. Фреймы стандарта IEEE 802.2 имеют фиксированный размер заголовка в 16 байт и переменный размер полезной нагрузки до 1490 байт. Заголовок состоит из шести байт для адреса назначения, шести байт для адреса источника, двух байт для поля длины, одного байта для точки доступа к службе назначения (DSAP) и одного байта для точки доступа к службе источника (SSAP). Поля DSAP и SSAP указывают на протокол верхнего уровня или службу, использующую фрейм Ethernet, например IPX или NetBIOS.

Формат IEEE 802.2 SNAP

IEEE 802.2 SNAP - это вариация формата IEEE 802.2, которая добавляет к полезной нагрузке трейлер подуровня. Он был определен стандартом IEEE 802.2 и также известен как Ethernet SNAP или Ethernet 802.2 SNAP. Фреймы привязки по стандарту IEEE 802.2 имеют фиксированный размер заголовка в 22 байта и переменный размер полезной нагрузки до 1484 байт. Заголовок состоит из шести байт для адреса назначения, шести байт для адреса источника, двух байт для поля длины, одного байта для DSAP, одного байта для SSAP, двух байт для поля управления и трех байт для

уникального идентификатора организации (OUI). Поле control всегда имеет значение 0x03, что указывает на то, что в кадре используется привязка. Поле OUI указывает поставщика или организацию, которые определяют поле type, которое следует за полем OUI в трейлере. В поле тип указывается протокол полезной нагрузки, такой как IPv4, IPv6 или ARP.

4) Какой тип кадров Ethernet используется в анализируемой сети? Почему именно его применение позволяет сети функционировать?



- Скорость
- Надежность
- Безопасность: Ethernet включает встроенные функции безопасности, включая шифрование и аутентификацию, для защиты данных от несанкционированного доступа.
- Стандартизация
- Масштабируемость
- Низкие накладные расходы

5) Как можно определить тип используемого коммутационного оборудования, используя сетевую статистику?

Захват трафика, анализ кадров и используемых протоколов, таблиц маршрутизации

6) На какие адреса сетевого уровня осуществляются широковещательные рассылки?

255.255.255.255
Или последние адреса в сети, по используемой маске

7) На какой канальный адрес осуществляются широковещательные рассылки?

ff:ff:ff:ff:ff:ff

8) Для чего применяются перехваченные широковещательные рассылки в Части 3?

Ответ был дан

9) В Части 4 при разном использовании утилиты traceroute вы получили разные данные. Почему?

В некоторых сетях маршрутизаторы могут обрабатывать разные типы трафика по-разному. Это может привести к тому, что пакеты ICMP, UDP и TCP могут следовать по разным маршрутам, что повлияет на время отклика и количество хопов, некоторые протоколы могут быть просто проигнорированы

10) Как изменяется загрузка интерфейса в Части 5. п. 3? Почему?

Нетрудно заметить как возрастает объем принятых данных в секунду, пока не упирается в пропускную способность сетевой карты

11) Какие выводы вы сделали в Части 7, п.4?

Всё очевидно, новые подключения с внешних консолей ведут к появлению новых соединений в таблице ss

12) На каком уровне модели OSI работает vnstat?

На канальном