Министерство науки и высшего образования Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования

«Национальный исследовательский университет ИТМО»

Факультет информационных технологий и программирования

Практическая работа № 3

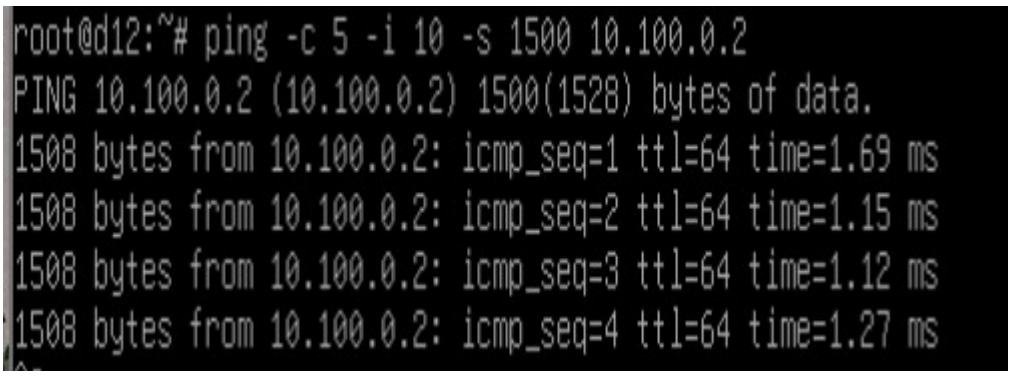
Мониторинг сетевого трафика на хосте на примере работы с утилитами диагностики и мониторинга сетевых соединений в Linux

Выполнил студент группы № M3302

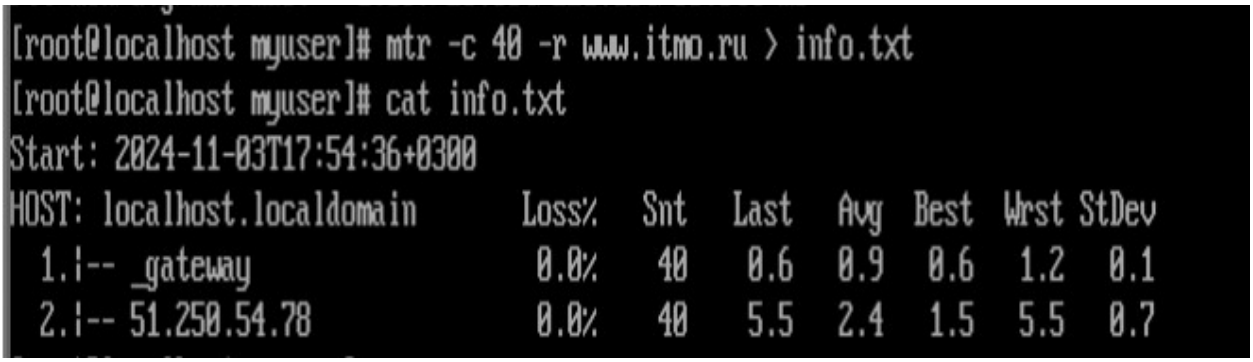
Суворин Ярослав Владимирович

Санкт-Петербург
2024

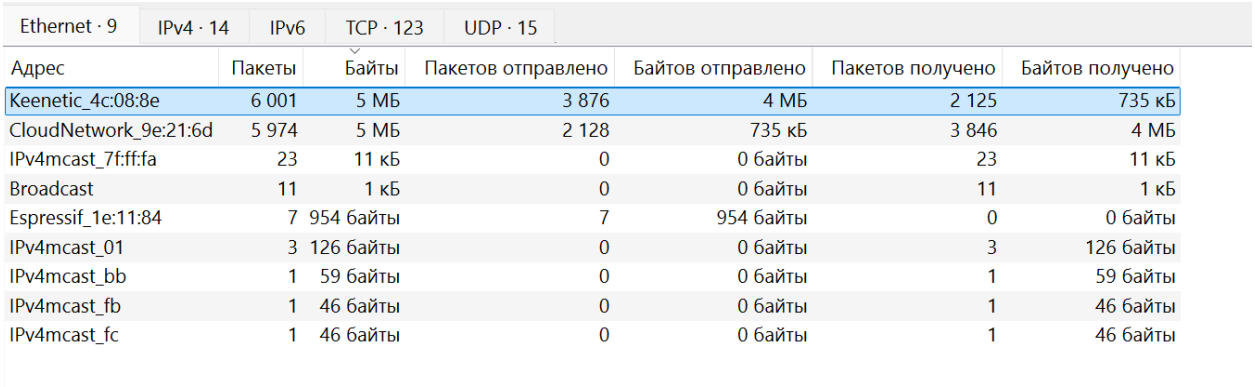
Артефакты:
1. Тексты команд, консольный вывод и полученный файл из Части 2.
п. 2 Команда ping, которая интервалом 10 секунд отправляет 5 пакетов размером 1500 байт на машину c7-1



п. 6 Команда, которая сохранит в файл расширенную статистику работы mtr при отправке 40 пакетов

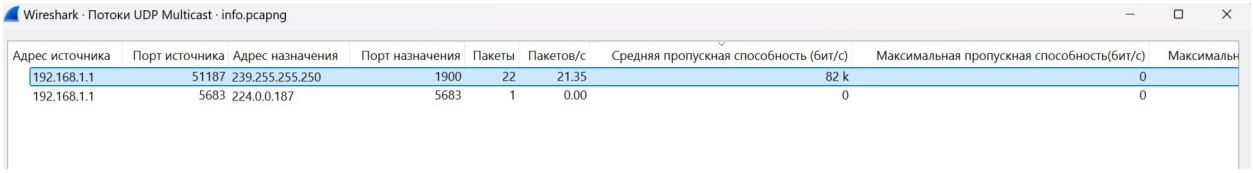


2. Графики, тексты фильтров и ответы на вопросы из Части 3.
п. 2 Используя инструментарий статистики, определяю
a. Узел с максимальной активностью (по объему переданных данных)


Ethernet · 9 | IPv4 · 14 | IPv6 | TCP · 123 | UDP · 15

Адрес	Пакеты	Байты	Пакетов отправлено	Байтов отправлено	Пакетов получено	Байтов получено
Keenetic_4c:08:8e	6 001	5 МБ	3 876	4 МБ	2 125	735 кБ
CloudNetwork_9e:21:6d	5 974	5 МБ	2 128	735 кБ	3 846	4 МБ
IPv4mcast_7f:ff:fa	23	11 кБ	0	0 байты	23	11 кБ
Broadcast	11	1 кБ	0	0 байты	11	1 кБ
Espressif_1e:11:84	7	954 байты	7	954 байты	0	0 байты
IPv4mcast_01	3	126 байты	0	0 байты	3	126 байты
IPv4mcast_bb	1	59 байты	0	0 байты	1	59 байты
IPv4mcast_fb	1	46 байты	0	0 байты	1	46 байты
IPv4mcast_fc	1	46 байты	0	0 байты	1	46 байты

b. Узел, осуществивший наибольшее количество широковещательных рассылок



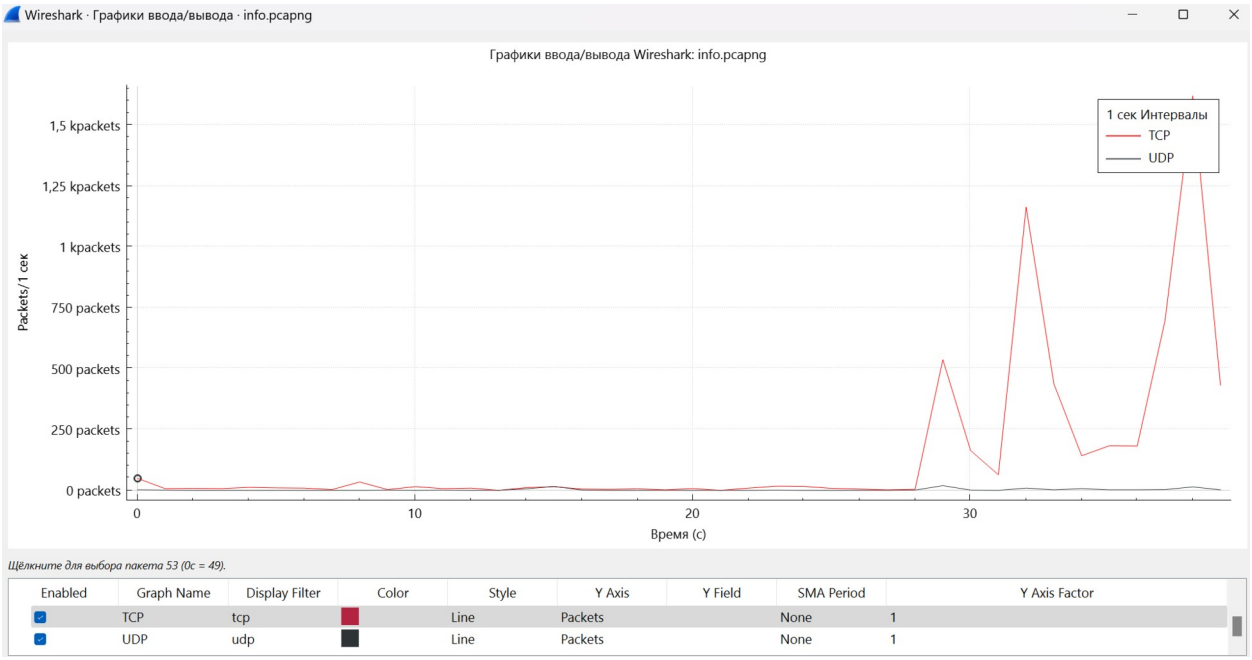
Адрес источника	Порт источника	Адрес назначения	Порт назначения	Пакеты	Пакетов/с	Средняя пропускная способность (бит/с)	Максимальная пропускная способность(бит/с)	Максимальн
192.168.1.1	51187	239.255.255.250	1900	22	21.35	82 k	0	
192.168.1.1	5683	224.0.0.187	5683	1	0.00	0	0	

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

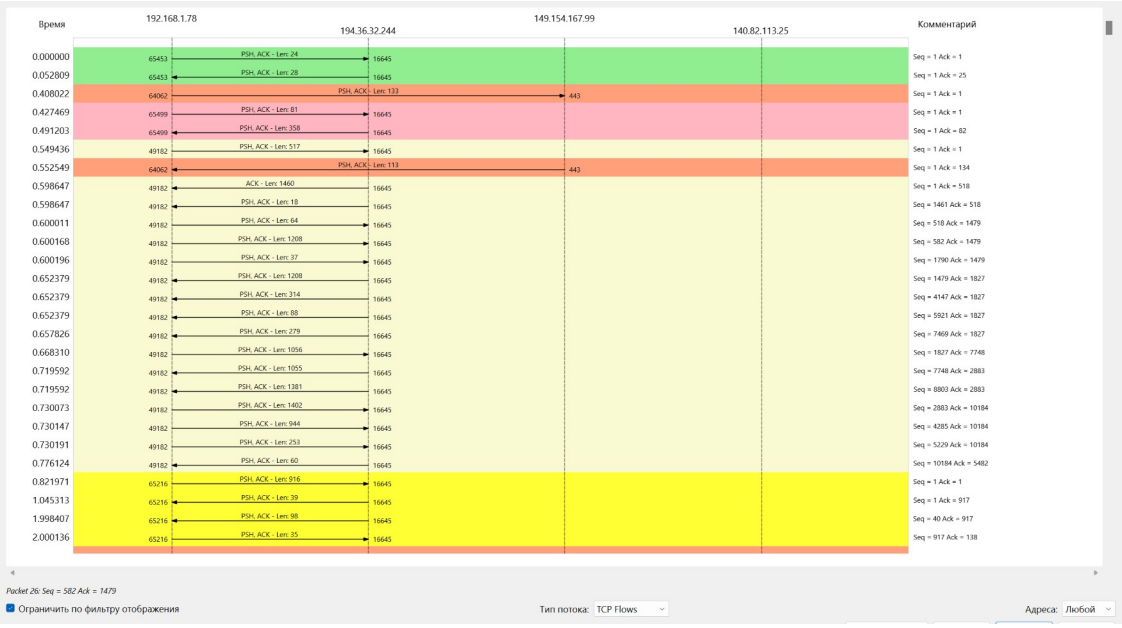
Ethernet · 9 | IPv4 · 14 | IPv6 | TCP · 123 | UDP · 15

Адрес	Порт	Пакеты	Байты	Пакетов отправлено	Байтов отправлено	Пакетов получено	Байтов получено
194.36.32.244	16645	5 821	5 МБ	3 778	4 МБ	2 043	725 кБ
192.168.1.78	49300	1 437	2 МБ	336	31 кБ	1 101	2 МБ
192.168.1.78	49225	853	976 кБ	222	89 кБ	631	887 кБ
192.168.1.78	49222	237	166 кБ	127	146 кБ	110	21 кБ
192.168.1.78	49217	377	414 кБ	90	11 кБ	287	403 кБ
192.168.1.78	49228	219	196 кБ	72	13 кБ	147	183 кБ
192.168.1.78	49189	203	200 кБ	63	21 кБ	140	179 кБ
192.168.1.78	64062	77	11 кБ	45	6 кБ	32	4 кБ
192.168.1.78	49373	70	45 кБ	37	34 кБ	33	11 кБ
192.168.1.78	49264	93	76 кБ	35	9 кБ	58	67 кБ
149.154.167.99	443	77	11 кБ	32	4 кБ	45	6 кБ

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

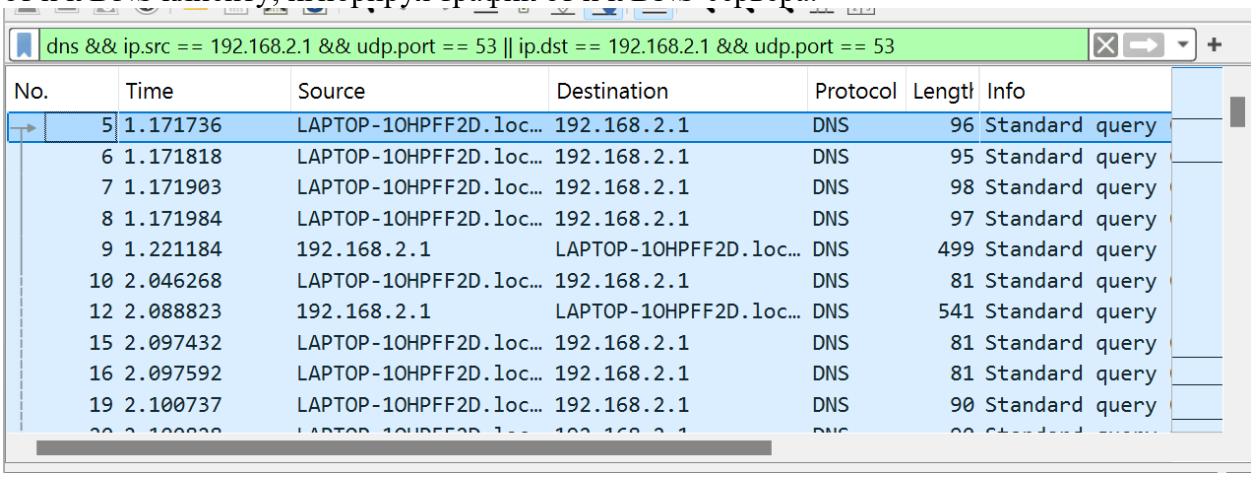


e. Постройте диаграмму связей только для пакетов, содержащих сообщения протокола HTTPS (пункт Flow Graph)

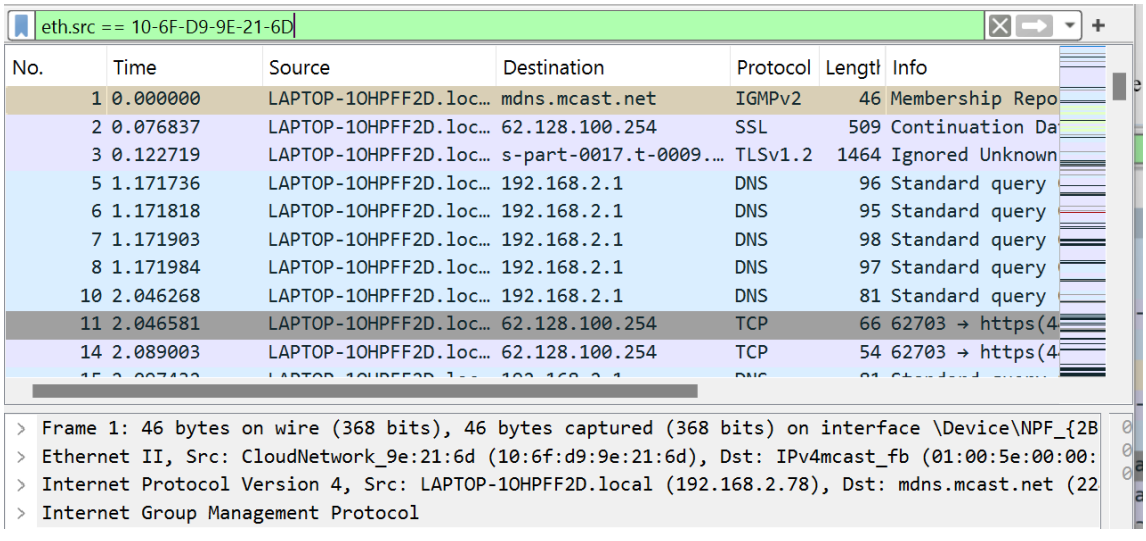


п. 3 Фильтры, которые выделяют из общего числа пакеты

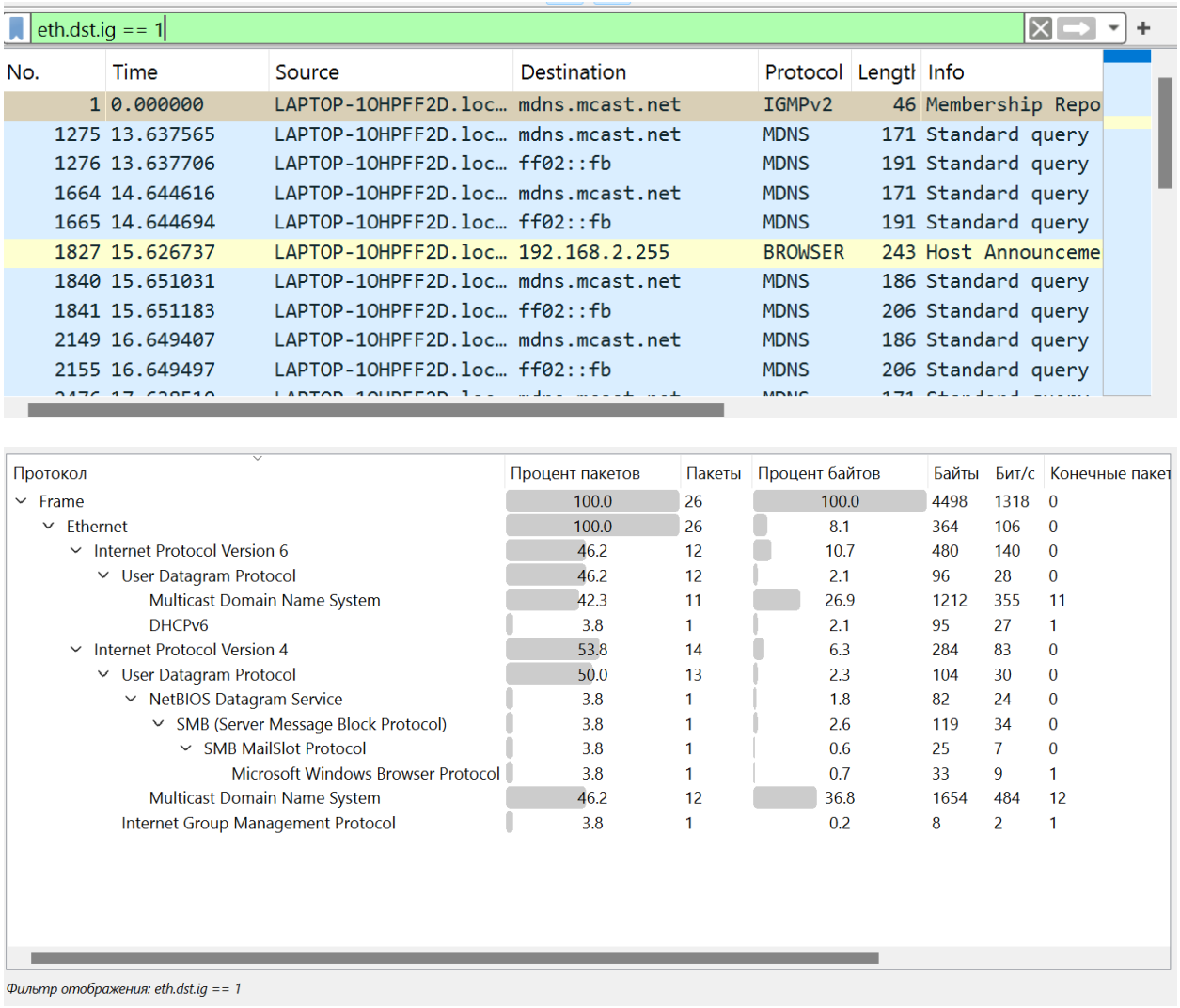
a. Отбирающие сообщения протокола DNS (53 порт udp и tcp) относящиеся только к взаимодействию DNS клиента на хосте и внешних серверов. То есть в случае, если на вашем компьютере будет запущен и DNS-сервер, фильтр должен отбирать только трафик от и к DNS клиенту, игнорируя трафик от и к DNS-сервера.



b. Все кадры Ethernet, отправленные с сетевого интерфейса хоста.



c. Напишите фильтр, отбирающий только широковещательные сообщения. Определите назначение 3-х широковещательных рассылок разных протоколов (или тех, которые удалось обнаружить).



eth.dst.ig == 1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	LAPTOP-1OHPFF2D.loc…	mdns.mcast.net	IGMPv2	46	Membership Repo
1275	13.637565	LAPTOP-1OHPFF2D.loc…	mdns.mcast.net	MDNS	171	Standard query
1276	13.637706	LAPTOP-1OHPFF2D.loc…	ff02::fb	MDNS	191	Standard query
1664	14.644616	LAPTOP-1OHPFF2D.loc…	mdns.mcast.net	MDNS	171	Standard query
1665	14.644694	LAPTOP-1OHPFF2D.loc…	ff02::fb	MDNS	191	Standard query
1827	15.626737	LAPTOP-1OHPFF2D.loc…	192.168.2.255	BROWSER	243	Host Announceme
1840	15.651031	LAPTOP-1OHPFF2D.loc…	mdns.mcast.net	MDNS	186	Standard query
1841	15.651183	LAPTOP-1OHPFF2D.loc…	ff02::fb	MDNS	206	Standard query
2149	16.649407	LAPTOP-1OHPFF2D.loc…	mdns.mcast.net	MDNS	186	Standard query
2155	16.649497	LAPTOP-1OHPFF2D.loc…	ff02::fb	MDNS	206	Standard query

Протокол	Процент пакетов	Пакеты	Процент байтов	Байты	Бит/с	Конечные пакет
Frame	100.0	26	100.0	4498	1318	0
Ethernet	100.0	26	8.1	364	106	0
Internet Protocol Version 6	46.2	12	10.7	480	140	0
User Datagram Protocol	46.2	12	2.1	96	28	0
Multicast Domain Name System	42.3	11	26.9	1212	355	11
DHCPv6	3.8	1	2.1	95	27	1
Internet Protocol Version 4	53.8	14	6.3	284	83	0
User Datagram Protocol	50.0	13	2.3	104	30	0
NetBIOS Datagram Service	3.8	1	1.8	82	24	0
SMB (Server Message Block Protocol)	3.8	1	2.6	119	34	0
SMB MailSlot Protocol	3.8	1	0.6	25	7	0
Microsoft Windows Browser Protocol	3.8	1	0.7	33	9	1
Multicast Domain Name System	46.2	12	36.8	1654	484	12
Internet Group Management Protocol	3.8	1	0.2	8	2	1

Фильтр отображения: eth.dst.ig == 1

User Datagram Protocol, Internet Group Management Protocol

3. Тексты команд и консольный вывод из Части 4, п.2, команды traceroute, которые

a. определяют маршрут до хоста 8.8.8.8 с помощью ICMP

```
[root@localhost ~]# traceroute -I 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (10.100.0.1)  97.849 ms  0.353 ms  0.251 ms
 2  dns.google (8.8.8.8)  1.048 ms  0.865 ms  0.688 ms
```

b. определяют маршрут до хоста 8.8.8.8 с помощью UDP

с. определяют маршрут до хоста 8.8.8.8 с помощью TCP

```
[root@localhost ~]# traceroute -T 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  * * *
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

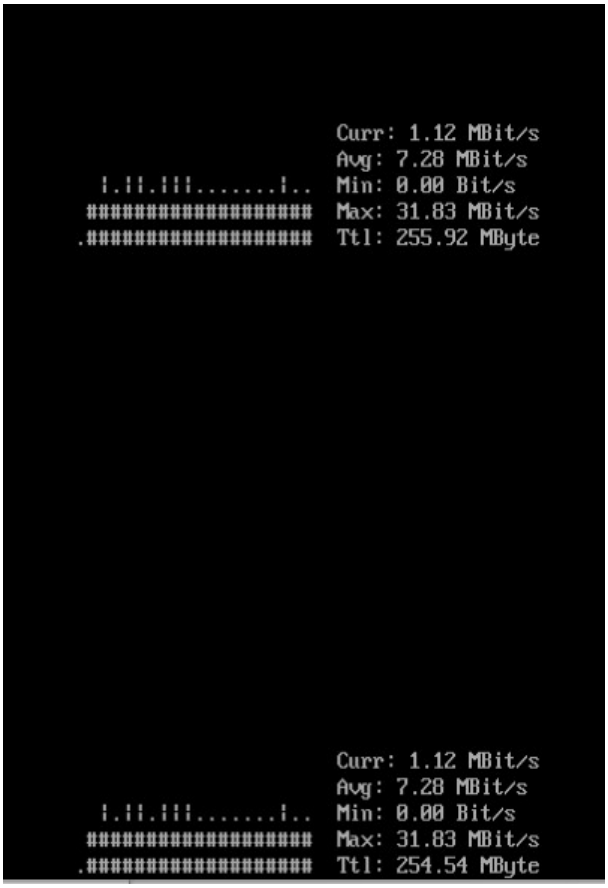
d. позволяют определить используется ли по маршруту фрагментация IPv4

```
[root@localhost ~]# traceroute -F 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (10.100.0.1)  96.383 ms  0.315 ms  0.271 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

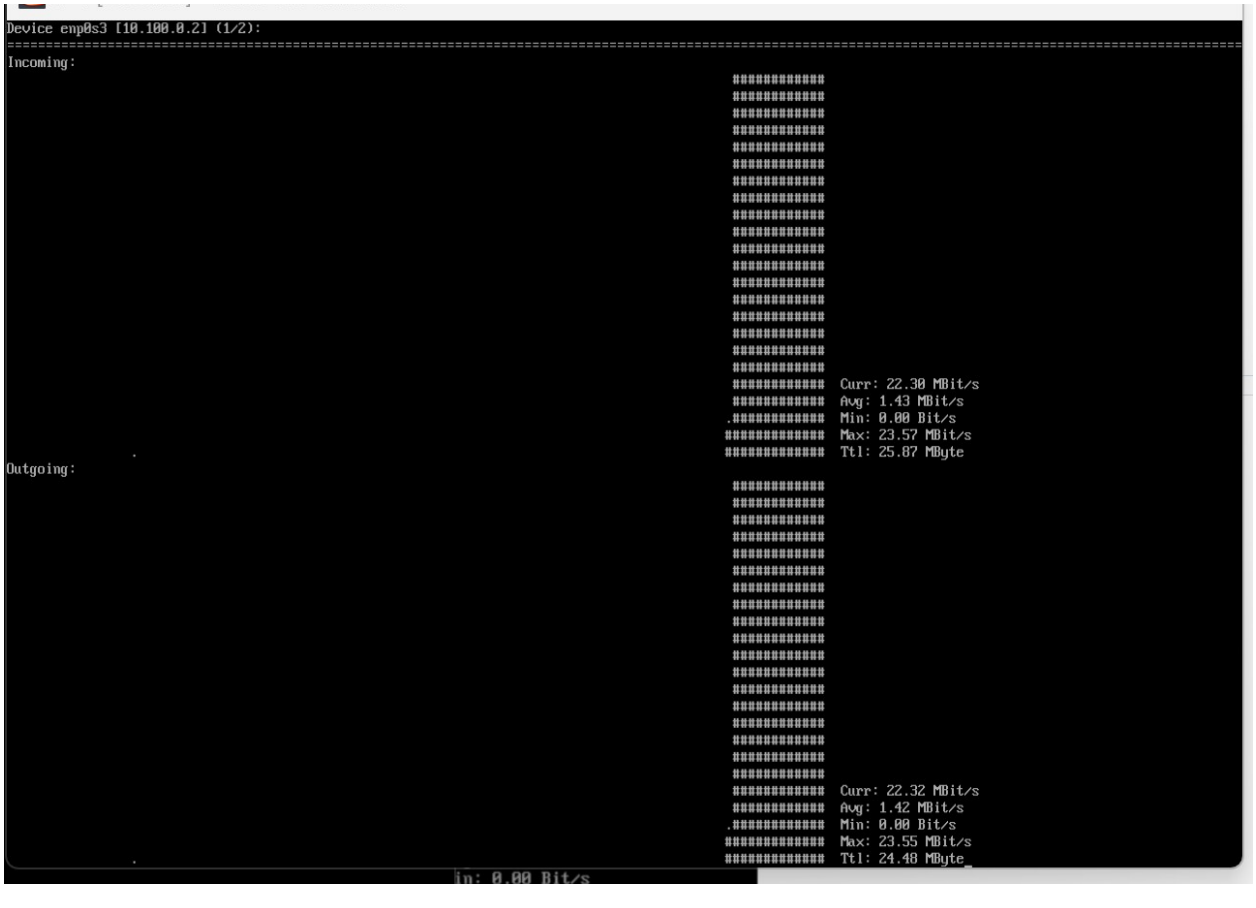
4. Тексты команд и консольный вывод из Части 5,
п.2
На хосте c7-1 последовательно с помощью утилиты nload получил данные о загрузке интерфейса, на который отправляет трафик хост c7-2

п.3
Изменял размер пакета, передаваемого утилитой ping пакета от 100 до 60100 с шагом 10000. Определил, как меняется загрузка на сетевом интерфейсе

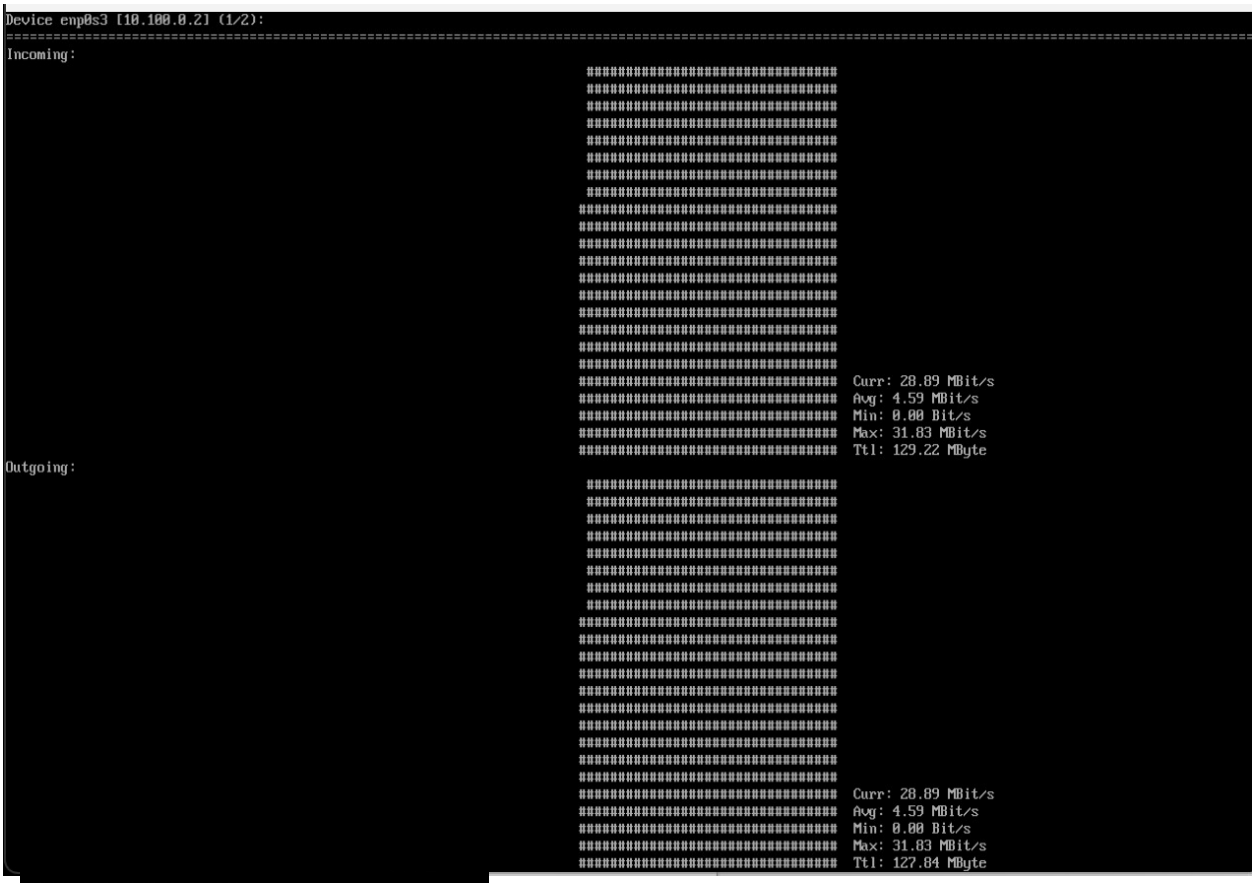
100


Curr: 1.12 MBit/s
Avg: 7.28 MBit/s
Min: 0.00 Bit/s
Max: 31.83 MBit/s
Ttl: 255.92 MByte
Curr: 1.12 MBit/s
Avg: 7.28 MBit/s
Min: 0.00 Bit/s
Max: 31.83 MBit/s
Ttl: 254.54 MByte

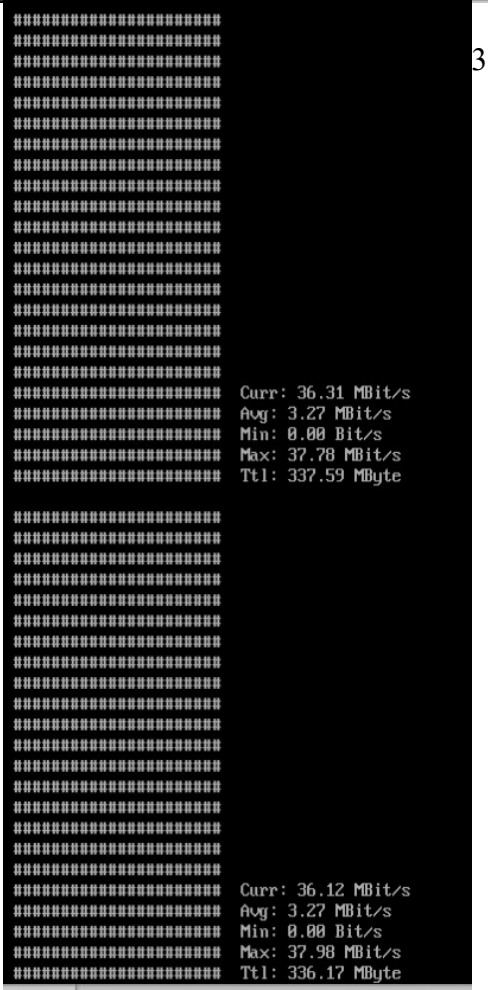
10100


Device enp0s3 [10.100.0.2] (1/2):
Incoming:
Curr: 22.30 MBit/s
Avg: 1.43 MBit/s
Min: 0.00 Bit/s
Max: 23.57 MBit/s
Ttl: 25.87 MByte
Outgoing:
Curr: 22.32 MBit/s
Avg: 1.42 MBit/s
Min: 0.00 Bit/s
Max: 23.55 MBit/s
Ttl: 24.48 MByte

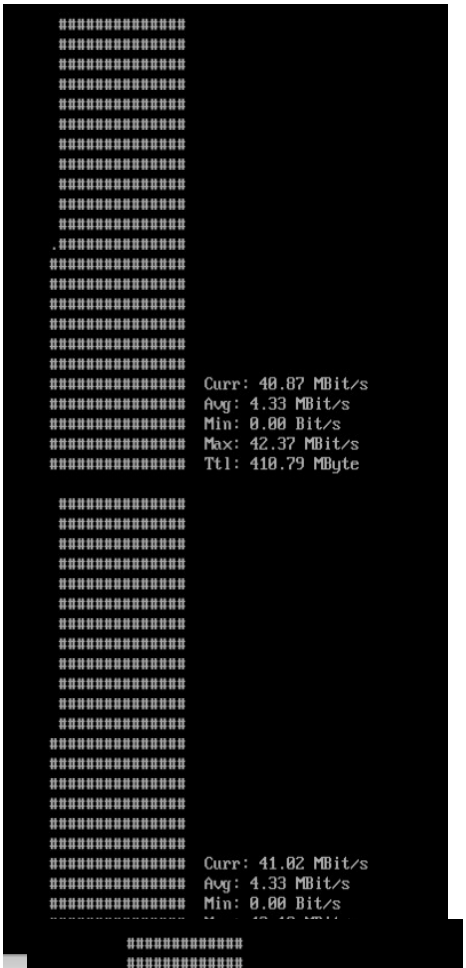
20100


Device enp0s3 [10.100.0.2] (1/2):
Incoming:
Curr: 28.89 MBit/s
Avg: 4.59 MBit/s
Min: 0.00 Bit/s
Max: 31.83 MBit/s
Ttl: 129.22 MByte
Outgoing:
Curr: 28.89 MBit/s
Avg: 4.59 MBit/s
Min: 0.00 Bit/s
Max: 31.83 MBit/s
Ttl: 127.84 MByte

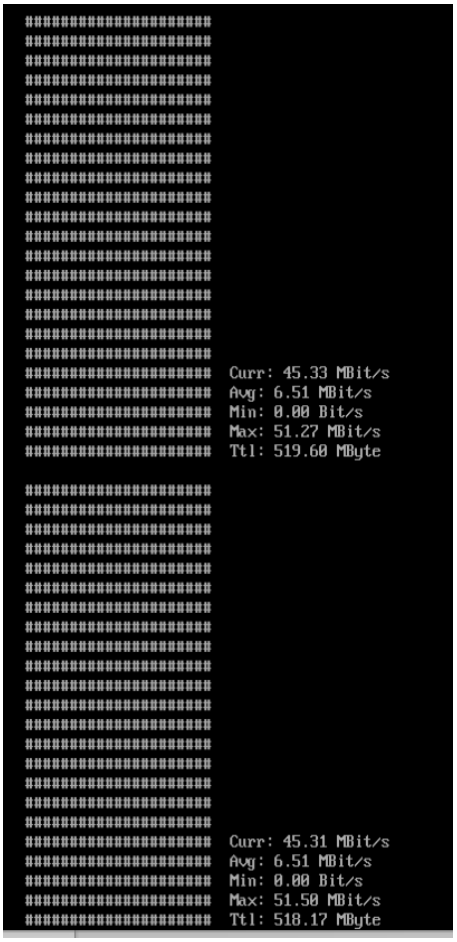
30100


Curr: 36.31 MBit/s
Avg: 3.27 MBit/s
Min: 0.00 Bit/s
Max: 37.78 MBit/s
Ttl: 337.59 MByte
Curr: 36.12 MBit/s
Avg: 3.27 MBit/s
Min: 0.00 Bit/s
Max: 37.98 MBit/s
Ttl: 336.17 MByte

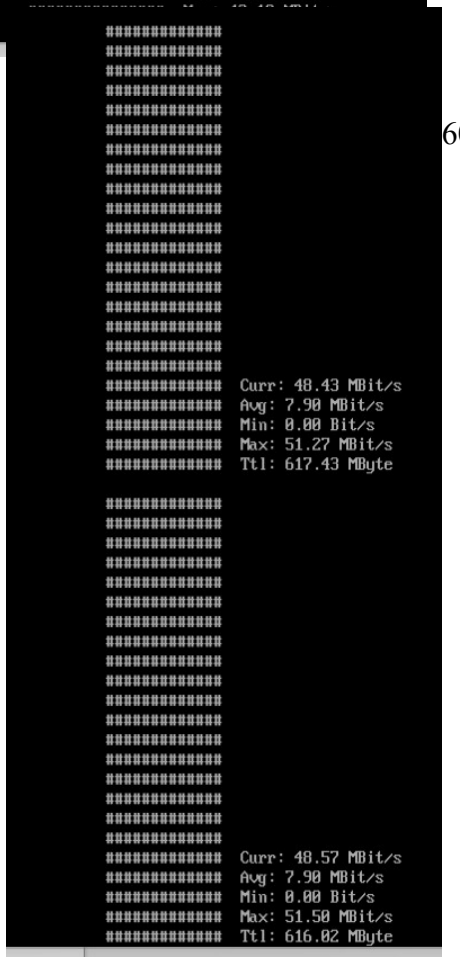
40100



50100



60100



5. Тексты команд и консольный вывод из Части 6
п.4.

```
[root@localhost ~]# vnstat -i enp0s3 -l
Monitoring enp0s3...    (press CTRL-C to stop)

   rx:         0 bit/s      0 p/s          tx:         0 bit/s      0 p/s^C


 enp0s3  /  traffic statistics

                           rx         |       tx
--------------------------------------+------------------
  bytes                    48,03 KiB  |        48,03 KiB
--------------------------------------+------------------
          max          196,00 kbit/s  |    196,00 kbit/s
      average           14,05 kbit/s  |     14,05 kbit/s
          min              0 bit/s    |         0 bit/s
--------------------------------------+------------------
  packets                       503    |             503
--------------------------------------+------------------
          max              250 p/s    |         250 p/s
      average               17 p/s    |          17 p/s
          min                0 p/s    |           0 p/s
--------------------------------------+------------------
  time                  28 seconds
```

6. Тексты команд и консольный вывод (или его часть) из Части 7
п.2

```
root@d12:~# ssh root@10.100.0.2
```

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      872/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1028/master
tcp6       0      0 :::22                   :::*                    LISTEN      872/sshd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1028/master
udp        0      0 127.0.0.1:323           0.0.0.0:*                           649/chronyd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1254/dhclient
udp6       0      0 ::1:323                 :::*                                649/chronyd
```

п. 3

```
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      872/sshd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1028/master
tcp6       0      0 :::22                   :::*                    LISTEN      872/sshd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1028/master
udp        0      0 127.0.0.1:323           0.0.0.0:*                           649/chronyd
udp        0      0 0.0.0.0:68              0.0.0.0:*                           1254/dhclient
udp6       0      0 ::1:323                 :::*                                649/chronyd
Active UNIX domain sockets (only servers)
Proto RefCnt Flags       Type       State         I-Node   PID/Program name     Path
unix  2      [ ACC ]     STREAM     LISTENING     17922    1028/master          private/proxywrite
unix  2      [ ACC ]     STREAM     LISTENING     17925    1028/master          private/smtp
unix  2      [ ACC ]     STREAM     LISTENING     17934    1028/master          private/error
unix  2      [ ACC ]     STREAM     LISTENING     17937    1028/master          private/retry
unix  2      [ ACC ]     STREAM     LISTENING     17940    1028/master          private/discard
unix  2      [ ACC ]     STREAM     LISTENING     17943    1028/master          private/local
unix  2      [ ACC ]     STREAM     LISTENING     12300    1/systemd            /run/lvm/lvmetad.s
unix  2      [ ACC ]     STREAM     LISTENING     17946    1028/master          private/virtual
unix  2      [ ACC ]     STREAM     LISTENING     12046    1/systemd            /run/systemd/priva
unix  2      [ ACC ]     STREAM     LISTENING     17949    1028/master          private/lmtp
```

скрипт из п.4

```
#!/bin/bash

port1=":"

if [[ $1 == "" ]]
then
        port1=$port1"22"
else
        port1=$port1$1
fi

netstat -lnptu | awk '{if ($4 ~ "'$port1'$") {print $4, $5}}' | sort -k2 | uniq -c
```

п. 8

PID 7256
SENT 0.170
RECEIVED 0.045 KB/sec

7. Тексты команд из части 8
п. 1

```
[root@localhost ~]# tcpdump -vv -i enp0s3 port 4444 or port 9999 -w file_name
```

п. 2
Считывание:

```
[root@localhost ~]# nc -l -p 9999 > newfile
```

Передача:

```
root@d12:/home/myuser# cat file.txt | nc 10.100.0.2 9999
```

Файлы file.txt и newfile соответственно:

```
root@d12:/home/myuser# cat file.txt
aaaaaaaaaaaa d d d d d d  dv fv fvfvfvf  f f f f f f f f f f  dad ewdwe dw d w f f v dfv df v dv d vd v df  ABOBA cd  e fe f e fe f a
```

```
[root@localhost ~]# cat newfile
aaaaaaaaaaaa d d d d d d  dv fv fvfvfvf  f f f f f f f f f f  dad ewdwe dw d w f f v dfv df v dv d vd v df  ABOBA cd  e fe f e fe f a
```

п. 3

```
root@d12:/home/myuser# nc 10.100.0.2 4444
Hey now
You are a rock star
get the show on
get paid
```

```
[root@localhost ~]# nc -lp 4444
Hey now
You are a rock star
get the show on
get paid
```

1. По какому протоколу работает утилита mtr? Как это можно определить?
Утилита **mtr** (My Traceroute) сочетает функционал ping и traceroute, отправляя пакеты на каждый узел в маршруте для анализа задержек и потерь. Протокол, который она использует, зависит от конфигурации:

- **ICMP** по умолчанию на большинстве систем, аналогично ping.
- **UDP** (если указано в параметрах) для работы, аналогично traceroute по UDP.
- Определить протокол можно, проанализировав трафик утилиты через tcpdump или Wireshark.

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

Типичные столбцы **mtr**:

- **Host** — IP или доменное имя узла.
- **Loss%** — процент потерянных пакетов.
- **Sent** — количество отправленных пакетов.
- **Last** — время отклика последнего пакета.
- **Avg** — среднее время отклика.
- **Best** — минимальное время отклика.
- **Worst** — максимальное время отклика.
- **StDev** — стандартное отклонение времени отклика (измеряет колебания задержки).

Дополнительные статистики включают стандартное отклонение, более детальную информацию о маршруте и отдельные задержки.

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

Основные типы кадров Ethernet:

- **Ethernet II** — наиболее распространённый формат, поддерживающий IPv4 и IPv6.
- **802.3** — старый стандарт без типа протокола, поддерживающий верхнеуровневые протоколы через дополнительный заголовок 802.2.
- **SNAP** — вариант 802.3 с поддержкой нестандартных протоколов.

Отличия заключаются в структуре кадров: в Ethernet II присутствует поле типа протокола, тогда как 802.3 использует длину кадра.

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

Чаще всего используется **Ethernet II**. Этот тип позволяет сети функционировать, так как поддерживает современные протоколы IP (IPv4 и IPv6), обеспечивая маршрутизацию и связь между устройствами.

5. Как можно определить тип используемого коммутационного оборудования, используя сетевую статистику? Сделайте предположения о типе коммутационного оборудования использовался в сети на основании собранного трафика.

Тип оборудования можно предположить, анализируя:

- **Задержки** и **пропускную способность**: высокопроизводительные коммутаторы создают минимальные задержки.
- **Таблицы MAC-адресов**: управляемые коммутаторы поддерживают большее количество MAC-адресов и могут применяться для сегментации сети.
- **Поддержка VLAN**: если в сети есть кадры, содержащие теги 802.1Q, оборудование поддерживает VLAN.

Обычно управляемые коммутаторы предоставляют больше возможностей для конфигурации и мониторинга трафика, тогда как неуправляемые — только базовую коммутацию.

6. На какие адреса сетевого уровня осуществляются широковещательные рассылки?

Широковещательные рассылки на сетевом уровне отправляются на **IPv4-адрес 255.255.255.255** (локальный широковещательный) или **директед-адреса** (например, 192.168.1.255 для локальной сети 192.168.1.0/24).

7. На какой канальный адрес осуществляются широковещательные рассылки?

На канальном уровне широковещательные кадры отправляются на **MAC-адрес FF:FF:FF:FF:FF**

8. Для чего применяются перехваченные широковещательные рассылки в Части 3? Протоколы для распределения информации и поддержания связи между устройствами.

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

Traceroute использует разные протоколы (UDP, ICMP, TCP) для построения маршрута. Разные протоколы могут по-разному обрабатываться промежуточными маршрутизаторами и фаерволами, что приводит к различиям в маршруте (например, некоторые узлы могут блокировать ICMP, но пропускать TCP-пакеты).

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

С увеличением размера пакетов, отправляемых с **ping flood**, **загрузка интерфейса** также возрастает, так как больший размер пакетов требует больше пропускной способности сети для обработки увеличенного объёма данных.

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

Мы можем собрать информацию о всех входящих соединениях на определённый порт(22) к хосту, чтобы определить IP-адреса, которые чаще всего подключаются. Этот анализ

полезен для мониторинга активности и выявления потенциально подозрительных IP-адресов.

12. На каком уровне модели OSI работает vnstat?

Утилита **vnstat** работает на **канальном уровне** (уровень 2) модели OSI, так как она отслеживает трафик интерфейса, собирая данные непосредственно на уровне передачи данных, не анализируя содержимое сетевых пакетов.