clМИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики

Мегафакультет трансляционных информационных технологий

Факультет информационных технологий и программирования

Лабораторная работа №3

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

Выполнила студент группы №**M33091**

Зыонг Тхи Хуэ Линь
Исрат
Проверил

САНКТ-ПЕТЕРБУРГ

2024

Артефакты

Ират

1. **Тексты команд и консольный вывод из Части 1. п. 8**

   с7-1 с помощью утилиты ping проверьте доступность внешней сети, послав 5 эхо-запросов на сервер 8.8.8.8

```
[root@localhost ~]# ping -c 5 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=59 time=42.10 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=59 time=94.5 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=59 time=46.4 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=59 time=47.7 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=59 time=43.0 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 14ms
rtt min/avg/max/mdev = 42.988/54.917/94.522/19.889 ms
[root@localhost ~]# _
```

2. **Тексты команд, консольный вывод и полученный файл из Части 2. п. 2,7**

   с7-2 отправляют 10 пакетов с интервалом 10 секунд на машину с7-1

```
[root@localhost ~]# ping -c 10 -i 10 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.447 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.713 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=1.24 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.966 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=1.16 ms
64 bytes from 10.0.0.1: icmp_seq=6 ttl=64 time=0.868 ms
64 bytes from 10.0.0.1: icmp_seq=7 ttl=64 time=0.384 ms
64 bytes from 10.0.0.1: icmp_seq=8 ttl=64 time=1.14 ms
64 bytes from 10.0.0.1: icmp_seq=9 ttl=64 time=0.381 ms
64 bytes from 10.0.0.1: icmp_seq=10 ttl=64 time=0.606 ms

--- 10.0.0.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 180ms
rtt min/avg/max/mdev = 0.381/0.789/1.239/0.315 ms
[root@localhost ~]# _
```

с7-2 отправляет 5 пакетов размером 1500 байт на машину с7-1

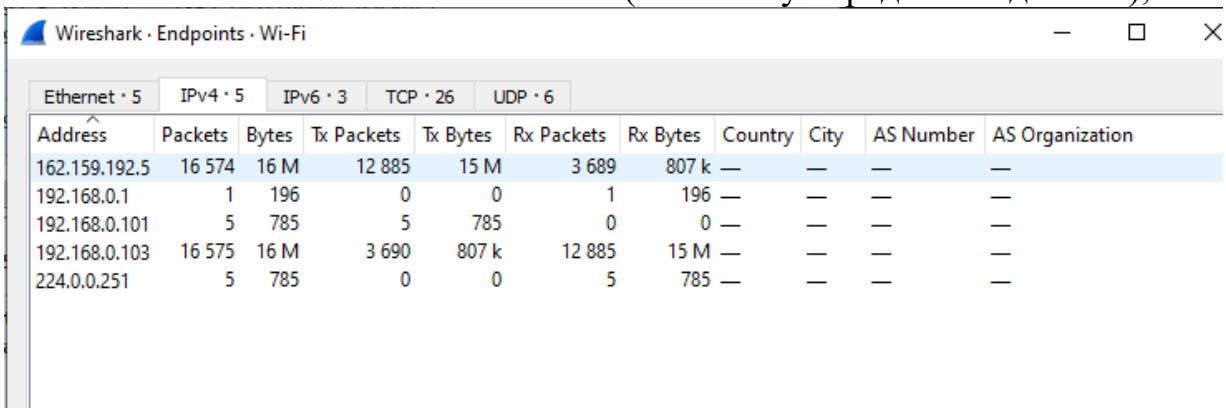
```
[root@localhost ~]# ping -c 5 -s 15000 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 15000(15028) bytes of data.
15008 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=1.35 ms
15008 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=4.14 ms
15008 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.562 ms
15008 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.643 ms
15008 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=1.40 ms

--- 10.0.0.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 12ms
rtt min/avg/max/mdev = 0.562/1.618/4.137/1.306 ms
[root@localhost ~]#
```

С хоста с7-1

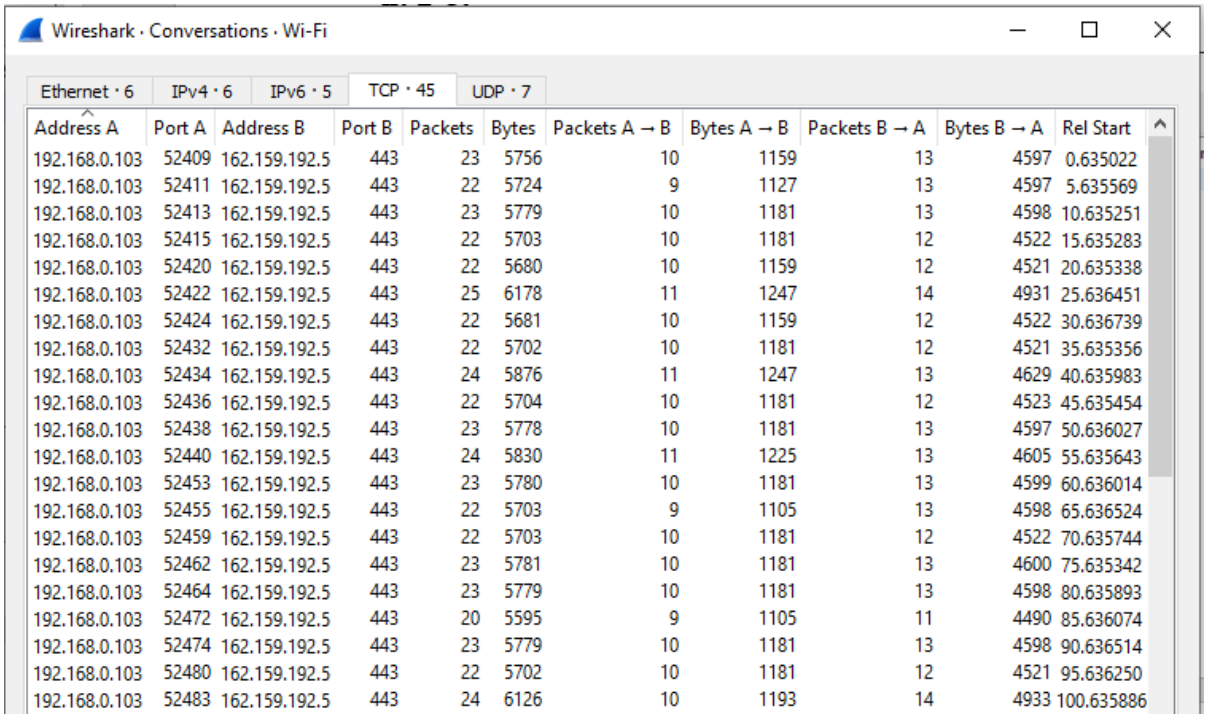
```
[root@localhost ~]# mtr -rw -c 40 www.itmo.ru > mtr_report_itmo
[root@localhost ~]# cat mtr_report_itmo
Start: Thu Feb 29 13:06:17 2024
HOST: localhost.localdomain          Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- _gateway                      0.0%    40    0.3   0.6   0.3   1.6   0.3
  2.|-- 172.16.0.1                    0.0%    40   93.5  30.2  13.8 107.6  19.3
  3.|-- 172.68.9.1                    0.0%    40   20.0  32.8  15.6  96.0  17.3
  4.|-- ae12-177.RT1.M9.MSK.RU.retn.net 0.0%  40   30.9  37.5  18.5 138.9  21.0
  5.|-- ae2-11.RT.OV.SPB.RU.retn.net   0.0%    40   25.8  33.6  25.4  65.9   9.1
  6.|-- GW-ITMO.retn.net               0.0%    40   26.1  43.0  25.1 267.6  39.7
  7.|-- 77.234.192.167                 0.0%    40   31.8  44.3  26.6 156.3  33.0
  8.|-- 77.234.204.10                  0.0%    40   26.9  36.9  25.6  85.1  13.9
[root@localhost ~]# _
```

3. Графики, тексты фильтров и ответы на вопросы из Части 3. п. 2-5.

2.а Узел с максимальной активностью (по объему переданных данных),

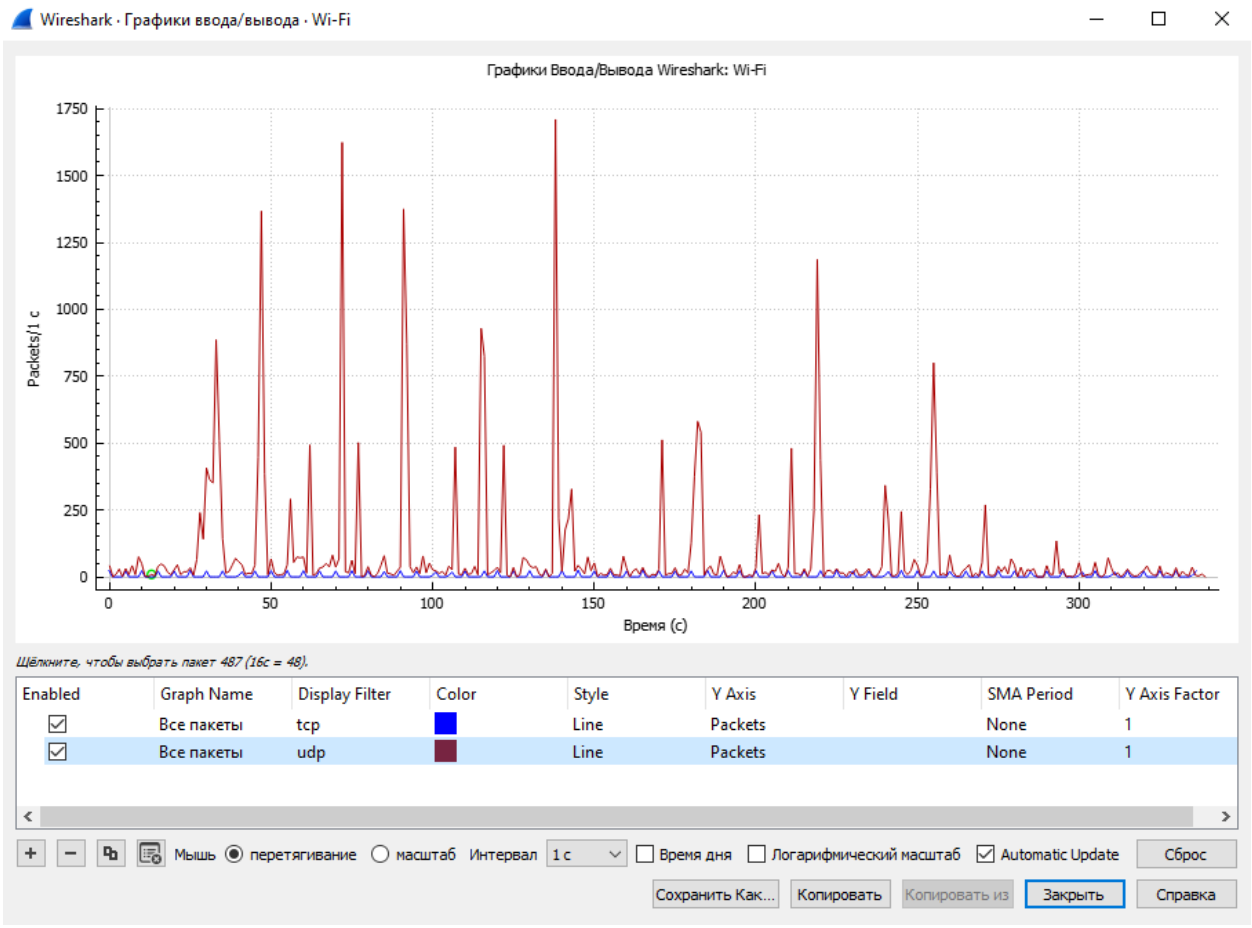


Самый активный TCP-порт на хосте (по количеству переданных пакетов)

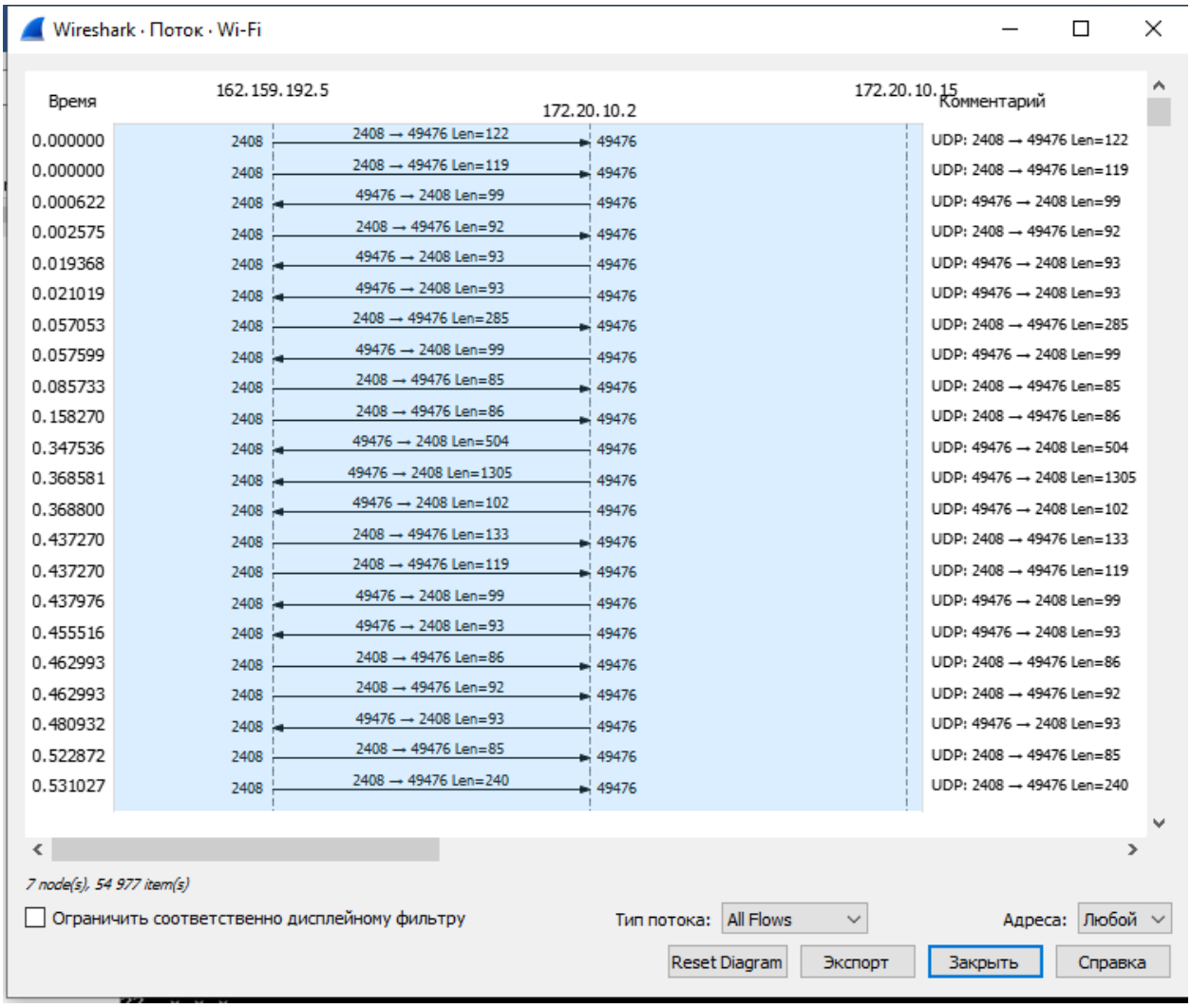


Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start
192.168.0.103	52409	162.159.192.5	443	23	5756	10	1159	13	4597	0.635022
192.168.0.103	52411	162.159.192.5	443	22	5724	9	1127	13	4597	5.635569
192.168.0.103	52413	162.159.192.5	443	23	5779	10	1181	13	4598	10.635251
192.168.0.103	52415	162.159.192.5	443	22	5703	10	1181	12	4522	15.635283
192.168.0.103	52420	162.159.192.5	443	22	5680	10	1159	12	4521	20.635338
192.168.0.103	52422	162.159.192.5	443	25	6178	11	1247	14	4931	25.636451
192.168.0.103	52424	162.159.192.5	443	22	5681	10	1159	12	4522	30.636739
192.168.0.103	52432	162.159.192.5	443	22	5702	10	1181	12	4521	35.635356
192.168.0.103	52434	162.159.192.5	443	24	5876	11	1247	13	4629	40.635983
192.168.0.103	52436	162.159.192.5	443	22	5704	10	1181	12	4523	45.635454
192.168.0.103	52438	162.159.192.5	443	23	5778	10	1181	13	4597	50.636027
192.168.0.103	52440	162.159.192.5	443	24	5830	11	1225	13	4605	55.635643
192.168.0.103	52453	162.159.192.5	443	23	5780	10	1181	13	4599	60.636014
192.168.0.103	52455	162.159.192.5	443	22	5703	9	1105	13	4598	65.636524
192.168.0.103	52459	162.159.192.5	443	22	5703	10	1181	12	4522	70.635744
192.168.0.103	52462	162.159.192.5	443	23	5781	10	1181	13	4600	75.635342
192.168.0.103	52464	162.159.192.5	443	23	5779	10	1181	13	4598	80.635893
192.168.0.103	52472	162.159.192.5	443	20	5595	9	1105	11	4490	85.636074
192.168.0.103	52474	162.159.192.5	443	23	5779	10	1181	13	4598	90.636514
192.168.0.103	52480	162.159.192.5	443	22	5702	10	1181	12	4521	95.636250
192.168.0.103	52483	162.159.192.5	443	24	6126	10	1193	14	4933	100.635886

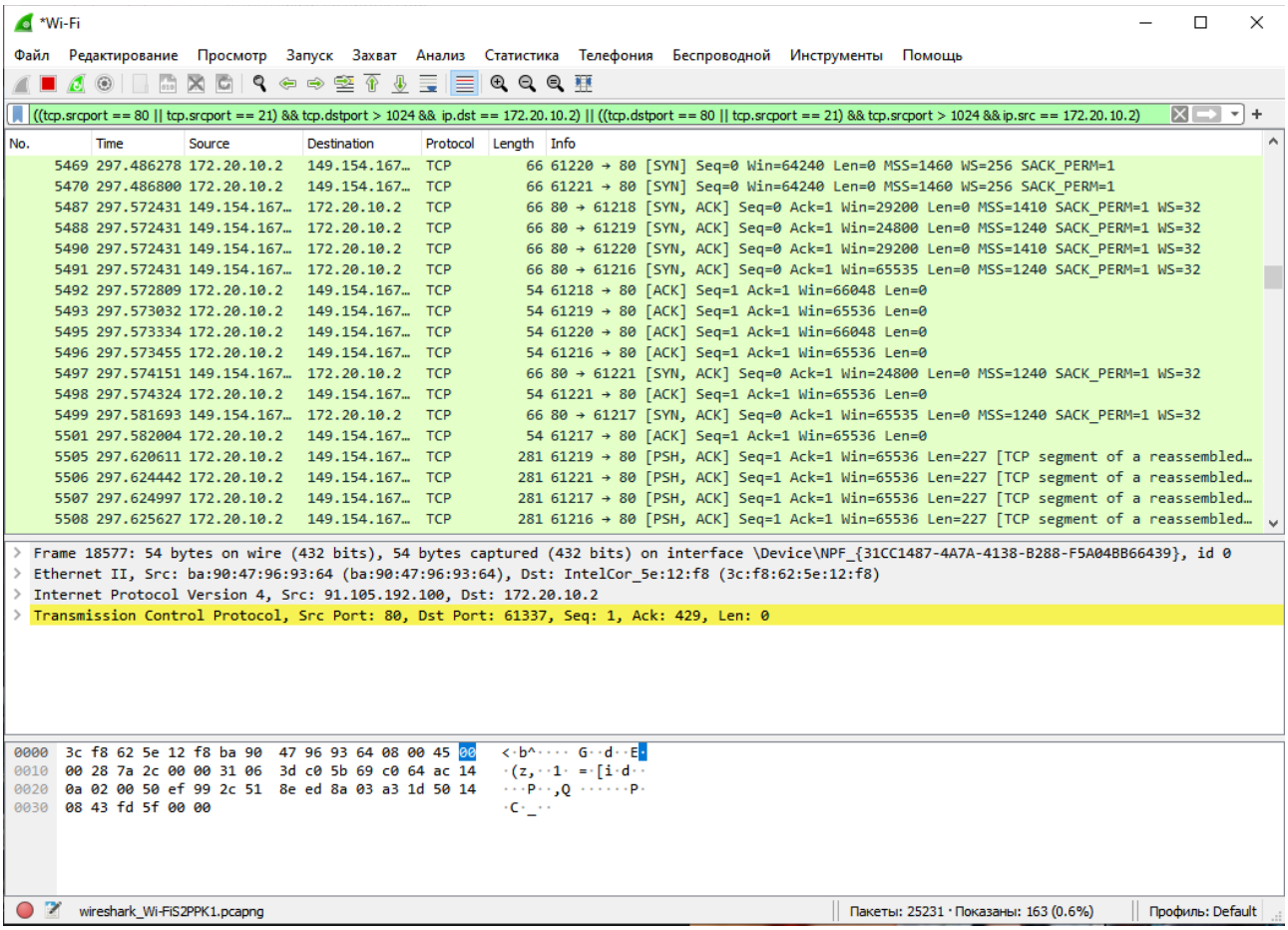
Постройте на одной координатной сетке постройте графики интенсивности TCP и UDP трафика (пункт Io Graphs).



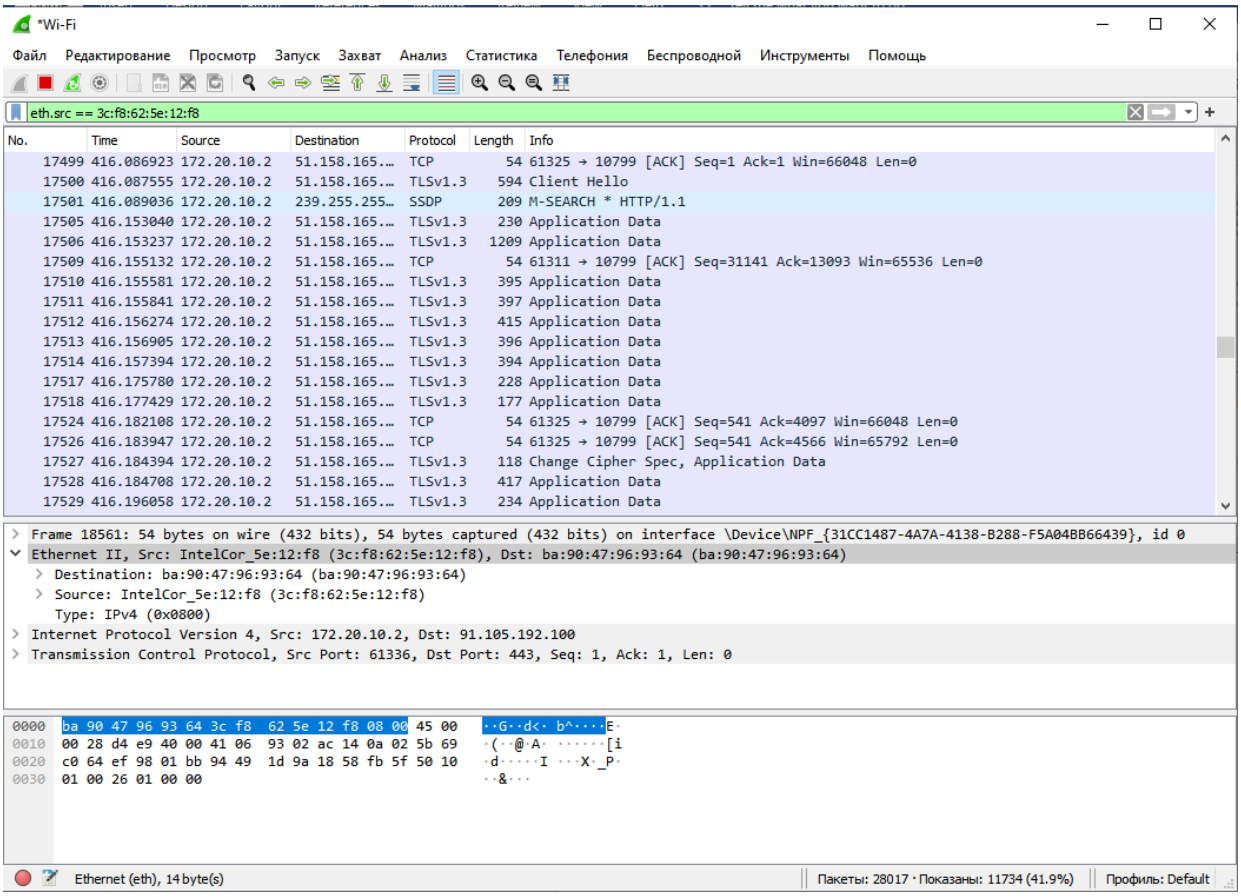
Постройте диаграмму связей только для пакетов, содержащих сообщения протокола HTTPS (пункт Flow Graph)



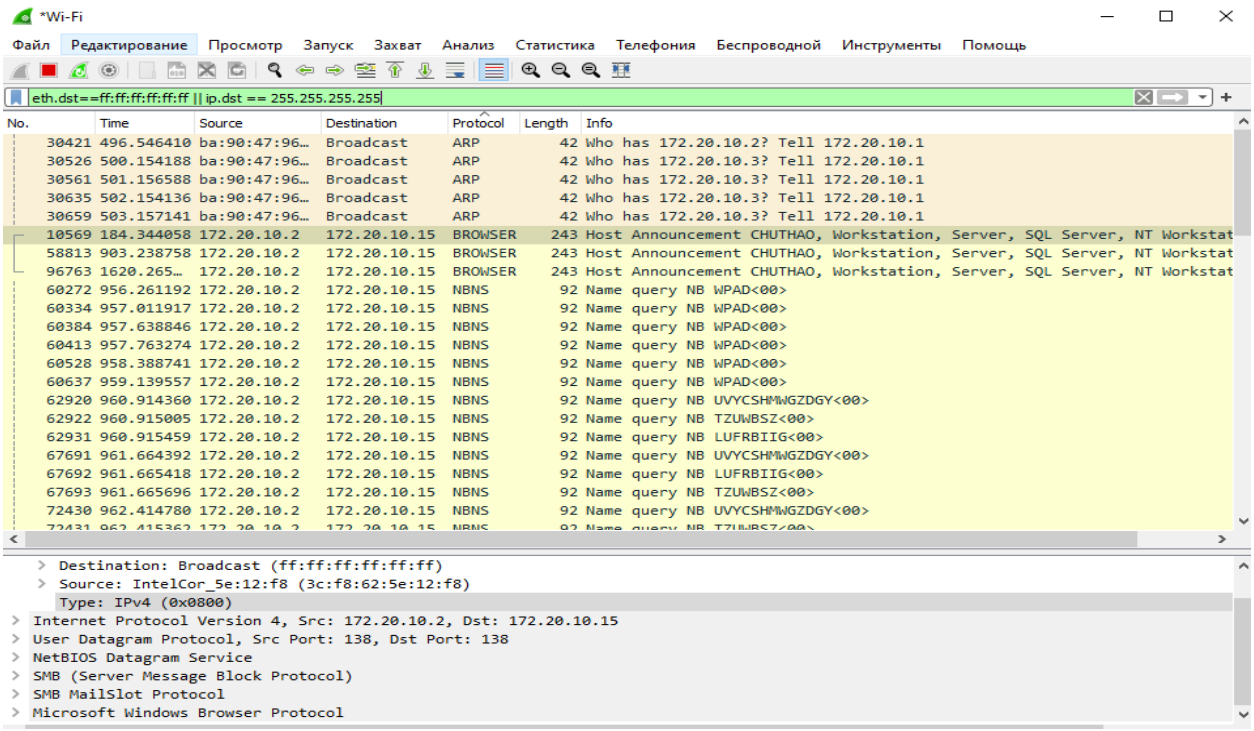
3.a.


*Wi-Fi
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
((tcp.srcport == 80 || tcp.srcport == 21) && tcp.dstport > 1024 && ip.dst == 172.20.10.2) || ((tcp.dstport == 80 || tcp.srcport == 21) && tcp.srcport > 1024 && ip.src == 172.20.10.2)
No. Time Source Destination Protocol Length Info
5469 297.486278 172.20.10.2 149.154.167… TCP 66 61220 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5470 297.486800 172.20.10.2 149.154.167… TCP 66 61221 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
5487 297.572431 149.154.167… 172.20.10.2 TCP 66 80 → 61218 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1410 SACK_PERM=1 WS=32
5488 297.572431 149.154.167… 172.20.10.2 TCP 66 80 → 61219 [SYN, ACK] Seq=0 Ack=1 Win=24800 Len=0 MSS=1240 SACK_PERM=1 WS=32
5490 297.572431 149.154.167… 172.20.10.2 TCP 66 80 → 61220 [SYN, ACK] Seq=0 Ack=1 Win=29200 Len=0 MSS=1410 SACK_PERM=1 WS=32
5491 297.572431 149.154.167… 172.20.10.2 TCP 66 80 → 61216 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1240 SACK_PERM=1 WS=32
5492 297.572809 172.20.10.2 149.154.167… TCP 54 61218 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
5493 297.573032 172.20.10.2 149.154.167… TCP 54 61219 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
5495 297.573334 172.20.10.2 149.154.167… TCP 54 61220 → 80 [ACK] Seq=1 Ack=1 Win=66048 Len=0
5496 297.573455 172.20.10.2 149.154.167… TCP 54 61216 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
5497 297.574151 149.154.167… 172.20.10.2 TCP 66 80 → 61221 [SYN, ACK] Seq=0 Ack=1 Win=24800 Len=0 MSS=1240 SACK_PERM=1 WS=32
5498 297.574324 172.20.10.2 149.154.167… TCP 54 61221 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
5499 297.581693 149.154.167… 172.20.10.2 TCP 66 80 → 61217 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1240 SACK_PERM=1 WS=32
5501 297.582004 172.20.10.2 149.154.167… TCP 54 61217 → 80 [ACK] Seq=1 Ack=1 Win=65536 Len=0
5505 297.620611 172.20.10.2 149.154.167… TCP 281 61219 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=227 [TCP segment of a reassembled…
5506 297.624442 172.20.10.2 149.154.167… TCP 281 61221 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=227 [TCP segment of a reassembled…
5507 297.624997 172.20.10.2 149.154.167… TCP 281 61217 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=227 [TCP segment of a reassembled…
5508 297.625627 172.20.10.2 149.154.167… TCP 281 61216 → 80 [PSH, ACK] Seq=1 Ack=1 Win=65536 Len=227 [TCP segment of a reassembled…
Frame 18577: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{31CC1487-4A7A-4138-B288-F5A04BB66439}, id 0
Ethernet II, Src: ba:90:47:96:93:64 (ba:90:47:96:93:64), Dst: IntelCor_5e:12:f8 (3c:f8:62:5e:12:f8)
Internet Protocol Version 4, Src: 91.105.192.100, Dst: 172.20.10.2
Transmission Control Protocol, Src Port: 80, Dst Port: 61337, Seq: 1, Ack: 429, Len: 0
0000 3c f8 62 5e 12 f8 ba 90 47 96 93 64 08 00 45 00
0010 00 28 7a 2c 00 00 31 06 3d c0 5b 69 c0 64 ac 14
0020 0a 02 00 50 ef 99 2c 51 8e ed 8a 03 a3 1d 50 14
0030 08 43 fd 5f 00 00
wireshark_Wi-FiS2PPK1.pcapng
Пакеты: 25231 · Показаны: 163 (0.6%)
Профиль: Default

b.


*Wi-Fi
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь
eth.src == 3c:f8:62:5e:12:f8
No. Time Source Destination Protocol Length Info
17499 416.086923 172.20.10.2 51.158.165.… TCP 54 61325 → 10799 [ACK] Seq=1 Ack=1 Win=66048 Len=0
17500 416.087555 172.20.10.2 51.158.165.… TLSv1.3 594 Client Hello
17501 416.089036 172.20.10.2 239.255.255… SSDP 209 M-SEARCH * HTTP/1.1
17505 416.153040 172.20.10.2 51.158.165.… TLSv1.3 230 Application Data
17506 416.153237 172.20.10.2 51.158.165.… TLSv1.3 1209 Application Data
17509 416.155132 172.20.10.2 51.158.165.… TCP 54 61311 → 10799 [ACK] Seq=31141 Ack=13093 Win=65536 Len=0
17510 416.155581 172.20.10.2 51.158.165.… TLSv1.3 395 Application Data
17511 416.155841 172.20.10.2 51.158.165.… TLSv1.3 397 Application Data
17512 416.156274 172.20.10.2 51.158.165.… TLSv1.3 415 Application Data
17513 416.156905 172.20.10.2 51.158.165.… TLSv1.3 396 Application Data
17514 416.157394 172.20.10.2 51.158.165.… TLSv1.3 394 Application Data
17517 416.175780 172.20.10.2 51.158.165.… TLSv1.3 228 Application Data
17518 416.177429 172.20.10.2 51.158.165.… TLSv1.3 177 Application Data
17524 416.182108 172.20.10.2 51.158.165.… TCP 54 61325 → 10799 [ACK] Seq=541 Ack=4097 Win=66048 Len=0
17526 416.183947 172.20.10.2 51.158.165.… TCP 54 61325 → 10799 [ACK] Seq=541 Ack=4566 Win=65792 Len=0
17527 416.184394 172.20.10.2 51.158.165.… TLSv1.3 118 Change Cipher Spec, Application Data
17528 416.184708 172.20.10.2 51.158.165.… TLSv1.3 417 Application Data
17529 416.196058 172.20.10.2 51.158.165.… TLSv1.3 234 Application Data
Frame 18561: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{31CC1487-4A7A-4138-B288-F5A04BB66439}, id 0
Ethernet II, Src: IntelCor_5e:12:f8 (3c:f8:62:5e:12:f8), Dst: ba:90:47:96:93:64 (ba:90:47:96:93:64)
Destination: ba:90:47:96:93:64 (ba:90:47:96:93:64)
Source: IntelCor_5e:12:f8 (3c:f8:62:5e:12:f8)
Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 172.20.10.2, Dst: 91.105.192.100
Transmission Control Protocol, Src Port: 61336, Dst Port: 443, Seq: 1, Ack: 1, Len: 0
0000 ba 90 47 96 93 64 3c f8 62 5e 12 f8 08 00 45 00
0010 00 28 d4 e9 40 00 41 06 93 02 ac 14 0a 02 5b 69
0020 c0 64 ef 98 01 bb 94 49 1d 9a 18 58 fb 5f 50 10
0030 01 00 26 01 00 00
Ethernet (eth), 14 byte(s)
Пакеты: 28017 · Показаны: 11734 (41.9%)
Профиль: Default

C.



3.c 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**, где ff:ff:ff:ff:ff:ff - адрес широковещательной рассылки.

Назначение нескольких широковещательных рассылок разных протоколов:

- **ARP (Address Resolution Protocol)** - протокол, используемый для связывания IP-адресов с MAC-адресами в локальной сети. Широковещательная рассылка ARP-запросов отправляется всем устройствам в сети для определения MAC-адреса устройства с определенным IP-адресом.
- **Domain Name System (DNS)** - протокол, используемый для разрешения доменных имен в IP-адреса. Широковещательная рассылка DNS-запросов отправляется всем устройствам в сети для получения соответствующих IP-адресов.
- **Протокол TCP (Transmission Control Protocol)** является протоколом транспортного уровня, который не использует широковещательные рассылки напрямую. Однако, при работе с протоколами прикладного уровня, такими как DNS, могут использоваться широковещательные рассылки.

3.d Определить адреса, на которые поступают данные кадры и пакеты для канального и сетевого уровня.

3.e Напишите фильтры для каждой из трех широковещательных рассылок, выбранных в пункте 3-c.

- Для канального уровня:
  eth.dst == ff:ff:ff:ff:ff:ff && <protocol>
  eth.src == ff:ff:ff:ff:ff:ff && <protocol>
- Для сетевого уровня: ip.dst, ip.src.
  ip.dst == <ip address> && <protocol>
  ip.src == <ip address> && <protocol>

3.f На основании собранной статистики и анализа адресов определить, к какому типу коммутационного оборудования подключен используемый компьютер (концентратор, коммутатор или маршрутизатор).

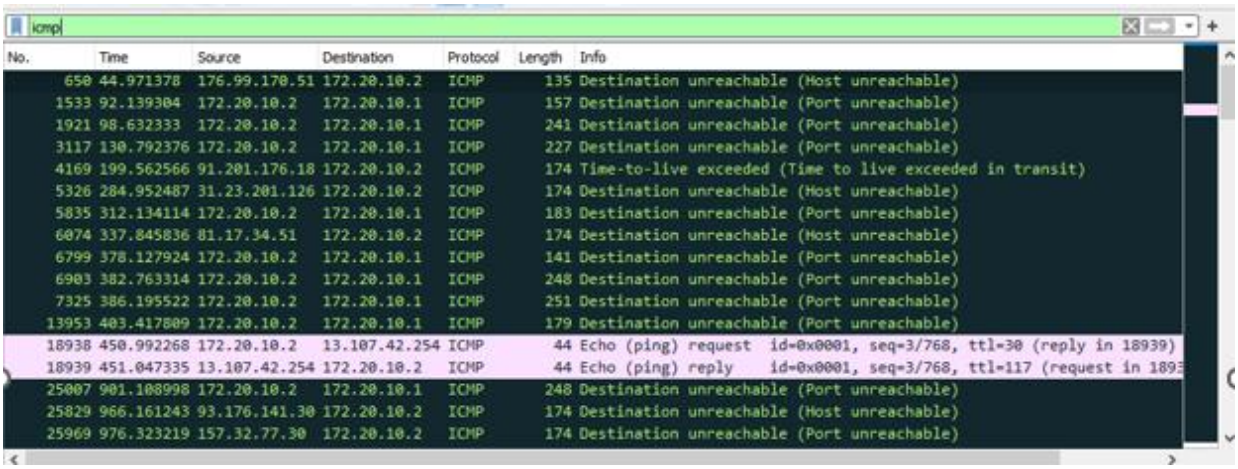
- Если на компьютер подключен концентратор, то в статистике должно быть много широковещательного трафика и мало трафика с уникальными адресами.
- Если на компьютер подключен коммутатор, то в статистике должно быть мало широковещательного трафика и много трафика с уникальными адресами.
- Если на компьютер подключен маршрутизатор, то в статистике должны быть разные сети и много трафика с разными адресами.

⇨ **Маршрутизатор**

4.

```
[root@localhost ~]# mtr -rw -c 111 -b ya.ru > mtr_report_ya
[root@localhost ~]# cat mtr_report_ya
Start: Thu Feb 29 13:18:31 2024
HOST: localhost.localdomain   Loss%   Snt   Last   Avg  Best  Wrst StDev
  1.|-- _gateway (10.0.2.2)     0.0%   111    0.3   0.4   0.2   1.3   0.2
  2.|-- 172.16.0.1              0.9%   111   17.8  42.5  14.5 405.0  51.1
  3.|-- 172.68.9.1               0.9%   111   22.7  40.5  14.9 280.5  42.9
  4.|-- 109.239.136.76           0.9%   111   25.5  48.6  15.7 414.0  52.7
  5.|-- ???                     100.0   111    0.0   0.0   0.0   0.0   0.0
  6.|-- ya.ru (87.250.250.242)  0.0%   111   31.6  46.8  17.6 533.4  67.9
```

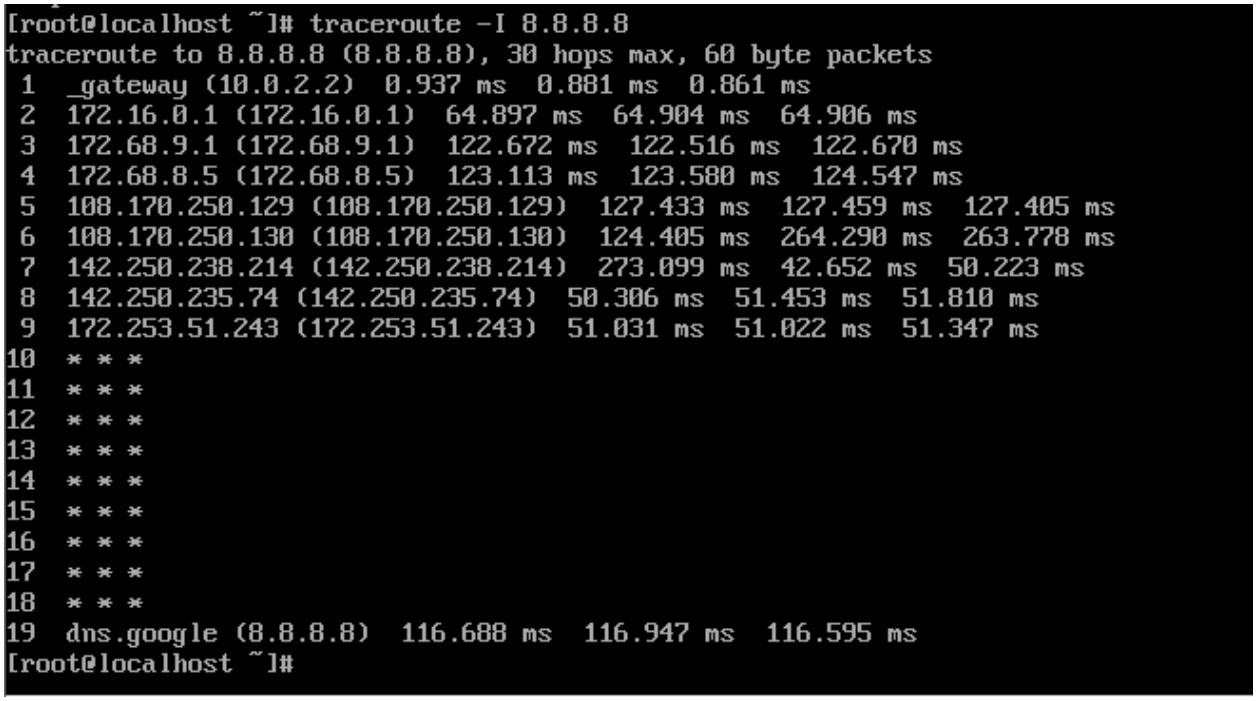
5.



No.	Time	Source	Destination	Protocol	Length	Info
650	44.971378	176.99.170.51	172.20.10.2	ICMP	135	Destination unreachable (Host unreachable)
1533	92.139304	172.20.10.2	172.20.10.1	ICMP	157	Destination unreachable (Port unreachable)
1921	98.632333	172.20.10.2	172.20.10.1	ICMP	241	Destination unreachable (Port unreachable)
3117	130.792376	172.20.10.2	172.20.10.1	ICMP	227	Destination unreachable (Port unreachable)
4169	199.562566	91.201.176.18	172.20.10.2	ICMP	174	Time-to-live exceeded (Time to live exceeded in transit)
5326	284.952487	31.23.201.126	172.20.10.2	ICMP	174	Destination unreachable (Host unreachable)
5835	312.134114	172.20.10.2	172.20.10.1	ICMP	183	Destination unreachable (Port unreachable)
6074	337.845836	81.17.34.51	172.20.10.2	ICMP	174	Destination unreachable (Host unreachable)
6799	378.127924	172.20.10.2	172.20.10.1	ICMP	141	Destination unreachable (Port unreachable)
6903	382.763314	172.20.10.2	172.20.10.1	ICMP	248	Destination unreachable (Port unreachable)
7325	386.195522	172.20.10.2	172.20.10.1	ICMP	251	Destination unreachable (Port unreachable)
13953	403.417809	172.20.10.2	172.20.10.1	ICMP	179	Destination unreachable (Port unreachable)
18938	450.992268	172.20.10.2	13.107.42.254	ICMP	44	Echo (ping) request id=0x0001, seq=3/768, ttl=30 (reply in 18939)
18939	451.047335	13.107.42.254	172.20.10.2	ICMP	44	Echo (ping) reply id=0x0001, seq=3/768, ttl=117 (request in 1893
25007	901.108998	172.20.10.2	172.20.10.1	ICMP	248	Destination unreachable (Port unreachable)
25829	966.161243	93.176.141.30	172.20.10.2	ICMP	174	Destination unreachable (Host unreachable)
25969	976.323219	157.32.77.30	172.20.10.2	ICMP	174	Destination unreachable (Port unreachable)

4. Тексты команд и консольный вывод из Части 4, п.2.

маршрут до хоста 8.8.8.8 с помощью ICMP

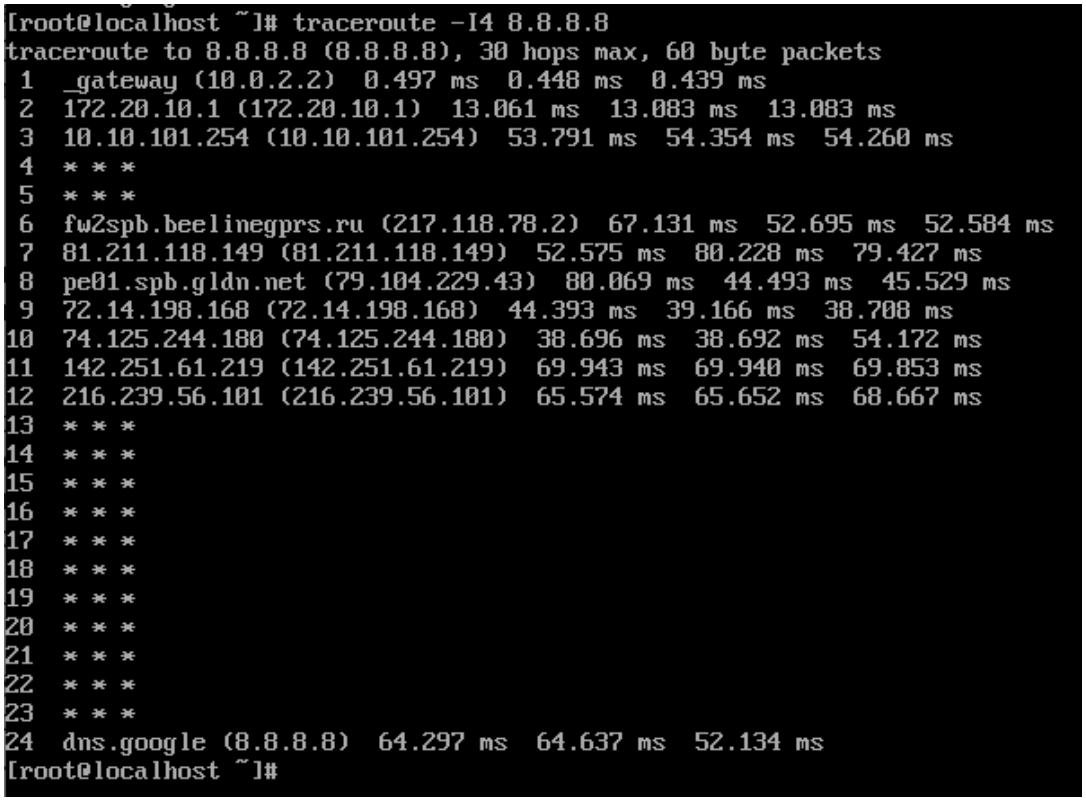


маршрут до хоста 8.8.8.8 с помощью UDP

```
[root@localhost ~]# traceroute -U 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.2)  2.506 ms  2.460 ms  2.107 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  * * *
[root@localhost ~]#
```

маршрут до хоста 8.8.8.8 с помощью TCP

Ipv4

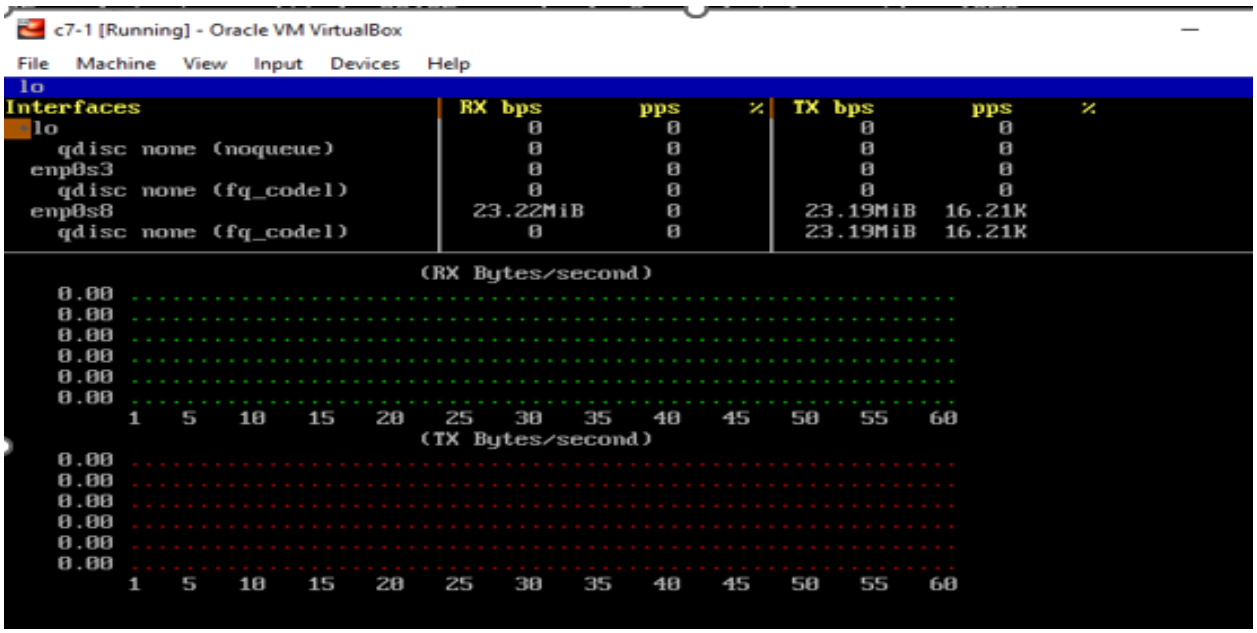


Линь

5. Тексты команд и консольный вывод из Части 5, п.2.

```
[root@localhost ~]# ping -f 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
_
```

```
[root@localhost ~]# ping 10.0.2.15 -f -s 100
PING 10.0.2.15 (10.0.2.15) 100(128) bytes of data.
^C
--- 10.0.2.15 ping statistics ---
2163783 packets transmitted, 2163783 received, 0% packet loss, time 20828ms
rtt min/avg/max/mdev = 0.003/0.003/0.514/0.003 ms, ipg/ewma 0.009/0.003 ms
[root@localhost ~]# ping 10.0.2.15 -f -s 10100
PING 10.0.2.15 (10.0.2.15) 10100(10128) bytes of data.
.^
--- 10.0.2.15 ping statistics ---
289791 packets transmitted, 289791 received, 0% packet loss, time 4464ms
rtt min/avg/max/mdev = 0.004/0.005/0.254/0.003 ms, ipg/ewma 0.015/0.004 ms
[root@localhost ~]# ping 10.0.2.15 -f -s 20100
PING 10.0.2.15 (10.0.2.15) 20100(20128) bytes of data.
.^
--- 10.0.2.15 ping statistics ---
103710 packets transmitted, 103710 received, 0% packet loss, time 2166ms
rtt min/avg/max/mdev = 0.005/0.006/0.226/0.004 ms, ipg/ewma 0.020/0.006 ms
[root@localhost ~]# ping 10.0.2.15 -f -s 30100
PING 10.0.2.15 (10.0.2.15) 30100(30128) bytes of data.
^C
--- 10.0.2.15 ping statistics ---
74579 packets transmitted, 74579 received, 0% packet loss, time 1944ms
rtt min/avg/max/mdev = 0.007/0.008/0.255/0.004 ms, ipg/ewma 0.026/0.008 ms
[root@localhost ~]# ping 10.0.2.15 -f -s 40100
PING 10.0.2.15 (10.0.2.15) 40100(40128) bytes of data.
.^
--- 10.0.2.15 ping statistics ---
50739 packets transmitted, 50739 received, 0% packet loss, time 1631ms
rtt min/avg/max/mdev = 0.008/0.009/0.245/0.005 ms, ipg/ewma 0.032/0.009 ms
[root@localhost ~]# ping 10.0.2.15 -f -s 50100
PING 10.0.2.15 (10.0.2.15) 50100(50128) bytes of data.
^C
--- 10.0.2.15 ping statistics ---
33195 packets transmitted, 33195 received, 0% packet loss, time 1259ms
rtt min/avg/max/mdev = 0.009/0.010/0.255/0.006 ms, ipg/ewma 0.037/0.014 ms
[root@localhost ~]# _
```



6. **Тексты команд и консольный вывод из Части 6, п.4.**

```
[root@localhost ~]# ping 10.0.2.15 -f -c 500
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
500 packets transmitted, 500 received, 0% packet loss, time 4ms
rtt min/avg/max/mdev = 0.003/0.003/0.041/0.003 ms, ipg/ewma 0.009/0.003 ms
[root@localhost ~]#
```

```
[root@localhost ~]# vnstat -i enp0s3
Database updated: Wed Feb 28 16:36:55 2024

   enp0s3 since 02/28/2024

          rx:  1 KiB      tx:  1 KiB      total:  2 KiB

   monthly
                     rx      |     tx      |    total    |   avg. rate
     ------------------------+-------------+-------------+---------------
       Feb '24         1 KiB |       1 KiB |       2 KiB |    0.00 kbit/s
     ------------------------+-------------+-------------+---------------
     estimated         --    |      --     |      --     |

   daily
                     rx      |     tx      |    total    |   avg. rate
     ------------------------+-------------+-------------+---------------
         today         1 KiB |       1 KiB |       2 KiB |    0.00 kbit/s
     ------------------------+-------------+-------------+---------------
     estimated         --    |      --     |      --     |
[root@localhost ~]#
```

7. **Тексты команд и консольный вывод (или его часть) из Части 7, п.2-4, 8,9.**

```
[root@localhost ~]# ssh root@10.0.2.15
root@10.0.2.15's password:
Last login: Wed Feb 28 16:46:29 2024 from 10.0.2.15
[root@localhost ~]# _
```

```
[root@localhost ~]# netstat -plnt
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN      1310/master
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      996/sshd
tcp6       0      0 ::1:25                  :::*                    LISTEN      1310/master
tcp6       0      0 :::22                   :::*                    LISTEN      996/sshd
[root@localhost ~]# _
```

```
[root@localhost ~]# netstat -apn | grep ':22' | awk '{print $5}' | cut -d: -f1 | uniq -c
      1 0.0.0.0
      6 10.0.2.15
      1
[root@localhost ~]# _
```

```
[root@localhost ~]# netstat -tuna | grep ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.15:43354         ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.15:43352         ESTABLISHED
tcp        0      0 10.0.2.15:43350         10.0.2.15:22            ESTABLISHED
tcp        0      0 10.0.2.15:43354         10.0.2.15:22            ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.15:43350         ESTABLISHED
tcp        0      0 10.0.2.15:43352         10.0.2.15:22            ESTABLISHED
[root@localhost ~]# netstat -tun state eastablished
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.2.15:22            10.0.2.15:43354         ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.15:43352         ESTABLISHED
tcp        0      0 10.0.2.15:43350         10.0.2.15:22            ESTABLISHED
tcp        0      0 10.0.2.15:43354         10.0.2.15:22            ESTABLISHED
tcp        0      0 10.0.2.15:22            10.0.2.15:43350         ESTABLISHED
tcp        0      0 10.0.2.15:43352         10.0.2.15:22            ESTABLISHED
[root@localhost ~]#
```

```
top - 17:09:57 up  1:13,  1 user,  load average: 0.00, 0.01, 0.05
Tasks:  92 total,   1 running,  90 sleeping,   1 stopped,   0 zombie
%Cpu(s):  0.0 us,  0.0 sy,  0.0 ni,100.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  1882084 total,  1545396 free,   193208 used,   143480 buff/cache
KiB Swap:  2097148 total,  2097148 free,        0 used.  1539144 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
    1 root      20   0  128024   6640   4156 S   0.0  0.4   0:01.08 systemd
    2 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kthreadd
    4 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kworker/0:0H
    5 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kworker/u2:0
    6 root      20   0       0      0      0 S   0.0  0.0   0:00.06 ksoftirqd/0
    7 root      rt   0       0      0      0 S   0.0  0.0   0:00.00 migration/0
    8 root      20   0       0      0      0 S   0.0  0.0   0:00.00 rcu_bh
    9 root      20   0       0      0      0 S   0.0  0.0   0:00.59 rcu_sched
   10 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 lru-add-drain
   11 root      rt   0       0      0      0 S   0.0  0.0   0:00.03 watchdog/0
   13 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kdevtmpfs
   14 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 netns
   15 root      20   0       0      0      0 S   0.0  0.0   0:00.00 khungtaskd
   16 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 writeback
   17 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kintegrityd
   18 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 bioset
   19 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 bioset
   20 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 bioset
   21 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kblockd
   22 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 md
   23 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 edac-poller
   24 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 watchdogd
   30 root      20   0       0      0      0 S   0.0  0.0   0:00.00 kswapd0
   31 root      25   5       0      0      0 S   0.0  0.0   0:00.00 ksmd
   32 root      39  19       0      0      0 S   0.0  0.0   0:00.02 khugepaged
   33 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 crypto
   41 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kthrotld
   43 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kmpath_rdacd
   44 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kaluad
   45 root       0 -20       0      0      0 S   0.0  0.0   0:00.00 kpsmoused
```

8. Тексты команд из части 8, п. 1-3, и, если выполнялся, п.4

1

```
[root@localhost ~]# sudo tcpdump -i enp0s3 -A 'port 9999 or port 4444'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
```

2

```
[root@localhost ~]# nc -w 5 10.0.2.15 9999 < file.txt
```

```
[root@localhost ~]# nc -l 9999 > received_file.txt
```

3

```
[root@localhost ~]# cat received_file.txt
Name: Duong Thi Hue Linh
Group: M33091
Dec: sbdfhg sfauf suafg asfhua ahsfua agsf agf agsf asgf fhsa hasjfh
[root@localhost ~]# _
```

4

```
[root@localhost ~]# nc -u -l -p 4444
Hi! How are you?
Fine! And you?
So am i!
```

5

```
[root@localhost ~]# nc -l -p 4445 -e /bin/bash
```

```
[root@localhost ~]# nc 10.0.2.15 4445
host name
localhost.localdomain
uname -r
4.18.0-483.el8.x86_64
hostname -I
10.0.2.15
```

Вопросы и задания

1. **По какому протоколу работает утилита *mtr*? Как вы это определили?**

   Internet Control Message Protocol (ICMP)

   mtr – это альтернатива программе traceroute. Объединяя функции ping и traceroute, mtr позволяет постоянно опрашивать удаленный сервер и отслеживать изменения задержки и производительности с течением времени.

2. **Опишите значения столбцов статистики, выводимой утилитой mtr.**

   Loss% - показывает процент потери пакетов на каждом переходе
   Snt подсчитывается количество отправленных пакетов.
   Last, Avg, Best и Wrst - все измерения задержки в миллисекундах
   Last - это задержка последнего отправленного пакета
   Avg - это средняя задержка всех пакетов, в то время как Best и Wrst отображают лучшее (самое короткое) и худшее (самое длинное) время приема-передачи для пакета к этому хосту
   В большинстве случаев в центре внимания должен быть средний столбец Avg. Последний столбец, StDev, предоставляет стандартное отклонение задержек для каждого хоста. Чем выше стандартное отклонение, тем больше разница между измерениями задержки.

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

Кадр	Протоколы
Ethernet II	IPX, IP, Apple Talk Phase I
Ethernet 802.3	IPX
Ethernet 802.2	IPX, FTAM
Ethernet SNAP	IPX, IP, Apple Talk Phase II

   Отличаются полями заголовка. Разные типы кадра имеют различный формат и значение MTU. В компьютерных сетях термин Maximum Transmission Unit (MTU) используется для определения максимального размера блока (в байтах), который может быть передан на канальном уровне сетевой модели OSI.

4. **Какой тип кадров Ethernet используется в анализируемой сети? Почему именно он?**

   Ethernet II. В нем есть поле для указания типа протокола верхнего уровня

5. **Как можно определить тип используемого коммутационного оборудования, используя сетевую статистику? Какой тип коммутационного оборудования использовался в сети?**

   Используя описание источников и адреса назначения, а так же используемые при передаче протоколы.

6. **На какие адреса сетевого уровня осуществляются широковещательные рассылки?**

   Используются широковещательные адреса, вид которых зависит от протокола. Так, в IP-сетях широковещательные адреса формируются следующим образом: к адресу подсети прибавляется побитовая инверсия маски подсети (то есть все биты адреса подсети, соответствующие нулям в маске, устанавливаются в «1»). Например, если адрес сети равен 192.168.0.0, маска подсети 255.255.255.0, то широковещательный адрес будет 192.168.0.255.

7. **На какой канальный адрес осуществляются широковещательные рассылки?**

   Используется широковещательный MAC-адрес FF:FF:FF:FF:FF:FF для передачи служебных датаграмм (например, ARP-запросов). Датаграммы, отправленные на такой адрес, принимаются всеми сетевыми устройствами локальной сети.

8. **Для чего применяются перехваченные широковещательные рассылки в Части 3 п. 3-е?**

   Большинство перехваченных передач предназначались для обнаружения устройств. В нашем случае MNDP (Mikrotik Network Discovery Protocol) использовался winbox для обнаружения сетевых устройств (Проверено специально).

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

   Поскольку большинство этих узлов находятся за фаерволами, защищающими от ненужного трафика и обеспечивающими безопасность, поэтому отображаются звезды. Лучшие результаты были получены при

использовании ICMP вместо UDP или TCP, поскольку он предназначен для диагностики сети и разрешен большинством фаерволов

10. Какая из утилит из Части 5 вам больше понравилась? Почему?

По нашему мнению, bmon был лучшим, поскольку он отображает информацию в более организованном виде, в остальном все они служат одной цели.ss

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

Линейно

12. На каком уровне модели OSI работает vnstat?

vnstat не является обычным монитором трафика, он использует статистику, предоставляемую кернелом в качестве источника информации, поэтому если мы действительно должны поместить его в модель OSI, то он будет находиться на уровне приложений (уровень 7).

13. Как с помощью утилиты ip просмотреть arp-кэш и как его очистить. В каких случаях может понадобиться последняя операция?

Очистка: arp –d или netsh interface ip delete arpcache или ip route flush

14. Напишите команду tcpdump, выводящую все пакеты с хоста 192.168.0.254 и содержащего udp или идущего на tcp порт 80.

tcpdump src 192.168.9.254 and udp or port 80