

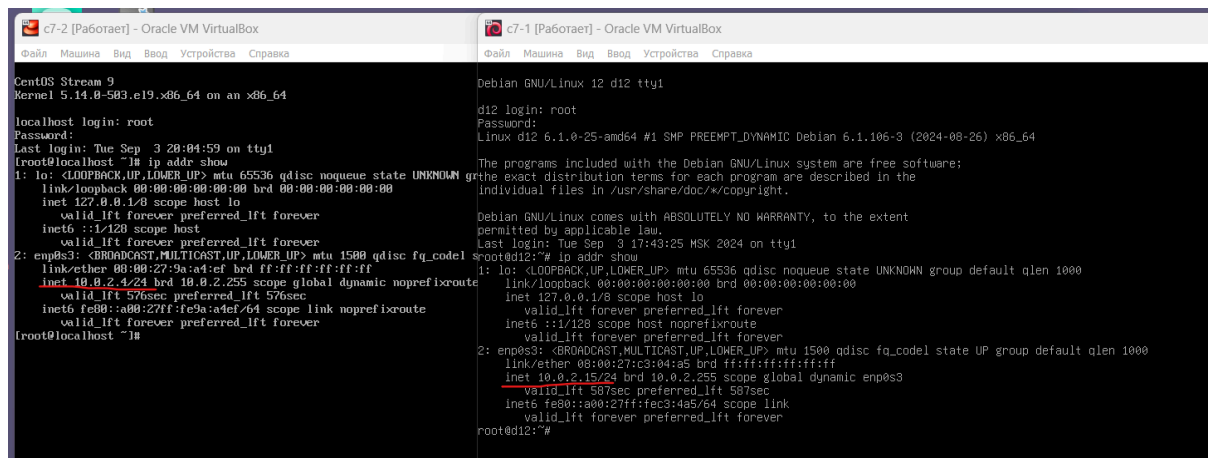
Лабораторная работа №3. Мониторинг сетевого трафика на хосте на
примере работы с
утилитами диагностики и мониторинга сетевых соединений в Linux

Выполнили студенты группы М3311
Авсюкевич Анастасия
Худашов Богдан

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.

Артефакты:

Часть 1 пункт 3:



The screenshot shows two side-by-side Oracle VM VirtualBox windows. The left window is titled 'c7-2 [Работает] - Oracle VM VirtualBox' and displays the CentOS Stream 9 network configuration. The right window is titled 'c7-1 [Работает] - Oracle VM VirtualBox' and displays the Debian GNU/Linux 12 network configuration.

```
CentOS Stream 9
Kernel 5.14.0-503.el9.x86_64 on an x86_64

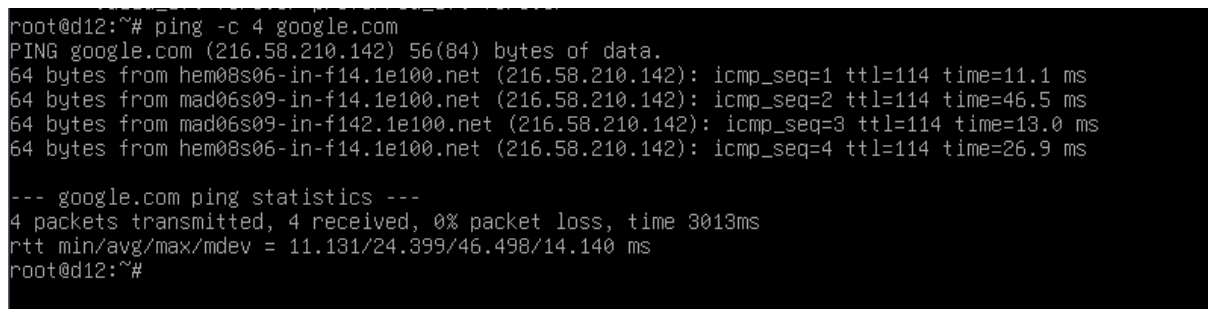
localhost login: root
Password:
Last login: Tue Sep 3 20:04:59 on tty1
[root@localhost ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:9a:a4:ef brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute
        valid_lft 576sec preferred_lft 576sec
    inet6 fe80::a00:27ff:fe9a:a4ef/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@localhost ~]#
```

```
Debian GNU/Linux 12 d12 tty1
d12 login: root
Password:
Linux d12 6.1.0-25-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.106-3 (2024-08-26) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Sep 3 17:43:25 MSK 2024 on tty1
root@d12:~# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:c3:04:a5 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute
        valid_lft 576sec preferred_lft 576sec
    inet6 fe80::a00:27ff:fec3:4a5/64 scope link
        valid_lft forever preferred_lft forever
root@d12:~#
```

Часть 1 пункт 5:

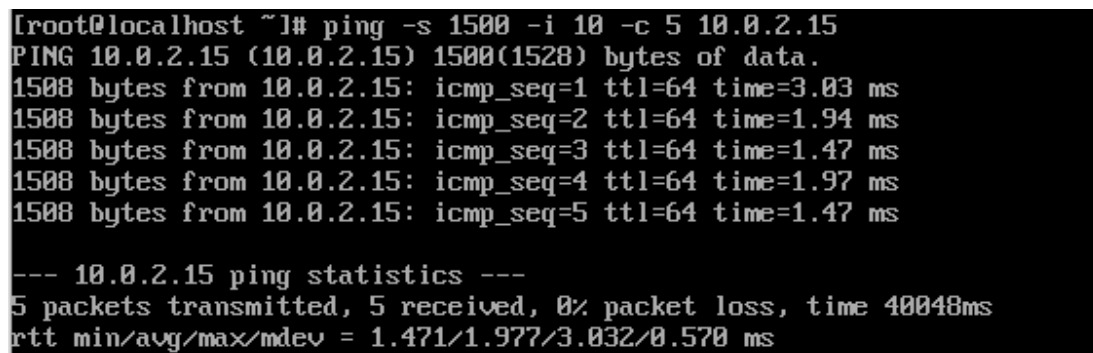


The screenshot shows a terminal window with the output of a ping command and its statistics.

```
root@d12:~# ping -c 4 google.com
PING google.com (216.58.210.142) 56(84) bytes of data.
64 bytes from hem08s06-in-f14.1e100.net (216.58.210.142): icmp_seq=1 ttl=114 time=11.1 ms
64 bytes from mad06s09-in-f14.1e100.net (216.58.210.142): icmp_seq=2 ttl=114 time=46.5 ms
64 bytes from mad06s09-in-f142.1e100.net (216.58.210.142): icmp_seq=3 ttl=114 time=13.0 ms
64 bytes from hem08s06-in-f14.1e100.net (216.58.210.142): icmp_seq=4 ttl=114 time=26.9 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3013ms
rtt min/avg/max/mdev = 11.131/24.399/46.498/14.140 ms
root@d12:~#
```

1. Тексты команд, консольный вывод и полученный файл из Части 2. п. 2,6



The screenshot shows a terminal window with the output of a ping command and its statistics.

```
[root@localhost ~]# ping -s 1500 -i 10 -c 5 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 1500(1528) bytes of data.
1500 bytes from 10.0.2.15: icmp_seq=1 ttl=64 time=3.03 ms
1500 bytes from 10.0.2.15: icmp_seq=2 ttl=64 time=1.94 ms
1500 bytes from 10.0.2.15: icmp_seq=3 ttl=64 time=1.47 ms
1500 bytes from 10.0.2.15: icmp_seq=4 ttl=64 time=1.97 ms
1500 bytes from 10.0.2.15: icmp_seq=5 ttl=64 time=1.47 ms

--- 10.0.2.15 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 40048ms
rtt min/avg/max/mdev = 1.471/1.977/3.032/0.570 ms
```

Пункт 3:

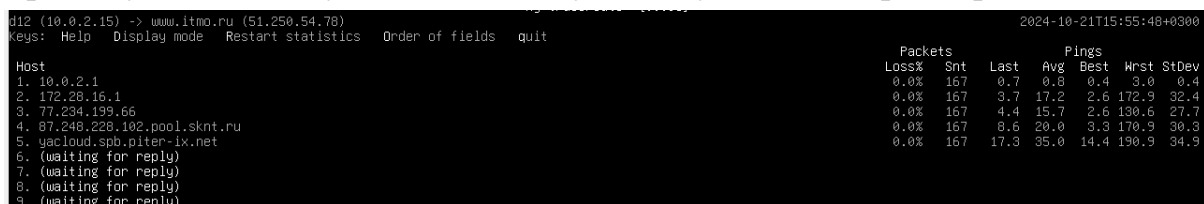
Ключ `-f` в утилите `ping` используется для отправки пакетов в "flood" режиме, что означает, что пакеты будут отправляться максимально быстро, без ожидания ответа. Это может быть полезно для тестирования пропускной способности сети, но также может перегружать сеть и целевой хост.

Пункт 4:

`mtr www.itmo.ru`

Пункт 5:

При запуске `mtr`, вы увидите таблицу с следующими параметрами:



```


d12 (10.0.2.15) -> www.itmo.ru (51.250.54.78) 2024-10-21T15:55:48+0300
keys: Help Display mode Restart statistics Order of fields quit

Host                                     Packets  Loss%  Snt  Last  Avg  Best  Wrst  StDev
1. 10.0.2.1                             0.0%    167   0.7   0.8   0.4   3.0   0.4
2. 172.28.16.1                           0.0%    167   3.7  17.2   2.6  172.9  32.4
3. 77.234.199.66                         0.0%    167   4.4  15.7   2.6  130.6  27.7
4. 87.248.228.102.pool.sknt.ru           0.0%    167   8.6  20.0   3.3  170.9  30.3
5. yacloud.spb.piter-ix.net              0.0%    167  17.3  35.0  14.4  190.9  34.9
6. (waiting for reply)
7. (waiting for reply)
8. (waiting for reply)
9. (waiting for reply)
```

1. Host: имя узла или IP-адрес.
2. Loss%: процент потерянных пакетов.
3. Snt: количество отправленных пакетов.
4. Last: время последнего ответа от узла.
5. Avg: среднее время ответа.
6. Best: лучшее время ответа.
7. Wrst: худшее время ответа.
8. StDev: стандартное отклонение времени ответа.

Эти параметры помогают анализировать качество соединения и выявлять проблемы в сети.

Пункт 6:



```

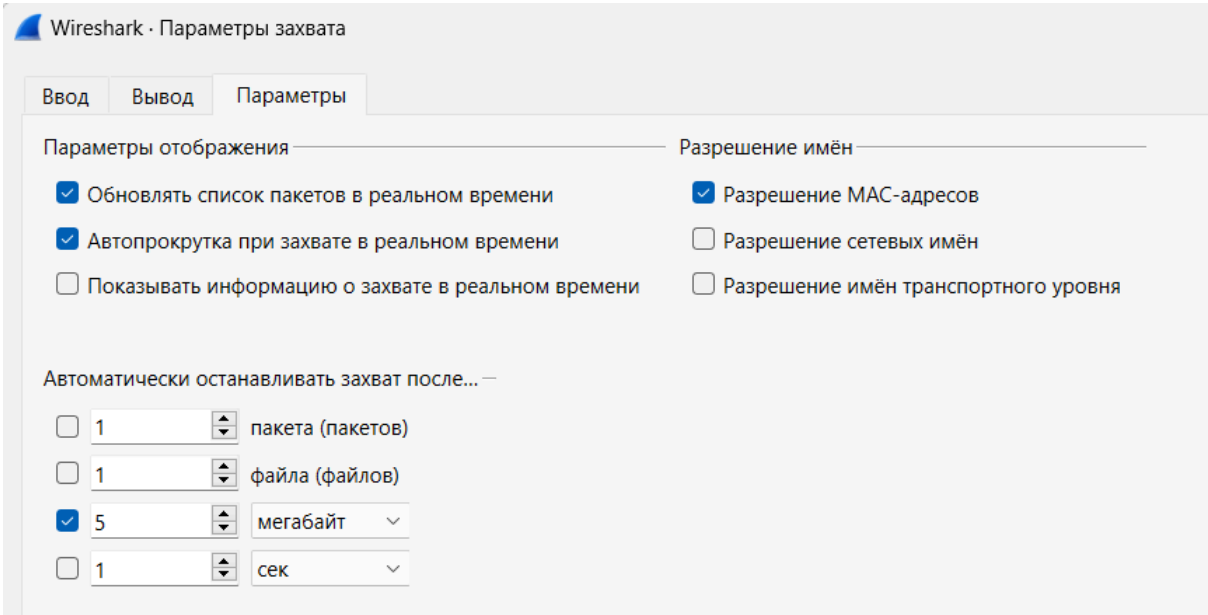
root@d12:~# mtr -r -c 40 www.itmo.ru > mtr_statistic.txt
```

`-r`: режим отчета (report mode), который выводит результаты в более компактном формате.

Результат:

```
root@d12:~# cat mtr_statistic.txt
Start: 2024-10-21T15:57:47+0300
HOST: d12
Loss%  Snt  Last   Avg    Best  Wrst  StDev
1. |-- 10.0.2.1      0.0%   40    0.7    0.8    0.4    1.4    0.2
2. |-- 172.28.16.1   0.0%   40    4.0   22.8    2.6   440.4   71.7
3. |-- 77.234.199.66 0.0%   40    5.6   22.1    3.3   381.3   61.9
4. |-- 87.248.228.102.pool.sknt. 0.0%   40   10.0   28.1    3.3   329.4   58.5
5. |-- yacloud.spb.piter-ix.net 0.0%   40   21.2   35.1   15.3   270.0   46.2
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 0.0%   40   24.6   53.4   23.7   566.0   88.9
```

2. Графики, тексты фильтров и ответы на вопросы из Части 3. п. 2-3.
Пункт 1:



Пункт 2а:
Фильтр по байтам

Ethernet · 15		IPv4 · 82		IPv6 · 5	TCP · 305	UDP · 37		
Адрес	Пакеты	Байты	Пакетов отправлено	Байтов отправлено	Пакетов получено	Байтов получено	Страна	
192.168.8.185	8 250	5 МБ	4 427	1 МБ	3 823	4 МБ		
82.202.230.55	671	768 кБ	523	749 кБ	148	19 кБ		

Пункт 2b:

Фильтр: eth.dst == ff:ff:ff:ff:ff:ff и кол-во пакетов

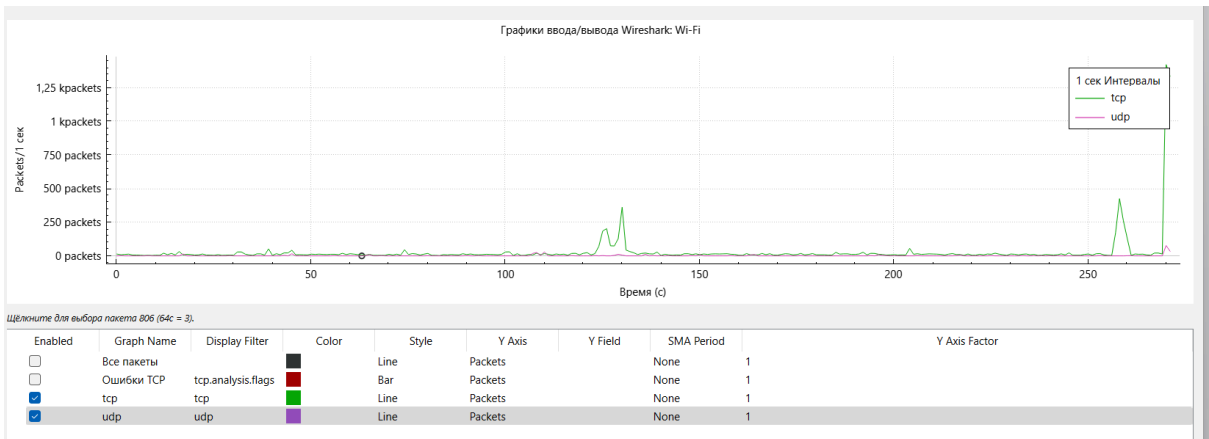
Ethernet · 16		IPv4 · 81	IPv6 · 4	TCP · 234	UDP · 22			
Адрес А	Адрес В	Пакеты	Байт	ИД потока	Packets A → B	Bytes A → B	Packets B → A	
e0:d4:e8:f1:c9:35	4c:5e:0c:5e:e4:89	8 264	5 МБ	0	4 426	1 МБ	3 838	
00:08:9b:c5:6c:31	01:00:5e:7f:ff:fa	15	4 кБ	5	15	4 кБ	0	
e0:d4:e8:f1:c9:35	33:33:00:00:00:fb	8 884 байты		7	8	884 байты	0	
e0:d4:e8:f1:c9:35	01:00:5e:00:00:fb	8 724 байты		6	8	724 байты	0	
e0:d4:e8:f1:c9:35	01:00:5e:00:00:fc	6 305 байты		3	6	305 байты	0	
4c:5e:0c:5e:e4:89	ff:ff:ff:ff:ff:ff	5 820 байты		1	5	820 байты	0	
e0:d4:e8:f1:c9:35	33:33:00:00:00:16	5 450 байты		10	5	450 байты	0	
00:08:9b:c5:6c:31	01:00:5e:00:00:fb	3 576 байты		4	3	576 байты	0	
00:08:9b:c5:6c:31	ff:ff:ff:ff:ff:ff	2 496 байты		14	2	496 байты	0	
0c:4d:e9:b9:8c:78	01:00:5e:00:00:fb	2 166 байты		8	2	166 байты	0	
e0:d4:e8:f1:c9:35	01:00:5e:00:00:02	2 92 байты		11	2	92 байты	0	
4c:5e:0c:5e:e4:89	01:00:5e:00:00:01	2 84 байты		2	2	84 байты	0	

Пункт 2с:

Фильтр: tcp и кол-во пакетов

Ethernet · 16		IPv4 · 81	IPv6 · 4	TCP · 234	UDP · 22								
Адрес А	Порт А	Адрес В	Порт В	Пакеты	Байт	ИД потока	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Отн. время начала	Продолж	
192.168.8.185	50614	82.202.230.55	443	671	768 кБ	184	148	19 кБ	523	749 кБ	270.252472	1.0	
192.168.8.185	49884	172.64.41.4	443	527	105 кБ	12	270	36 кБ	257	70 кБ	6.519743	264.	
192.168.8.185	50498	87.248.204.0	80	405	467 кБ	85	89	6 кБ	316	461 кБ	129.453496	30.	
192.168.8.185	50492	213.155.157.168	80	355	348 кБ	79	99	16 кБ	256	333 кБ	125.166989	2.7	
192.168.8.185	50641	5.255.255.77	443	324	311 кБ	199	78	6 кБ	246	304 кБ	270.588287	0.5	

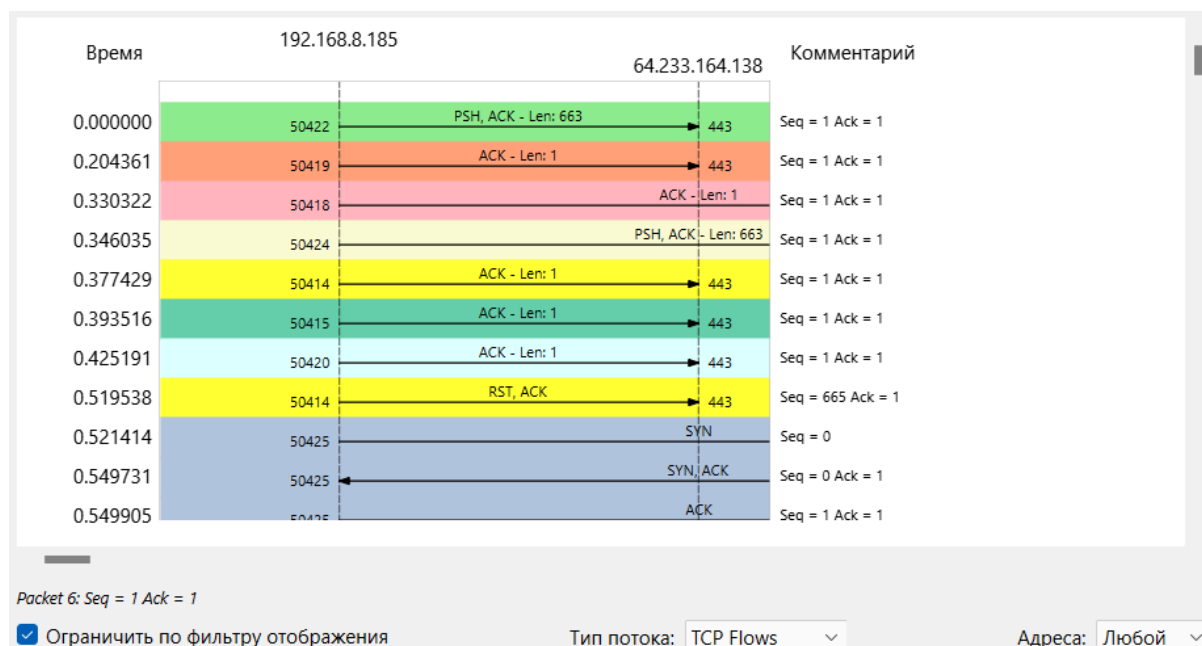
Пункт 2д:



Почти все 5мб в одну секунду загрузились в конце, это был пик активности в виде открывания страниц в браузере.

Пункт 2е:

Фильтр: tcp.port == 443



АСК означает, что машина, отправляющая пакет с АСК, подтверждает данные, которые она получила от другой машины. В TCP, как только соединение установлено, *все* пакеты, отправленные любой из сторон, будут содержать АСК, даже если это просто повторное подтверждение данных, которые уже подтверждены.

PSH — это указание отправителя, что если реализация TCP принимающей машины еще не предоставила полученные данные коду, который считывает данные

Пункт 3a:

`udp.port==53 || tcp.port==53 && ip.src == [номер ip]`

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка						
(udp.port == 53 or tcp.port == 53) and (ip.src == 192.168.8.185)						
No.	Time	Source	Destination	Protocol	Length	Info
498	43.299617	192.168.8.185	192.168.8.1	DNS	70	Standard query 0xaea4 A c.pki.goog
1583	123.674958	192.168.8.185	192.168.8.1	DNS	86	Standard query 0xa05c A fe2cr.update.microsoft.com
1693	125.156376	192.168.8.185	192.168.8.1	DNS	86	Standard query 0x60b1 A download.windowsupdate.com
2156	128.504353	192.168.8.185	192.168.8.1	DNS	92	Standard query 0xf535 A geo.prod.do.dsp.mp.microsoft.com
2180	128.787206	192.168.8.185	192.168.8.1	DNS	94	Standard query 0x54ea A kv601.prod.do.dsp.mp.microsoft.com
2220	129.050145	192.168.8.185	192.168.8.1	DNS	94	Standard query 0x88a1 A cp601.prod.do.dsp.mp.microsoft.com
2260	129.424658	192.168.8.185	192.168.8.1	DNS	89	Standard query 0xf2d3 A au.download.windowsupdate.com
2286	129.762073	192.168.8.185	192.168.8.1	DNS	89	Standard query 0xeb2b A v10.events.data.microsoft.com

Порт 53 - DNS порт

Пункт 3b:

`eth.src==[MAC-адрес]`

No.	Time	Source	Destination	Protocol	Length	Info
1577	122.693185	192.168.8.185	64.233.164.102	TCP	55	[TCP Spurious Retransmission] 50483 → 443 [ACK] Seq=0 Ack=1 Win=13...
1578	122.853881	192.168.8.185	64.233.164.102	TCP	717	[TCP Retransmission] 50488 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131072...
1579	123.038133	192.168.8.185	64.233.164.138	TCP	55	[TCP Spurious Retransmission] 50484 → 443 [ACK] Seq=0 Ack=1 Win=13...
1580	123.062621	192.168.8.185	64.233.164.138	TCP	55	[TCP Spurious Retransmission] 50481 → 443 [ACK] Seq=0 Ack=1 Win=13...
1581	123.110234	192.168.8.185	64.233.164.138	TCP	55	[TCP Spurious Retransmission] 50480 → 443 [ACK] Seq=0 Ack=1 Win=13...
1582	123.671656	192.168.8.185	64.233.164.102	TCP	55	[TCP Spurious Retransmission] 50482 → 443 [ACK] Seq=0 Ack=1 Win=13...
1583	123.674958	192.168.8.185	192.168.8.1	DNS	86	Standard query 0xa05c A fe2cr.update.microsoft.com
1584	123.687267	192.168.8.185	64.233.164.102	TCP	717	[TCP Retransmission] 50489 → 443 [PSH, ACK] Seq=1 Ack=1 Win=131072...
1586	123.694687	192.168.8.185	52.152.180.158	TCP	66	50491 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
1587	123.703240	192.168.8.185	64.233.164.102	TCP	55	[TCP Spurious Retransmission] 50483 → 443 [ACK] Seq=0 Ack=1 Win=13...
1589	123.820865	192.168.8.185	52.152.180.158	TCP	54	50491 → 443 [ACK] Seq=1 Ack=1 Win=131328 Len=0
1590	123.822859	192.168.8.185	52.152.180.158	TLSv1.2	263	Client Hello (SNI=fe2cr.update.microsoft.com)
1591	123.849517	192.168.8.185	172.64.41.4	TLSv1.2	93	Application Data
1593	123.941267	192.168.8.185	172.64.41.4	TCP	54	49884 → 443 [ACK] Seq=1799 Ack=4775 Win=511 Len=0

> Frame 1583: 86 bytes on wire (688 bits), 86 bytes captured (688 bits) on interface 0
 > Ethernet II, Src: Intel_f1:c9:35 (e0:d4:e8:f1:c9:35), Dst: Routerboardc_5e:00:00:00:00:00
 > Internet Protocol Version 4, Src: 192.168.8.185, Dst: 192.168.8.1
 > User Datagram Protocol, Src Port: 63530, Dst Port: 53
 > Domain Name System (query)

Пункт 3с:

eth.dst == ff:ff:ff:ff:ff:ff

No.	Time	Source	Destination	Protocol	Length	Info
220	20.499075	192.168.8.1	255.255.255.255	MNDP	164	5678 → 5678 Len=122
1008	80.501733	192.168.8.1	255.255.255.255	MNDP	164	5678 → 5678 Len=122
2950	140.522855	192.168.8.1	255.255.255.255	MNDP	164	5678 → 5678 Len=122
3175	158.185706	Sonos_c4:5c:4a	Broadcast	ARP	60	ARP Announcement for 192.168.8.188
3685	198.376824	192.168.8.10	192.168.8.255	BROWSER	248	Local Master Announcement MYNAS, Workstation, Server, Print Queue
3686	198.376824	192.168.8.10	192.168.8.255	BROWSER	248	Domain/Workgroup Announcement NAS, NT Workstation, Domain Enum
3700	200.534544	192.168.8.1	255.255.255.255	MNDP	164	5678 → 5678 Len=122
3991	222.182503	Sonos_c4:5c:30	Broadcast	ARP	60	ARP Announcement for 192.168.8.189
5298	260.547278	192.168.8.1	255.255.255.255	MNDP	164	5678 → 5678 Len=122

1. ARP (Address Resolution Protocol)

Назначение: ARP используется для сопоставления IP-адресов с MAC-адресами в локальной сети. Когда устройство хочет отправить пакет другому устройству в той же сети, оно использует ARP для выяснения, какой MAC-адрес соответствует известному IP-адресу. Устройство отправляет широковещательный запрос ARP, и устройство с соответствующим IP-адресом отвечает своим MAC-адресом.

2. MNDP (Multicast Node Discovery Protocol)

Назначение: MNDP используется для обнаружения устройств в локальной сети, особенно в сетях на основе протокола UPnP (Universal Plug and Play). Устройства отправляют широковещательные сообщения MNDP для объявления своего присутствия и предоставления информации о своих возможностях другим устройствам в сети. Это позволяет автоматизировать процесс обнаружения и настройки сетевых устройств.

3. BROWSER (Windows Internet Name Service - WINS)

Назначение: Протокол BROWSER используется для обнаружения ресурсов и служб в сети Windows. Он позволяет компьютерам находить друг друга по именам, а не по IP-адресам. Устройства отправляют широковещательные запросы для получения списка доступных ресурсов (например, принтеров или файловых серверов) в локальной сети. Это помогает пользователям легко находить и подключаться к сетевым ресурсам.

Пункт 4:

Так как пакеты отправлялись не только через broadcast внутри сети, использовались протоколы ip и ethernet, можно предположить, что это маршрутизатор. Ну и для типа сети Wi-Fi - это однозначно роутер.

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

ICMP:

```
root@d12:~# traceroute -I 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.0.2.1 (10.0.2.1)  0.520 ms * *
 2  172.28.16.1 (172.28.16.1)  3.714 ms * *
 3  77.234.199.66 (77.234.199.66)  3.107 ms * *
 4  87.248.228.102.pool.sknt.ru (87.248.228.102)  6.418 ms * *
 5  72.14.216.110 (72.14.216.110)  5.440 ms * *
 6  172.253.76.91 (172.253.76.91)  4.446 ms * *
 7  74.125.244.181 (74.125.244.181)  7.792 ms * *
 8  142.251.51.187 (142.251.51.187)  16.233 ms * *
 9  172.253.51.187 (172.253.51.187)  12.903 ms * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  dns.google (8.8.8.8)  10.980 ms  10.652 ms  22.747 ms
```

UDP:


```
19 dns.google (8.8.8.8) 10.980 ms 10.852 ms 12.111 ms
root@d12:~# traceroute 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.0.2.1 (10.0.2.1)  7.947 ms  7.568 ms  6.843 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  * * *
```

TCP:

```
root@d12:~# 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  * * *
```

Отключает фрагментацию пакетов:

```
root@dl2:~# traceroute -F 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1  10.0.2.1 (10.0.2.1)  94.617 ms  94.306 ms  93.628 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  * * *
```

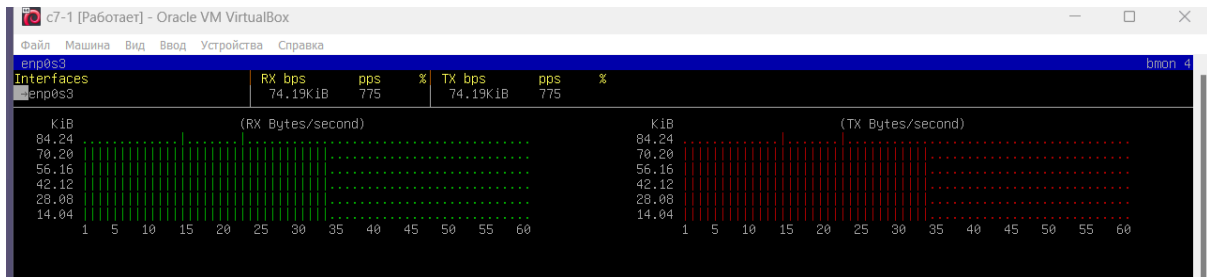
- -F: указывает, что фрагментация должна быть запрещена (do not fragment).
- -M 1400: устанавливает максимальный размер пакета (в данном случае 1400 байт). Если пакет превышает этот размер, он будет отброшен, и вы сможете увидеть, где происходит фрагментация.

Трассировка используется для диагностики проблем сети. Ее может запросить ваш хостинг- или интернет-провайдер. В этом случае предоставьте скриншот или текст вывода команды. Если сайт работает, а трассировка до него не доходит, значит запросы фильтруются на пути к цели. Отсутствие трассировки не означает наличие проблемы.

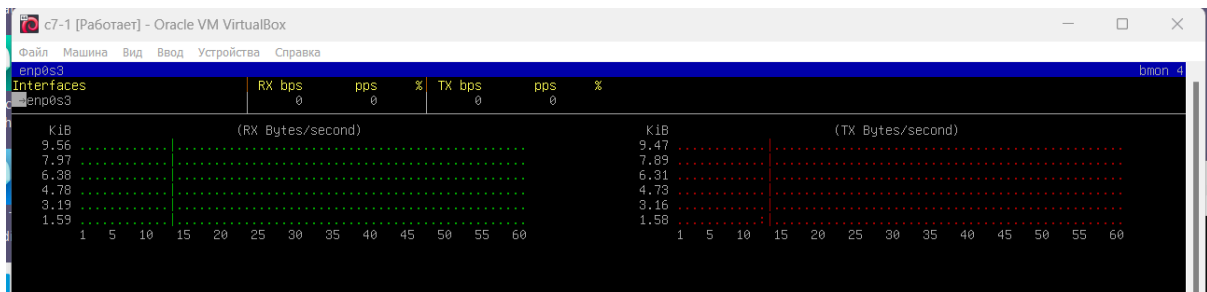
Иногда трассировка с помощью UDP не работает, это может произойти потому, что фаервол блокирует все лишние пакеты.

4. Тексты команд и консольный вывод из Части 5, п.2-3.

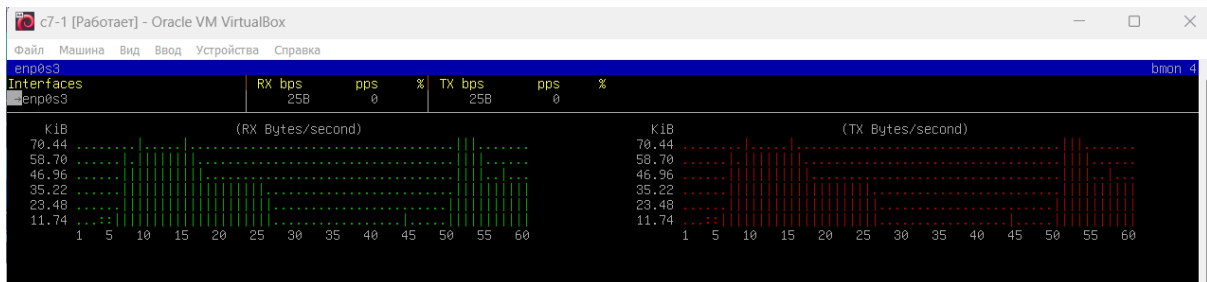
`bmon -p enp0s3`



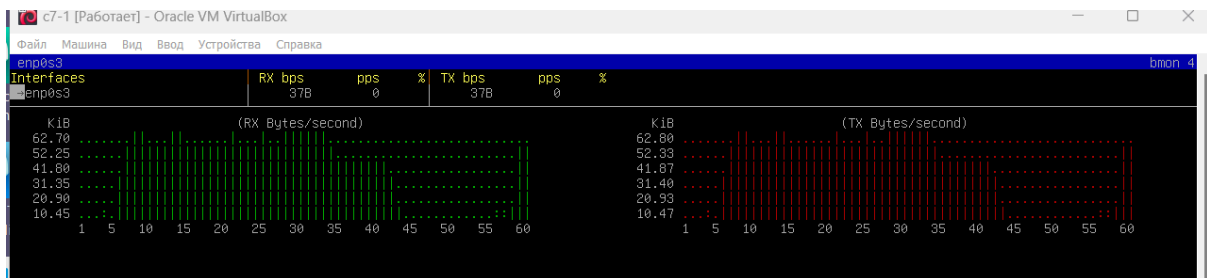
100:



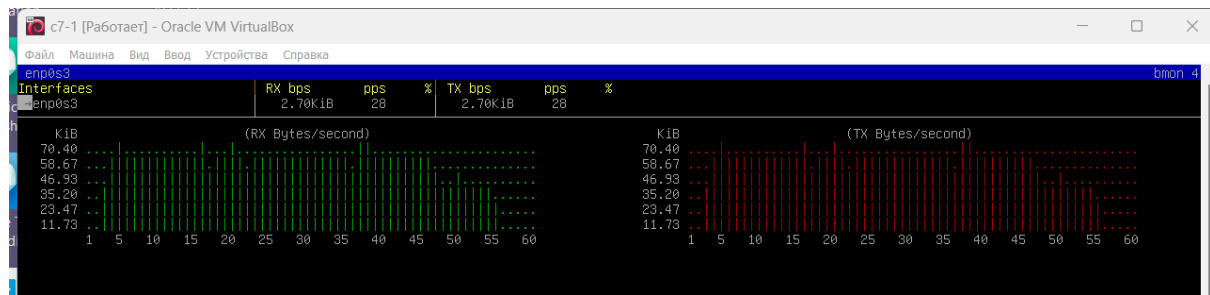
10100:



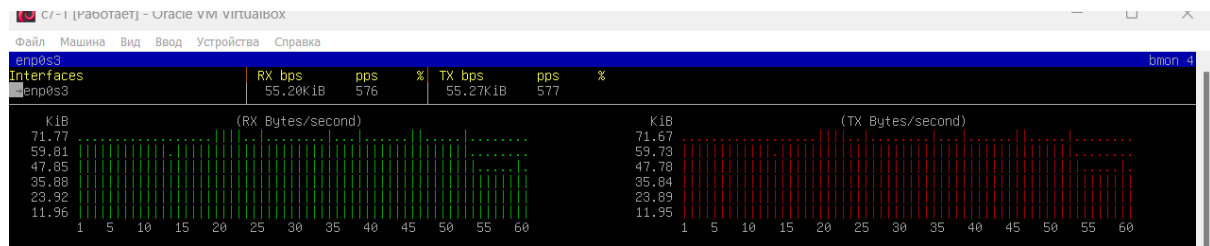
20100:



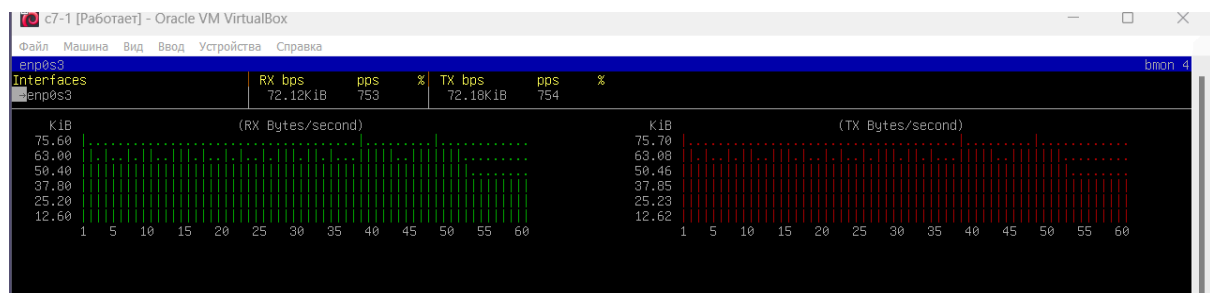
30100:



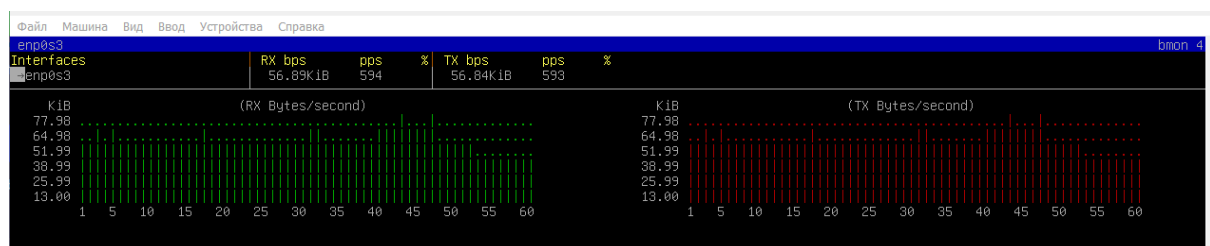
40100:



50100:



60100:



Нагрузка байт/сек не превышает 80 Кб, при этом с увеличением размеры пакетов она,естественно, растет.

Максимальная пропускная способность зависит от многих параметров (потери, задержки, кол-во хопов, удалённость удаленного хоста и т.д.)

```
[root@localhost ~]# ping -f -c 100 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
100 packets transmitted, 100 received, 0% packet loss, time 262ms
rtt min/avg/max/mdev = 0.675/1.576/2.534/0.405 ms, ipg/ewma 2.642/1.580 ms
[root@localhost ~]# ping -f -c 10100 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
10100 packets transmitted, 10100 received, 0% packet loss, time 19789ms
rtt min/avg/max/mdev = 0.241/1.733/87.295/5.490 ms, pipe 8, ipg/ewma 1.959/1.148 ms
[root@localhost ~]# ping -f -c 20100 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
20100 packets transmitted, 20100 received, 0% packet loss, time 36724ms
rtt min/avg/max/mdev = 0.238/1.625/102.440/5.257 ms, pipe 8, ipg/ewma 1.827/1.157 ms
[root@localhost ~]# ping -f -c 30100 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
30100 packets transmitted, 30100 received, 0% packet loss, time 52453ms
rtt min/avg/max/mdev = 0.237/1.510/101.039/4.868 ms, pipe 9, ipg/ewma 1.742/1.096 ms
[root@localhost ~]# ping -f -c 40100 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.

--- 10.0.2.15 ping statistics ---
40100 packets transmitted, 40100 received, 0% packet loss, time 66652ms
rtt min/avg/max/mdev = 0.237/1.487/101.228/4.926 ms, pipe 9, ipg/ewma 1.662/0.890 ms
[root@localhost ~]# ping -f -c 50100 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
```

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

```
root@d12:~# vnstat -i enp0s3
Database updated: 2024-10-23 00:00:00

enp0s3 since 2024-10-22

      rx: 60,18 KiB      tx: 57,62 KiB      total: 117,79 KiB

monthly
      rx      |      tx      |      total      |      avg. rate
-----+-----+-----+-----
  2024-10  60,18 KiB |  57,62 KiB | 117,79 KiB |      426 bit/s
-----+-----+-----+-----
estimated 20,08 MiB | 19,34 MiB | 39,42 MiB |
daily
      rx      |      tx      |      total      |      avg. rate
-----+-----+-----+-----
yesterday 60,18 KiB | 57,62 KiB | 117,79 KiB |      11 bit/s
-----+-----+-----+-----
estimated  --      |      --      |      --      |
```

6. Тексты команд и консольный вывод (или его часть) из Части 7, п.2, 3, 8 и скрипт из п.4.

Пункт 2:

```
root@d12:~# netstat -tuln
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
udp      0      0 0.0.0.0:68              0.0.0.0:*
```

Пункт 3:

```
root@d12:~# netstat -tun
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 10.0.2.4:22            10.0.2.15:33574        ESTABLISHED
tcp        0      0 10.0.2.4:22            10.0.2.15:33590        ESTABLISHED
tcp        0      0 10.0.2.4:22            10.0.2.15:45736        ESTABLISHED
```

Пункт 4:

```
#!/bin/bash
PORT=${1:-22}

echo "Connection amount | Address"

netstat -tun | grep :$PORT | grep ESTABLISHED | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort -nr

root@d12:~# ./con_amount
Connection amount | Address
3 10.0.2.15
```

Пункт 8:

```
NetHogs version 0.8.7-2
```

PID	USER	PROGRAM	DEV	SENT	RECEIVED
1153	root	sshd: root@pts/0	enp0s3	2.331	0.265 KB/sec
?	root	unknown TCP		0.000	0.000 KB/sec
TOTAL				2.331	0.265 KB/sec

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

Пункт 1:

```
root@d12:~# tcpdump -i enp0s3 port 9999 or 4444 -A
tcpdump: verbose output suppressed, use -v(v)... for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Пункт 2:

```
root@d12:~# nc -l -p 9999 > received_file.txt
root@d12:~# cat received_file.txt
jkarsun lcyang ydskrn uajlsif jvyaksnt kdyrksn jdalitld lgldseqnff skafjglk jsagfds hfjdksasrg ksaltybs lasrtun kcastnv lasrynsf hfakdrb qgdsg nvmasdr fjadlga
lasrovnsr llsaeng lsgdsn laqunf

[root@localhost ~]# cat file.txt
jkarsun lcyang ydskrn uajlsif jvyaksnt kdyrksn jdalitld lgldseqnff skafjglk jsagfds hfjdksasrg ksaltybs lasrtun kcastnv lasrynsf hfakdrb qgdsg nvmasdr fjadlga
lasrovnsr llsaeng lsgdsn laqunf
[root@localhost ~]# nc 10.0.2.4 9999 < file.txt
```

Пункт 3:

```
[root@localhost ~]# nc -u 10.0.2.4 4444
Hi! How are you?
So am I!
```

```
root@d12:~# nc -l -u -p 4444
Hi! How are you?
So am I!
```

```
root@d12:~# nc -u 10.0.2.15 4444
Fine! And you?
```

```
[root@localhost ~]# nc -l -u -p 4444
Fine! And you?
```

Пункт 4:

```
15:44:44.747571 IP 10.0.2.15.42436 > 10.0.2.4.9999: Flags [P.], seq 1:193, ack 1, win 251, options [nop,nop,TS val 483785841 ecr 2228485114], length 192
E...TH0.0...
...
...P.I.
...jksrns lcyngang ydskkrn ujaIsIf jvyaksnt kdyrksn jdaltld lgldseqnff skafjglk jsagfids hfjdksasrg ksaltybs lasrtun kcastnv lasrynsf hfakdrb qgdsg nvmasdr
fjadlga lasrovnsr llsaeng lsgdsn laqunf
```

```
16:08:16.568672 IP 10.0.2.15.37006 > 10.0.2.4.4444: UDP, length 17
E...@.0..
...
.....\..]dHi! How are you?
.
16:08:48.422979 IP 10.0.2.4.56661 > 10.0.2.15.4444: UDP, length 15
E..+>i@.0..F
...
....U.\...;Fine! And you?
16:09:12.060463 IP 10.0.2.15.37006 > 10.0.2.4.4444: UDP, length 9
E..%..@.0...
...
.....\....So am I!
.....
```

Вопросы и задания:

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

Утилита mtr комбинирует функциональность утилит ping и traceroute. Она может работать как по протоколу ICMP, так и по UDP или TCP. Это можно определить, используя флаг -u для UDP или -T для TCP. По умолчанию mtr использует ICMP.

Пример команды для определения:

```
mtr -u example.com
```

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

Основные столбцы вывода mtr:

- HOST: имя хоста или IP-адрес.
- Loss%: процент потерянных пакетов.
- Snt: количество отправленных пакетов.
- Last: время последнего ответа.
- Avg: среднее время ответа.

- Best: лучшее время ответа.
- Wrst: худшее время ответа.
- StDev: стандартное отклонение времени ответа.

Дополнительные статистики могут включать:

- Jitter: изменение времени задержки между пакетами.
- TTL: время жизни пакета.

Флаги:

- -r Помещает mtr в режим отчета. В этом режиме, mtr обработает количество циклов, определенных опцией -с, затем отобразит статистику и завершит работу. Этот режим полезен для генерации статистики о качестве сети.
- -с COUNT Установить количество циклов, после которых mtr завершит работу.
- -s BYTES Размер посылаемых пакетов.
- -t Вынуждает mtr использовать curses based terminal interface если доступно.
- -n Не использовать DNS. Отображать IP-адреса.
- -o fields order Используйте эту опцию, чтобы определить отображаемые поля, например -o "LSD NBAW"
- -i, -interval SECONDS Интервал эхо-запроса ICMP

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

Базовых форматов кадров (raw formats) существует всего два - Ethernet II и Ethernet 802.3. Эти форматы отличаются назначением всего одного поля.

Основные типы кадров Ethernet:

- кадр 802.3/LLC (кадр 802.3/802.2 или кадр Novell 802.2);
- кадр Raw 802.3 (или кадр Novell 802.3);
- кадр Ethernet DIX (или кадр Ethernet II);
- кадр Ethernet SNAP.

Наглядное отличие в размере data:

Кадр 802.3/LLC										
6	6	2	1	1	1(2)	46-1497 (1496)				4
DA	SA	L	DSAP	SSAP	Control	Data				FCS
Заголовок LLC										

Кадр Raw 802.3/Novell 802.3

6	6	2	46-1500							4
DA	SA	L	Data							FCS

Кадр Ethernet DIX (II)

6	6	2	46-1500							4
DA	SA	T	Data							FCS

Кадр Ethernet SNAP

6	6	2	1	1	1	3	2	46-1492		4
DA	SA	L	DSAP	SSAP	Control	OUI	T	Data		FCS
			AA	AA	03	000000				
Заголовок LLC						Заголовок SNAP				

Также можно сказать, что типы работают с разными протоколами:

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

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

Используется Ethernet II, который работает уже на уровне IP-адресов, именно это позволяет сети функционировать.

Он поддерживает множество протоколов и является стандартом для большинства локальных сетей. Его применение позволяет легко интегрировать различные протоколы и устройства.

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

Тип коммутационного оборудования можно определить по:

- Статистике потерь пакетов.
- Временам задержки.
- Количеству пересылаемых пакетов.

Если наблюдаются высокие потери пакетов и большие задержки, это может указывать на использование устаревших или перегруженных коммутаторов. Если трафик равномерный и потерь нет - значит используются современные управляемые коммутаторы.

Если нужно определить именно уровень принадлежности коммутационного оборудования, можно посмотреть на протоколы, используемые при коммуникации broadcast и multicast, и их соотношения в статистике. Так, коммутаторы используются на канальном уровне и используют протокол IP и MAC-адреса, маршрутизаторы же на сетевом уровне и выполняют коммуникацию локальной сети и интернета.

Если пакеты отправлялись не только через broadcast внутри сети, то есть использовались протоколы ip и ethernet, как в лабораторной, можно предположить, что это маршрутизатор. С другой стороны, по отсутствию vlan, stp, lldp, cdp и по наличию передачи arp-пакетов можно сказать, что это неуправляемый коммутатор.

6. На какие адреса сетевого уровня осуществляются широковещательные рассылки?

Широковещательные рассылки на уровне сетевого протокола осуществляются на адреса:

- IPv4: 255.255.255.255 (все узлы в сети).
- Локальная широковещательная адресация (например, 192.168.1.255).

7. На какой канальный адрес осуществляются широковещательные рассылки?

Широковещательные рассылки на канальном уровне осуществляются на MAC-адрес FF:FF:FF:FF:FF:FF, который адресует все устройства в локальной сети.

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

Перехваченные широковещательные рассылки могут использоваться для анализа сетевого трафика, диагностики проблем в сети или для обнаружения устройств в локальной сети.

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

Разные результаты могут быть вызваны:

- Изменениями в маршрутизации сети.
- Наличием фильтров или ограничений на промежуточных маршрутизаторах.
- Разными протоколами (UDP, ICMP), которые могут обрабатываться по-разному.

В нашем случае вероятней всего разные данные получились из-за использования разных протоколов. В зависимости от выбранного протокола, отправляется ICMP, UDP или TCP пакет. Предназначение протоколов различно, поэтому различаются способы отправки пакетов и гарантированность их доставки.

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

Загрузка интерфейса может увеличиваться из-за:

- Увеличения объема передаваемых данных.
- Пикового трафика, когда много устройств одновременно используют сеть.

Максимальная пропускная способность зависит от многих параметров: потери, задержки, удалённость, вычислительная мощность взаимодействующих хостов, особенности протоколов (TCP или UDP), размер буферов транспортного протокола, статистика ошибок и перегрузки, топология и загруженность сети, алгоритмы маршрутизации, а

также скорость и качество сетевых устройств, влияние протоколов сетевого уровня.

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

Передаются не только пакеты, содержащие непосредственную информацию, но и такие пакеты, как Seq , Ack и Win, обеспечивающие успешную передачу данных и функционирование соединения.

12. На каком уровне модели OSI работает vnstat?

vnstat работает на уровне 2 (канальном) модели OSI