

МИНИСТЕРСТВО 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
По дисциплине «Телекоммуникационные системы и технологии»
Мониторинг сетевого трафика на хосте и работа с утилитами диагностики и
мониторинга сетевых соединений в Linux

Выполнили студенты группы М33081
Аль Даббагх Харит Хуссейн
Мазумдер Шоувик
Миах Такбир

Проверила
Шараева Кристина Витальевна

САНКТ-ПЕТЕРБУРГ

2022

СОДЕРЖАНИЕ

Артефакты	2
Вопросы и задания.....	15

АРТЕФАКТЫ

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



c7-1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
[root@localhost ~]# ping 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=0.386 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=0.391 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=0.419 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=0.429 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=0.401 ms
64 bytes from 10.0.0.2: icmp_seq=6 ttl=64 time=0.348 ms
^C
--- 10.0.0.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5046ms
rtt min/avg/max/mdev = 0.348/0.395/0.429/0.034 ms
[root@localhost ~]#
```




c7-1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
[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=106 time=6.57 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=106 time=6.27 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=106 time=6.26 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=106 time=7.34 ms
64 bytes from 8.8.8.8: icmp_seq=5 ttl=106 time=6.46 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4216ms
rtt min/avg/max/mdev = 6.269/6.586/7.349/0.408 ms
[root@localhost ~]#
```

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


 c7-2 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
[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=0.749 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.464 ms
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.395 ms
64 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.593 ms
64 bytes from 10.0.0.1: icmp_seq=5 ttl=64 time=0.419 ms
64 bytes from 10.0.0.1: icmp_seq=6 ttl=64 time=0.671 ms
64 bytes from 10.0.0.1: icmp_seq=7 ttl=64 time=0.423 ms
64 bytes from 10.0.0.1: icmp_seq=8 ttl=64 time=0.631 ms
64 bytes from 10.0.0.1: icmp_seq=9 ttl=64 time=0.340 ms
64 bytes from 10.0.0.1: icmp_seq=10 ttl=64 time=0.422 ms

--- 10.0.0.1 ping statistics ---
10 packets transmitted, 10 received, 0% packet loss, time 90006ms
rtt min/avg/max/mdev = 0.340/0.510/0.749/0.133 ms
[root@localhost ~]# ping -c 5 -s 1500 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 1500(1528) bytes of data.
1500 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=0.804 ms
1500 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=0.471 ms
1500 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.484 ms
1500 bytes from 10.0.0.1: icmp_seq=4 ttl=64 time=0.471 ms
ping: sendmsg: Network is unreachable

--- 10.0.0.1 ping statistics ---
5 packets transmitted, 4 received, 20% packet loss, time 4002ms
rtt min/avg/max/mdev = 0.471/0.557/0.804/0.144 ms
[root@localhost ~]# _
```

 c7-1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
[root@localhost ~]# mtr -rw -c 40 www.itmo.ru > mtrReport.txt
[root@localhost ~]# cat mtrReport.txt
Start: Tue Mar 22 11:02:36 2022
HOST: localhost.localdomain

```

	Loss%	Snt	Last	Avg	Best	Wrst	StDev
1.!-- gateway	0.0%	40	0.3	0.3	0.2	0.4	0.0
2.!-- 192.168.88.1	0.0%	40	0.6	0.6	0.6	0.9	0.0
3.!-- 192.168.1.1	0.0%	40	0.9	0.9	0.8	1.1	0.0
4.!-- ???	100.0	40	0.0	0.0	0.0	0.0	0.0
5.!-- 176.241.97.153	0.0%	40	2.0	1.9	1.5	2.2	0.0
6.!-- oct-cr01-be2.78.spb.mts-internet.net	75.0%	40	1.9	2.1	1.8	2.5	0.0
7.!-- kivi-cr02-ae8.78.hel.mts-internet.net	0.0%	40	7.9	9.2	7.4	20.5	3.0
8.!-- ae52.edge4.Stockholm2.Level3.net	32.5%	40	16.7	15.7	13.7	26.8	3.2
9.!-- 4.69.162.181	0.0%	40	38.3	39.0	38.0	46.6	1.8
10.!-- BR2.Amsterdam1.surf.net	0.0%	40	38.6	42.6	38.0	87.3	8.4
11.!-- ae0-4.RT.OU.SPB.RU.retn.net	0.0%	40	112.3	74.6	72.1	112.3	7.9
12.!-- GW-ITMO.retn.net	0.0%	40	45.1	45.8	45.0	59.1	2.3
13.!-- 77.234.192.167	0.0%	40	47.2	52.7	46.7	201.3	25.1
14.!-- 77.234.204.10	0.0%	40	47.0	47.2	46.8	49.8	0.4

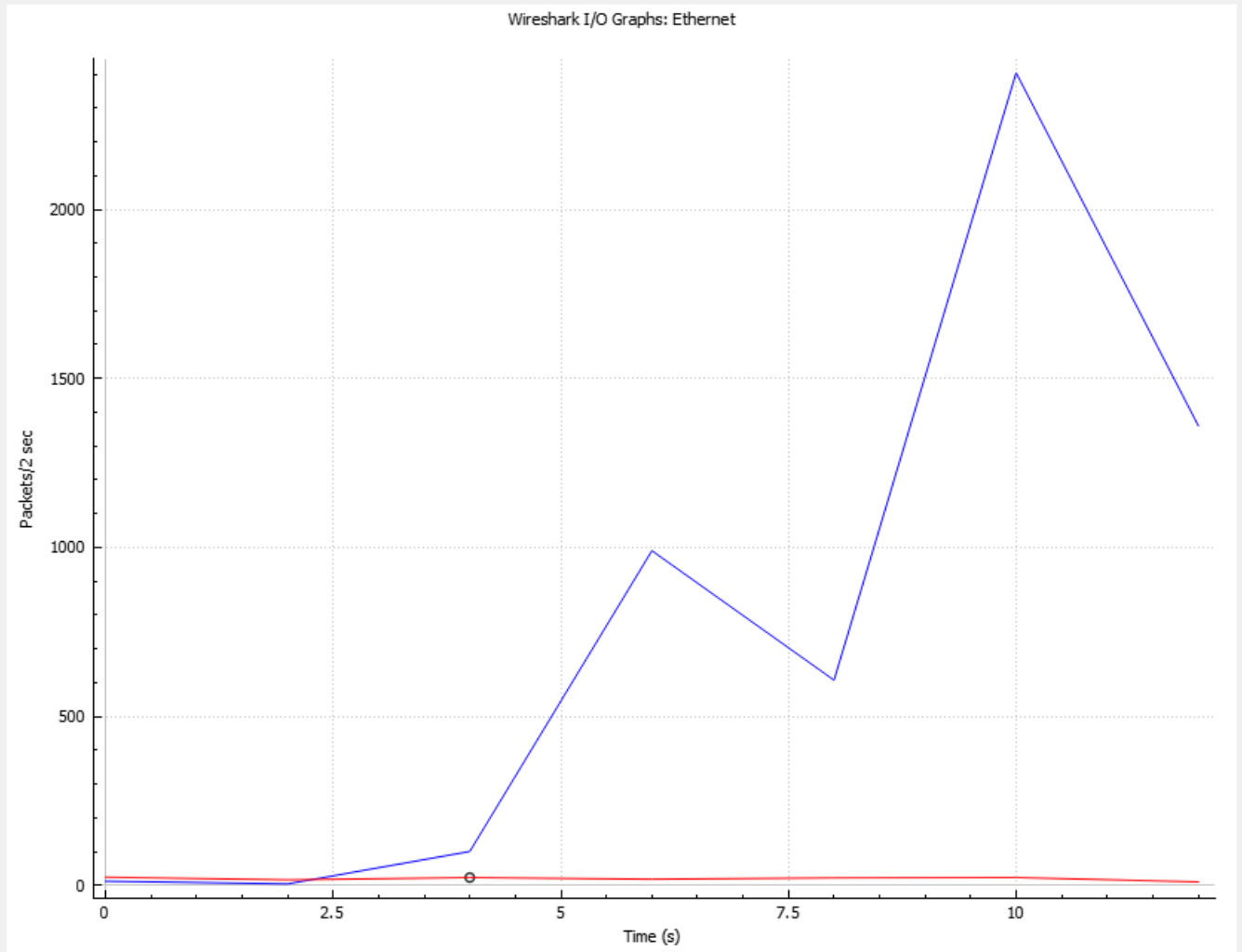
```
[root@localhost ~]# _
```

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

Wireshark · Endpoints · Ethernet											
Ethernet · 10		IPv4 · 27		IPv6 · 3		TCP · 50		UDP · 30			
Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes	Country	City	AS Number	AS Organization	
192.168.88.254	5,516	4792 k	2,033	385 k	3,483	4407 k	—	—	—	—	
74.125.111.138	3,450	3397 k	2,282	3304 k	1,168	93 k	—	—	—	—	
173.194.73.119	963	789 k	598	760 k	365	28 k	—	—	—	—	
209.85.233.198	604	409 k	345	213 k	259	196 k	—	—	—	—	
74.125.131.198	175	78 k	101	70 k	74	8063	—	—	—	—	
212.188.37.109	47	26 k	20	12 k	27	14 k	—	—	—	—	
173.194.2.28	40	26 k	18	15 k	22	11 k	—	—	—	—	
212.188.49.82	38	26 k	18	15 k	20	11 k	—	—	—	—	

Wireshark · Conversations · Ethernet											
Ethernet · 7		IPv4 · 25		IPv6 · 2		TCP · 29		UDP · 21			
Address A	Address B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.88.1	255.255.255.255	1	191	1	191	0	0	5.397406	0.0000	—	—
192.168.88.253	239.192.152.143	36	6408	36	6408	0	0	0.000000	12.9988	3943	—
192.168.88.254	212.188.49.82	38	26 k	20	11 k	18	15 k	9.355740	2.1011	42 k	—
192.168.88.254	212.188.37.109	47	26 k	27	14 k	20	12 k	9.115174	2.2998	51 k	—
192.168.88.254	209.85.233.198	604	409 k	259	196 k	345	213 k	5.478892	6.8880	227 k	—
162.159.134.234	192.168.88.254	2	165	1	111	1	54	2.485477	0.0403	22 k	—
162.254.198.104	192.168.88.254	2	188	1	134	1	54	10.100516	0.0404	26 k	—
172.65.212.243	192.168.88.254	4	228	2	120	2	108	0.645217	0.7418	1294	—
172.65.226.29	192.168.88.254	4	228	2	120	2	108	2.528717	5.2123	184	—
192.168.88.254	192.168.88.1	18	2108	9	753	9	1355	5.470095	5.7620	1045	—

Wireshark · Conversations · Ethernet													
Ethernet · 7		IPv4 · 25		IPv6 · 2		TCP · 29		UDP · 21					
Address A	Port A	Address B	Port B	Packets	Bytes	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A	Rel Start	Duration	Bits/s A → B	Bits/s B → A
192.168.88.254	51334	74.125.111.138	443	2,070	2006 k	725	58 k	1,345	1947 k	10.400729	2.0363	229 k	—
192.168.88.254	51333	74.125.111.138	443	1,376	1386 k	439	30 k	937	1356 k	10.400609	2.6265	91 k	—
192.168.88.254	51324	173.194.73.119	443	963	789 k	365	28 k	598	760 k	5.571005	5.5964	41 k	—
192.168.88.254	51188	209.85.233.198	443	604	409 k	259	196 k	345	213 k	5.478892	6.8880	227 k	—
192.168.88.254	51326	74.125.131.198	443	175	78 k	74	8063	101	70 k	7.400834	4.1258	15 k	—
192.168.88.254	51327	212.188.37.109	443	24	14 k	12	5428	12	8966	9.115174	0.2101	206 k	—
192.168.88.254	51331	173.194.2.28	443	18	10 k	9	3147	9	7732	10.035052	0.0437	576 k	—
192.168.88.254	51330	212.188.49.82	443	17	10 k	8	3081	9	7725	9.656175	0.0496	496 k	—
192.168.88.254	51332	173.194.2.28	443	18	10 k	9	3044	9	7608	10.035146	0.0432	564 k	—
192.168.88.254	51329	212.188.49.82	443	17	10 k	8	2978	9	7592	9.656057	0.0495	481 k	—
192.168.88.254	51328	212.188.37.109	443	19	7351	11	4263	8	3088	9.321082	0.3336	102 k	—
192.168.88.254	51335	64.233.162.94	443	22	4930	10	2742	12	2188	11.233469	0.5526	39 k	—
192.168.88.254	51284	104.21.83.166	443	19	3701	8	1988	11	1713	9.823030	0.4807	33 k	—
192.168.88.254	51292	64.233.165.95	443	24	3555	11	1999	13	1556	7.381921	2.0127	7945	—
192.168.88.254	51299	74.125.131.101	443	15	2839	7	602	8	2237	8.901581	0.0372	129 k	—
192.168.88.254	51285	64.233.164.99	443	14	2256	6	967	8	1289	11.158498	0.0722	107 k	—
192.168.88.254	51322	64.233.162.95	443	9	1997	5	943	4	1054	5.490250	0.0898	84 k	—
192.168.88.254	51323	64.233.161.94	443	9	1994	5	940	4	1054	5.490790	0.0883	85 k	—
192.168.88.254	51325	64.233.161.94	443	9	1994	5	940	4	1054	5.603829	0.0913	82 k	—
192.168.88.254	51194	74.125.131.94	443	15	1853	7	1223	8	630	9.123525	0.0376	260 k	—
192.168.88.254	51235	142.251.1.139	443	14	1488	6	509	8	979	5.549196	0.0783	52 k	—
192.168.88.254	51922	3.65.102.105	443	7	604	4	324	3	280	0.034352	10.0713	257	—
192.168.88.254	51924	3.65.102.105	443	7	604	4	324	3	280	0.034398	10.0712	257	—
162.254.198.104	27034	192.168.88.254	59950	2	188	1	134	1	54	10.100516	0.0404	26 k	—
162.159.134.234	443	192.168.88.254	59939	2	165	1	111	1	54	2.485477	0.0403	22 k	—
172.65.212.243	443	192.168.88.254	51311	2	114	1	60	1	54	0.645217	0.0000	—	—
172.65.212.243	443	192.168.88.254	51313	2	114	1	60	1	54	1.386999	0.0000	—	—
172.65.226.29	443	192.168.88.254	51314	2	114	1	60	1	54	2.528717	0.0000	—	—
172.65.226.29	443	192.168.88.254	51310	2	114	1	60	1	54	7.740952	0.0000	—	—



Hover over the graph for details.

Enabled	Graph Name	Display Filter	Color	Style	Y Axis	Y Field	SMA Period	Y Ax
<input checked="" type="checkbox"/>	All Packets	tcp	Blue	Line	Packets		None	1
<input checked="" type="checkbox"/>	All Packets	udp	Red	Line	Packets		None	1

<

>

+

-

Fit

Info

Mouse ☒ drags ☐ zooms

Interval 2 sec ▾

☐ Time of day☐ Log scale☒ Automatic Update

Reset

Save As...

Copy

Copy from

Close

Help

The image displays a Wireshark packet capture analysis of an SSL/TLS handshake. The top pane shows the packet list with 56 packets. The middle pane shows the packet details for packet 54, which is a TLSv1.2 Application Data packet. The bottom pane shows the packet bytes and the corresponding hex and ASCII representations.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
2	0.000061	192.168.88.254	20.189.173.4	TCP	54	59315 → 443 [ACK] Seq=1 Ack=1 Win=1024 Len=0
3	0.000216	192.168.88.254	20.189.173.4	TLSv1.2	283	Client Hello
5	0.183605	192.168.88.254	20.189.173.4	TCP	54	59315 → 443 [ACK] Seq=230 Ack=1461 Win=1024 Len=0
8	0.183821	192.168.88.254	20.189.173.4	TCP	54	59315 → 443 [ACK] Seq=230 Ack=4381 Win=1024 Len=0
11	0.184022	192.168.88.254	20.189.173.4	TCP	54	59315 → 443 [ACK] Seq=230 Ack=6225 Win=1024 Len=0
12	0.186842	192.168.88.254	20.189.173.4	TLSv1.2	212	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
14	0.369510	192.168.88.254	20.189.173.4	TCP	54	59315 → 443 [ACK] Seq=388 Ack=6276 Win=1023 Len=0
15	0.369761	192.168.88.254	20.189.173.4	TLSv1.2	911	Application Data
16	0.369780	192.168.88.254	20.189.173.4	TCP	1494	59315 → 443 [ACK] Seq=1245 Ack=6276 Win=1023 Len=1440 [TCP segment of a reassembled PDU]
17	0.369788	192.168.88.254	20.189.173.4	TLSv1.2	381	Application Data
19	0.462501	192.168.88.254	162.159.135.234	TCP	54	59314 → 443 [ACK] Seq=1 Ack=357 Win=1026 Len=0
22	0.554774	192.168.88.254	20.189.173.4	TCP	54	59315 → 443 [ACK] Seq=3012 Ack=6683 Win=1022 Len=0
41	1.616911	192.168.88.254	162.159.135.234	TCP	54	59314 → 443 [ACK] Seq=1 Ack=642 Win=1025 Len=0
42	1.807841	192.168.88.254	23.32.99.125	TCP	54	58940 → 80 [FIN, ACK] Seq=1 Ack=1 Win=1025 Len=0
44	1.821423	192.168.88.254	23.32.99.125	TCP	54	58940 → 80 [ACK] Seq=2 Ack=2 Win=1025 Len=0
55	3.624917	192.168.88.254	172.65.253.13	TCP	54	[TCP ACKed unseen segment] 58916 → 443 [ACK] Seq=1 Ack=2 Win=1024 Len=0
56	3.987391	192.168.88.254	3.65.102.105	TLSv1.2	110	Application Data

Packet Details:

- Frame 2: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface \Device\NPF_{B9D57333-6819-48DC-B915-3CBDD48CFAE9}, id 0
- Ethernet II, Src: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b), Dst: Routerbo_5d:4e:68 (2c:c8:1b:5d:4e:68)
 - Destination: Routerbo_5d:4e:68 (2c:c8:1b:5d:4e:68)
 - Address: Routerbo_5d:4e:68 (2c:c8:1b:5d:4e:68)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Source: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b)
 - Address: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b)
 -0. = LG bit: Globally unique address (factory default)
 -0. = IG bit: Individual address (unicast)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 192.168.88.254, Dst: 20.189.173.4
- Transmission Control Protocol, Src Port: 59315, Dst Port: 443, Seq: 1, Ack: 1, Len: 0

***Ethernet**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

eth.dst == ff:ff:ff:ff:ff:ff || ip.dst == 255.255.255.255

No.	Time	Source	Destination	Protocol	Length	Info
400	3.975676	192.168.88.254	192.168.88.255	UDP	46	57865 → 5678 Len=4
411	5.140714	192.168.88.1	255.255.255.255	MNDP	191	5678 → 5678 Len=149
926	9.910742	192.168.88.254	192.168.88.255	NBNS	92	Name query NB DESKTOP-QEDDTPO<1c>
1163	10.661198	192.168.88.254	192.168.88.255	NBNS	92	Name query NB DESKTOP-QEDDTPO<1c>
1165	11.411284	192.168.88.254	192.168.88.255	NBNS	92	Name query NB DESKTOP-QEDDTPO<1c>

> Frame 400: 46 bytes on wire (368 bits), 46 bytes captured (368 bits) on interface \Device\NPF_{B9D57333-6819-4BDC-B915-3CBDD48CFAE9}, id 0

▼ Ethernet II, Src: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b), Dst: Broadcast (ff:ff:ff:ff:ff:ff)

▼ Destination: Broadcast (ff:ff:ff:ff:ff:ff)

Address: Broadcast (ff:ff:ff:ff:ff:ff)

.... 1. = LG bit: Locally administered address (this is NOT the factory default)

.... 1. = IG bit: Group address (multicast/broadcast)

▼ Source: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b)

Address: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b)

.... 0. = LG bit: Globally unique address (factory default)

.... 0. = IG bit: Individual address (unicast)

Type: IPv4 (0x0800)

▼ Internet Protocol Version 4, Src: 192.168.88.254, Dst: 192.168.88.255

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

> Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 32

Identification: 0xffd1 (65489)

> Flags: 0x00

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 128

Protocol: UDP (17)

Header Checksum: 0x07ad [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.88.254

Destination Address: 192.168.88.255

> User Datagram Protocol, Src Port: 57865, Dst Port: 5678

> Data (4 bytes)

```

0000  ff ff ff ff ff 04 d9 f5 d3 5b 5b 08 00 45 00  .....E
0010  00 20 ff d1 00 00 80 11 07 ad c0 a8 58 fe c0 a8  .....X
0020  58 ff e2 09 16 2e 00 0c d4 4f 00 00 00 00  .....0

```

***Ethernet**

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.src == 192.168.88.254 && ip.dst == 192.168.88.255 && udp

No.	Time	Source	Destination	Protocol	Length	Info
400	3.975676	192.168.88.254	192.168.88.255	UDP	46	57865 → 5678 Len=4
926	9.910742	192.168.88.254	192.168.88.255	NBNS	92	Name query NB DESKTOP-QEDDTPO<1c>
1163	10.661198	192.168.88.254	192.168.88.255	NBNS	92	Name query NB DESKTOP-QEDDTPO<1c>
1165	11.411284	192.168.88.254	192.168.88.255	NBNS	92	Name query NB DESKTOP-QEDDTPO<1c>

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl>/>

No.	Time	Source	Destination	Protocol	Length	Info
1149	10.579644	185.199.111.133	192.168.88.254	TCP	60	443 → 59473 [ACK] Seq=13078 Ack=8645 Win=189952 Len=0
1150	10.580631	185.199.111.133	192.168.88.254	TLSv1.3	210	Application Data
1151	10.582446	192.168.88.254	185.199.111.133	TLSv1.3	197	Application Data
1152	10.595202	185.199.111.133	192.168.88.254	TCP	60	443 → 59473 [ACK] Seq=13234 Ack=8785 Win=190976 Len=0
1153	10.595695	185.199.111.133	192.168.88.254	TLSv1.3	217	Application Data
1154	10.596295	185.199.111.133	192.168.88.254	TCP	60	443 → 59473 [ACK] Seq=13397 Ack=8925 Win=192000 Len=0
1155	10.597196	185.199.111.133	192.168.88.254	TLSv1.3	216	Application Data
1156	10.597208	192.168.88.254	185.199.111.133	TCP	54	59473 → 443 [ACK] Seq=9068 Ack=13559 Win=261376 Len=0
1157	10.597669	192.168.88.254	185.199.111.133	TLSv1.3	197	Application Data
1158	10.613292	185.199.111.133	192.168.88.254	TCP	60	443 → 59473 [ACK] Seq=13559 Ack=9068 Win=193536 Len=0
1159	10.613779	185.199.111.133	192.168.88.254	TLSv1.3	217	Application Data
1160	10.628650	185.199.111.133	192.168.88.254	TCP	60	443 → 59473 [ACK] Seq=13722 Ack=9211 Win=194560 Len=0
1161	10.629490	185.199.111.133	192.168.88.254	TLSv1.3	263	Application Data
1162	10.629501	192.168.88.254	185.199.111.133	TCP	54	59473 → 443 [ACK] Seq=9211 Ack=13931 Win=262656 Len=0
1163	10.661198	192.168.88.254	192.168.88.255	NBNS	92	Name query NB DESKTOP-QEDDTPO<1c>
1164	11.406215	192.168.88.254	152.199.19.161	TCP	54	[TCP Retransmission] 51216 → 443 [FTN, ACK] Seq=1 Ack=1 Win=1023 Len=0
1165	11.411284	192.168.88.254	192.168.88.255	NBNS	92	Name query NB DE

> Frame 1157: 197 bytes on wire (1576 bits), 197 bytes captured (1576 bits) on interface \Device\NPF_{...}

> Ethernet II, Src: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b), Dst: Routerbo_5d:4e:68 (2c:c8:1b:5d:4e:68)

> Destination: Routerbo_5d:4e:68 (2c:c8:1b:5d:4e:68)

> Source: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b)

> Address: Routerbo_5d:4e:68 (2c:c8:1b:5d:4e:68)

> Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.88.254, Dst: 185.199.111.133

> Transmission Control Protocol, Src Port: 59473, Dst Port: 443, Seq: 9068, Ack: 13559, Len: 143

> Transport Layer Security

Wireshark - Resolved Addresses

Hosts	Ports	Capture File Comments
2c:c8:1b		All entries
Address	Name	
2c:c8:1b:5d:4e:68	Routerbo_5d:4e:68	
2c:c8:1b:5d:4e:69	Routerbo_5d:4e:69	
2c:c8:1b	Routerboard.com	

*Ethernet

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
3487	116.003488	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5375/53300, ttl=2 (no response found!)
3488	116.003923	192.168.1.1	192.168.88.254	ICMP	106	Time-to-live exceeded (Time to live exceeded in transit)
3497	116.008693	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5376/21, ttl=3 (no response found!)
3498	116.150675	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5377/277, ttl=4 (no response found!)
3499	116.160421	176.241.97.153	192.168.88.254	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
3500	116.236314	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5378/533, ttl=1
3501	116.313897	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5379/789, ttl=1
3502	116.391326	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5380/1045, ttl=1
3503	116.468766	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5381/1301, ttl=1
3504	116.482092	212.188.33.199	192.168.88.254	ICMP	110	Time-to-live exceeded (Time to live exceeded in transit)
3505	116.546516	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5382/1557, ttl=1
3506	116.571695	212.188.33.199	192.168.88.254	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
3507	116.623864	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5383/1813, ttl=1
3508	116.701498	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5384/2069, ttl=1
3509	116.721852	104.4.29	192.168.88.254	ICMP	78	Time-to-live exceeded (Time to live exceeded in transit)
3510	116.770664	192.168.88.254	87.250.250.242	ICMP	78	Echo (ping) request id=0x0001, seq=5385/2325, ttl=1
3511	116.798217	87.250.250.242	192.168.88.254	ICMP	78	Echo (ping) reply id=0x0001, seq=5385/2325, ttl=0

> Frame 74: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface \Device\NPF_{89057333-6819-4BDC-8915-3CBDD48CFAE9},

> Ethernet II, Src: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b), Dst: Routerbo_5d:4e:68 (2c:c8:1b:5d:4e:68)

> Destination: Routerbo_5d:4e:68 (2c:c8:1b:5d:4e:68)

> Source: ASUSTekC_d3:5b:5b (04:d9:f5:d3:5b:5b)

> Address: Routerbo_5d:4e:68 (2c:c8:1b:5d:4e:68)

> Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.88.254, Dst: 87.250.250.242

> Internet Control Message Protocol

Crash Report - Oracle VM VirtualBox

File Machine View Input Devices Help

IP	Loss%	Snt	Last	Avg	Best	Worst	St
1.1-- gateway (10.0.2.2)	0.0%	111	0.3	0.3	0.2	0.5	0.0
2.1-- 192.168.88.1	0.0%	111	0.7	0.8	0.6	7.2	0.0
3.1-- 192.168.1.1	0.0%	111	0.8	1.1	0.7	6.1	0.0
4.1-- ???	100.0%	111	0.0	0.0	0.0	0.0	0.0
5.1-- 176.241.97.153	0.0%	111	2.1	2.2	1.9	3.6	0.0
6.1-- oct-cr01-be2.70.spb.mts-internet.net (212.188.1.101)	87.4%	111	3.1	2.1	1.8	3.1	0.0
7.1-- mag9-cr02-be1.70.spb.mts-internet.net (212.188.2.38)	96.4%	111	13.4	13.3	13.2	13.4	0.0
8.1-- ???	100.0%	111	0.0	0.0	0.0	0.0	0.0
9.1-- a197-cr04-be31.77.msk.mts-internet.net (212.188.56.14)	20.8%	111	14.6	14.4	14.1	16.4	0.0
10.1-- 212.188.33.199	0.0%	111	25.6	15.3	14.3	43.2	0.0
11.1-- sas-32z6-lag-2-1.yndx.net (87.250.239.287)	77.5%	111	20.3	20.4	20.3	20.7	0.0
12.1-- 10.4.6.1	5.4%	111	22.3	23.0	21.7	34.7	0.0
13.1-- ya.ru (87.250.250.242)	0.0%	111	19.9	20.0	19.9	20.5	0.0

(root@localhost ~)#

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

c7-1 [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help

```
This method uses well-known "half-open technique", which prevents applications on the destination host from seeing our probes at all. Normally, a tcp syn is sent. For non-listened ports we receive tcp reset, and all is done. For active listening ports we receive tcp syn+ack, but answer by tcp reset (instead of expected tcp ack), this way the remote tcp session is dropped even without the application ever taking notice.
```

There is a couple of options for **tcp** method:

syn,ack,fin,rst,psh,urg,ece,cwr

Sets specified tcp flags for probe packet, in any combination.

```
[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 (10.0.2.2) 0.264 ms 0.463 ms 0.210 ms
 2 192.168.88.1 (192.168.88.1) 0.687 ms 0.731 ms *
 3 * * *
 4 * * *
 5 * * *
 6 * oct-cr01-be2.78.spb.mts-internet.net (212.188.1.101) 2.461 ms *
 7 bor-cr02-ae5.78.spb.mts-internet.net (212.188.28.14) 2.457 ms 2.332 ms *
 8 * * *
 9 * * *
10 * * *
11 * * 72.14.232.85 (72.14.232.85) 24.977 ms
12 142.251.61.221 (142.251.61.221) 6.610 ms 6.621 ms *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 dns.google (8.8.8.8) 5.798 ms 5.897 ms 5.807 ms
[root@localhost ~]# _
```

Right Ctrl

```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[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) 0.166 ms 0.141 ms 0.091 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 ~]# _

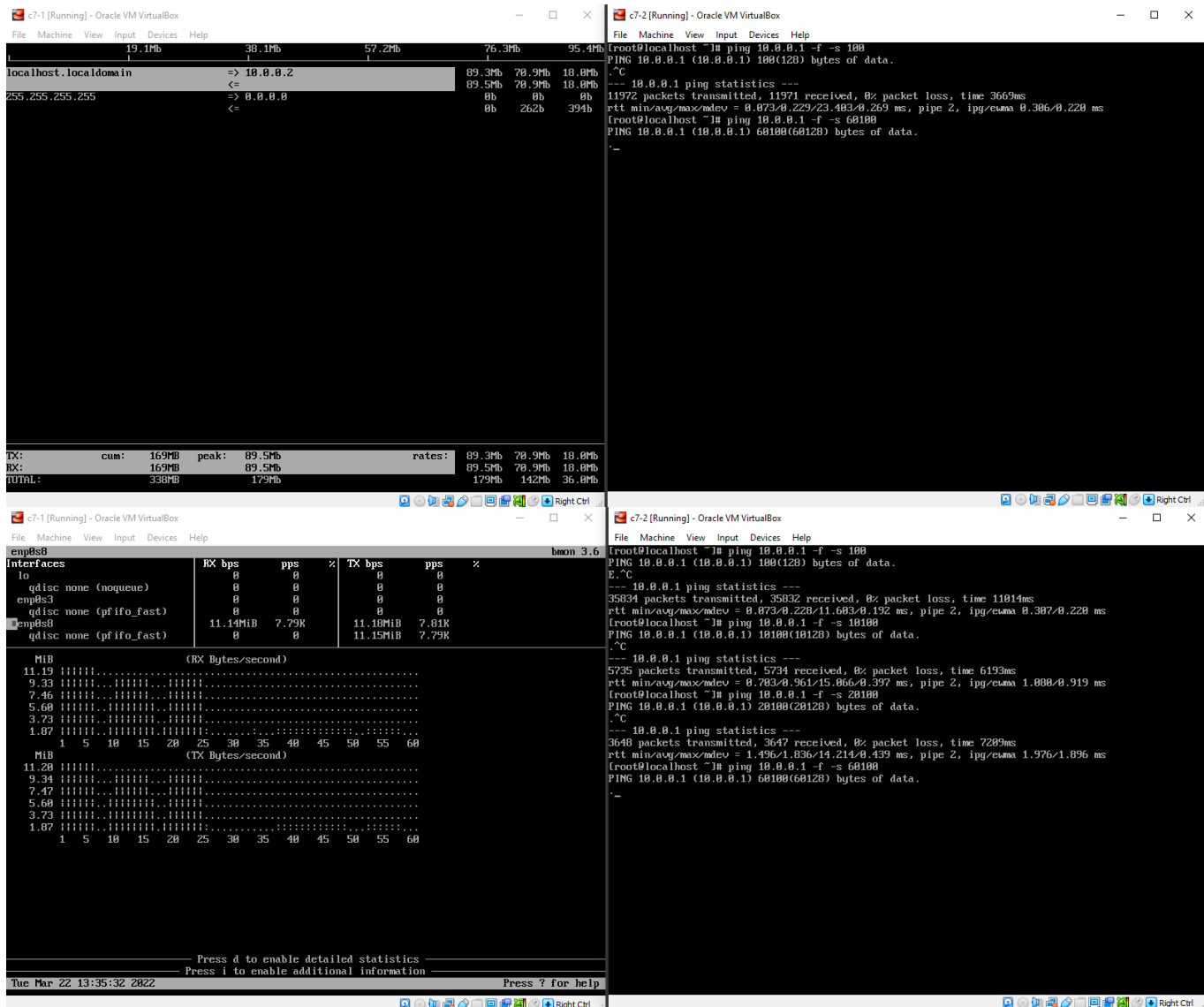
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost ~]# traceroute -T 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 60 byte packets
 1 gateway (10.0.2.2) 0.419 ms 0.178 ms 0.240 ms
 2 * * *
 3 * * *
 4 * * *
 5 * * *
 6 * * *
 7 * * *
 8 * * *
 9 * * *
10 * * *
11 * * *
12 * * *
13 * * *
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 * * *
24 * * *
25 * * *
26 * * *
27 * * *
28 * * *
29 * * *
30 * * *
[root@localhost ~]#
```

```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
13 216.239.56.113 (216.239.56.113) 7.645 ms 7.831 ms 7.709 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 dns.google (8.8.8.8) 6.033 ms 6.255 ms 6.170 ms
[root@localhost ~]# traceroute -I --mtu 8.8.8.8
traceroute to 8.8.8.8 (8.8.8.8), 30 hops max, 65000 byte packets
 1 gateway (10.0.2.2) 0.332 ms F=1500 0.118 ms 0.086 ms
 2 192.168.88.1 (192.168.88.1) 0.531 ms 0.614 ms 0.611 ms
 3 192.168.1.1 (192.168.1.1) 1.040 ms 1.122 ms 0.862 ms
 4 * * *
 5 176.241.97.153 (176.241.97.153) 2.333 ms 2.216 ms 2.308 ms
 6 * * *
 7 bor-cr02-ae5.78.spb.mts-internet.net (212.188.28.14) 2.750 ms 2.491 ms 2.412 ms
 8 74.125.49.108 (74.125.49.108) 2.583 ms 2.978 ms 3.015 ms
 9 172.253.76.91 (172.253.76.91) 2.737 ms 2.744 ms 2.418 ms
10 74.125.244.180 (74.125.244.180) 3.823 ms 6.117 ms 2.423 ms
11 72.14.232.85 (72.14.232.85) 3.002 ms 3.110 ms 3.249 ms
12 142.251.61.221 (142.251.61.221) 6.946 ms 8.384 ms 6.728 ms
13 216.239.56.113 (216.239.56.113) 7.912 ms 8.332 ms 7.900 ms
14 * * *
15 * * *
16 * * *
17 * * *
18 * * *
19 * * *
20 * * *
21 * * *
22 * * *
23 dns.google (8.8.8.8) 6.481 ms 6.165 ms 5.903 ms
[root@localhost ~]#
```

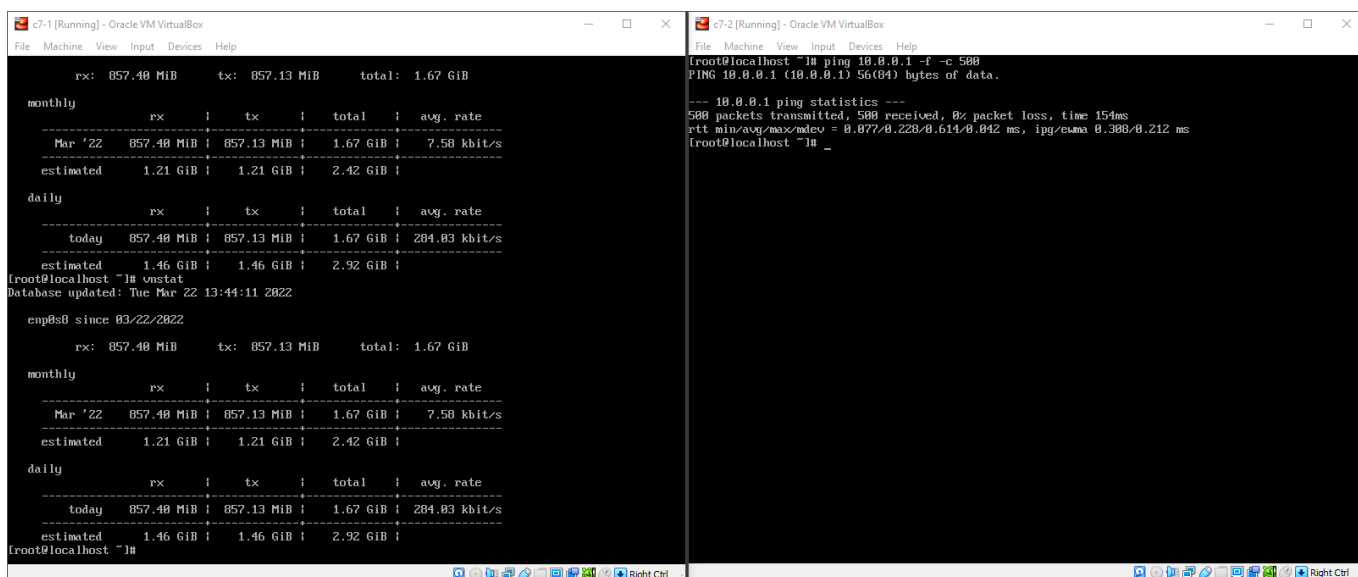
5. Тексты команд и консольный вывод из Части 5, п.2.

```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Device enp0s8 (10.0.0.1) (2/3):
=====
Incoming:
=====
...
Outgoing:
=====
...
Curr: 0.00 Bit/s
Avg: 6.57 MBit/s
Min: 0.00 Bit/s
Max: 87.53 MBit/s
Ttl: 164.67 Mbyte

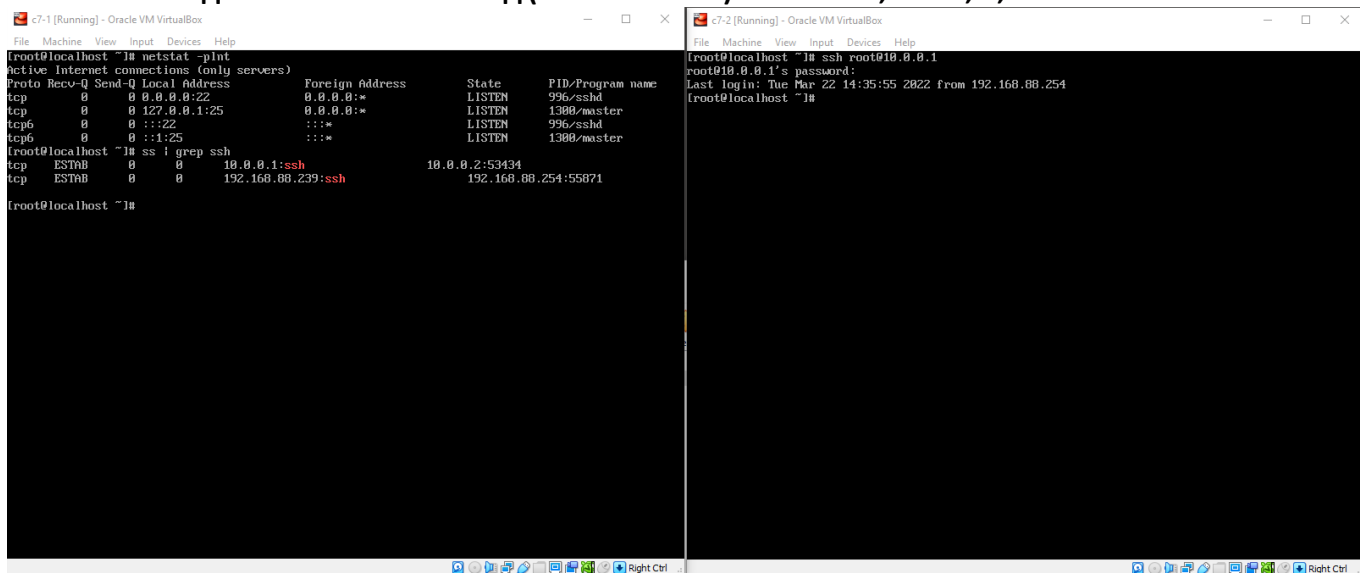
c7-2 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost ~]# ping 10.0.0.1 -f -s 100
PING 10.0.0.1 (10.0.0.1) 100(120) bytes of data.
.
--- 10.0.0.1 ping statistics ---
11285 packets transmitted, 11285 received, 0% packet loss, time 3619ms
rtt min/avg/max/mdev = 0.874/0.240/25.404/0.666 ms, pipe 2, ipg/cwnd 0.320/0.225 ms
[root@localhost ~]# ping 10.0.0.1 -f -s 10100
PING 10.0.0.1 (10.0.0.1) 10100(10120) bytes of data.
.
--- 10.0.0.1 ping statistics ---
2239 packets transmitted, 2239 received, 0% packet loss, time 2497ms
rtt min/avg/max/mdev = 0.789/1.020/26.899/1.161 ms, pipe 3, ipg/cwnd 1.116/1.009 ms
[root@localhost ~]# ping 10.0.0.1 -f -s 20100
PING 10.0.0.1 (10.0.0.1) 20100(20120) bytes of data.
.
--- 10.0.0.1 ping statistics ---
1946 packets transmitted, 1945 received, 0% packet loss, time 3927ms
rtt min/avg/max/mdev = 1.457/1.302/26.881/1.212 ms, pipe 3, ipg/cwnd 2.819/1.798 ms
[root@localhost ~]# ping 10.0.0.1 -f -s 30100
PING 10.0.0.1 (10.0.0.1) 30100(30120) bytes of data.
.
--- 10.0.0.1 ping statistics ---
1883 packets transmitted, 1881 received, 0% packet loss, time 5582ms
rtt min/avg/max/mdev = 1.526/2.799/27.995/1.594 ms, pipe 3, ipg/cwnd 2.923/2.616 ms
[root@localhost ~]# ping 10.0.0.1 -f -s 60100
PING 10.0.0.1 (10.0.0.1) 60100(60120) bytes of data.
.
--- 10.0.0.1 ping statistics ---
621 packets transmitted, 620 received, 0% packet loss, time 3332ms
rtt min/avg/max/mdev = 4.532/5.201/21.720/1.191 ms, pipe 2, ipg/cwnd 5.375/5.067 ms
[root@localhost ~]#
```



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



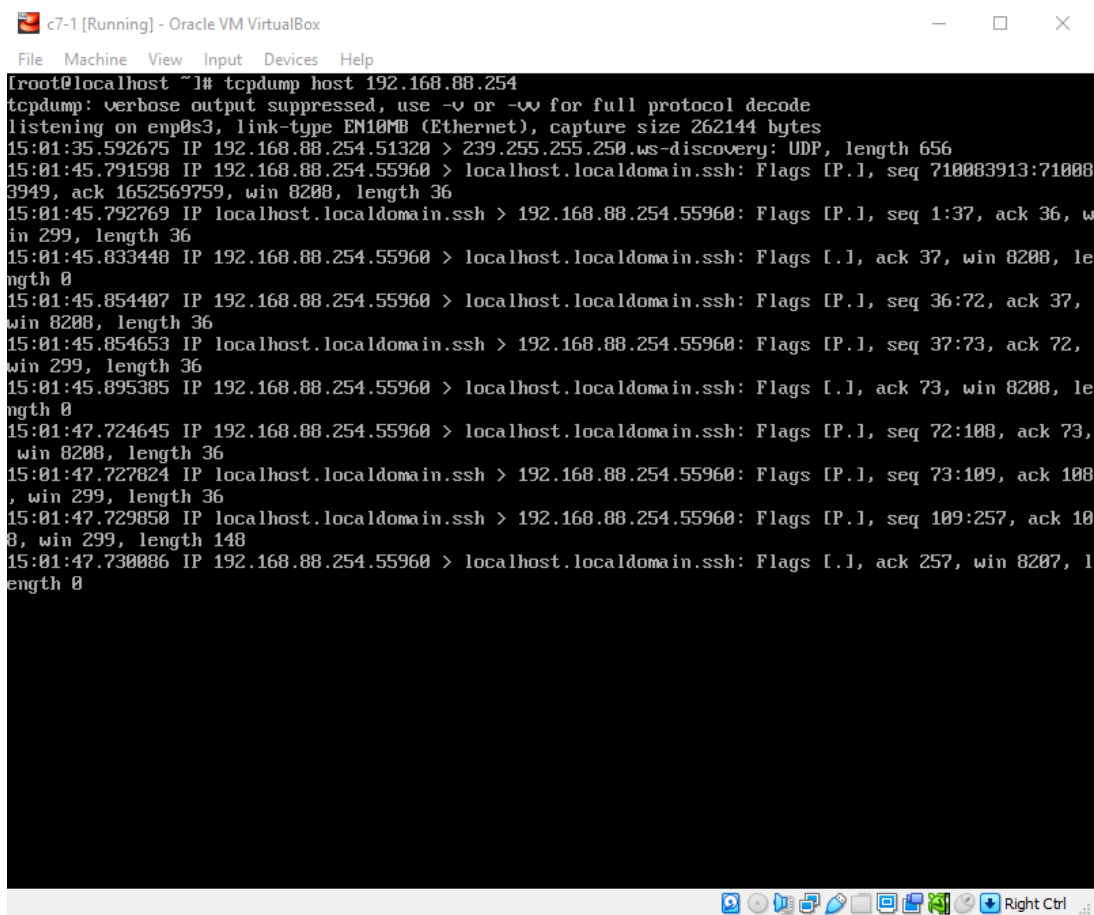
7. Тексты команд и консольный вывод (или его часть) из Части 7, п.2-4, 8,9.



The image shows two side-by-side Oracle VM VirtualBox terminal windows. The left window, titled 'c7-1 [Running] - Oracle VM VirtualBox', displays the output of the command 'netstat -plnt'. The output shows active Internet connections for the 'sshd' service, listening on port 22. The right window, titled 'c7-2 [Running] - Oracle VM VirtualBox', displays the output of the command 'ssh root@10.0.0.1'. The output shows the SSH connection details, including the last login time and the IP address of the remote host.

```
File Machine View Input Devices Help
[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 0.0.0.0:22              0.0.0.0:*               LISTEN      996/sshd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1300/master
tcp6       0      0 :::22                  :::*                    LISTEN      996/sshd
tcp6       0      0 :::22                  :::*                    LISTEN      1300/master
[root@localhost ~]# ss -t grep ssh
tcp        0      0 10.0.0.1:ssh            10.0.0.2:53434         ESTAB      0
tcp        0      0 192.168.88.239:ssh      192.168.88.254:55871   ESTAB      0
[root@localhost ~]#
```

```
File Machine View Input Devices Help
[root@localhost ~]# ssh root@10.0.0.1
root@10.0.0.1's password:
Last login: Tue Mar 22 14:35:55 2022 from 192.168.88.254
[root@localhost ~]#
```



The image shows a single Oracle VM VirtualBox terminal window titled 'c7-1 [Running] - Oracle VM VirtualBox'. It displays the output of the command 'tcpdump host 192.168.88.254'. The output shows a series of network packets, including a 'ws-discovery' UDP packet and several SSH packets. The SSH packets show the establishment of a connection, with flags like 'P.I.' and sequence numbers.

```
File Machine View Input Devices Help
[root@localhost ~]# tcpdump host 192.168.88.254
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on em0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
15:01:35.592675 IP 192.168.88.254.51320 > 239.255.255.250.ws-discovery: UDP, length 656
15:01:45.791598 IP 192.168.88.254.55960 > localhost.localdomain.ssh: Flags [P.I], seq 710083913:710083949, ack 1652569759, win 8208, length 36
15:01:45.792769 IP localhost.localdomain.ssh > 192.168.88.254.55960: Flags [P.I], seq 1:37, ack 36, win 299, length 36
15:01:45.833448 IP 192.168.88.254.55960 > localhost.localdomain.ssh: Flags [..], ack 37, win 8208, length 0
15:01:45.854407 IP 192.168.88.254.55960 > localhost.localdomain.ssh: Flags [P.I], seq 36:72, ack 37, win 8208, length 36
15:01:45.854653 IP localhost.localdomain.ssh > 192.168.88.254.55960: Flags [P.I], seq 37:73, ack 72, win 299, length 36
15:01:45.895385 IP 192.168.88.254.55960 > localhost.localdomain.ssh: Flags [..], ack 73, win 8208, length 0
15:01:47.724645 IP 192.168.88.254.55960 > localhost.localdomain.ssh: Flags [P.I], seq 72:108, ack 73, win 8208, length 36
15:01:47.727824 IP localhost.localdomain.ssh > 192.168.88.254.55960: Flags [P.I], seq 73:109, ack 108, win 299, length 36
15:01:47.729850 IP localhost.localdomain.ssh > 192.168.88.254.55960: Flags [P.I], seq 109:257, ack 108, win 299, length 148
15:01:47.730086 IP 192.168.88.254.55960 > localhost.localdomain.ssh: Flags [..], ack 257, win 8207, length 0
```

c7-1 [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

NetHogs version 0.0.5

PID	USER	PROGRAM	DEV	SENT	RECEIVED
1747	root	sshd: root@pts/0	enp0s0	1.039	0.039 KB/sec
?	root	unknown TCP		0.000	0.000 KB/sec
TOTAL				1.039	0.039 KB/sec

c7-2 [Running] - Oracle VM VirtualBox

FileMachineViewInputDevicesHelp

top - 14:49:03 up 14 min, 2 users, load average: 0.00, 0.02, 0.05

Tasks: 93 total, 1 running, 92 sleeping, 0 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

Mem: 3888372 total, 3565568 free, 185040 used, 128764 buff/cache

Mem Swap: 039676 total, 039676 free, 0 used, 3580340 avail Mem

PID	USER	PR	NI	UIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
1	root	20	0	120804	6640	4164	S	0.0	0.2	0:01.62	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	kuworker/0:0H
5	root	20	0	0	0	0	S	0.0	0.0	0:00.00	kuworker/0:2:0
6	root	20	0	0	0	0	S	0.0	0.0	0:00.03	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	0:00.22	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	0:00.04	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	khumtaskd
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	khlockd
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
25	root	20	0	0	0	0	S	0.0	0.0	0:00.07	kuworker/0:1
30	root	20	0	0	0	0	S	0.0	0.0	0:00.00	ksmcpd0
31	root	25	5	0	0	0	S	0.0	0.0	0:00.00	kcmd
32	root	39	19	0	0	0	S	0.0	0.0	0:00.00	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	kaload

ВОПРОСЫ И ЗАДАНИЯ

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

mtr работает с ICMP, ICMP - это вспомогательный протокол, который используется в основном для диагностики сети.

2. Опишите значения столбцов статистики, выводимой утилитой mtr.

Loss% = процент пакетов, на которые не был получен ответ ICMP.

Snt = Количество пакетов, отправленных в каждый хоп.

Last = Время обхода последнего зонда traceroute, в миллисекундах.

Avg = Среднее время обхода всех зондов traceroute, в миллисекундах.

Best = Наименьшее время обхода всех зондов traceroute, в миллисекундах.

Wrst = Наибольшее время прохождения в обе стороны среди всех зондов traceroute, в миллисекундах.

StDev = Стандартное отклонение результатов зондирования до каждого хопа.

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

Классический Ethernet - в природе в настоящее время не встречается

Ethernet II - он же Arpa, в нём есть поле EtherType - определяющее тип вложения

Ethernet 802.3 - от Novell, он же RAW. В нём поле другое - Length - длина вложения. Заточенный он только под IPX.

Ethernet 802.2 - он же LLC. Имеет поле Length и LLC - позволяя внутри кадра держать несколько независимых потоков данных

Ethernet SNAP - к тому что выше добавляется поле SNAP - позволяя ещё более гибко разруливать потоки данных внутри кадра. Часто встречается в сложных сетях, в которых есть ether channel или прочие кастомные протоколы.

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

Ethernet II - он же Arpa, в нём есть поле EtherType - определяющее тип вложения

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

Судя по физическому адресу устройства (Включен в отслеживаемый кадр), первая половина его называется OUI (Organizational Unique Identifier), и они распространяются производителям организацией IEEE.

6. На какие адреса сетевого уровня осуществляются широковещательные рассылки?

Для уровня-2: Адрес ff:ff:ff:ff:ff:ff:ff:ff является широковещательным адресом.

Для уровня-3: Это последний адрес подсети. Например, для сети 192.168.1.0/24 широковещательный адрес 192.168.1.255

7. На какой канальный адрес осуществляются широковещательные рассылки?

Адрес ff:ff:ff:ff:ff:ff:ff:ff является широковещательным адресом для канального уровня.

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.

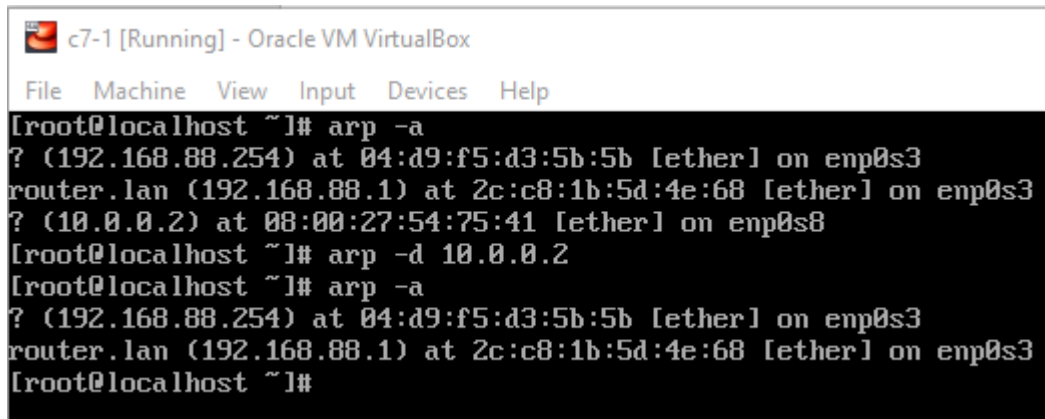
11. Как изменяется загрузка интерфейса в Части 5. п. 3? Почему?

Скорость не превышает 11,2 MiB, так как это максимальная скорость для данного интерфейса (100mbps).

12. На каком уровне модели OSI работает vnstat?

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

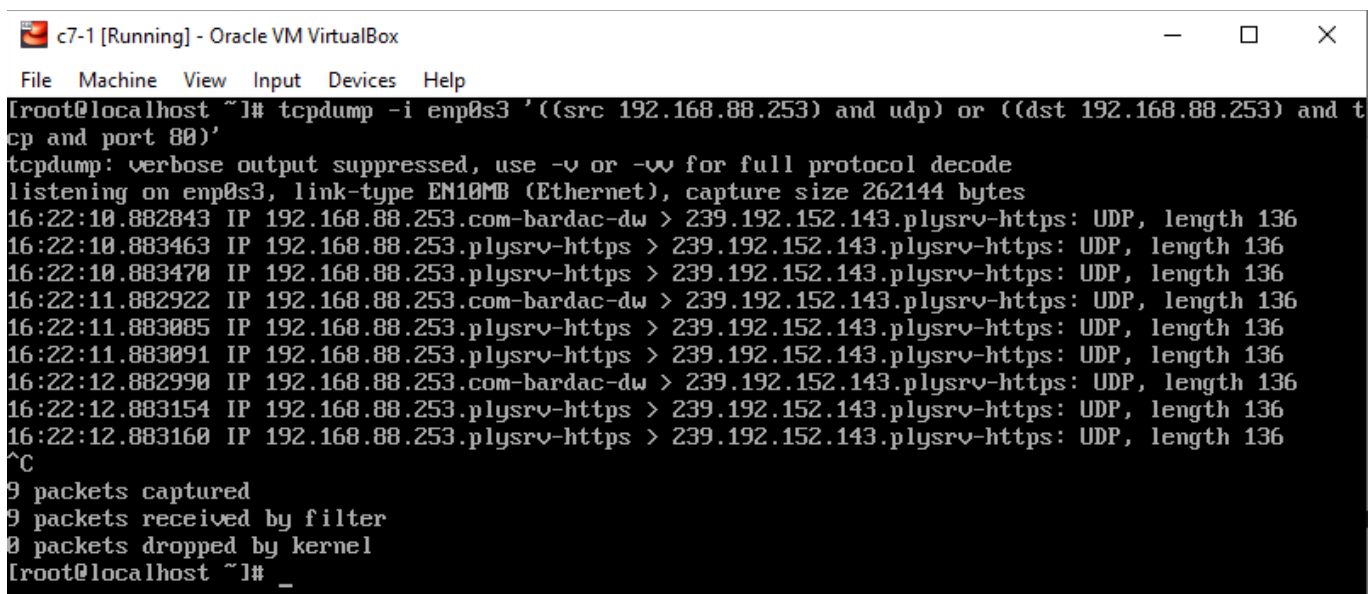
13. Как с помощью утилиты ip просмотреть arp-кэш и как его очистить. В каких случаях может понадобиться последняя операция?



```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost ~]# ip netns exec ns1 ip netns exec ns2 arp -a
? (192.168.88.254) at 04:d9:f5:d3:5b:5b [ether] on enp0s3
router.lan (192.168.88.1) at 2c:c8:1b:5d:4e:68 [ether] on enp0s3
? (10.0.0.2) at 08:00:27:54:75:41 [ether] on enp0s8
[root@localhost ~]# ip netns exec ns1 ip netns exec ns2 arp -d 10.0.0.2
[root@localhost ~]# ip netns exec ns1 ip netns exec ns2 arp -a
? (192.168.88.254) at 04:d9:f5:d3:5b:5b [ether] on enp0s3
router.lan (192.168.88.1) at 2c:c8:1b:5d:4e:68 [ether] on enp0s3
[root@localhost ~]#
```

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

Просто заменить 192.168.88.253 на 192.168.0.254 (скриншот для собственного тестирования)



```
c7-1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
[root@localhost ~]# tcpdump -i enp0s3 '((src 192.168.88.253) and udp) or ((dst 192.168.88.253) and t
cp and port 80)'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on enp0s3, link-type EN10MB (Ethernet), capture size 262144 bytes
16:22:10.882843 IP 192.168.88.253.com-bardac-dw > 239.192.152.143.plysrv-https: UDP, length 136
16:22:10.883463 IP 192.168.88.253.plysrv-https > 239.192.152.143.plysrv-https: UDP, length 136
16:22:10.883470 IP 192.168.88.253.plysrv-https > 239.192.152.143.plysrv-https: UDP, length 136
16:22:11.882922 IP 192.168.88.253.com-bardac-dw > 239.192.152.143.plysrv-https: UDP, length 136
16:22:11.883085 IP 192.168.88.253.plysrv-https > 239.192.152.143.plysrv-https: UDP, length 136
16:22:11.883091 IP 192.168.88.253.plysrv-https > 239.192.152.143.plysrv-https: UDP, length 136
16:22:12.882990 IP 192.168.88.253.com-bardac-dw > 239.192.152.143.plysrv-https: UDP, length 136
16:22:12.883154 IP 192.168.88.253.plysrv-https > 239.192.152.143.plysrv-https: UDP, length 136
16:22:12.883160 IP 192.168.88.253.plysrv-https > 239.192.152.143.plysrv-https: UDP, length 136
^C
9 packets captured
9 packets received by filter
0 packets dropped by kernel
[root@localhost ~]# _
```