

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА



Институт радиоэлектроники и информационных технологий
Кафедра информатики и систем управления

ОТЧЕТ

по лабораторной работе №5

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

(подпись)

Гай В.Е.
(фамилия, и.,о.)

СТУДЕНТ:

(подпись)

Карпычева А.Ю.
(фамилия, и.,о.)

18-АС
(шифр группы)

Работа защищена «__» _____

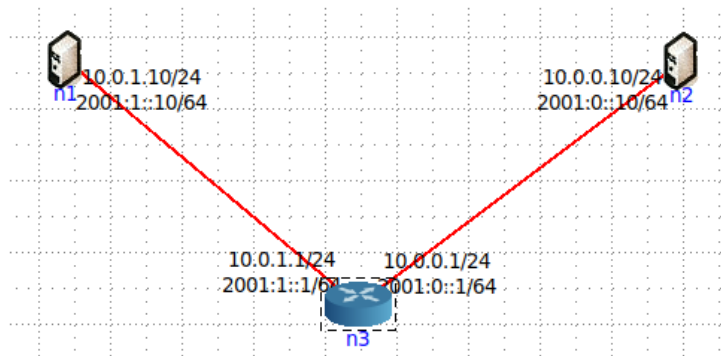
С оценкой _____

Нижний Новгород 2021

Задание

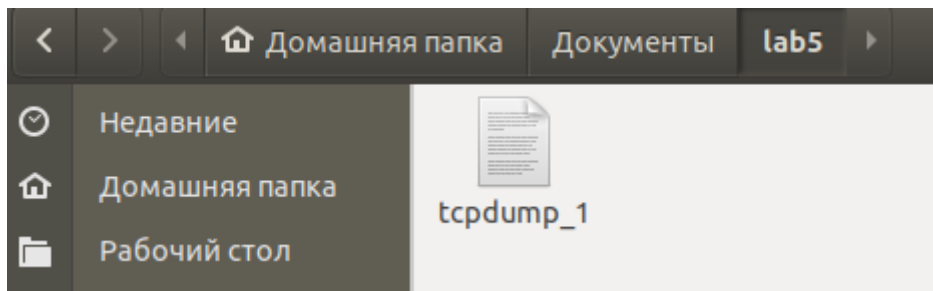
Работа с анализатором протоколов tcpdump

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.



```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.45435/n1.conf# tcpdump -c 10 -l | tee /home/core/Документы/lab5/tcpdump_1
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
16:10:03.724300 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
16:10:03.996424 IP 10.0.0.10 > n1: ICMP echo request, id 54, seq 1, length 64
16:10:03.996439 IP n1 > 10.0.0.10: ICMP echo reply, id 54, seq 1, length 64
16:10:05.001396 IP 10.0.0.10 > n1: ICMP echo request, id 54, seq 2, length 64
16:10:05.001424 IP n1 > 10.0.0.10: ICMP echo reply, id 54, seq 2, length 64
16:10:05.724723 IP _gateway > 224.0.0.5: OSPFv2, Hello, length 44
16:10:06.025607 IP 10.0.0.10 > n1: ICMP echo request, id 54, seq 3, length 64
16:10:06.025646 IP n1 > 10.0.0.10: ICMP echo reply, id 54, seq 3, length 64
16:10:07.049251 IP 10.0.0.10 > n1: ICMP echo request, id 54, seq 4, length 64
16:10:07.049279 IP n1 > 10.0.0.10: ICMP echo reply, id 54, seq 4, length 64
10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.45435/n1.conf#
```

```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.45435/n2.conf# ping 10.0.1.10
PING 10.0.1.10 (10.0.1.10) 56(84) bytes of data.
64 bytes from 10.0.1.10: icmp_seq=1 ttl=63 time=0.062 ms
64 bytes from 10.0.1.10: icmp_seq=2 ttl=63 time=0.142 ms
64 bytes from 10.0.1.10: icmp_seq=3 ttl=63 time=0.188 ms
64 bytes from 10.0.1.10: icmp_seq=4 ttl=63 time=0.146 ms
64 bytes from 10.0.1.10: icmp_seq=5 ttl=63 time=0.135 ms
64 bytes from 10.0.1.10: icmp_seq=6 ttl=63 time=0.123 ms
64 bytes from 10.0.1.10: icmp_seq=7 ttl=63 time=0.132 ms
64 bytes from 10.0.1.10: icmp_seq=8 ttl=63 time=0.132 ms
64 bytes from 10.0.1.10: icmp_seq=9 ttl=63 time=0.132 ms
^C
--- 10.0.1.10 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8173ms
rtt min/avg/max/mdev = 0.062/0.132/0.188/0.032 ms
root@n2:/tmp/pycore.45435/n2.conf#
```



2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

```

Терминал
Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.44167/n1.conf# tcpdump -c 5 -xx 'ether host ff:ff:ff:ff:ff:ff'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
20:07:30.364771 IP 10.0.0.10.36476 > 10.0.0.255.9999: UDP, length 5
    0x0000:  ffff ffff ffff 0000 00aa 0000 0800 4500
    0x0010:  0021 3a63 4000 4011 eb60 0a00 000a 0a00
    0x0020:  00ff 8e7c 270f 000d 566e 6865 6c6c 0a
20:07:31.853885 IP 10.0.0.10.57485 > 10.0.0.255.9999: UDP, length 5
    0x0000:  ffff ffff ffff 0000 00aa 0000 0800 4500
    0x0010:  0021 3a8e 4000 4011 eb35 0a00 000a 0a00
    0x0020:  00ff e08d 270f 000d 045d 6865 6c6c 0a
20:07:33.388198 IP 10.0.0.10.57087 > 10.0.0.255.9999: UDP, length 5
    0x0000:  ffff ffff ffff 0000 00aa 0000 0800 4500
    0x0010:  0021 3a94 4000 4011 eb2f 0a00 000a 0a00
    0x0020:  00ff deff 270f 000d 05eb 6865 6c6c 0a
20:07:34.828462 IP 10.0.0.10.32771 > 10.0.0.255.9999: UDP, length 5
    0x0000:  ffff ffff ffff 0000 00aa 0000 0800 4500
    0x0010:  0021 3b8f 4000 4011 ea34 0a00 000a 0a00
    0x0020:  00ff 8003 270f 000d 64e7 6865 6c6c 0a
20:07:36.593617 IP 10.0.0.10.33176 > 10.0.0.255.9999: UDP, length 5
    0x0000:  ffff ffff ffff 0000 00aa 0000 0800 4500
    0x0010:  0021 3bc6 4000 4011 e9fd 0a00 000a 0a00
    0x0020:  00ff 8198 270f 000d 6352 6865 6c6c 0a
5 packets captured

```

```

Терминал
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.44167/n2.conf# echo "hell" | socat - UDP4-DATAGRAM:10.0.0.255:9999,broadcast
root@n2:/tmp/pycore.44167/n2.conf# echo "hell" | socat - UDP4-DATAGRAM:10.0.0.255:9999,broadcast
root@n2:/tmp/pycore.44167/n2.conf# echo "hell" | socat - UDP4-DATAGRAM:10.0.0.255:9999,broadcast
root@n2:/tmp/pycore.44167/n2.conf# echo "hell" | socat - UDP4-DATAGRAM:10.0.0.255:9999,broadcast
root@n2:/tmp/pycore.44167/n2.conf# echo "hell" | socat - UDP4-DATAGRAM:10.0.0.255:9999,broadcast
root@n2:/tmp/pycore.44167/n2.conf#

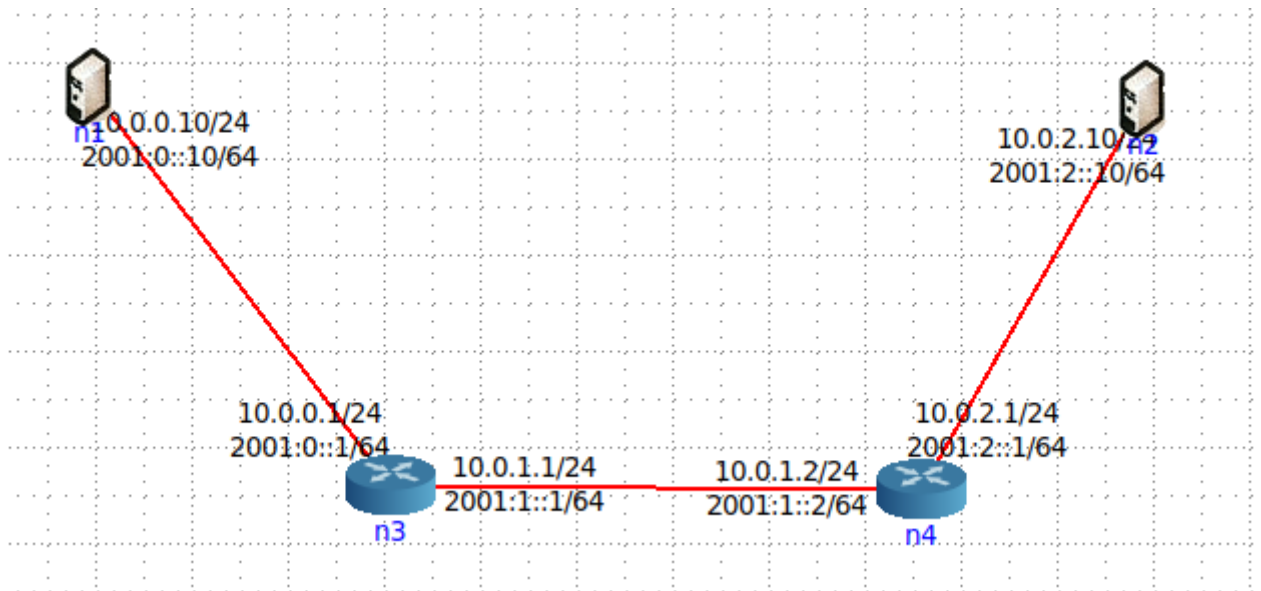
```

3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования пакетов воспользоваться утилитой ping.

```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.45435/n1.conf# tcpdump -c 3 -XX 'dst host 10.0.1.10 and ip proto \icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
17:10:27.499550 IP 10.0.0.10 > n1: ICMP echo request, id 38, seq 1, length 64
    0x0000: 0000 00aa 0003 0000 00aa 0002 0800 4500 .....E.
    0x0010: 0054 6935 4000 3f01 bd60 0a00 000a 0a00 .Ti5@.?.....
    0x0020: 010a 0800 c262 0026 0001 53a4 3b60 0000 ....b.&..S.;..
    0x0030: 0000 e09e 0700 0000 0000 1011 1213 1415 .....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!""#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 67
17:10:28.500859 IP 10.0.0.10 > n1: ICMP echo request, id 38, seq 2, length 64
    0x0000: 0000 00aa 0003 0000 00aa 0002 0800 4500 .....E.
    0x0010: 0054 6992 4000 3f01 bd03 0a00 000a 0a00 .Ti.@.?.....
    0x0020: 010a 0800 895c 0026 0002 54a4 3b60 0000 ....\.&..T.;..
    0x0030: 0000 18a4 0700 0000 0000 1011 1213 1415 .....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!""#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 67
17:10:29.513282 IP 10.0.0.10 > n1: ICMP echo request, id 38, seq 3, length 64
    0x0000: 0000 00aa 0003 0000 00aa 0002 0800 4500 .....E.
    0x0010: 0054 69ab 4000 3f01 bcea 0a00 000a 0a00 .Ti.@.?.....
    0x0020: 010a 0800 232b 0026 0003 55a4 3b60 0000 ....#+.&..U.;..
    0x0030: 0000 7dd4 0700 0000 0000 1011 1213 1415 ...}.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!""#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 67
3 packets captured
3 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.45435/n1.conf#
```

```
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.45435/n2.conf# ping 10.0.1.10
PING 10.0.1.10 (10.0.1.10) 56(84) bytes of data.
64 bytes from 10.0.1.10: icmp_seq=1 ttl=63 time=0.162 ms
64 bytes from 10.0.1.10: icmp_seq=2 ttl=63 time=0.159 ms
64 bytes from 10.0.1.10: icmp_seq=3 ttl=63 time=0.192 ms
64 bytes from 10.0.1.10: icmp_seq=4 ttl=63 time=0.077 ms
64 bytes from 10.0.1.10: icmp_seq=5 ttl=63 time=0.124 ms
64 bytes from 10.0.1.10: icmp_seq=6 ttl=63 time=0.138 ms
64 bytes from 10.0.1.10: icmp_seq=7 ttl=63 time=0.136 ms
^C
--- 10.0.1.10 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6077ms
rtt min/avg/max/mdev = 0.077/0.141/0.192/0.033 ms
root@n2:/tmp/pycore.45435/n2.conf#
```

4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 7. Результат работы программы писать в файл.



```
Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.33003/n1.conf# tcpdump -c 7 -w /home/core/Документы/lab5/tcpdump_4
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
7 packets captured
18 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.33003/n1.conf#
```

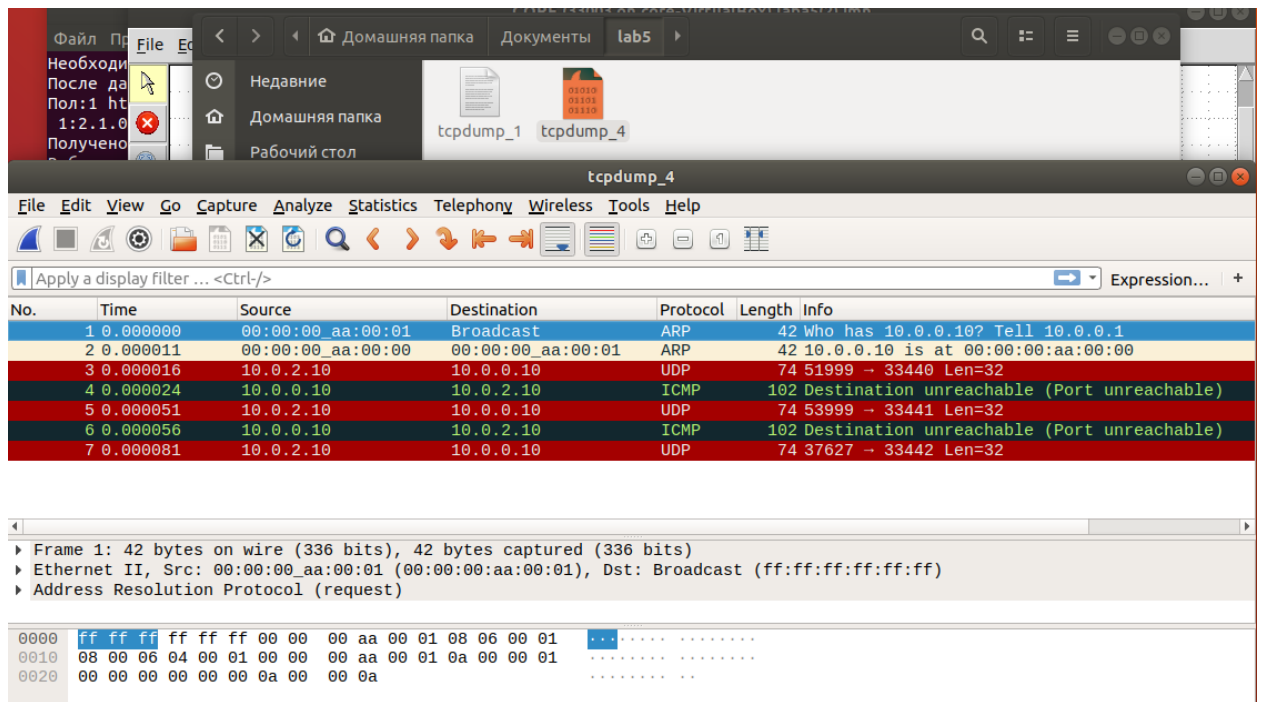
```
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.33003/n2.conf# traceroute 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 60 byte packets
 1 _gateway (10.0.2.1)  0.066 ms  0.010 ms  0.008 ms
 2 10.0.1.1 (10.0.1.1)  0.037 ms  0.011 ms  0.011 ms
 3 10.0.0.10 (10.0.0.10)  0.042 ms  0.016 ms  0.016 ms
root@n2:/tmp/pycore.33003/n2.conf#
```



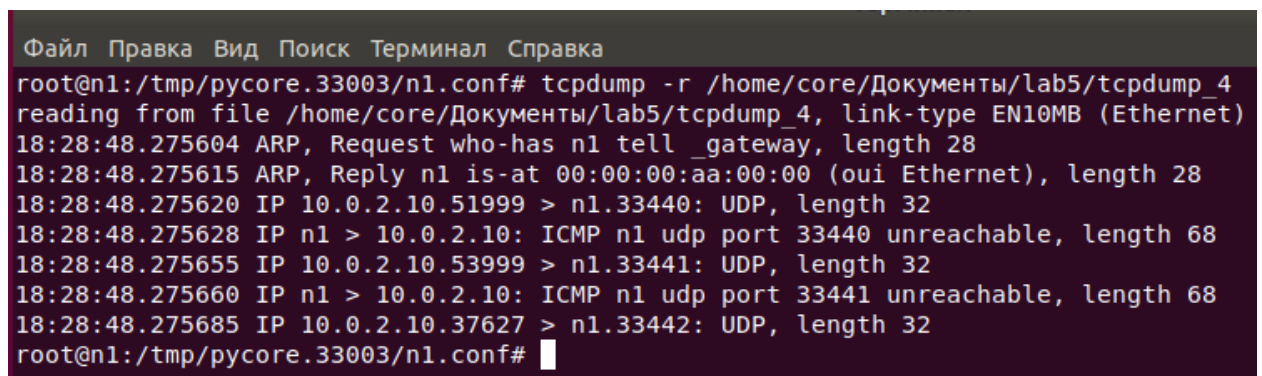
```

Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.33003/n1.conf# tcpdump -c 7 -XX
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:30:14.002398 IP 10.0.2.10.46553 > n1.33440: UDP, length 32
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 003c 7f91 0000 0111 240d 0a00 020a 0a00 .<.....$.
    0x0020: 000a b5d9 82a0 0028 bc0b 4041 4243 4445 .....(..@ABCDE
    0x0030: 4647 4849 4a4b 4c4d 4e4f 5051 5253 5455 FGHIJKLMNOPQRSTU
    0x0040: 5657 5859 5a5b 5c5d 5e5f VWXYZ[\]^_
18:30:14.002415 IP n1 > 10.0.2.10: ICMP n1 udp port 33440 unreachable, length 68
    0x0000: 0000 00aa 0001 0000 00aa 0000 0800 45c0 .....E.
    0x0010: 0058 b75c 0000 4001 ac75 0a00 000a 0a00 .X.\..@..u.....
    0x0020: 020a 0303 134a 0000 0000 4500 003c 7f91 .....J....E..<..
    0x0030: 0000 0111 240d 0a00 020a 0a00 000a b5d9 ....$.
    0x0040: 82a0 0028 bc0b 4041 4243 4445 4647 4849 ...(..@ABCDEFGHI
    0x0050: 4a4b 4c4d 4e4f 5051 5253 5455 5657 5859 JKLMNOPQRSTUVWXY
    0x0060: 5a5b 5c5d 5e5f Z[\]^_
18:30:14.003857 IP 10.0.2.10.53784 > n1.33441: UDP, length 32
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 003c 7f92 0000 0111 240c 0a00 020a 0a00 .<.....$.
    0x0020: 000a d218 82a1 0028 9fcb 4041 4243 4445 .....(..@ABCDE
    0x0030: 4647 4849 4a4b 4c4d 4e4f 5051 5253 5455 FGHIJKLMNOPQRSTU
    0x0040: 5657 5859 5a5b 5c5d 5e5f VWXYZ[\]^_
18:30:14.003870 IP n1 > 10.0.2.10: ICMP n1 udp port 33441 unreachable, length 68
    0x0000: 0000 00aa 0001 0000 00aa 0000 0800 45c0 .....E.
    0x0010: 0058 b75d 0000 4001 ac74 0a00 000a 0a00 .X.]..@..t.....
    0x0020: 020a 0303 134a 0000 0000 4500 003c 7f92 .....J....E..<..
    0x0030: 0000 0111 240c 0a00 020a 0a00 000a d218 ....$.
    0x0040: 82a1 0028 9fcb 4041 4243 4445 4647 4849 ...(..@ABCDEFGHI
    0x0050: 4a4b 4c4d 4e4f 5051 5253 5455 5657 5859 JKLMNOPQRSTUVWXY
    0x0060: 5a5b 5c5d 5e5f Z[\]^_
18:30:14.003903 IP 10.0.2.10.34362 > n1.33442: UDP, length 32
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 003c 7f93 0000 0111 240b 0a00 020a 0a00 .<.....$.
    0x0020: 000a 863a 82a2 0028 eba8 4041 4243 4445 .....(..@ABCDE
    0x0030: 4647 4849 4a4b 4c4d 4e4f 5051 5253 5455 FGHIJKLMNOPQRSTU
    0x0040: 5657 5859 5a5b 5c5d 5e5f VWXYZ[\]^_
18:30:14.003908 IP n1 > 10.0.2.10: ICMP n1 udp port 33442 unreachable, length 68
    0x0000: 0000 00aa 0001 0000 00aa 0000 0800 45c0 .....E.
    0x0010: 0058 b75e 0000 4001 ac73 0a00 000a 0a00 .X.^..@..s.....
    0x0020: 020a 0303 134a 0000 0000 4500 003c 7f93 .....J....E..<..
    0x0030: 0000 0111 240b 0a00 020a 0a00 000a 863a ....$.
    0x0040: 82a2 0028 eba8 4041 4243 4445 4647 4849 ...(..@ABCDEFGHI
    0x0050: 4a4b 4c4d 4e4f 5051 5253 5455 5657 5859 JKLMNOPQRSTUVWXY
    0x0060: 5a5b 5c5d 5e5f Z[\]^_
18:30:14.003937 IP 10.0.2.10.46049 > n1.33443: UDP, length 32
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 003c 7f94 0000 0211 230a 0a00 020a 0a00 .<.....#.
    0x0020: 000a b3e1 82a3 0028 be00 4041 4243 4445 .....(..@ABCDE
    0x0030: 4647 4849 4a4b 4c4d 4e4f 5051 5253 5455 FGHIJKLMNOPQRSTU
    0x0040: 5657 5859 5a5b 5c5d 5e5f VWXYZ[\]^_
7 packets captured
16 packets received by filter
7 packets dropped by kernel
root@n1:/tmp/pycore.33003/n1.conf#

```



5. Прочсть программой tcpdump созданный в предыдущем пункте файл.



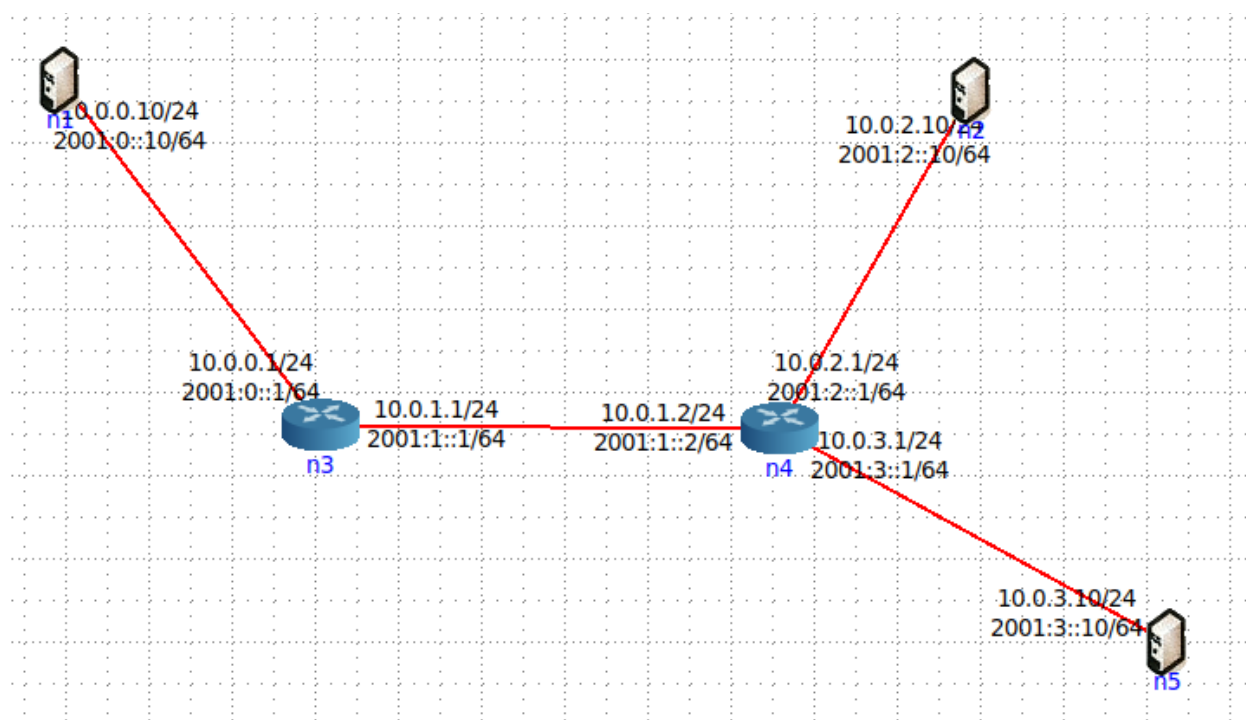
```

root@n1:/tmp/pycore.33003/n1.conf# tcpdump -XX -r /home/core/Документы/lab5/tcpdump_4
reading from file /home/core/Документы/lab5/tcpdump_4, link-type EN10MB (Ethernet)
18:28:48.275604 ARP, Request who-has n1 tell _gateway, length 28
    0x0000:  ffff ffff ffff 0000 00aa 0001 0806 0001  .....
    0x0010:  0800 0604 0001 0000 00aa 0001 0a00 0001  .....
    0x0020:  0000 0000 0000 0a00 000a                .....
18:28:48.275615 ARP, Reply n1 is-at 00:00:00:aa:00:00 (oui Ethernet), length 28
    0x0000:  0000 00aa 0001 0000 00aa 0000 0806 0001  .....
    0x0010:  0800 0604 0002 0000 00aa 0000 0a00 000a  .....
    0x0020:  0000 00aa 0001 0a00 0001                .....
18:28:48.275620 IP 10.0.2.10.51999 > n1.33440: UDP, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  .....E.
    0x0010:  003c 6568 0000 0111 3e36 0a00 020a 0a00  .<eh....>6.....
    0x0020:  000a cb1f 82a0 0028 a6c5 4041 4243 4445  .....(..@ABCDE
    0x0030:  4647 4849 4a4b 4c4d 4e4f 5051 5253 5455  FGHIJKLMNOPQRSTU
    0x0040:  5657 5859 5a5b 5c5d 5e5f                VWXYZ[\]^_
18:28:48.275628 IP n1 > 10.0.2.10: ICMP n1 udp port 33440 unreachable, length 68
    0x0000:  0000 00aa 0001 0000 00aa 0000 0800 45c0  .....E.
    0x0010:  0058 a73a 0000 4001 bc97 0a00 000a 0a00  .X.:..@.....
    0x0020:  020a 0303 134a 0000 0000 4500 003c 6568  ....J....E..<eh
    0x0030:  0000 0111 3e36 0a00 020a 0a00 000a cb1f  ....>6.....
    0x0040:  82a0 0028 a6c5 4041 4243 4445 4647 4849  ...(..@ABCDEFGHI
    0x0050:  4a4b 4c4d 4e4f 5051 5253 5455 5657 5859  JKLMNOPQRSTUVWXYZ
    0x0060:  5a5b 5c5d 5e5f                Z[\]^_
18:28:48.275655 IP 10.0.2.10.53999 > n1.33441: UDP, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  .....E.
    0x0010:  003c 6569 0000 0111 3e35 0a00 020a 0a00  .<ei....>5.....
    0x0020:  000a d2ef 82a1 0028 9ef4 4041 4243 4445  .....(..@ABCDE
    0x0030:  4647 4849 4a4b 4c4d 4e4f 5051 5253 5455  FGHIJKLMNOPQRSTU
    0x0040:  5657 5859 5a5b 5c5d 5e5f                VWXYZ[\]^_
18:28:48.275660 IP n1 > 10.0.2.10: ICMP n1 udp port 33441 unreachable, length 68
    0x0000:  0000 00aa 0001 0000 00aa 0000 0800 45c0  .....E.
    0x0010:  0058 a73b 0000 4001 bc96 0a00 000a 0a00  .X.;..@.....
    0x0020:  020a 0303 134a 0000 0000 4500 003c 6569  ....J....E..<ei
    0x0030:  0000 0111 3e35 0a00 020a 0a00 000a d2ef  ....>5.....
    0x0040:  82a1 0028 9ef4 4041 4243 4445 4647 4849  ...(..@ABCDEFGHI
    0x0050:  4a4b 4c4d 4e4f 5051 5253 5455 5657 5859  JKLMNOPQRSTUVWXYZ
    0x0060:  5a5b 5c5d 5e5f                Z[\]^_
18:28:48.275685 IP 10.0.2.10.37627 > n1.33442: UDP, length 32
    0x0000:  0000 00aa 0000 0000 00aa 0001 0800 4500  .....E.
    0x0010:  003c 656a 0000 0111 3e34 0a00 020a 0a00  .<ej....>4.....
    0x0020:  000a 92fb 82a2 0028 dee7 4041 4243 4445  .....(..@ABCDE
    0x0030:  4647 4849 4a4b 4c4d 4e4f 5051 5253 5455  FGHIJKLMNOPQRSTU
    0x0040:  5657 5859 5a5b 5c5d 5e5f                VWXYZ[\]^_
root@n1:/tmp/pycore.33003/n1.conf#

```


6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP,

ICMP



1-Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные с определенного IP-адреса.

```
Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.33003/n1.conf# tcpdump -c 4 -XX 'src host 10.0.3.10 and ip proto \icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
18:59:39.518245 IP 10.0.3.10 > n1: ICMP echo request, id 42, seq 1, length 64
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 0054 c252 4000 3e01 6343 0a00 030a 0a00 .T.R@.>.cC.....
    0x0020: 000a 0800 dcfb 002a 0001 ebbd 3b60 0000 .....*.....;`..
    0x0030: 0000 2de8 0700 0000 0000 1011 1213 1415 ..~.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 67
18:59:40.519039 IP 10.0.3.10 > n1: ICMP echo request, id 42, seq 2, length 64
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 0054 c2e2 4000 3e01 62b3 0a00 030a 0a00 .T..@.>.b.....
    0x0020: 000a 0800 b7f7 002a 0002 ecdb 3b60 0000 .....*.....;`..
    0x0030: 0000 51eb 0700 0000 0000 1011 1213 1415 ..Q.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 67
18:59:41.545719 IP 10.0.3.10 > n1: ICMP echo request, id 42, seq 3, length 64
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 0054 c395 4000 3e01 6200 0a00 030a 0a00 .T..@.>.b.....
    0x0020: 000a 0800 fe8e 002a 0003 edbd 3b60 0000 .....*.....;`..
    0x0030: 0000 0953 0800 0000 0000 1011 1213 1415 ...S.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 67
18:59:42.569690 IP 10.0.3.10 > n1: ICMP echo request, id 42, seq 4, length 64
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 0054 c478 4000 3e01 611d 0a00 030a 0a00 .T.x@.>.a.....
    0x0020: 000a 0800 e92f 002a 0004 eebd 3b60 0000 ...../*.....;`..
    0x0030: 0000 1db1 0800 0000 0000 1011 1213 1415 .....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 67
4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.33003/n1.conf# tcpdump -c 4 -XX 'src host 10.0.2.10 and ip proto \icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
```

```
root@n5:/tmp/pycore.33003/n5.conf# ping 10.0.0.10
PING 10.0.0.10 (10.0.0.10) 56(84) bytes of data.
64 bytes from 10.0.0.10: icmp_seq=1 ttl=62 time=0.096 ms
64 bytes from 10.0.0.10: icmp_seq=2 ttl=62 time=0.070 ms
64 bytes from 10.0.0.10: icmp_seq=3 ttl=62 time=0.146 ms
64 bytes from 10.0.0.10: icmp_seq=4 ttl=62 time=0.170 ms
64 bytes from 10.0.0.10: icmp_seq=5 ttl=62 time=0.162 ms
64 bytes from 10.0.0.10: icmp_seq=6 ttl=62 time=0.073 ms
^C
--- 10.0.0.10 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5103ms
rtt min/avg/max/mdev = 0.070/0.110/0.170/0.043 ms
```

2-Перехватить 3 пакета протокола UDP, отправленные с указанного IP

```
root@n1:/tmp/pycore.33003/n1.conf# tcpdump -c 3 -q 'src host 10.0.2.10 and ip proto \udp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:31:21.552134 IP 10.0.2.10.58560 > n1.33440: UDP, length 32
19:31:21.553805 IP 10.0.2.10.41350 > n1.33441: UDP, length 32
19:31:21.553892 IP 10.0.2.10.46872 > n1.33442: UDP, length 32
3 packets captured
```

```
root@n2:/tmp/pycore.33003/n2.conf# traceroute 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 60 byte packets
 1  _gateway (10.0.2.1)  0.037 ms  0.009 ms  0.007 ms
 2  10.0.1.1 (10.0.1.1)  0.021 ms  0.011 ms  0.010 ms
 3  10.0.0.10 (10.0.0.10)  0.033 ms  0.082 ms  0.019 ms
```

3-Перехватить все пакеты, кроме ICMP. Количество захватываемых пакетов ограничить 4.

```
Файл Правка Вид Поиск Терминал Справка
root@n1:/tmp/pycore.33003/n1.conf# tcpdump -c 4 -q 'src host 10.0.3.10 and not icmp'
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
19:14:05.701504 IP 10.0.3.10.43023 > n1.33440: UDP, length 32
19:14:05.702925 IP 10.0.3.10.51331 > n1.33441: UDP, length 32
19:14:05.703008 IP 10.0.3.10.53689 > n1.33442: UDP, length 32
19:14:05.703045 IP 10.0.3.10.57017 > n1.33443: UDP, length 32
4 packets captured
```

```
Файл Правка Вид Поиск Терминал Справка
root@n5:/tmp/pycore.33003/n5.conf# traceroute 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 60 byte packets
 1  _gateway (10.0.3.1)  0.038 ms  0.008 ms  0.008 ms
 2  10.0.1.1 (10.0.1.1)  0.022 ms  0.011 ms  0.010 ms
 3  10.0.0.10 (10.0.0.10)  0.033 ms  0.042 ms  0.025 ms
root@n5:/tmp/pycore.33003/n5.conf#
```

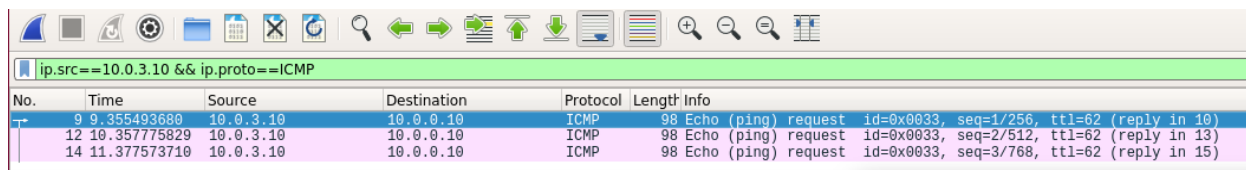
Работа с анализатором протоколов wireshark

1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.

ip.dst==10.0.0.255						
No.	Time	Source	Destination	Protocol	Length	Info
2	1.991062262	10.0.0.10	10.0.0.255	UDP	47	35241 → 9999 Len=5
3	6.327832824	10.0.0.10	10.0.0.255	UDP	47	39299 → 9999 Len=5
4	9.167702684	10.0.0.10	10.0.0.255	UDP	47	48854 → 9999 Len=5
5	11.310312207	10.0.0.10	10.0.0.255	UDP	47	58472 → 9999 Len=5
6	12.758318868	10.0.0.10	10.0.0.255	UDP	47	40056 → 9999 Len=5

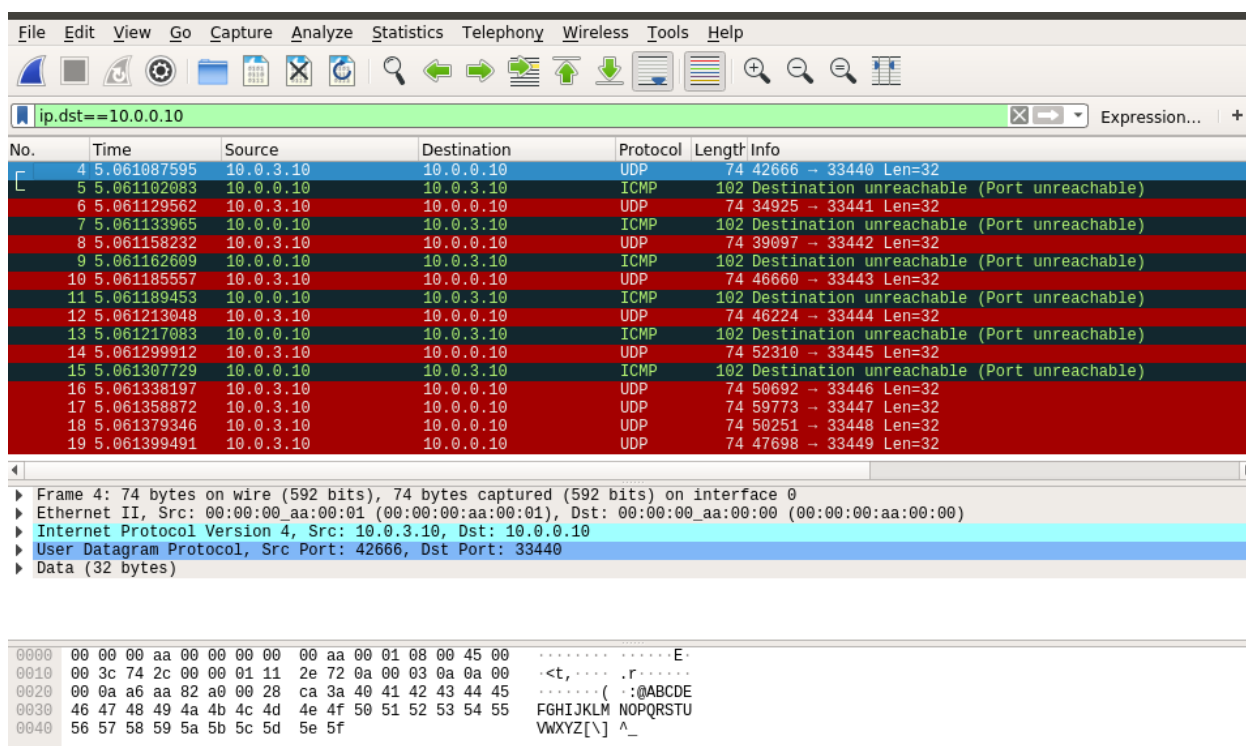
```
Терминал
Файл Правка Вид Поиск Терминал Справка
root@n2:/tmp/pycore.44167/n2.conf# echo "hell" | socat - UDP4-DATAGRAM:10.0.0.255:9999,broadcast
```

2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.



No.	Time	Source	Destination	Protocol	Length	Info
9	9.355493680	10.0.3.10	10.0.0.10	ICMP	98	Echo (ping) request id=0x0033, seq=1/256, ttl=62 (reply in 10)
12	10.357775829	10.0.3.10	10.0.0.10	ICMP	98	Echo (ping) request id=0x0033, seq=2/512, ttl=62 (reply in 13)
14	11.377573710	10.0.3.10	10.0.0.10	ICMP	98	Echo (ping) request id=0x0033, seq=3/768, ttl=62 (reply in 15)

3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.



No.	Time	Source	Destination	Protocol	Length	Info
4	5.061087595	10.0.3.10	10.0.0.10	UDP	74	42666 → 33440 Len=32
5	5.061102083	10.0.0.10	10.0.3.10	ICMP	102	Destination unreachable (Port unreachable)
6	5.061129562	10.0.3.10	10.0.0.10	UDP	74	34925 → 33441 Len=32
7	5.061133965	10.0.0.10	10.0.3.10	ICMP	102	Destination unreachable (Port unreachable)
8	5.061158232	10.0.3.10	10.0.0.10	UDP	74	39097 → 33442 Len=32
9	5.061162609	10.0.0.10	10.0.3.10	ICMP	102	Destination unreachable (Port unreachable)
10	5.061185557	10.0.3.10	10.0.0.10	UDP	74	46660 → 33443 Len=32
11	5.061189453	10.0.0.10	10.0.3.10	ICMP	102	Destination unreachable (Port unreachable)
12	5.061213048	10.0.3.10	10.0.0.10	UDP	74	46224 → 33444 Len=32
13	5.061217083	10.0.0.10	10.0.3.10	ICMP	102	Destination unreachable (Port unreachable)
14	5.061299912	10.0.3.10	10.0.0.10	UDP	74	52310 → 33445 Len=32
15	5.061307729	10.0.0.10	10.0.3.10	ICMP	102	Destination unreachable (Port unreachable)
16	5.061338197	10.0.3.10	10.0.0.10	UDP	74	50692 → 33446 Len=32
17	5.061358872	10.0.3.10	10.0.0.10	UDP	74	59773 → 33447 Len=32
18	5.061379346	10.0.3.10	10.0.0.10	UDP	74	50251 → 33448 Len=32
19	5.061399491	10.0.3.10	10.0.0.10	UDP	74	47698 → 33449 Len=32

Frame 4: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
 Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: 00:00:00_aa:00:00 (00:00:00:aa:00:00)
 Internet Protocol Version 4, Src: 10.0.3.10, Dst: 10.0.0.10
 User Datagram Protocol, Src Port: 42666, Dst Port: 33440
 Data (32 bytes)

```

0000  00 00 00 aa 00 00 00 00 aa 00 01 08 00 45 00  ....E.
0010  00 3c 74 2c 00 00 01 11 2e 72 0a 00 03 0a 0a 00  <t....r....
0020  00 0a a6 aa 82 a0 00 28 ca 3a 40 41 42 43 44 45  ....(:@ABCDE
0030  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55  FGHIJKLM NOPQRSTU
0040  56 57 58 59 5a 5b 5c 5d 5e 5f                   VWXYZ[\] ^_
  
```

```

Time | 10.0.0.1 | 10.0.3.10 |
fe80::200:ff:feaa:1 | 00:00:00_aa:00:00 |
| 224.0.0.5 | 10.0.0.10 |
| ff02::5 | 00:00:00_aa:00:01 |
0.000000000 | Hello Packet | | | OSPF: Hello Packet
| (0) |-----> (0) | | |
2.001114711 | Hello Packet | | | OSPF: Hello Packet
| (0) |-----> (0) | | |
4.003168237 | Hello Packet | | | OSPF: Hello Packet
| (0) |-----> (0) | | |
5.061087595 | | | 42666 → 33440 Len=32
| | | | UDP: 42666 →
33440 Len=32 | | | (42666) -----> (33440)
5.061102083 | | | Destination unreachable | ICMP: Destination
unreachable (Port unreachable) | | | (33440) <----- (42666)
5.061129562 | | | 34925 → 33441 Len=32 | UDP: 34925 →
33441 Len=32 | | | (34925) -----> (33441)
5.061133965 | | | Destination unreachable | ICMP: Destination
unreachable (Port unreachable) | | | (33441) <----- (34925)

```

4. Прочсть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.

tcpdump_4						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/> Expression... +						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	00:00:00_aa:00:01	Broadcast	ARP	42	Who has 10.0.0.10? Tell 10.0.0.1
2	0.000011	00:00:00_aa:00:00	00:00:00_aa:00:01	ARP	42	10.0.0.10 is at 00:00:00:aa:00:00
3	0.000016	10.0.2.10	10.0.0.10	UDP	74	51999 → 33440 Len=32
4	0.000024	10.0.0.10	10.0.2.10	ICMP	102	Destination unreachable (Port unreachable)
5	0.000051	10.0.2.10	10.0.0.10	UDP	74	53999 → 33441 Len=32
6	0.000056	10.0.0.10	10.0.2.10	ICMP	102	Destination unreachable (Port unreachable)
7	0.000081	10.0.2.10	10.0.0.10	UDP	74	37627 → 33442 Len=32

▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits)
 ▶ Ethernet II, Src: 00:00:00_aa:00:01 (00:00:00:aa:00:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
 ▶ Address Resolution Protocol (request)