

Минобрнауки России
Федеральное государственное бюджетное образовательное
учреждение высшего образования
НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
ИМ. Р.Е. АЛЕКСЕЕВА
ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ

Курс “Сети и телекоммуникация”
Отчет по лабораторной работе №1

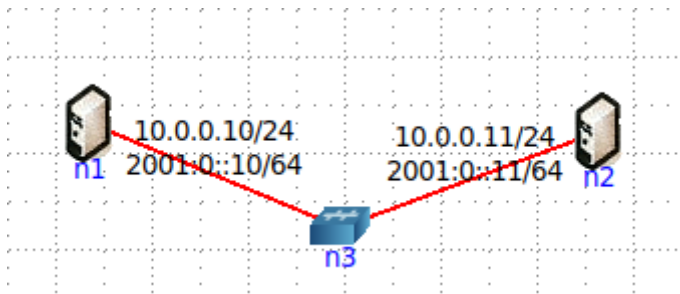
Выполнил: Соков С.А.

Проверил: Гай В.Е.

Нижний Новгород 2021

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
root@n1:/tmp/pycore.46169/n1.conf# tcpdump -c 10
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:43:50.174842 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 35, seq 7755, length 64
15:43:50.174864 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 7755, length 64
15:43:51.198521 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 35, seq 7756, length 64
15:43:51.198543 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 7756, length 64
15:43:52.222424 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 35, seq 7757, length 64
15:43:52.222486 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 7757, length 64
15:43:53.246935 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 35, seq 7758, length 64
15:43:53.246959 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 7758, length 64
15:43:54.270364 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 35, seq 7759, length 64
15:43:54.270387 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 7759, length 64
10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.46169/n1.conf# tcpdump -c 10 -w output.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10 packets captured
10 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.46169/n1.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
root@n1:/tmp/pycore.46169/n1.conf# tcpdump -c 5 -e -XX
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:47:32.382338 00:00:00:aa:00:01 (oui Ethernet) > 00:00:00:aa:00:00 (oui Ethernet), ethertype IPv4 (0x0800), length 98: 10.0.0.11 > 10.0.0.10: ICMP echo request, id 35, seq 7972, length 64
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 0054 2f3d 4000 4001 f737 0a00 0000 0a00 ..T/_@.0.0.0.0.0.0.
    0x0020: 000a 0800 3dd6 0023 1f24 e4d9 9760 0000 .....#.S.....
    0x0030: 0000 5ad5 0500 0000 0000 1011 1213 1415 ..Z.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 .....67
15:47:32.382370 00:00:00:aa:00:00 (oui Ethernet) > 00:00:00:aa:00:01 (oui Ethernet), ethertype IPv4 (0x0800), length 98: 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 7972, length 64
    0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
    0x0010: 0054 5948 0000 4001 0d4d 0a00 000a 0a00 ..TYH..@.0.0.0.0.0.0.
    0x0020: 000b 0000 45d6 0023 1f24 e4d9 9760 0000 .....#.S.....
    0x0030: 0000 5ad5 0500 0000 0000 1011 1213 1415 ..Z.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 .....67
15:47:33.406192 00:00:00:aa:00:00 (oui Ethernet) > 00:00:00:aa:00:00 (oui Ethernet), ethertype IPv4 (0x0800), length 98: 10.0.0.11 > 10.0.0.10: ICMP echo request, id 35, seq 7973, length 64
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 0054 2f3f 4000 4001 f735 0a00 0000 0a00 ..T/_@.0.0.0.0.0.0.
    0x0020: 000a 0800 0a78 0023 1f25 e5d9 9760 0000 .....#.S.....
    0x0030: 0000 8c32 0600 0000 0000 1011 1213 1415 ..2.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 .....67
15:47:33.406222 00:00:00:aa:00:00 (oui Ethernet) > 00:00:00:aa:00:01 (oui Ethernet), ethertype IPv4 (0x0800), length 98: 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 7973, length 64
    0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
    0x0010: 0054 5a1f 0000 4001 0c76 0a00 000a 0a00 ..TZ..@.0.0.0.0.0.0.
    0x0020: 000b 0000 1278 0023 1f25 e5d9 9760 0000 .....#.S.....
    0x0030: 0000 8c32 0600 0000 0000 1011 1213 1415 ..2.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 .....67
15:47:34.436615 00:00:00:aa:00:00 (oui Ethernet) > 00:00:00:aa:00:00 (oui Ethernet), ethertype IPv4 (0x0800), length 98: 10.0.0.11 > 10.0.0.10: ICMP echo request, id 35, seq 7974, length 64
    0x0000: 0000 00aa 0000 0000 00aa 0001 0800 4500 .....E.
    0x0010: 0054 2f4f 4000 4001 f6b5 0a00 0000 0a00 ..T/_@.0.0.0.0.0.0.
    0x0020: 000a 0800 9917 0023 1f26 e6d9 9760 0000 .....#.S.....
    0x0030: 0000 fc91 0600 0000 0000 1011 1213 1415 ..Z.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 .....67
5 packets captured
6 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.46169/n1.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.

```
root@n1:/tmp/pycore.46169/n1.conf# tcpdump -c 3 -XX 'dst host 10.0.0.11 and ip>
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
15:52:02.717994 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 8236, length 64
    0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
    0x0010: 0054 d957 0000 4001 8d3d 0a00 000a 0a00 ..T.W..@.=.....
    0x0020: 000b 0000 11ae 0023 202c f2da 9760 0000 .....#.S.....
    0x0030: 0000 7af4 0a00 0000 0000 1011 1213 1415 ..Z.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 .....67
15:52:03.742319 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 8237, length 64
    0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
    0x0010: 0054 d982 0000 4001 8d12 0a00 000a 0a00 ..T....@.....
    0x0020: 000b 0000 064e 0023 202d f3da 9760 0000 .....N.#.-....`..
    0x0030: 0000 8453 0b00 0000 0000 1011 1213 1415 ...S.....
    0x0040: 1617 1819 1a1b 1c1d 1e1f 2021 2223 2425 .....!"#$%
    0x0050: 2627 2829 2a2b 2c2d 2e2f 3031 3233 3435 &'()*+,-./012345
    0x0060: 3637 .....67
15:52:04.766631 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 35, seq 8238, length 64
    0x0000: 0000 00aa 0001 0000 00aa 0000 0800 4500 .....E.
    0x0010: 0054 d99b 0000 4001 8cf9 0a00 000a 0a00 ..T....@.....
    0x0020: 000b 0000 0eee 0023 202e f4da 9760 0000 .....#.S.....
    0x0030: 0000 7ab2 0b00 0000 0000 1011 1213 1415 ..Z.....
    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.46169/n1.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.

```
root@n2:/tmp/pycore.46169/n2.conf# traceroute -q 7 -I 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 60 byte packets
 1 10.0.0.10 (10.0.0.10) 0.039 ms 0.013 ms 0.012 ms 0.012 ms 0.013 ms 0.012 ms 0.012 ms
root@n2:/tmp/pycore.46169/n2.conf#
```

```
root@n1:/tmp/pycore.46169/n1.conf# tcpdump -c 7 -w output-2.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
7 packets captured
32 packets received by filter
0 packets dropped by kernel
```

```
root@n1:/tmp/pycore.46169/n1.conf# tcpdump -c 7 -r output-2.cap -xx -X
reading from file output-2.cap, link-type EN10MB (Ethernet)
21:02:21.340808 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 122, seq 1, length 40
    0x0000: 4500 003c 74d3 0000 0101 30da 0a00 000b  E..<t.....0.....
    0x0010: 0a00 000a 0800 81ff 007a 0001 4849 4a4b  .....z..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b  LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667             \]^_`abcdefg
21:02:21.340823 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 122, seq 1, length 40
    0x0000: 4500 003c 93b3 0000 4001 d2f9 0a00 000a  E..<....@.....
    0x0010: 0a00 000b 0000 89ff 007a 0001 4849 4a4b  .....z..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b  LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667             \]^_`abcdefg
21:02:21.340838 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 122, seq 2, length 40
    0x0000: 4500 003c 74d4 0000 0101 30d9 0a00 000b  E..<t.....0.....
    0x0010: 0a00 000a 0800 81fe 007a 0002 4849 4a4b  .....z..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b  LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667             \]^_`abcdefg
21:02:21.340843 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 122, seq 2, length 40
    0x0000: 4500 003c 93b4 0000 4001 d2f8 0a00 000a  E..<....@.....
    0x0010: 0a00 000b 0000 89fe 007a 0002 4849 4a4b  .....z..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b  LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667             \]^_`abcdefg
21:02:21.340853 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 122, seq 3, length 40
    0x0000: 4500 003c 74d5 0000 0101 30d8 0a00 000b  E..<t.....0.....
    0x0010: 0a00 000a 0800 81fd 007a 0003 4849 4a4b  .....z..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b  LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667             \]^_`abcdefg
21:02:21.340858 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 122, seq 3, length 40
    0x0000: 4500 003c 93b5 0000 4001 d2f7 0a00 000a  E..<....@.....
    0x0010: 0a00 000b 0000 89fd 007a 0003 4849 4a4b  .....z..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b  LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667             \]^_`abcdefg
21:02:21.340868 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 122, seq 4, length 40
    0x0000: 4500 003c 74d6 0000 0101 30d7 0a00 000b  E..<t.....0.....
    0x0010: 0a00 000a 0800 81fc 007a 0004 4849 4a4b  .....z..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b  LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667             \]^_`abcdefg
```

5. Прочсть программой tcpdump созданный в предыдущем пункте файл.


```

root@n1:/tmp/pycore.46169/n1.conf# tcpdump -c 7 -r output-2.cap
reading from file output-2.cap, link-type EN10MB (Ethernet)
21:02:21.340808 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 122, seq 1, length 40
21:02:21.340823 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 122, seq 1, length 40
21:02:21.340838 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 122, seq 2, length 40
21:02:21.340843 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 122, seq 2, length 40
21:02:21.340853 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 122, seq 3, length 40
21:02:21.340858 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 122, seq 3, length 40
21:02:21.340868 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 122, seq 4, length 40
root@n1:/tmp/pycore.46169/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 на определенный IP-адрес, чтобы он перехватывал пакеты, созданные утилитой ping. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (не включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3.

```

<1.conf# tcpdump -c 3 -x -X "dst host 10.0.0.11 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
12:22:02.080371 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 42, seq 527, length 64
    0x0000: 4500 0054 6d63 0000 4001 f931 0a00 000a  E..Tmc..@...1....
    0x0010: 0a00 000b 0000 94d2 002a 020f 3a87 a360  ....*....`
    0x0020: 0000 0000 cb39 0100 0000 0000 1011 1213  ....9.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
    0x0050: 3435 3637 4567
12:22:03.104586 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 42, seq 528, length 64
    0x0000: 4500 0054 6e06 0000 4001 f88e 0a00 000a  E..Tn...@.....
    0x0010: 0a00 000b 0000 0073 002a 0210 3b87 a360  ....s.*...;..`
    0x0020: 0000 0000 5e98 0100 0000 0000 1011 1213  ....^.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
    0x0050: 3435 3637 4567
12:22:04.128377 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 42, seq 529, length 64
    0x0000: 4500 0054 6e86 0000 4001 f80e 0a00 000a  E..Tn...@.....
    0x0010: 0a00 000b 0000 1215 002a 0211 3c87 a360  ....*...<..`
    0x0020: 0000 0000 4bf5 0100 0000 0000 1011 1213  ....K.....
    0x0030: 1415 1617 1819 1a1b 1c1d 1e1f 2021 2223  .....!"#
    0x0040: 2425 2627 2829 2a2b 2c2d 2e2f 3031 3233  $%&'()*+,-./0123
    0x0050: 3435 3637 4567
3 packets captured
3 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.34235/n1.conf#

```

2) Запустить tcpdump так, чтобы он перехватывал только пакеты протокола UDP, созданные утилитой traceroute. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 5.

```

root@n2:/tmp/pycore.34235/n2.conf# traceroute -q 5 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 60 byte packets
 1  10.0.0.10 (10.0.0.10)  0.055 ms  0.024 ms  0.032 ms  0.041 ms  0.023 ms

```

```

root@n1:/tmp/pycore.34235/n1.conf# tcpdump udp -c 5 -xx -X
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:39:58.162681 IP 10.0.0.11.51236 > 10.0.0.10.33434: UDP, length 32
    0x0000:  4500 003c 8aa3 0000 0111 1afa 0a00 000b  E..<.....
    0x0010:  0a00 000a c824 829a 0028 abc5 4041 4243  .....$...(..@ABC
    0x0020:  4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030:  5455 5657 5859 5a5b 5c5d 5e5f             TUVWXYZ[\]^_
13:39:58.163811 IP 10.0.0.11.35565 > 10.0.0.10.33435: UDP, length 32
    0x0000:  4500 003c 8aa4 0000 0111 1af9 0a00 000b  E..<.....
    0x0010:  0a00 000a 8aed 829b 0028 e8fb 4041 4243  .....(..@ABC
    0x0020:  4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030:  5455 5657 5859 5a5b 5c5d 5e5f             TUVWXYZ[\]^_
13:39:58.164116 IP 10.0.0.11.50865 > 10.0.0.10.33436: UDP, length 32
    0x0000:  4500 003c 8aa5 0000 0111 1af8 0a00 000b  E..<.....
    0x0010:  0a00 000a c6b1 829c 0028 ad36 4041 4243  .....(.6@ABC
    0x0020:  4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030:  5455 5657 5859 5a5b 5c5d 5e5f             TUVWXYZ[\]^_
13:39:58.165631 IP 10.0.0.11.41492 > 10.0.0.10.33437: UDP, length 32
    0x0000:  4500 003c 8aa6 0000 0111 1af7 0a00 000b  E..<.....
    0x0010:  0a00 000a a214 829d 0028 d1d2 4041 4243  .....(..@ABC
    0x0020:  4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030:  5455 5657 5859 5a5b 5c5d 5e5f             TUVWXYZ[\]^_
13:39:58.165691 IP 10.0.0.11.38289 > 10.0.0.10.33438: UDP, length 32
    0x0000:  4500 003c 8aa7 0000 0111 1af6 0a00 000b  E..<.....
    0x0010:  0a00 000a 9591 829e 0028 de54 4041 4243  .....(.T@ABC
    0x0020:  4445 4647 4849 4a4b 4c4d 4e4f 5051 5253  DEFGHIJKLMNOPQRS
    0x0030:  5455 5657 5859 5a5b 5c5d 5e5f             TUVWXYZ[\]^_
5 packets captured
16 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.34235/n1.conf#

```

3) Запустить tcpdump так, чтобы он сохранял только пакеты протокола ARP, отправленные на определенный IP-адрес, созданные утилитой traceroute. Открыть файл с распечаткой пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 2.

```

root@n2:/tmp/pycore.34235/n2.conf# traceroute -q 2 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 60 byte packets
 1  10.0.0.10 (10.0.0.10)  0.046 ms  0.015 ms
root@n2:/tmp/pycore.34235/n2.conf#

```

```

root@n1:/tmp/pycore.34235/n1.conf# tcpdump arp -c 2 -w arp.cap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
2 packets captured
4 packets received by filter
0 packets dropped by kernel
root@n1:/tmp/pycore.34235/n1.conf#

```

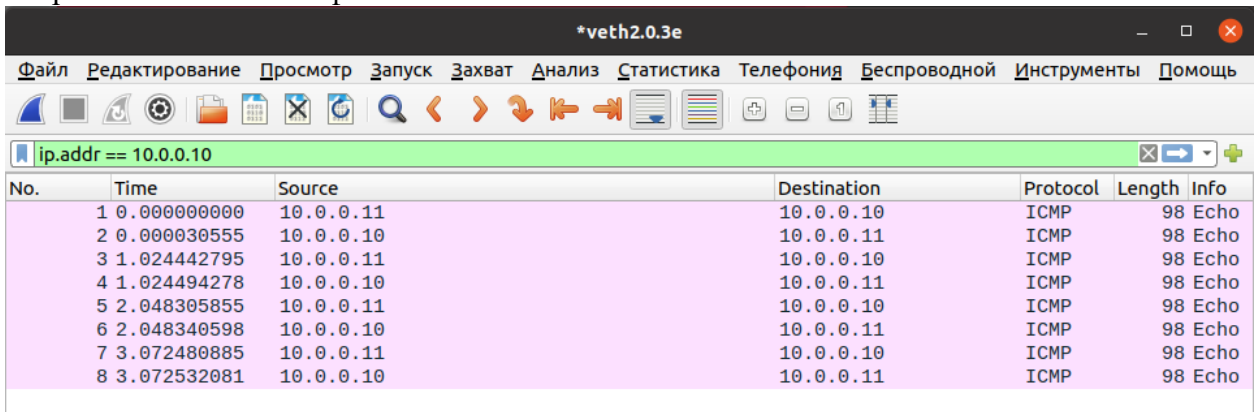
```

root@n1:/tmp/pycore.34235/n1.conf# tcpdump -c 2 -xx -X -r arp.cap
reading from file arp.cap, link-type EN10MB (Ethernet)
13:58:11.841039 ARP, Request who-has 10.0.0.11 tell 10.0.0.10, length 28
    0x0000: 0001 0800 0604 0001 0000 00aa 0000 0a00 .....
    0x0010: 000a 0000 0000 0000 0a00 000b .....
13:58:11.841074 ARP, Request who-has 10.0.0.10 tell 10.0.0.11, length 28
    0x0000: 0001 0800 0604 0001 0000 00aa 0001 0a00 .....
    0x0010: 000b 0000 0000 0000 0a00 000a .....
root@n1:/tmp/pycore.34235/n1.conf#

```

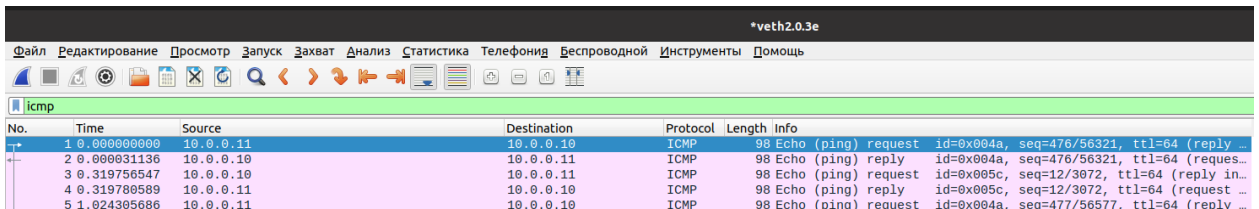
Работа с анализатором протоколов wireshark

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



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.0.11	10.0.0.10	ICMP	98	Echo
2	0.000030555	10.0.0.10	10.0.0.11	ICMP	98	Echo
3	1.024442795	10.0.0.11	10.0.0.10	ICMP	98	Echo
4	1.024494278	10.0.0.10	10.0.0.11	ICMP	98	Echo
5	2.048305855	10.0.0.11	10.0.0.10	ICMP	98	Echo
6	2.048340598	10.0.0.10	10.0.0.11	ICMP	98	Echo
7	3.072480885	10.0.0.11	10.0.0.10	ICMP	98	Echo
8	3.072532081	10.0.0.10	10.0.0.11	ICMP	98	Echo

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
1	0.000000000	10.0.0.11	10.0.0.10	ICMP	98	Echo (ping) request id=0x004a, seq=476/56321, ttl=64 (reply ...
2	0.000031136	10.0.0.10	10.0.0.11	ICMP	98	Echo (ping) reply id=0x004a, seq=476/56321, ttl=64 (request ...
3	0.319756547	10.0.0.10	10.0.0.11	ICMP	98	Echo (ping) request id=0x005c, seq=12/3072, ttl=64 (reply in ...
4	0.319780589	10.0.0.11	10.0.0.10	ICMP	98	Echo (ping) reply id=0x005c, seq=12/3072, ttl=64 (request ...
5	1.024305686	10.0.0.11	10.0.0.10	ICMP	98	Echo (ping) request id=0x004a, seq=477/56577, ttl=64 (reply ...

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.

```

root@n2:/tmp/pycore.34235/n2.conf# traceroute -I 10.0.0.10
traceroute to 10.0.0.10 (10.0.0.10), 30 hops max, 60 byte packets
 1  10.0.0.10 (10.0.0.10)  0.044 ms  0.015 ms  0.014 ms

```

Wireshark · Поток · veth1.0.3e

Время	10.0.0.11	10.0.0.10	00:00:00_aa:00:00 Комментарий
0.000000000	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=1/256, ttl=...
0.000019867	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=1/256, ttl=6...
0.000037163	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=2/512, ttl=...
0.000043726	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=2/512, ttl=6...
0.000056874	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=3/768, ttl=...
0.000063263	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=3/768, ttl=6...
0.000077754	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=4/1024, tt=...
0.000084154	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=4/1024, ttl=...
0.000097051	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=5/1280, tt=...
0.000103411	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=5/1280, ttl=...
0.000116320	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=6/1536, tt=...
0.000122584	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=6/1536, ttl=...
0.000136650	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=7/1792, tt=...
0.000143293	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=7/1792, ttl=...
0.000156545	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=8/2048, tt=...
0.000163044	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=8/2048, ttl=...
0.000176102	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=9/2304, tt=...
0.000182364	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=9/2304, ttl=...
0.000196393	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=10/2560, ...
0.000202704	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=10/2560, ttl=...
0.000215569	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=11/2816, ...
0.000221887	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=11/2816, ttl=...
0.000234675	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=12/3072, ...
0.000240951	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=12/3072, ttl=...
0.000254981	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=13/3328, ...
0.000261266	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=13/3328, ttl=...
0.000274046	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=14/3584, ...
0.000280324	Echo (ping) reply id=0x004c...		ICMP: Echo (ping) reply id=0x004c, seq=14/3584, ttl=...
0.000293385	Echo (ping) request id=0x00...		ICMP: Echo (ping) request id=0x004c, seq=15/3840, ...

Packet 29: ICMP: Echo (ping) request id=0x004c, seq=15/3840, ttl=5 (reply in 30)

☐ Ограничить соответственно дисплейному фильтру

Тип потока: All Flows

Адреса: Любой

[Справка](#) [Сброс Диаграммы](#) [Закрыть](#) [Save As...](#)

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


```
1 -----
2
3 0000 00 00 00 aa 00 00 00 00 aa 00 01 08 00 45 00 .....E.
4 0010 00 3c c5 65 00 00 01 01 e0 47 0a 00 00 0b 0a 00 .<.e.....G.....
5 0020 00 0a 08 00 82 52 00 27 00 01 48 49 4a 4b 4c 4d .....R.'..HIJKLM
6 0030 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTUVWXYZ[\]
7 0040 5e 5f 60 61 62 63 64 65 66 67 ^_`abcdefg
8
9 -----
10
11 0000 00 00 00 aa 00 01 00 00 00 aa 00 00 08 00 45 00 .....E.
12 0010 00 3c d0 f9 00 00 40 01 95 b3 0a 00 00 0a 0a 00 .<....@.....
13 0020 00 0b 00 00 8a 52 00 27 00 01 48 49 4a 4b 4c 4d .....R.'..HIJKLM
14 0030 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTUVWXYZ[\]
15 0040 5e 5f 60 61 62 63 64 65 66 67 ^_`abcdefg
16
17 -----
18
19 0000 00 00 00 aa 00 00 00 00 00 aa 00 01 08 00 45 00 .....E.
20 0010 00 3c c5 66 00 00 01 01 e0 46 0a 00 00 0b 0a 00 .<.f.....F.....
21 0020 00 0a 08 00 82 51 00 27 00 02 48 49 4a 4b 4c 4d .....Q.'..HIJKLM
22 0030 4e 4f 50 51 52 53 54 55 56 57 58 59 5a 5b 5c 5d NOPQRSTUVWXYZ[\]
23 0040 5e 5f 60 61 62 63 64 65 66 67 ^_`abcdefg
24
```

```
Терминал
root@n1:/tmp/pycore.45831/n1.conf# tcpdump -c 3 -r output3.cap -xx -X
reading from file output3.cap, link-type EN10MB (Ethernet)
11:50:30.404252 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 39, seq 1, leng
th 40
    0x0000: 4500 003c c565 0000 0101 e047 0a00 000b E...<.e.....G....
    0x0010: 0a00 000a 0800 8252 0027 0001 4849 4a4b .....R.'..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667 \]^_`abcdefg
11:50:30.404267 IP 10.0.0.10 > 10.0.0.11: ICMP echo reply, id 39, seq 1, length
40
    0x0000: 4500 003c d0f9 0000 4001 95b3 0a00 000a E...<....@.....
    0x0010: 0a00 000b 0000 8a52 0027 0001 4849 4a4b .....R.'..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667 \]^_`abcdefg
11:50:30.404282 IP 10.0.0.11 > 10.0.0.10: ICMP echo request, id 39, seq 2, leng
th 40
    0x0000: 4500 003c c566 0000 0101 e046 0a00 000b E...<.f.....F....
    0x0010: 0a00 000a 0800 8251 0027 0002 4849 4a4b .....Q.'..HIJK
    0x0020: 4c4d 4e4f 5051 5253 5455 5657 5859 5a5b LMNOPQRSTUVWXYZ[
    0x0030: 5c5d 5e5f 6061 6263 6465 6667 \]^_`abcdefg
root@n1:/tmp/pycore.45831/n1.conf#
```