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 №1

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_Гай В.Е.\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

Береснева М.А.\_

(подпись) (фамилия, и.,о.)

\_\_\_\_18-АС \_

(шифр группы)

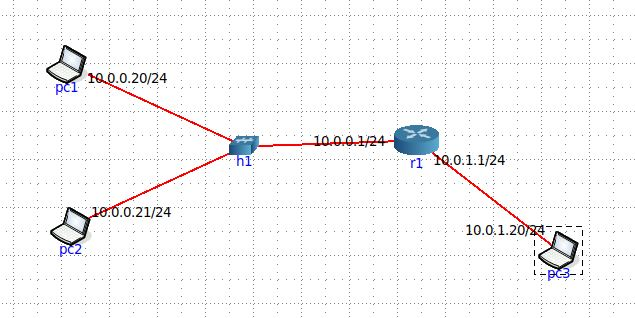
Работа защищена «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_

* оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Нижний Новгород 2021

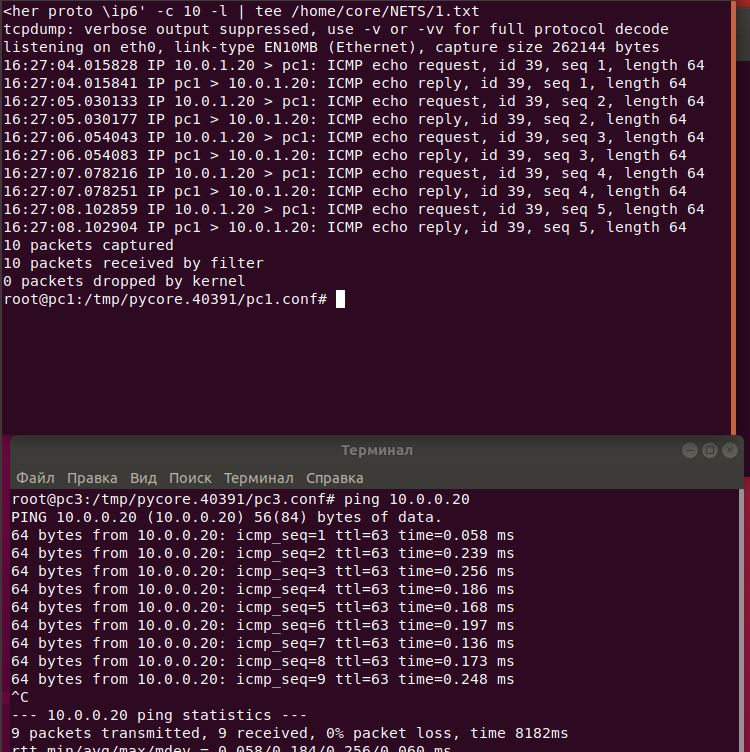
**Ход работы**

**Работа с анализатором протоколов tcpdump**

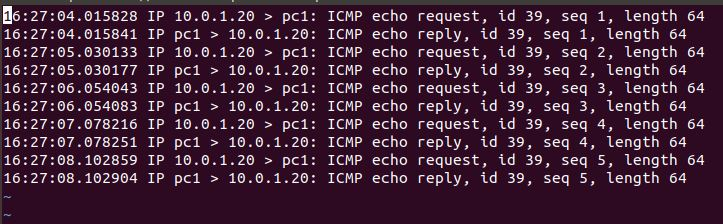


1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл:

*tcpdump ‘not dst host 224.0.0.5 and not ether proto \ip6' -c 10 -l | tee /home/core/NETS/1.txt*



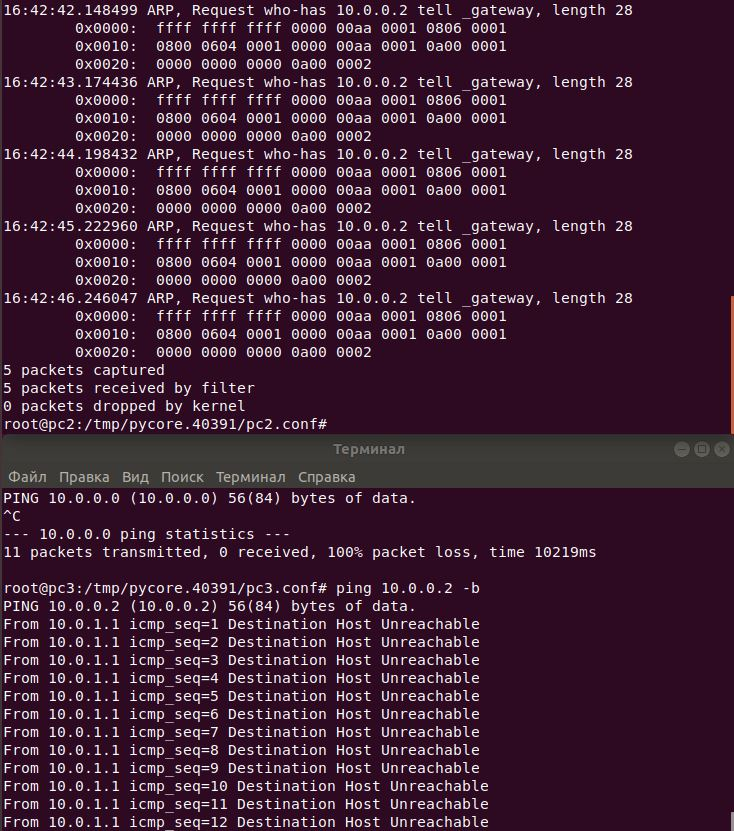
Просмотр файла через Vim:



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):

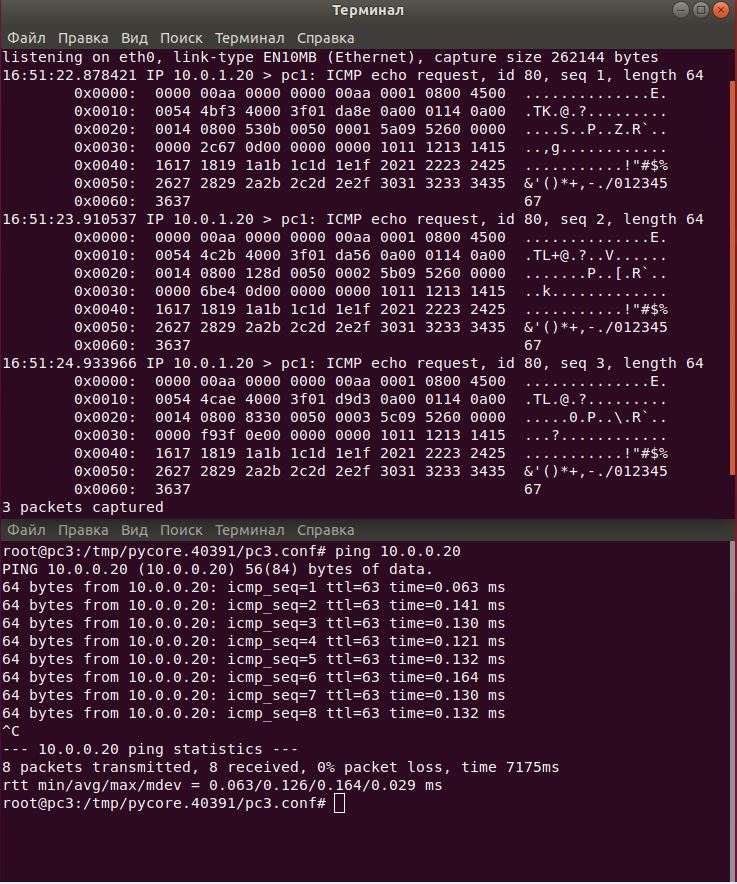
*tcpdump ‘not dst host 224.0.0.5 and not ether proto \ip6 and ether dst ff:ff:ff:ff:ff:ff' -c 5 -l -xx*

*| tee /home/core/NETS/2.txt*



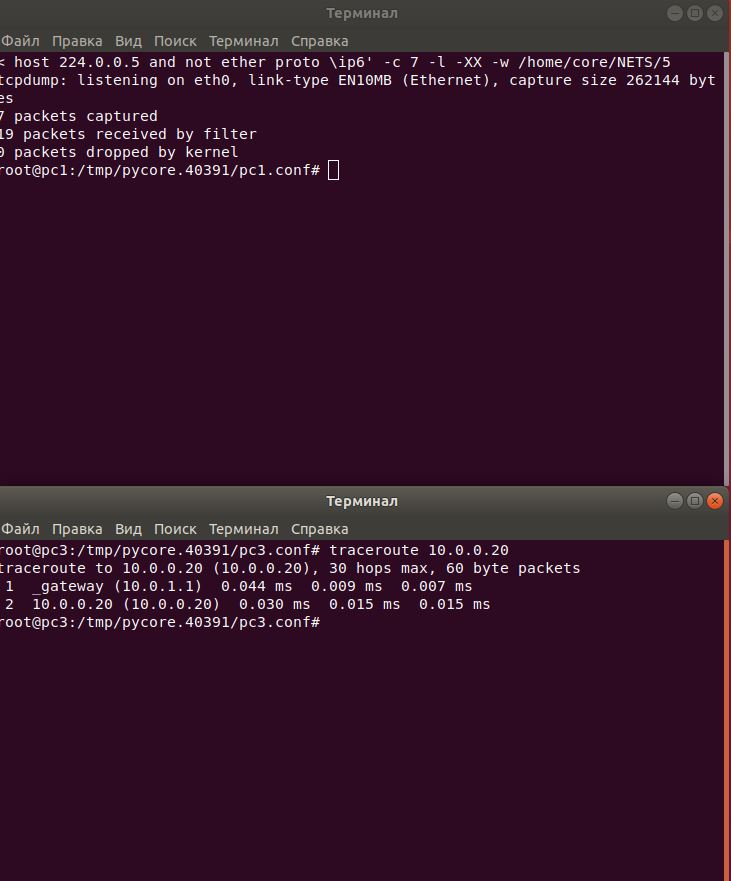
3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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

*tcpdump ‘not dst host 224.0.0.5 and not ether proto \ip6 and ether proto \icmp and dst host 10.0.1.20' -c 3 -l -XX | tee /home/core/NETS/3.txt*



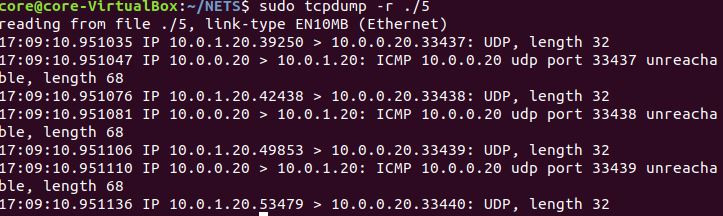
4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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

*tcpdump ‘not dst host 224.0.0.5 and not ether proto \ip6’ -c 7 -l -XX -w /home/core/NETS/5*



5. Прочесть программой tcpdump созданный в предыдущем пункте файл:

*tcpdump -r /home/core/NETS/5*



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

* Перехват всех широковещательных ARP пакетов без отображения времени в каждой строке:

*tcpdump -l -t 'ether proto \arp and ether dst ff:ff:ff:ff:ff:ff'*

* Перехват ICMP пакетов от конкретного узла в количестве 10 штук с записью результатов в бинарный файл traffic:

*tcpdump ‘ether dst 10.0.1.20’ -c 10 -l -w /home/traffic*

* Перехват UDP пакетов без протокола IPv6 с отображением их в ASCII и hex формате без заголовков канального уровня:

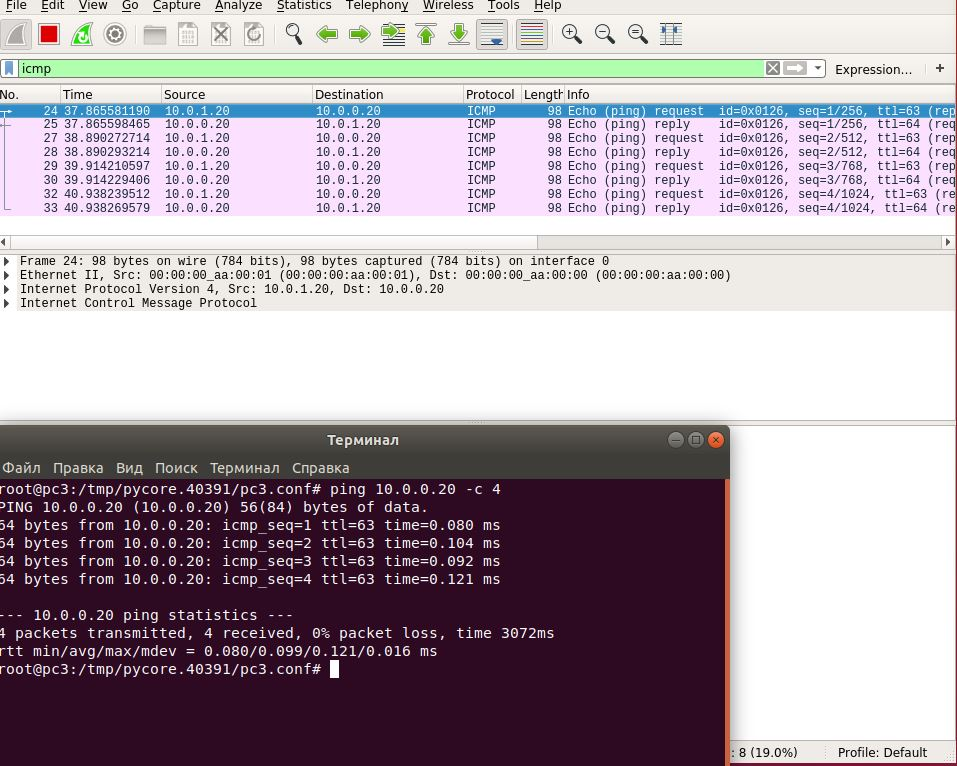
*tcpdump ‘ether proto \udp’ -l -X*

**Работа с анализатором протоколов wireshark**

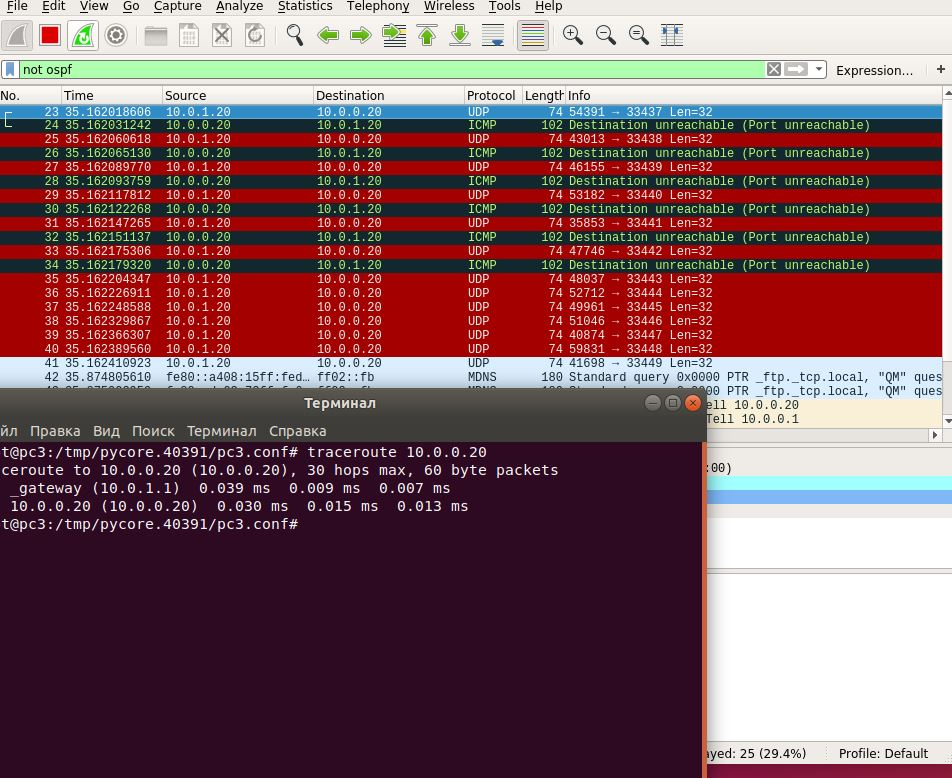
1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл:



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



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:



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

(слева - данные из файла, справа - flow graph)

