МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №1

«Работа с анализатором протоколов tcpdump и wireshark»

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

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

(подпись) (фамилия, и.,о.)

СТУДЕНТЫ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_ Сухоруков В.А.\_\_\_

(подпись) (фамилия, и.,о.)

\_\_\_\_\_\_\_19-В-2\_\_\_\_\_\_\_\_

(шифр группы)

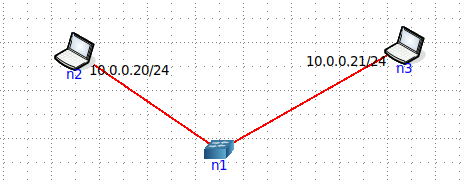
Работа защищена «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_

С оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

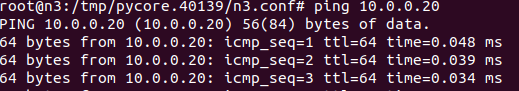
Нижний Новгород 2022

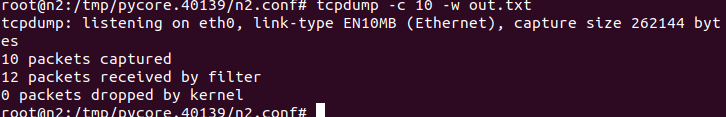
# Работа с анализатором протоколов tcpdump

Схема сети

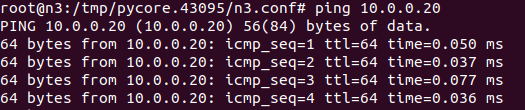


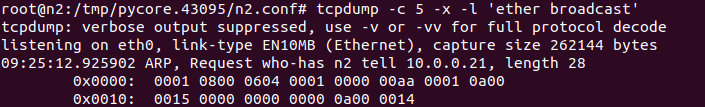
## 1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.



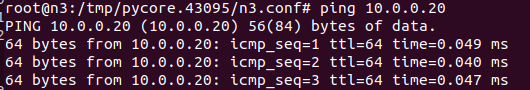


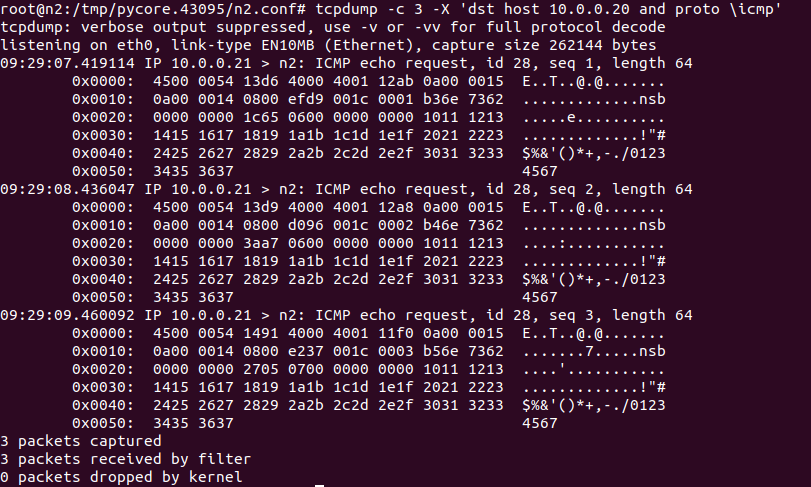
## Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе.



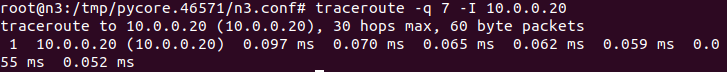


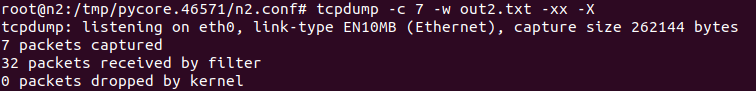
## Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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



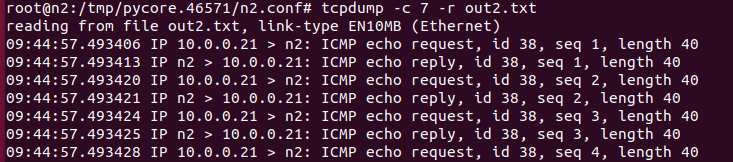


## Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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





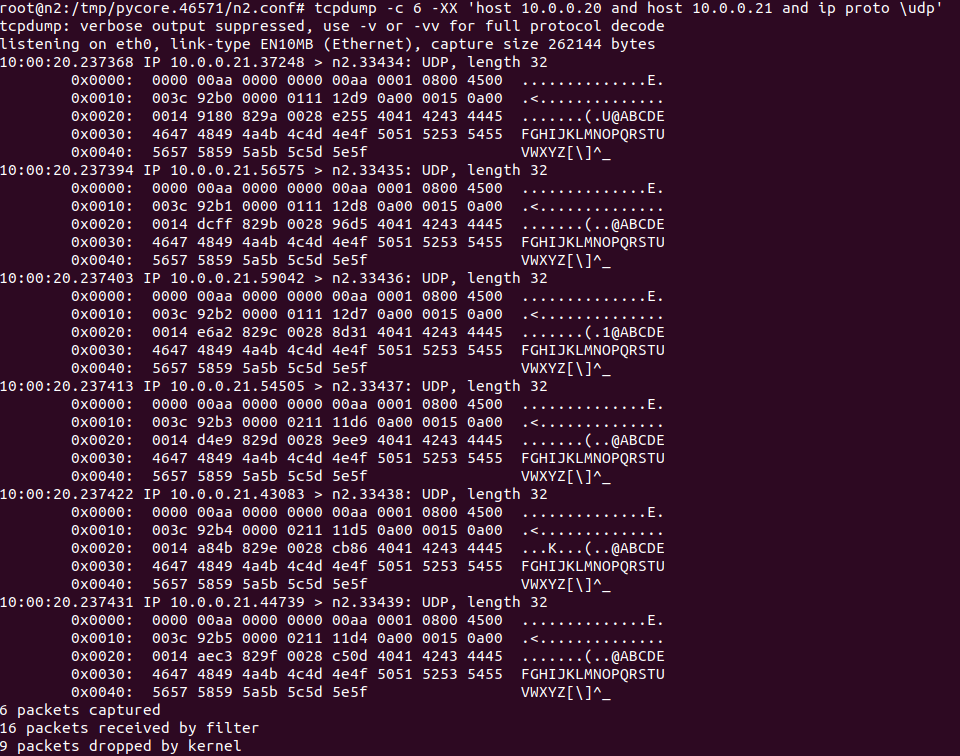
## Прочесть программой tcpdump созданный в предыдущем пункте файл.



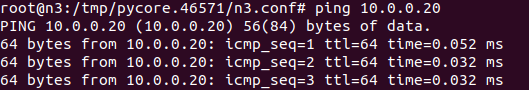
## Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

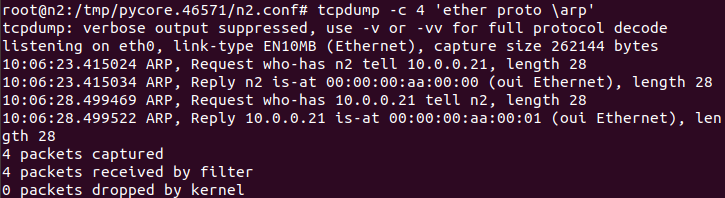
### Перехватить пакеты UDP отправленные с ПК 10.0.0.21 на ПК 10.0.0.20 и обратно. Отобразить пакет в ASCII и шестнадцатеричном виде с заголовком канального уровня. Ограничиться 6 пакетами.





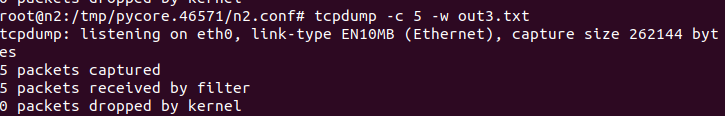
### Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ARP. Количество захватываемых пакетов ограничить 4.





### Запустить tcpdump так, чтобы он перехватил 5 пакетов, сохранить данные в файл.

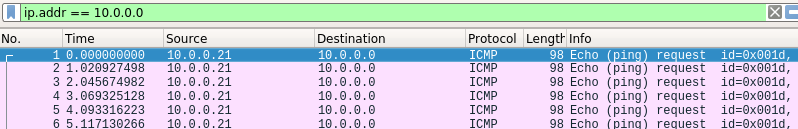




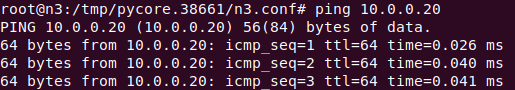
# Работа с анализатором протоколов wireshark

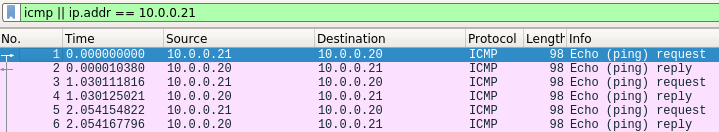
## Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат сохранить в текстовый файл.



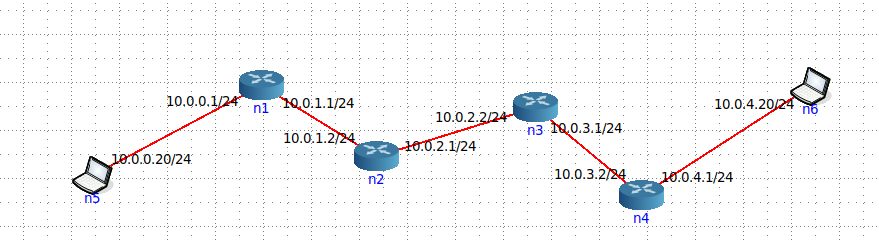


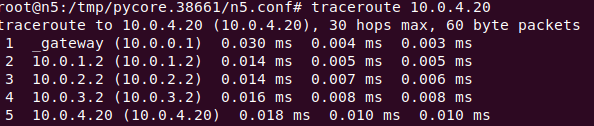
## Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

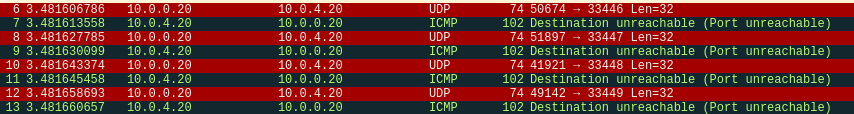


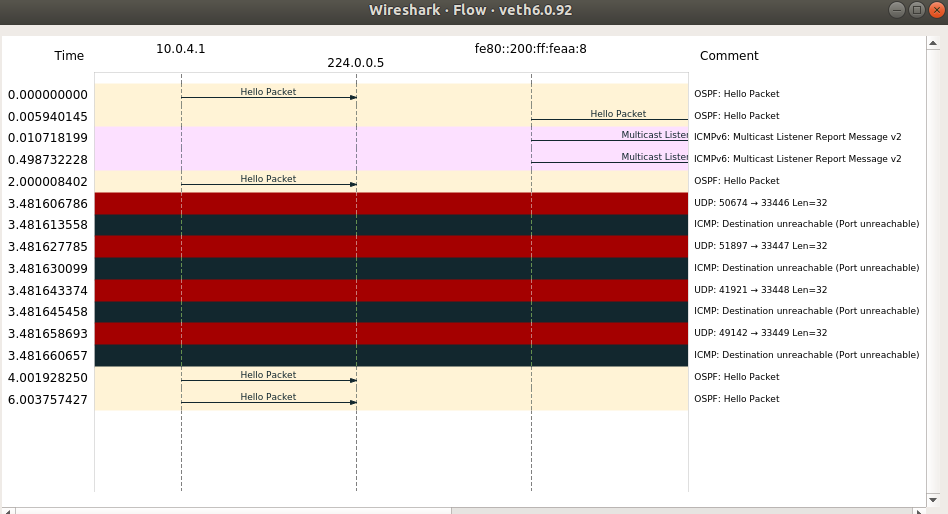


## Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму FlowGraph. Диаграмму сохранить либо в виде текстового файла, либо в виде изображения.









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

