МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра «Вычислительные системы и технологии»

ОТЧЁТ

по лабораторной работе №1

«Сети и телекоммуникации»

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Гай В.Е.

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Храмцова Д.А.

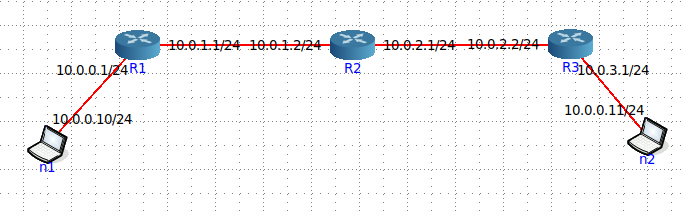
18-В-1

Нижний Новгород 2021

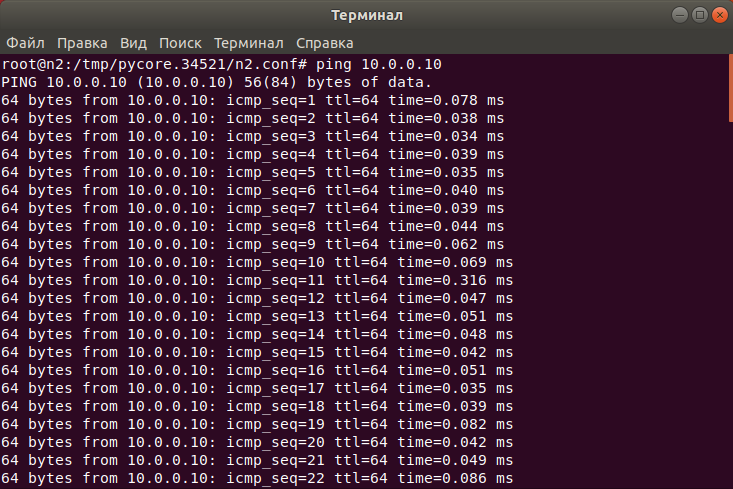
**Цель**: Познакомиться с анализатором протоколов tcpdump и сравнить его работу с работой анализатора wireshark.

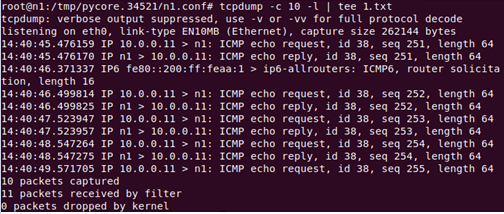
**Работа с анализатором протоколов tcpdump:**

Собираем схему:

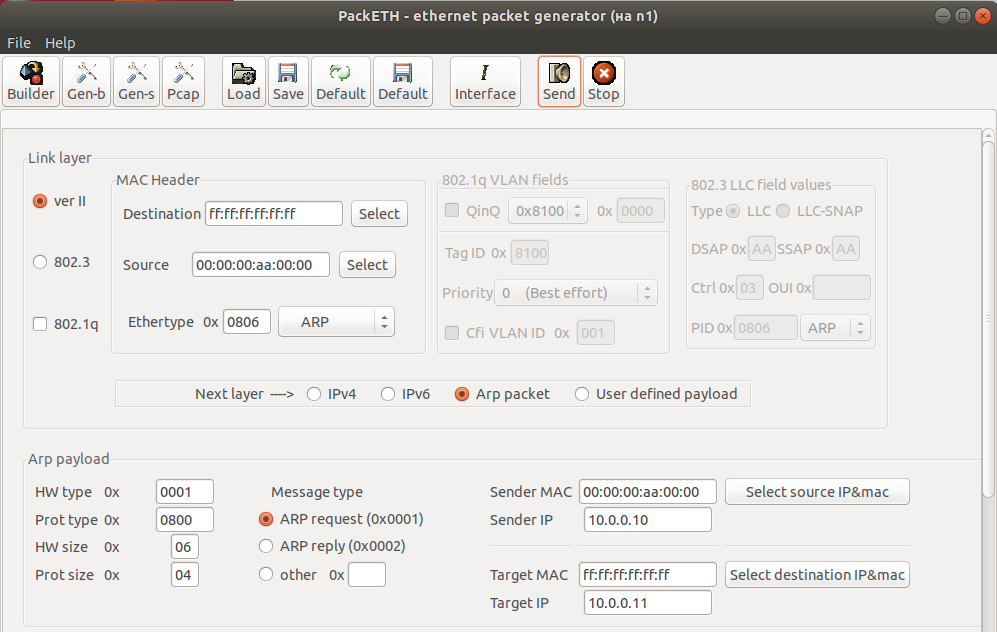


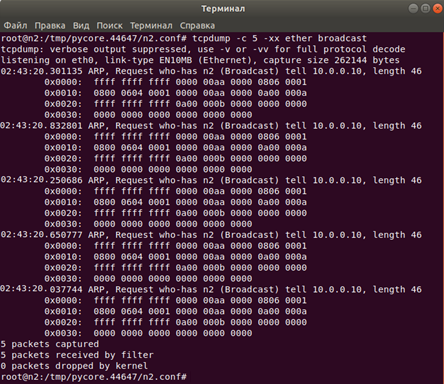
1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.





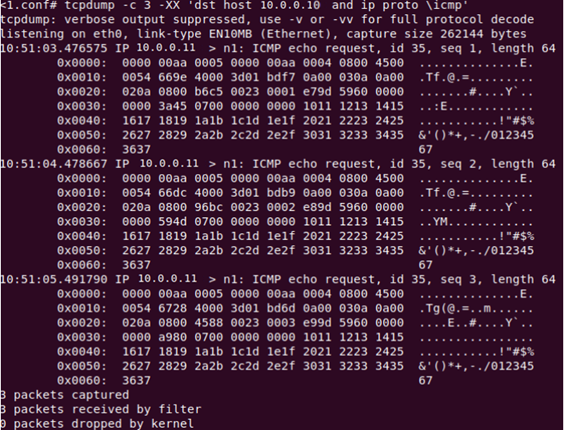
1. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня)





1. 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 возпользоваться утилитой ping.

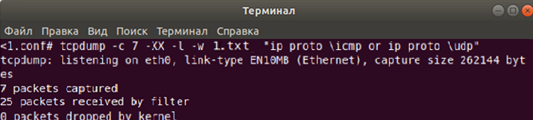
Команда: tcpdump -c 3 -XX ‘dst host 10.0.0.10 and ip proto \icmp’

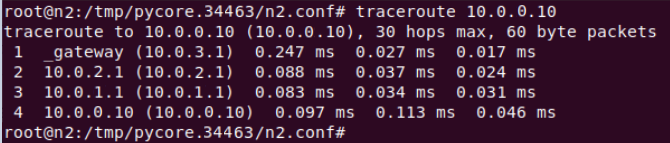


1. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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

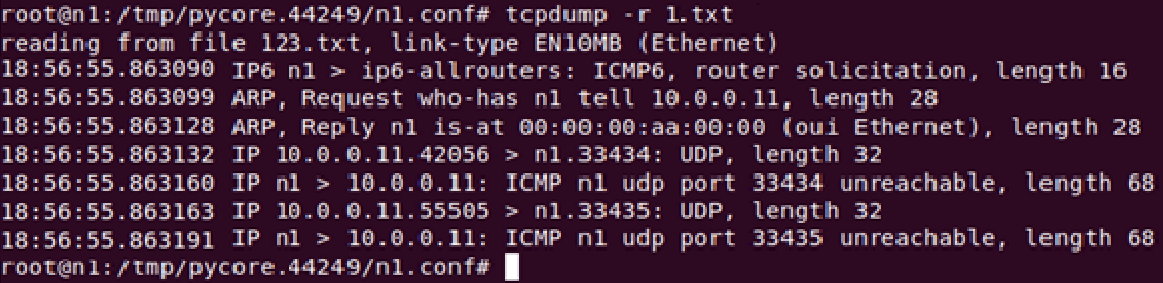
Команда: tcpdump -c 7 -XX -w out.log "ip proto \icmp or ip proto \udp"

Запуск tcpdump:



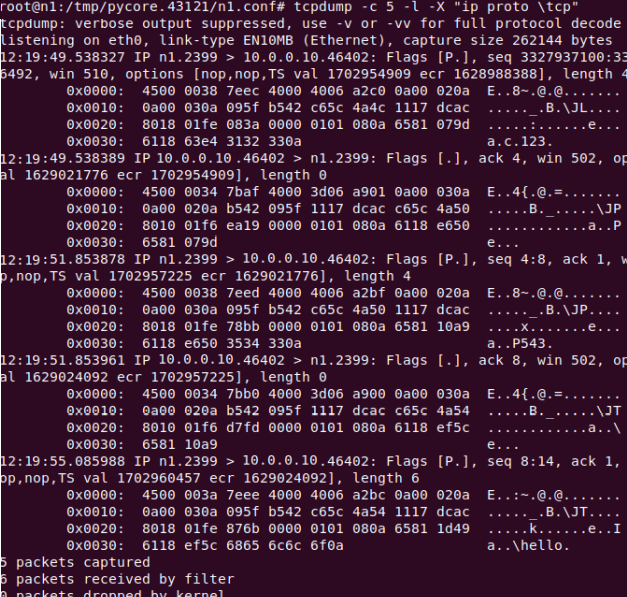


1. Прочесть программой tcpdump созданный в предыдущем пункте файл.

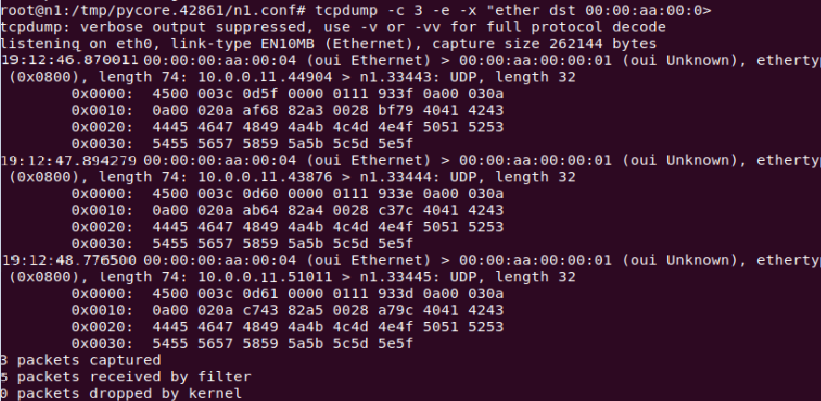


1. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP.

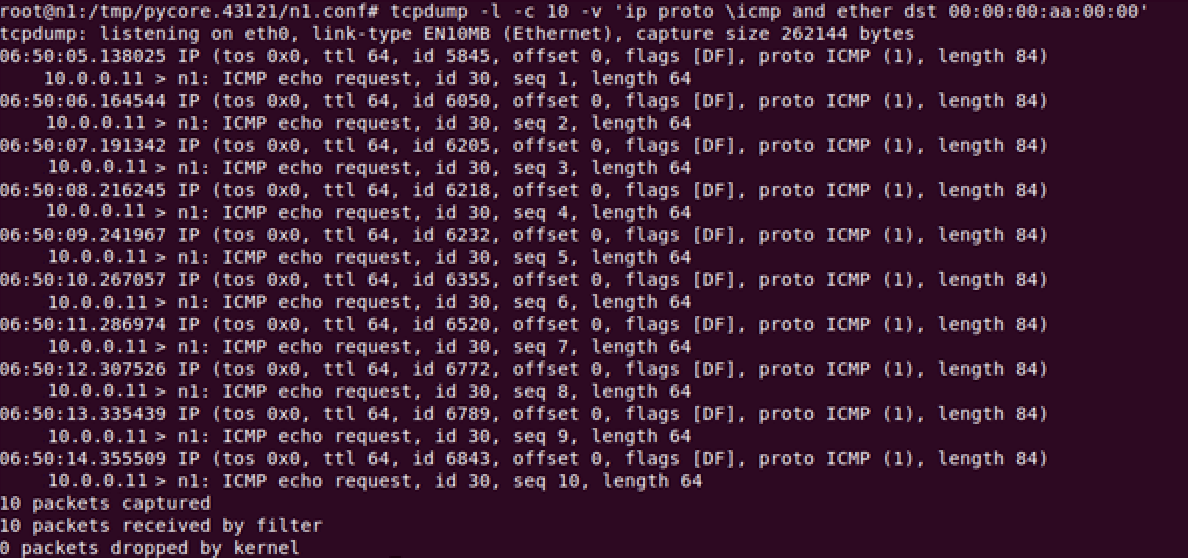
- Запустить tcpdump в режиме захвата пакетов, чтобы он перехватывал только пакеты протокола TCP. Отображал данные в шестнадцатеричной системе и ASCIIформате. Количество пакетов ограничить 5.

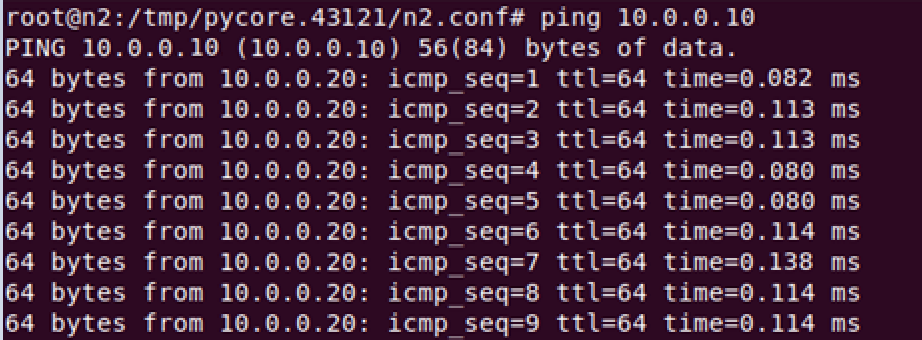


-Захватить 3 пакета протокола UDP, отправленных на определенный MAC-адрес. Отобразить данные канального уровня. Включить распечатку пакета в шестнадцатеричной системе.

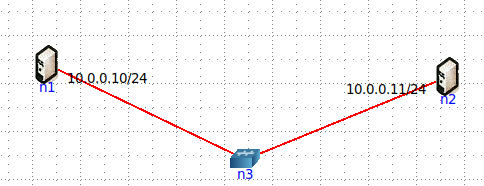


-Запустить tcpdump, перехватывающий пакеты только протокола ICMP с фильтром MAC-адреса получателя.. Количество захватываемых пакетов ограничить до 10. Для передачи пакетов воспользоваться утилитой ping. Вывод подробной информации

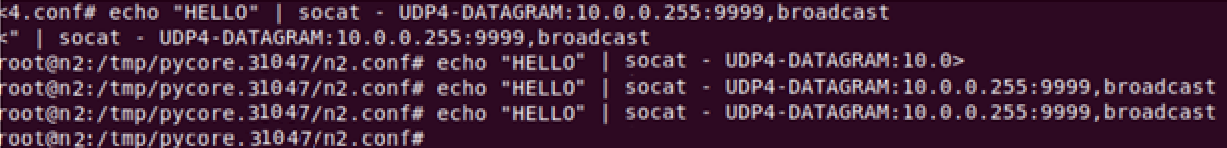


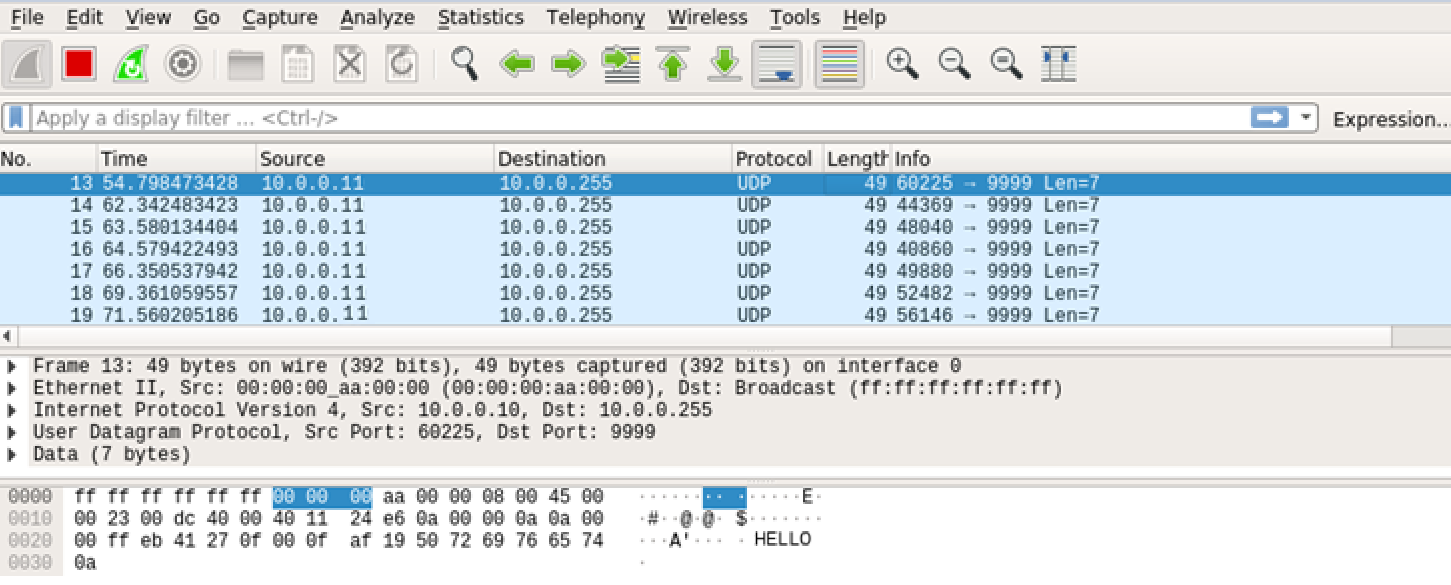


Wireshark

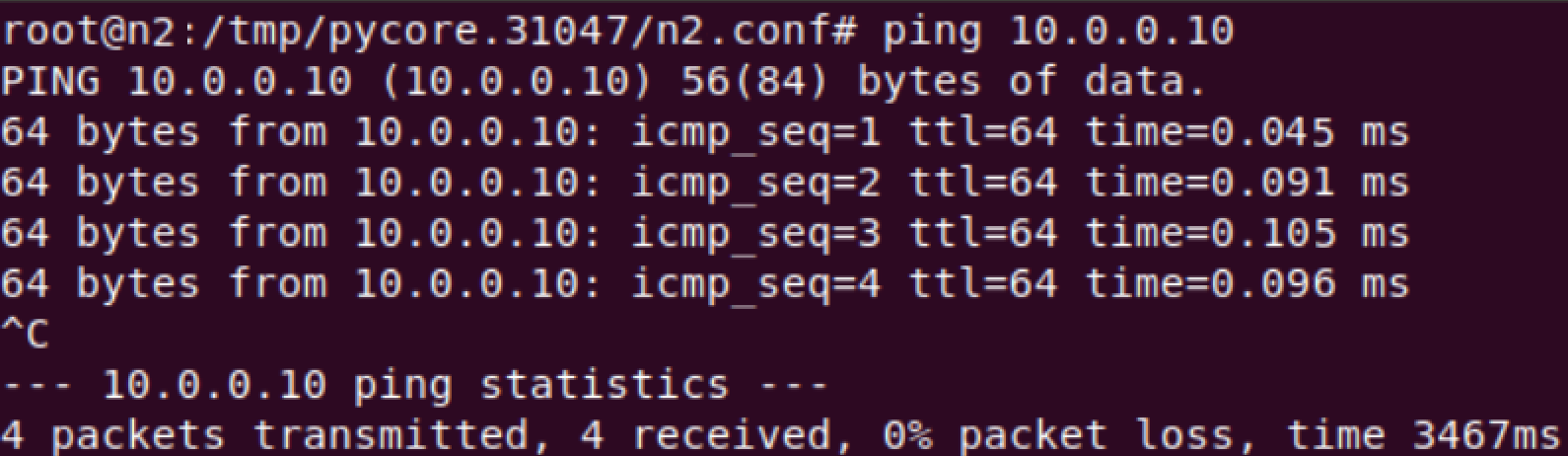


1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IPадресу). Результат сохранить в текстовый файл.



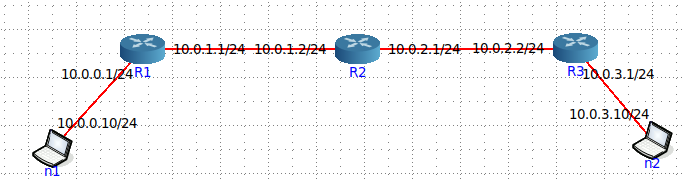


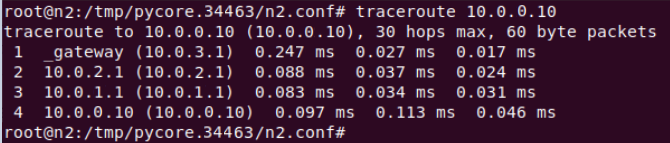
**2.** Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воcпользоваться утилитой ping. Результат сохранить в текстовый файл.

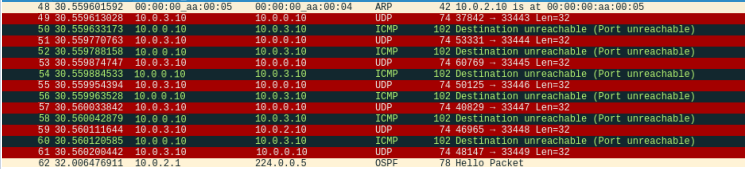


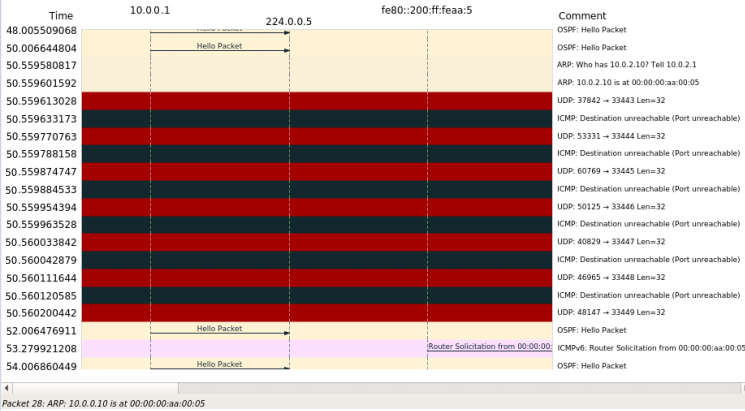


3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.









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

tcpdump:

