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:

Докукин Д.В.

Группа:

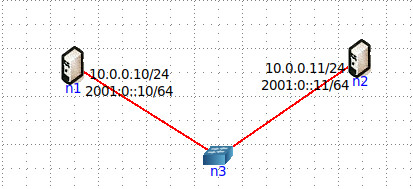
18-В-1

Нижний Новгород

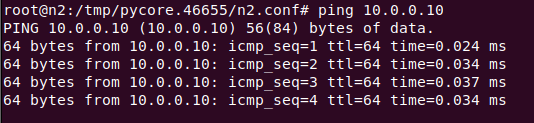
2021

Работа с анализатором протоколов tcpdump

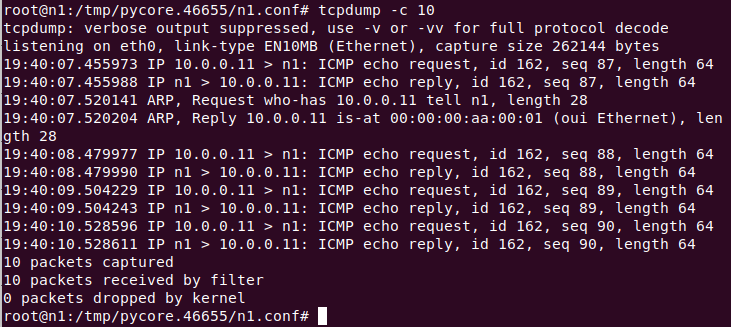
Соберём простую схему:

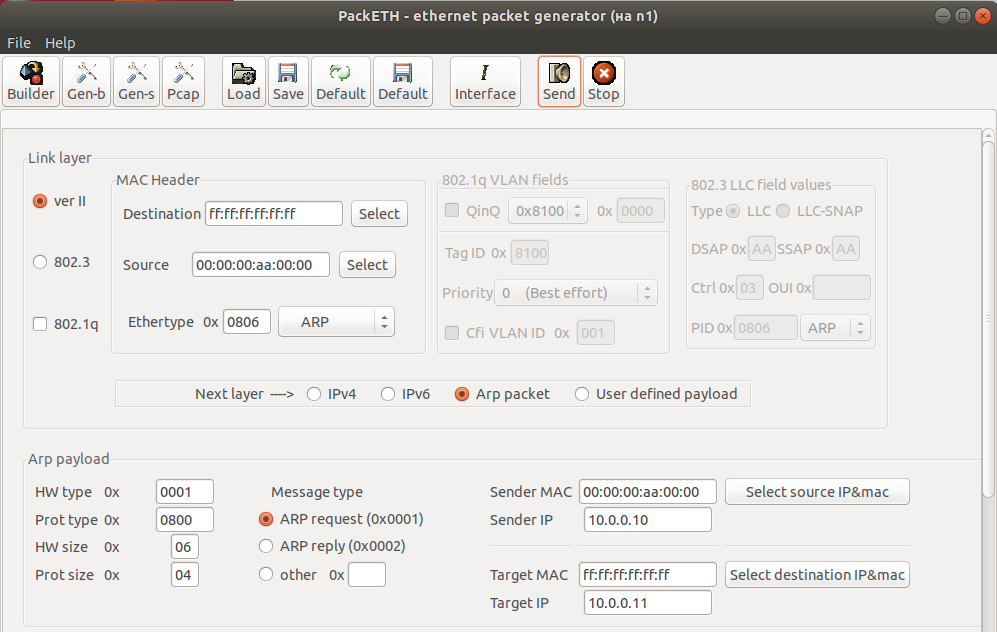
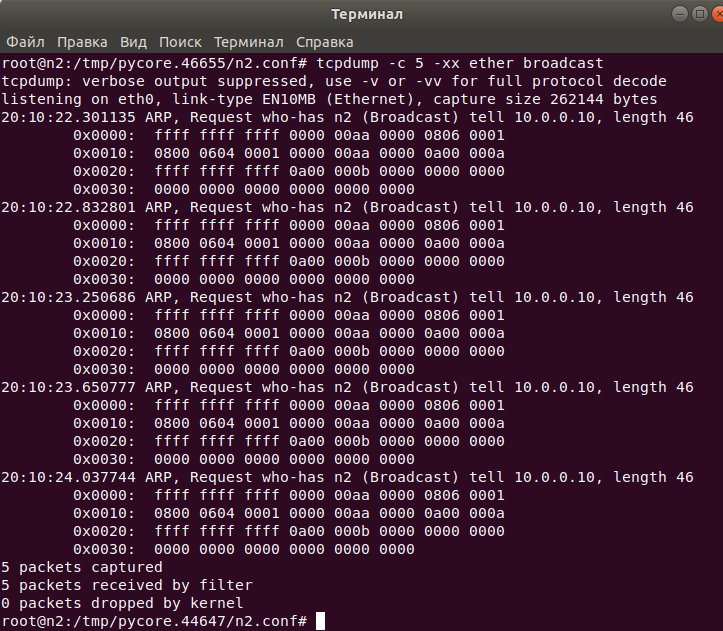
****

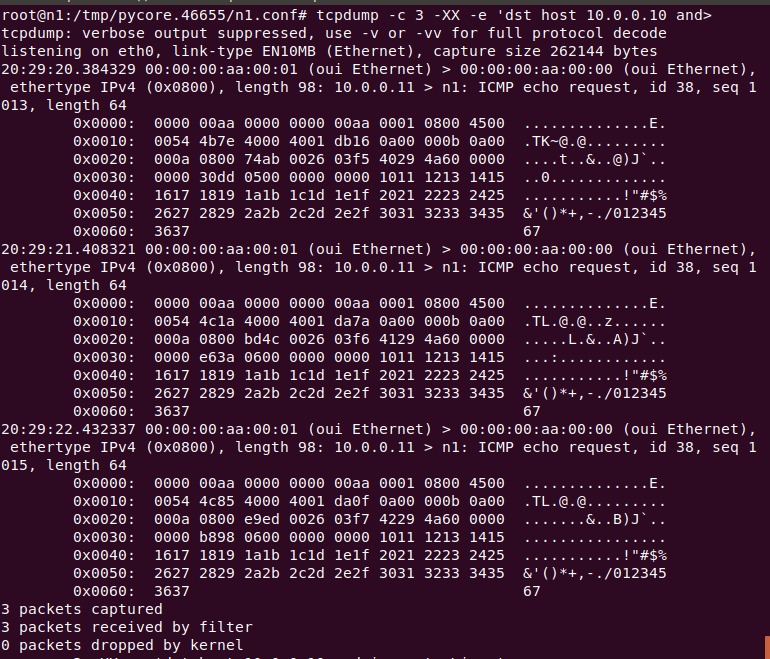
Проверим работоспособность сети командой ping



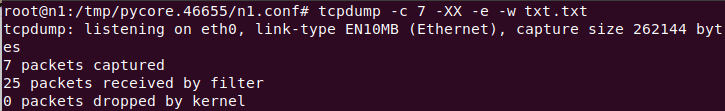
1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети. Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл.

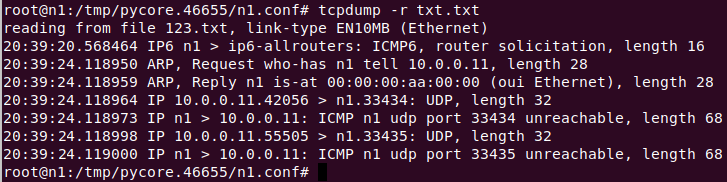


1. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).  
     
     
   
2. Запустить tcpdump так, чтобы он перехватывал только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

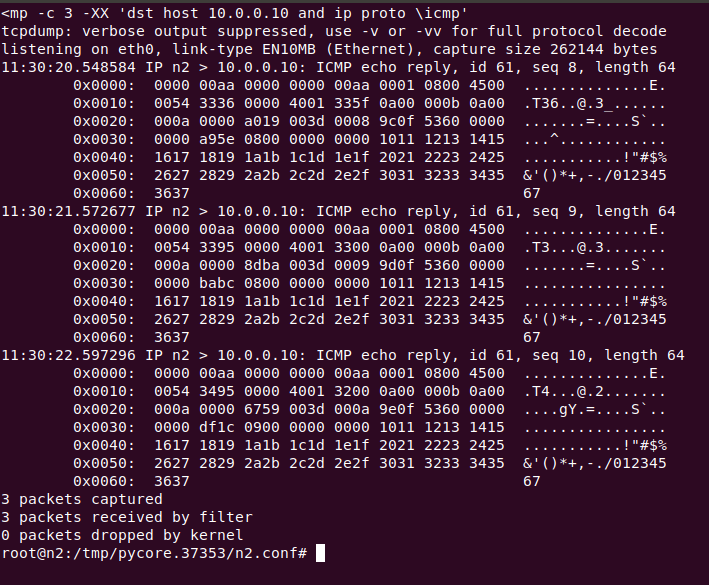


1. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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

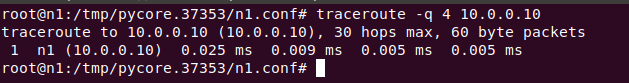


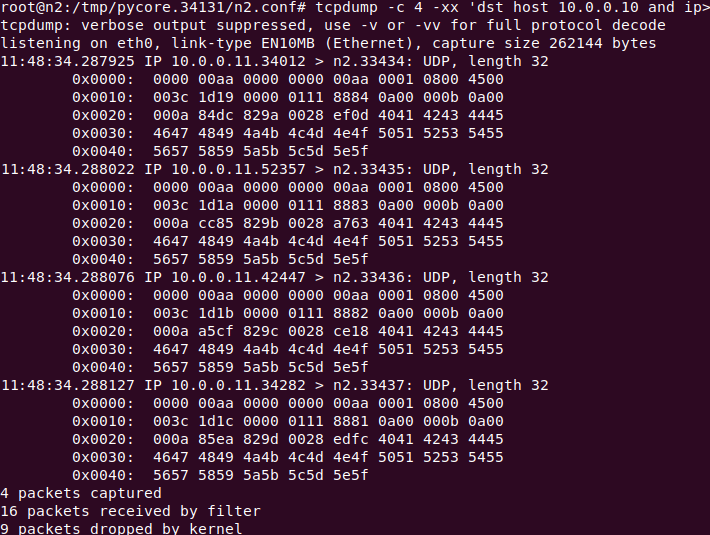
1. Прочесть программой tcpdump созданный в предыдущем пункте файл.
2. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP.

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

****

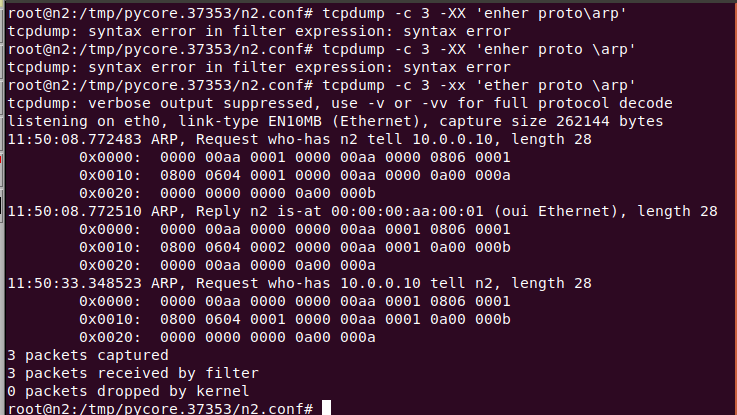
2) Запустить tcpdump для перехвата пакетов протокола UDP, отправленных на определенный IP-адрес, созданных утилитой traceroute. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов 4.



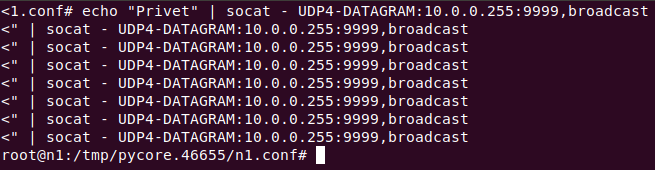


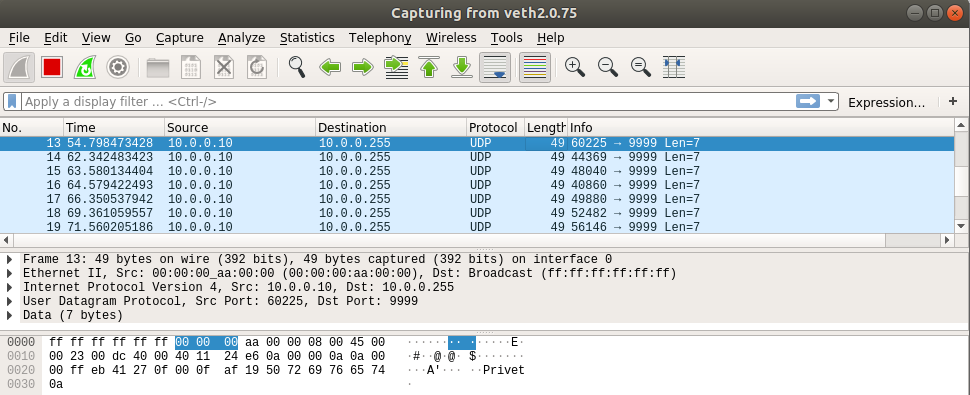
3) Запустить tcpdump для перехвата пакетов ARP, отправленных на определенный IP-адрес, созданных утилитой ping. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество пакетов ограничить 3.

Для генерирования пакетов c помощью ping.

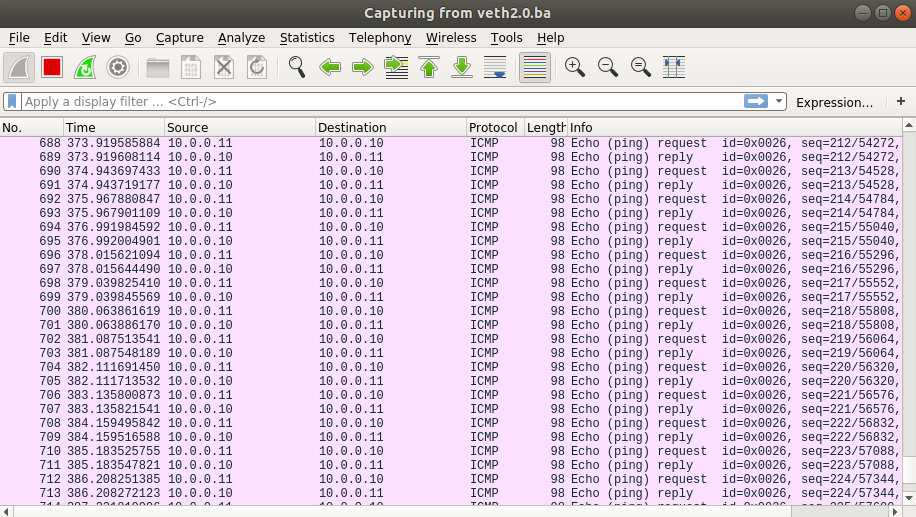
****

Работа с анализатором протоколов Wireshark:

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


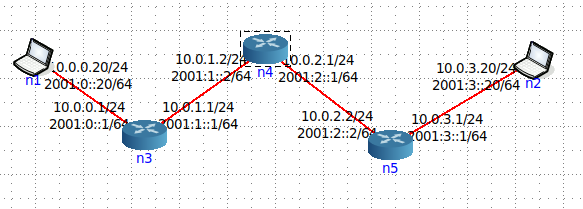


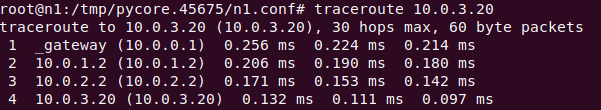
2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воcпользоваться утилитой ping. Результат сохранить в текстовый файл.

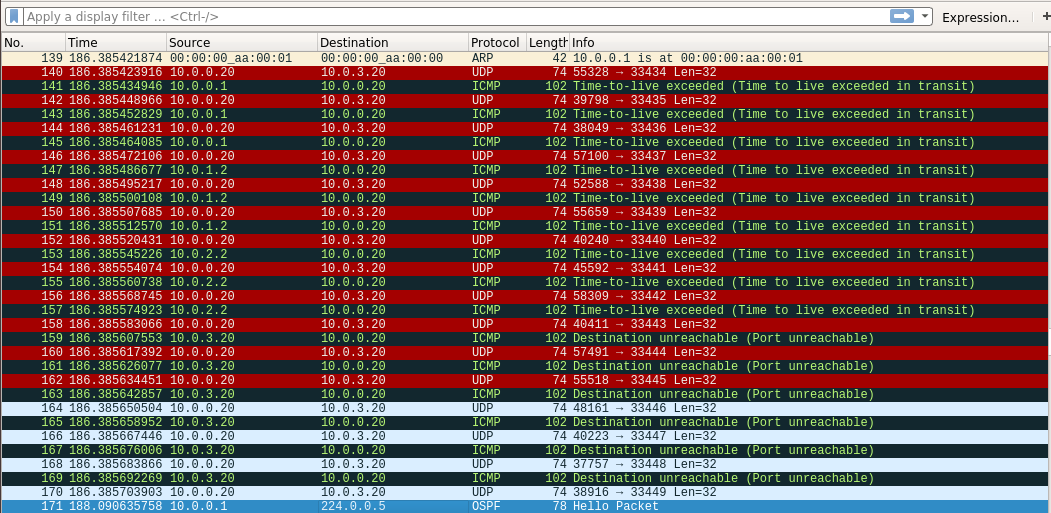


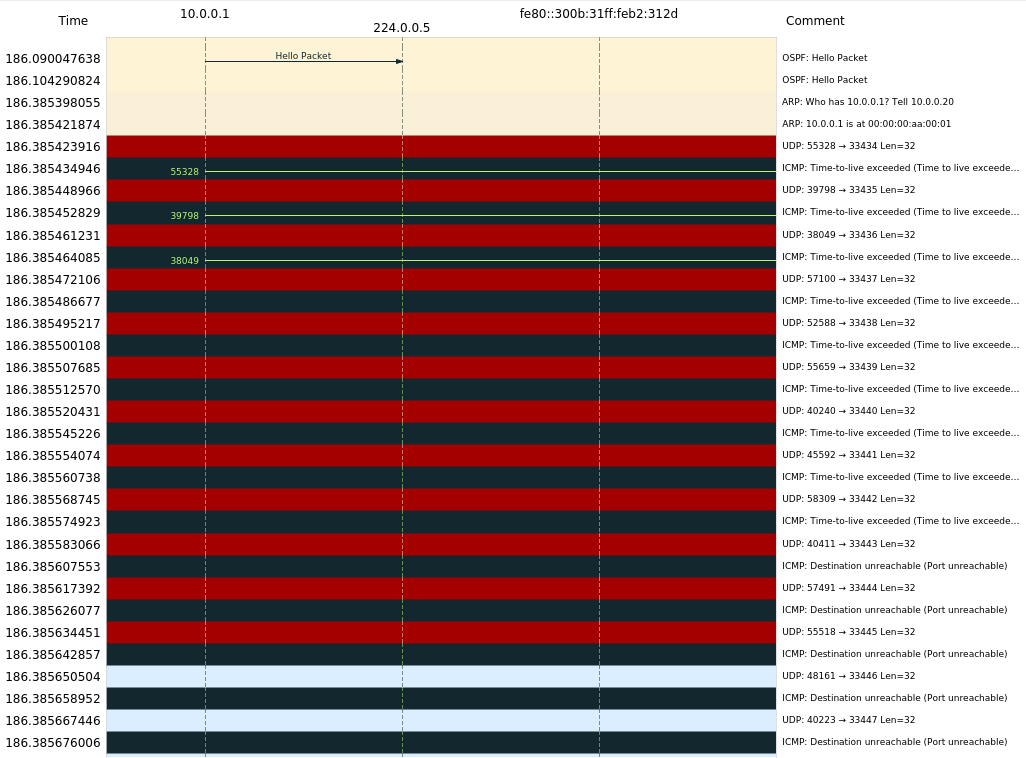
3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.

Cоберем схему:

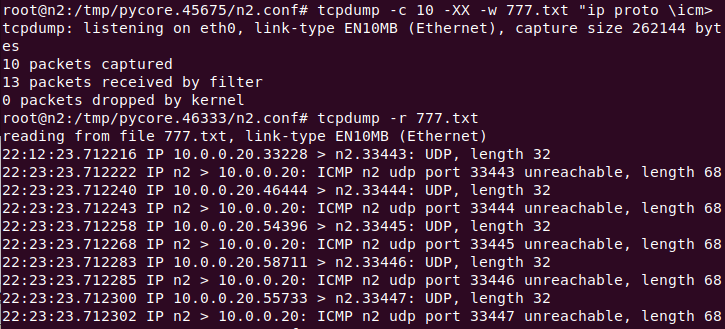


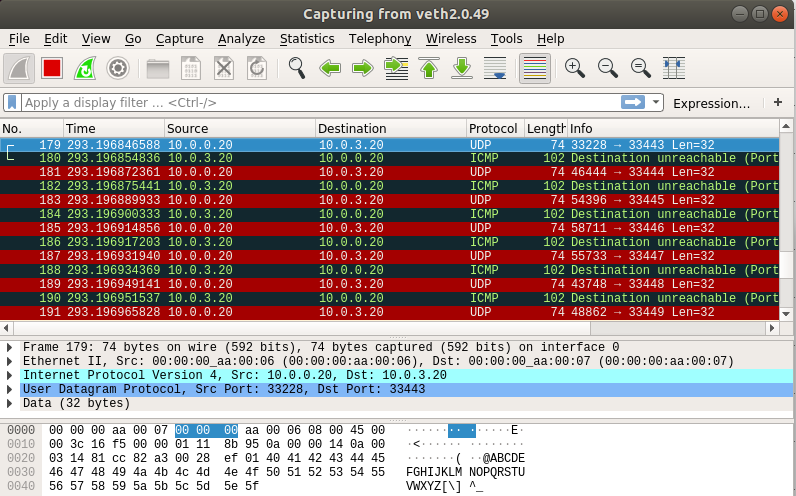






4. Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено утилитой wireshark.





Информация схожа. Wireshark подробнее описывает пересылаемые пакеты