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»

Отчет по лабораторной работе №1

по дисциплине сети и телекоммуникации

РУКОВОДИТЕЛЬ:

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

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Салтыков В. Е.

Группа 18 В-2

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

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

Нижний Новгород

2021 г.

**Задание на работу:**

**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.

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).

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 возпользоваться утилитой ping.

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.

5. Прочесть программой tcpdump созданный в предыдущем пункте файл.

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

**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.

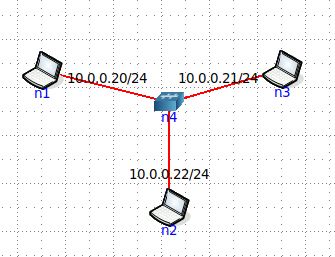
3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.

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

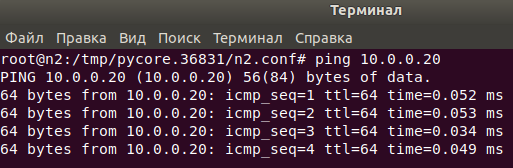
**Работа с анализатором протоколов tcpdump**

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

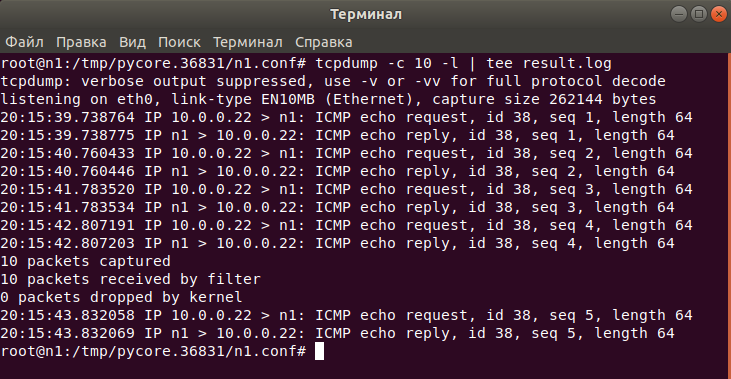
Структура сети:

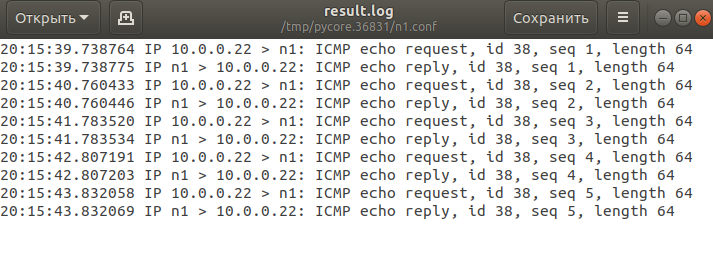


Передаем пакеты с хоста n2 на n1:



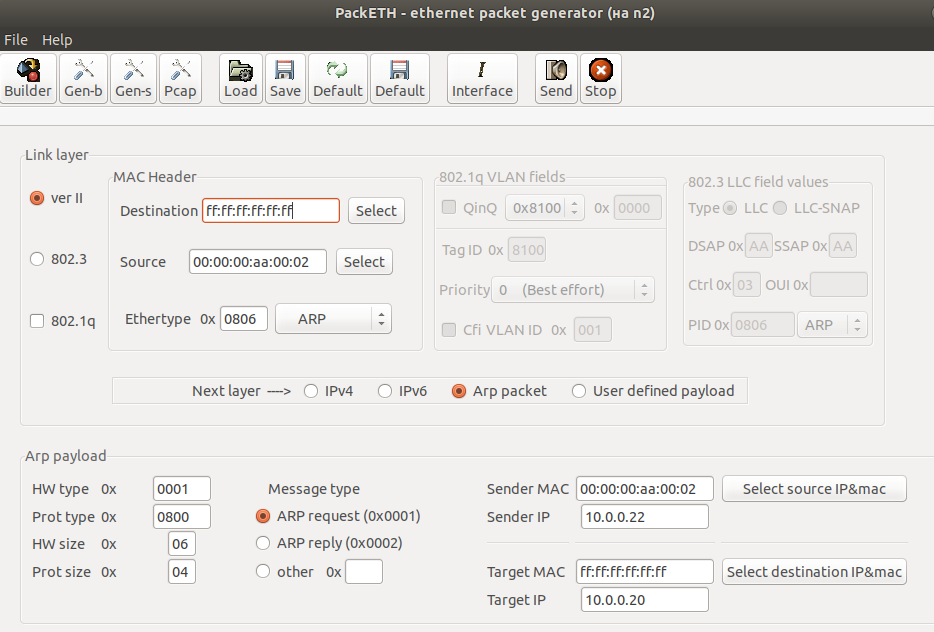
На хосте n1 запускаем tcpdump, где задаем нужные параметры:



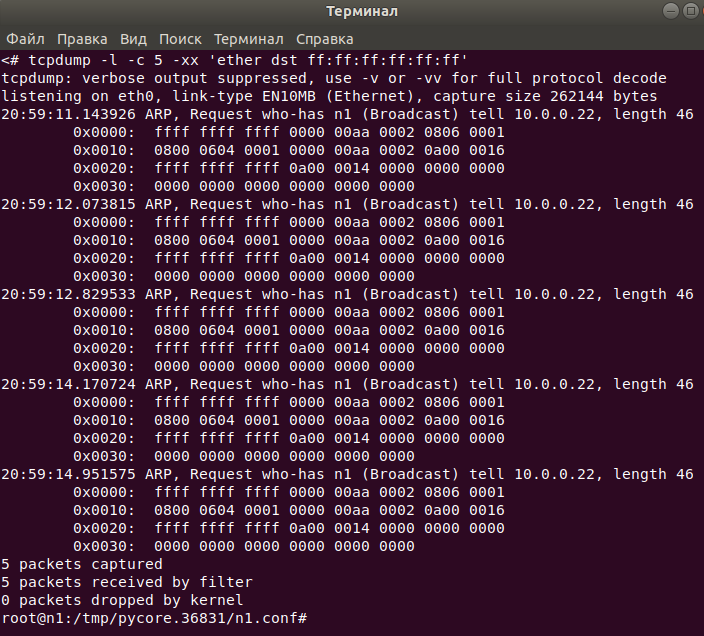


2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

Составляем широковещательный MAC-пакет на хосте n2 с помощью PackETH:

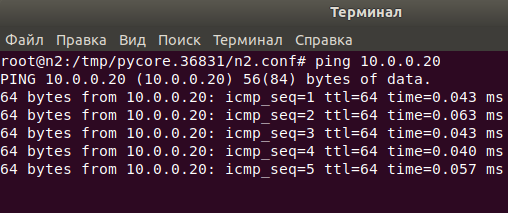


На другом хосте n1 запускаем tcpdump с нужными параметрами и фильтрами, совершаем 5 раз широковещательную рассылку (send) в PackETH:

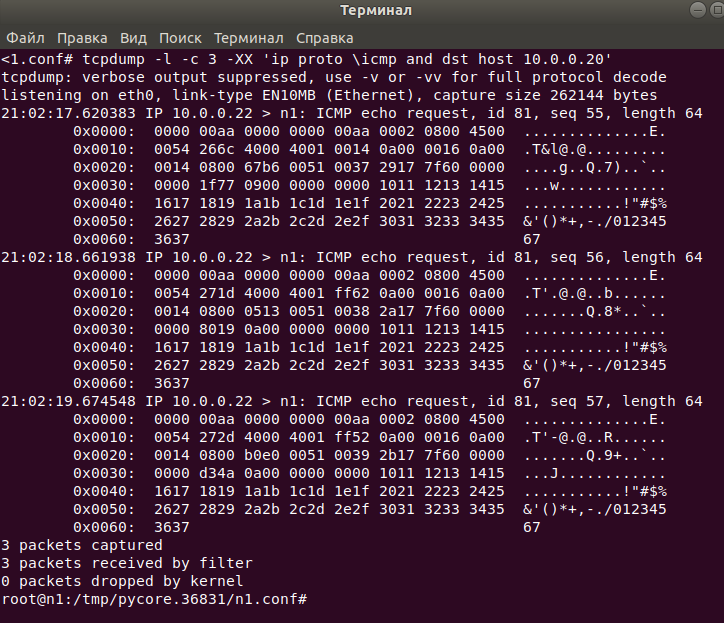


3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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

Передаем пакеты с хоста n2 на n1:

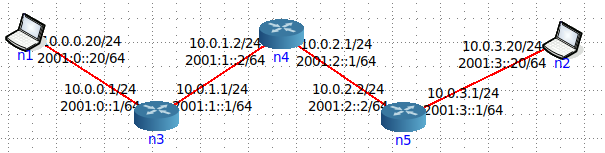


Запускаем tcpdump на хосте n1 c нужными параметрами и фильтрами:

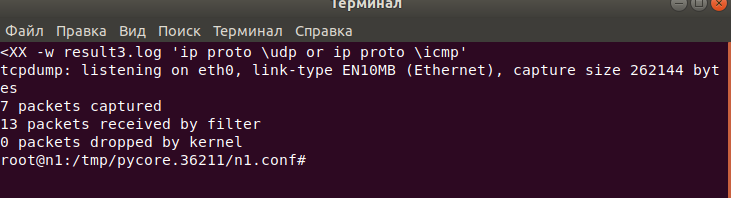


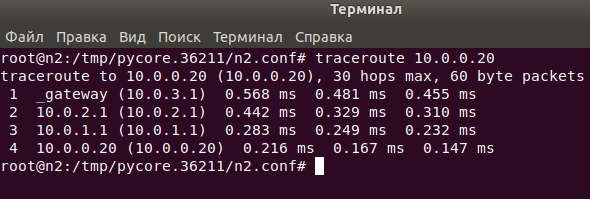
4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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

Увеличим структуру сети:

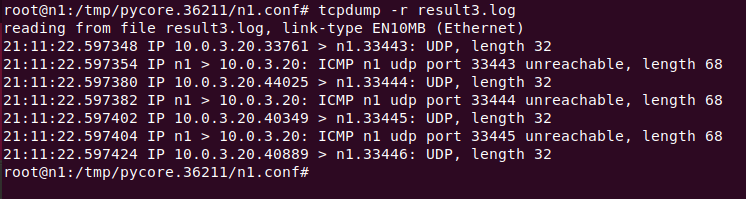


Запустим tcpdump на хосте n1 с нужными параметрами, фильтрами и одновременно передадим пакеты с хоста n2 с помощью утилиты traceroute:





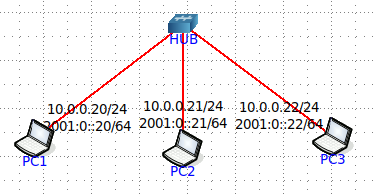
5. Прочесть программой tcpdump созданный в предыдущем пункте файл.



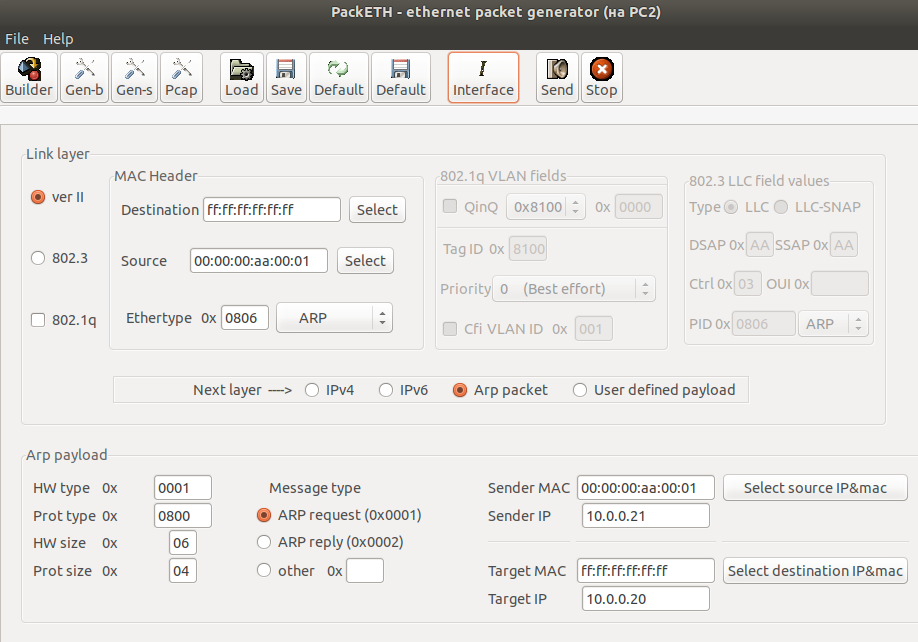
6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

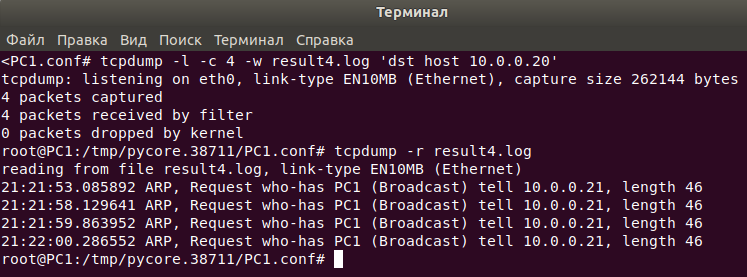
1) Запустить tcpdump в режиме перехвата широковещательного трафика (с фильтром ip-адреса получателя). Сохранять данные в двоичном формате. Количество захватываемых пакетов ограничить до 4-х. Широковещательную рассылку совершать с помощью PackETH.

Структура сети:



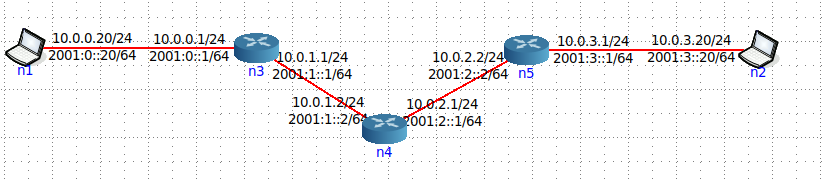
Составление кадра ARP, передача пакетов:



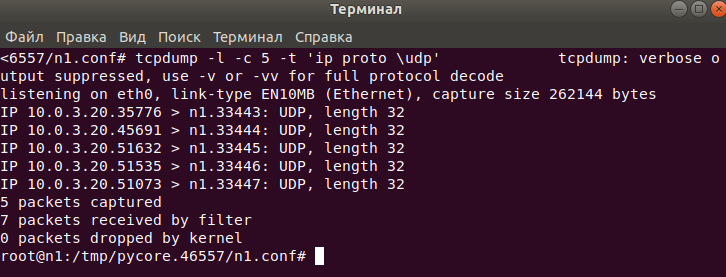


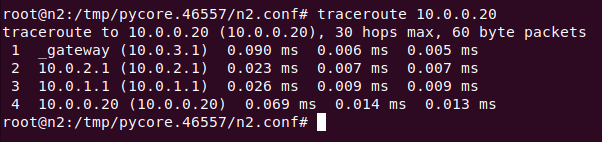
2) Запустить tcpdump, перехватывающий пакеты с фильтром протокола UDP. Не отображать метку времени в каждой строке. Количество захватываемых пакетов ограничить до 5. Для передачи пакетов воспользоваться утилитой traceroute.

Структура сети:



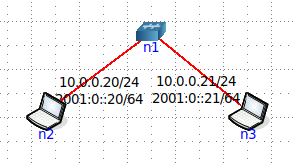
Передача пакетов:



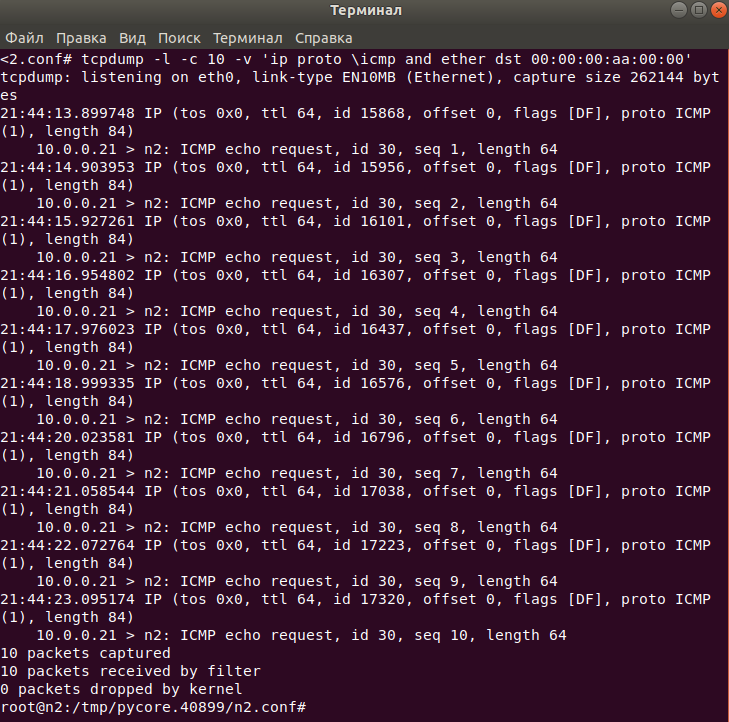


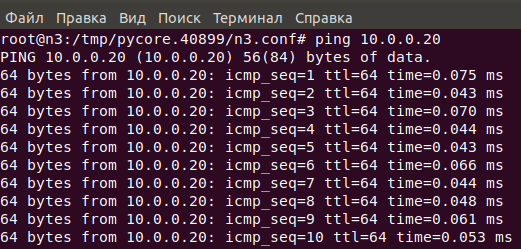
3) Запустить tcpdump, перехватывающий пакеты только протокола ICMP (с фильтром MAC-адреса получателя). Вывод подробной информации. Количество захватываемых пакетов ограничить до 10. Для передачи пакетов воспользоваться утилитой ping.

Структура сети:



Передача пакетов:

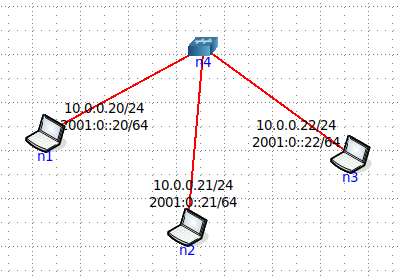




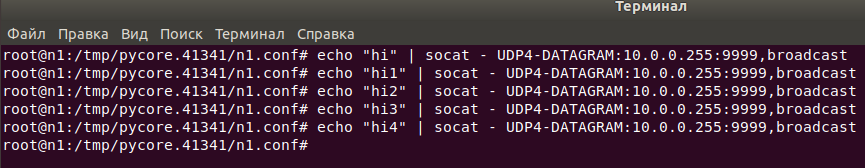
**Работа с анализатором протоколов wireshark**

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

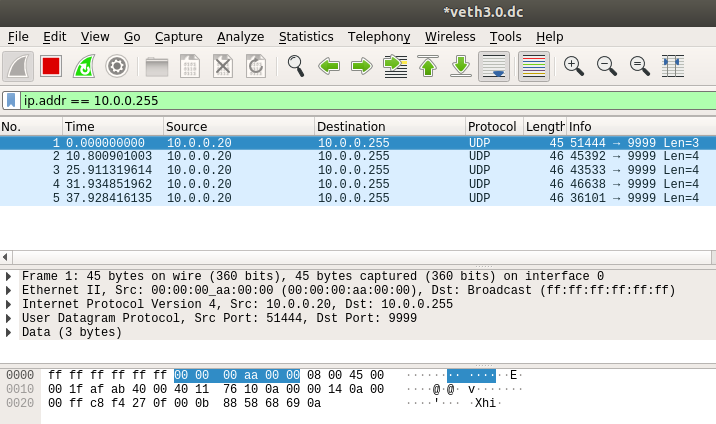
Структура сети:



Создаем широковещательный трафик на хосте n1:

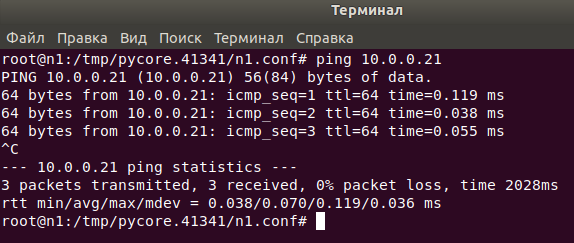


Захват пакетов с помощью Wireshark (фильтр по IP-адресу):

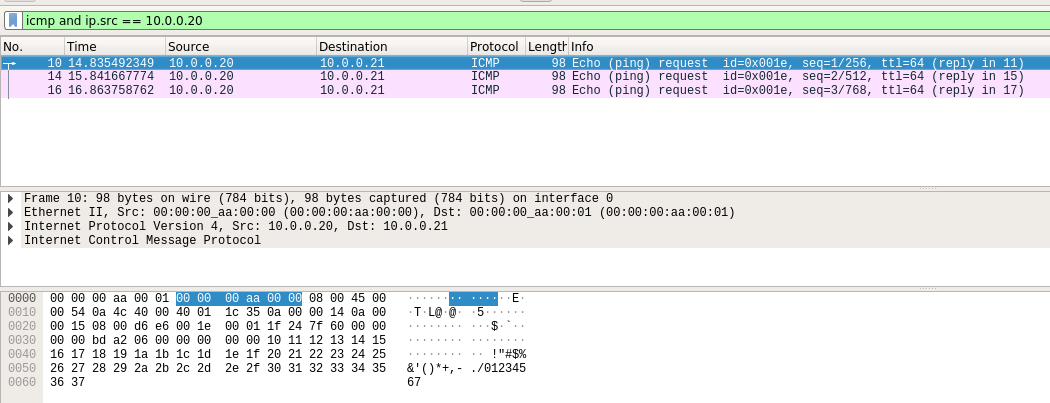


2. Захватить 3 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.

Передаем пакеты из хоста n1 в n2:

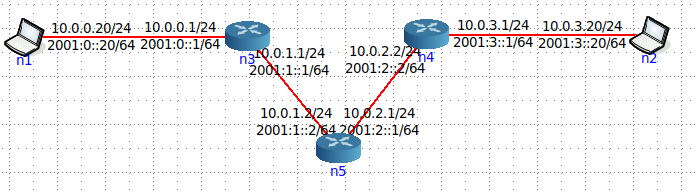


Захват пакетов с помощью Wireshark на хосте n2 (фильтр по протоколу ICMP и IP-адресу отправителя):

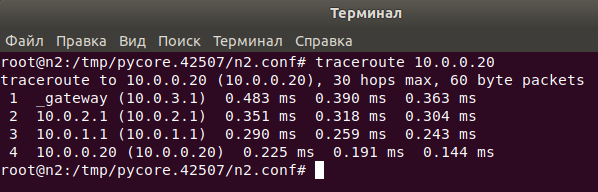


3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла, либо в виде изображения.

Структура сети:



Передадим пакеты при помощи утилиты traceroute с хоста n2:



Захват пакетов с помощью Wireshark на хосте n1:

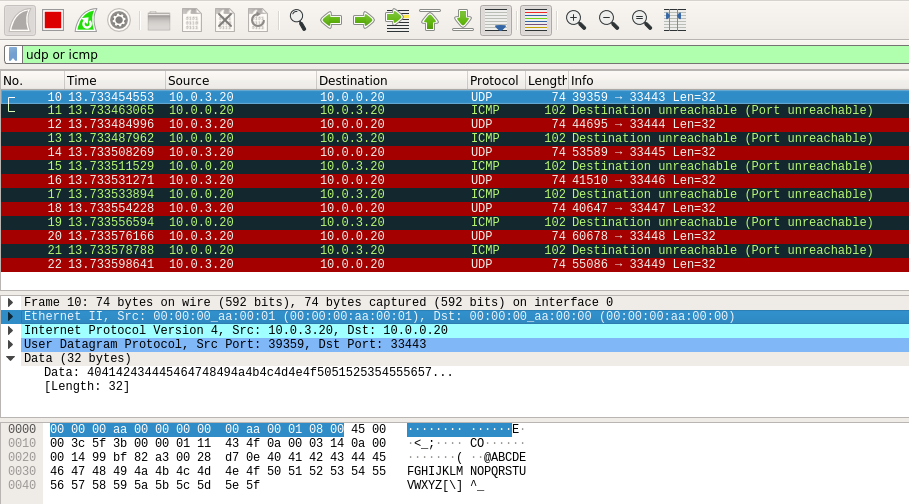
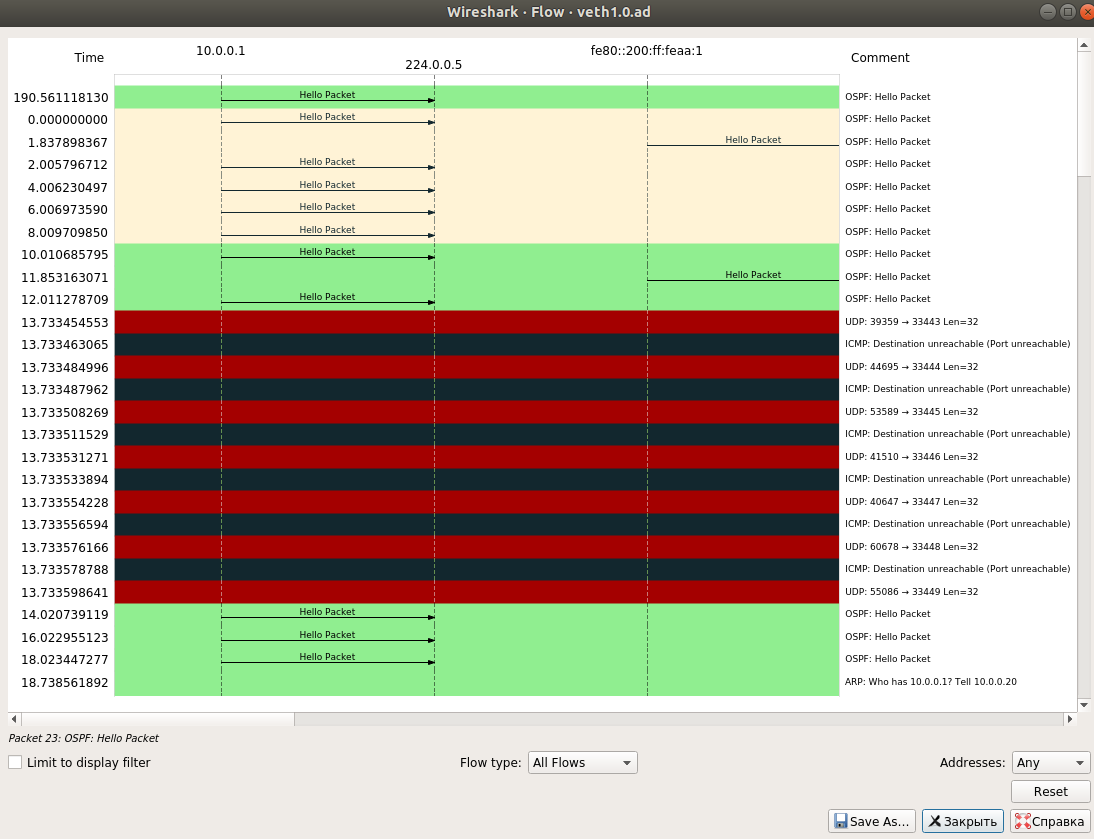
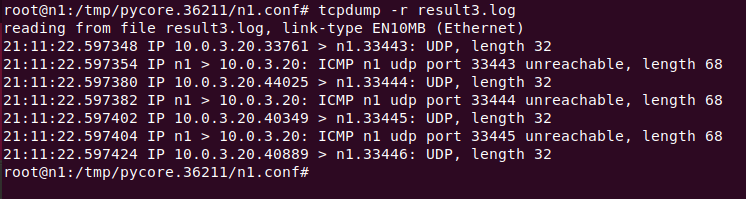
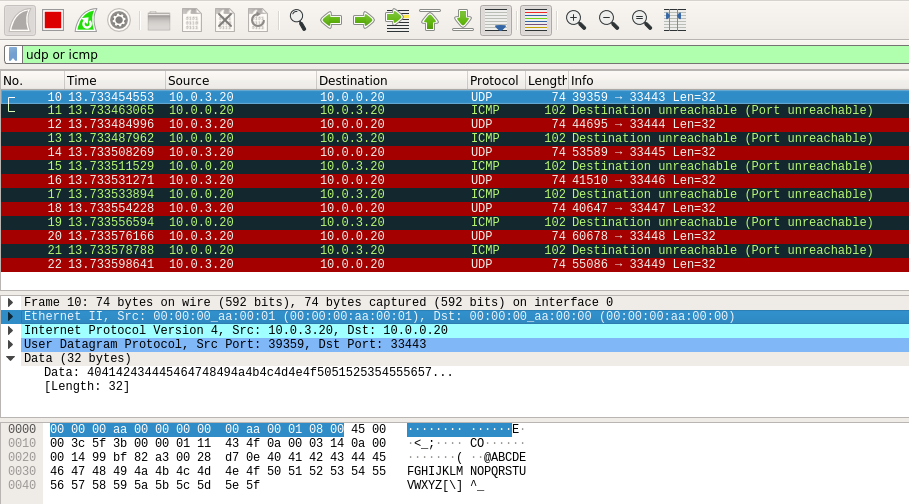


Диаграмма Flow Graph:



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





В Wireshark представлена более подробная информация о пересылаемых пакетах.