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:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Кожакин Р. А.

Группа 18-В-2

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

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

Нижний Новгород

2021 г.

**Задание:**

**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 воспользоваться 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).

2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping.

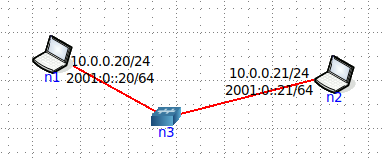
3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла, либо в виде изображения.

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

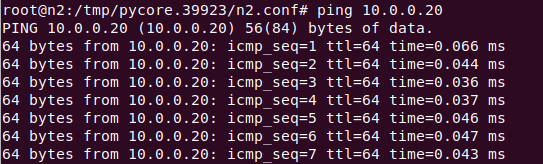
**Ход работы.**

1. Запустить tcpdump в режиме захвата всех пакетов, проходящих по сети.

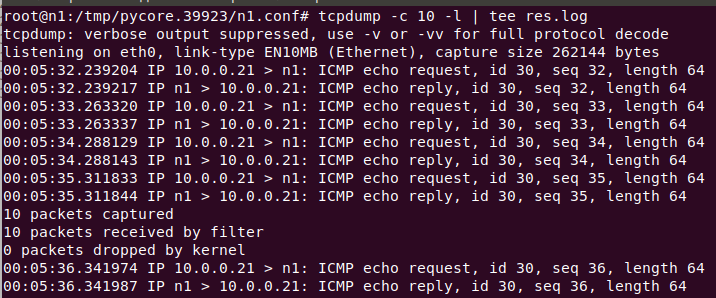
Количество захватываемых пакетов ограничить 10. Результаты протоколировать в файл. Создадим следующую сеть:



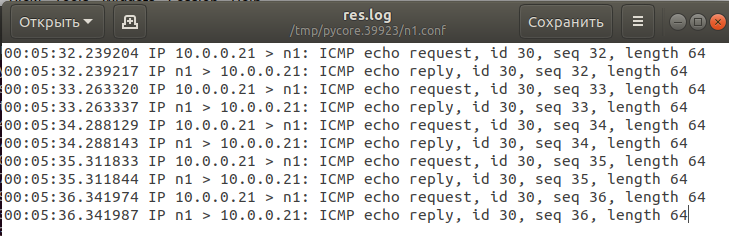
Запустим пинг с n2 на n1:



Далее запустим на n1 tcpdump с параметрами (количество захв. пакетов, куда сохранять):

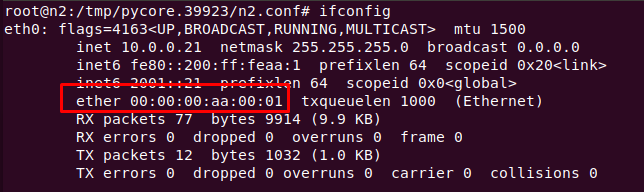


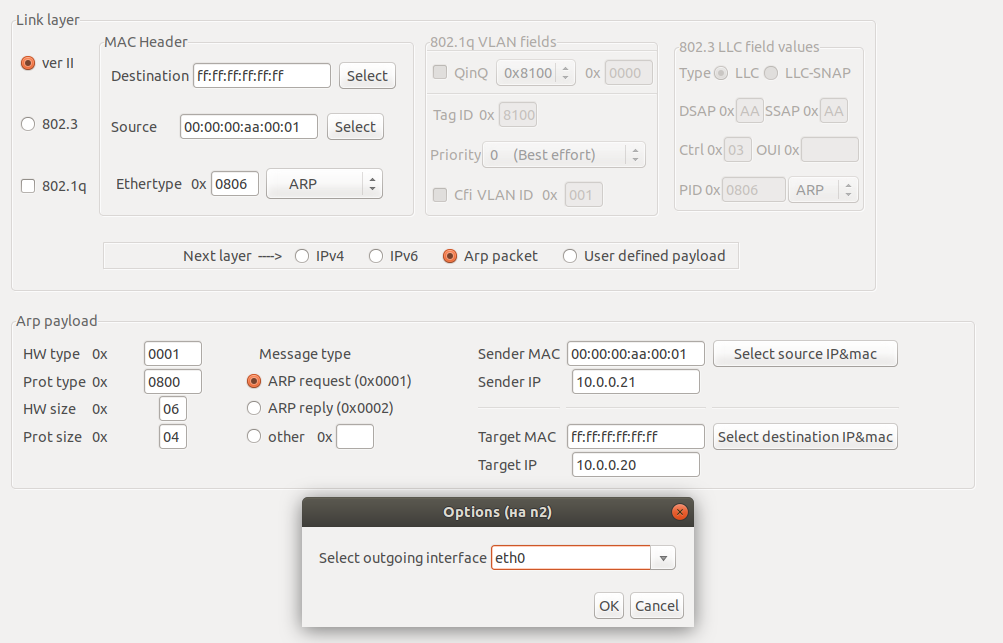
Просмотрим сохраненный файл с результатами:



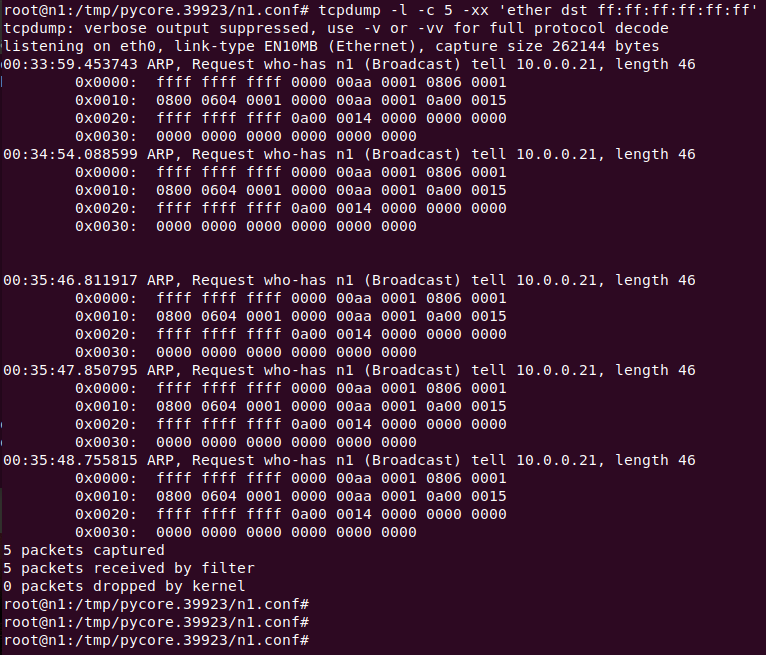
1. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

Открываем PackETH. Для запуска packEth в консоли выполняем команду «xhost +», в консоли n2 «DISPLAY=:0 packeth. Составляем широковещательный MAC-пакет на n2, при этом его MAC-адрес найдём с помощью ifconfig.





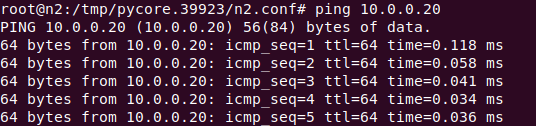
На другом компьютере запустим tcpdump. Совершаем широковещат. рассылку в PackEth:

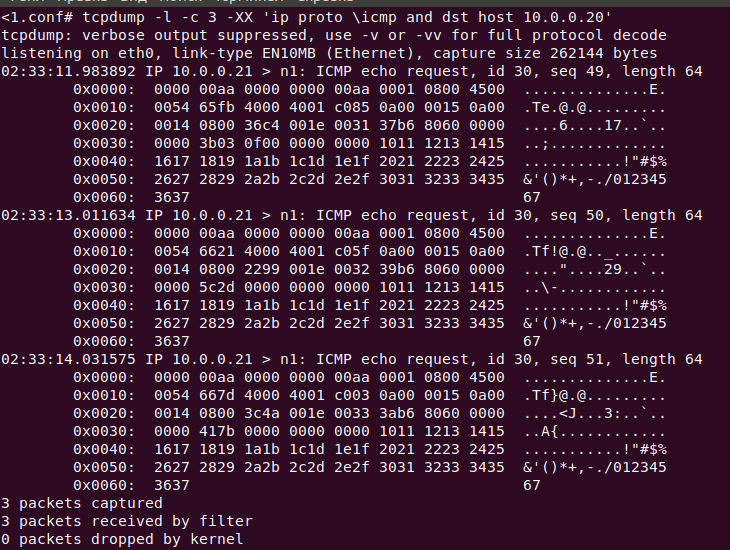


Всё прошло успешно.

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 воспользоваться утилитой ping.

Снова запускаем пинг с n2 на n1 и tcpdump, но уже с другими параметрами:

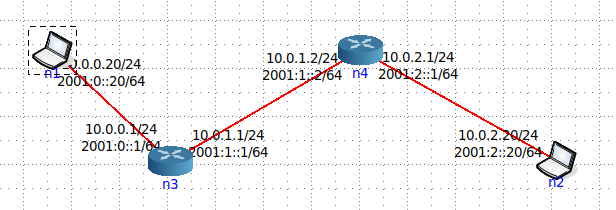




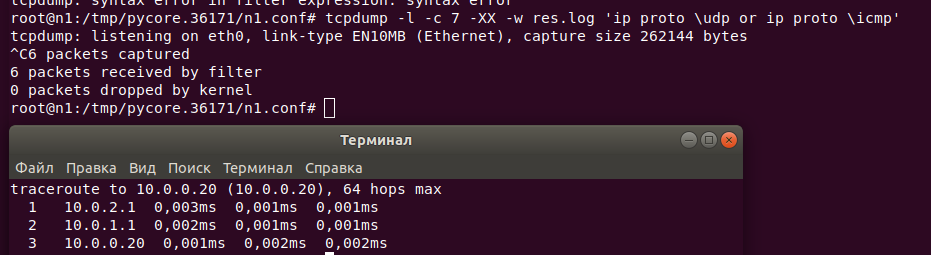
Успешно.

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.

Изменим структуру сети так, чтобы можно было определять маршруты:

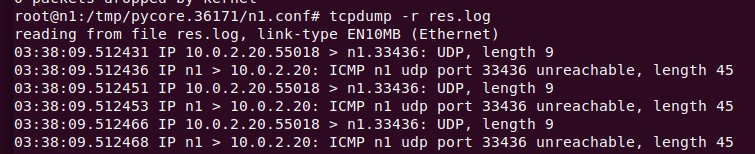


Создадим tcpdump c нужными параметрами на n1, чтобы он перехватил пакеты, созданные traceroute с n2:



1. Прочесть программой tcpdump созданный в предыдущем пункте файл.

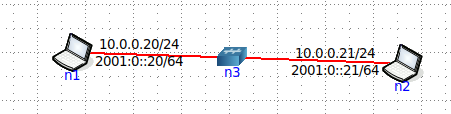
Так как файл мы сохраняли в двоичном режиме, его нужно открыть через консоль:

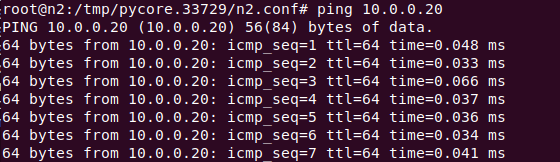


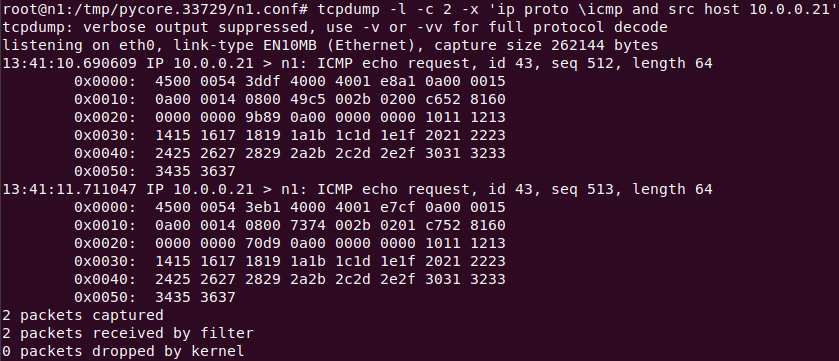
1. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP.

* Задание 1

Запустить tcpdump, чтобы он перехватывал пакеты протокола ICMP, отправленные с определенного IP-адреса. При этом включить распечатку пакета в шестнадцатеричной системе (без заголовка канального уровня). Для генерирования пакетов воспользоваться утилитой ping. Количество захватываемых пакетов ограничить 2.

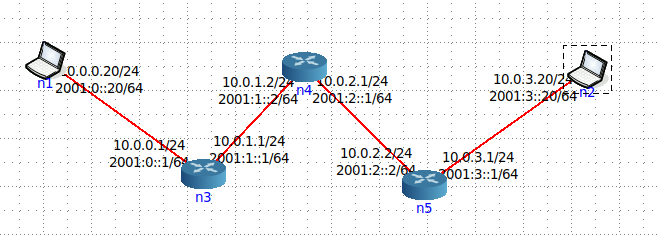


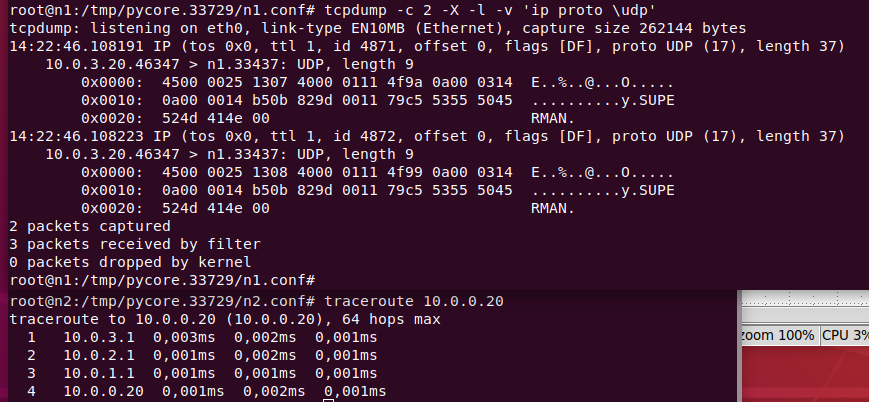




* Задание 2

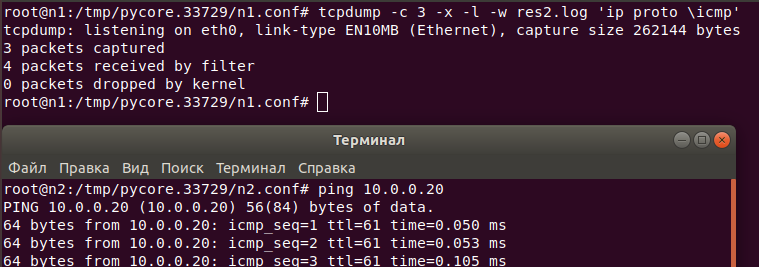
Запустить tcpdump, чтобы он перехватывал 2 пакета протокола UDP. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате. Отобразить подробную информацию. Для генерирования пакетов воспользоваться утилитой traceroute.

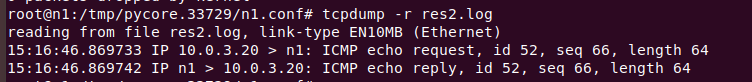




* Задание 3

Запустить tcpdump, чтобы он перехватывал пакеты протокола ICMP. При этом включить распечатку пакета в шестнадцатеричной системе (без заголовка канального уровня). Для генерирования пакетов воспользоваться утилитой ping. Количество захватываемых пакетов ограничить 2. Сохранять данные в двоичном режиме. Результат работы программы писать в файл, прочитать его.

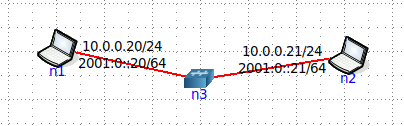




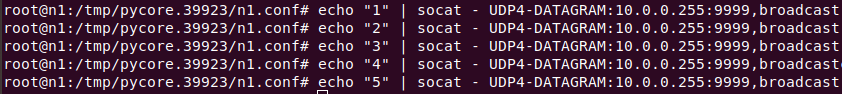
**Работа с анализатором протоколов wireshark**

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

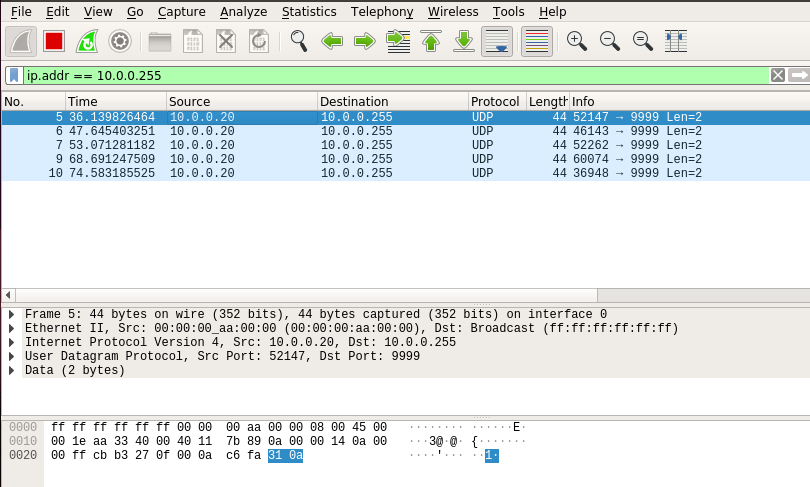
Вернемся к старой схеме:



Создаем широковещательный трафик на n1:

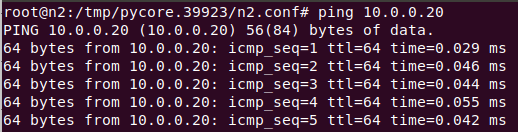


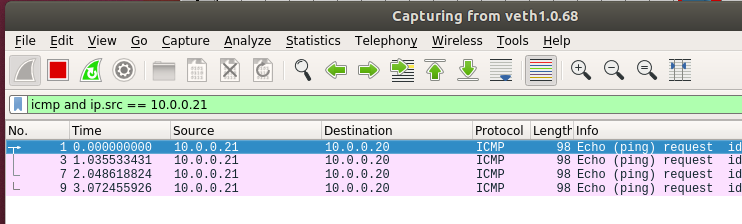
Захват 5 пакетов с помощью Wireshark (фильтр по IP-адресу):



1. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping.

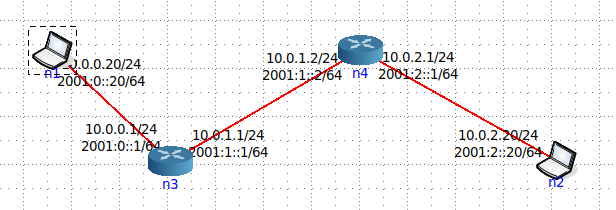
Ping из n2 в n1:



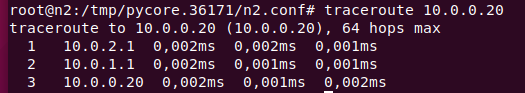
Применяем фильтр и получаем:

1. 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.

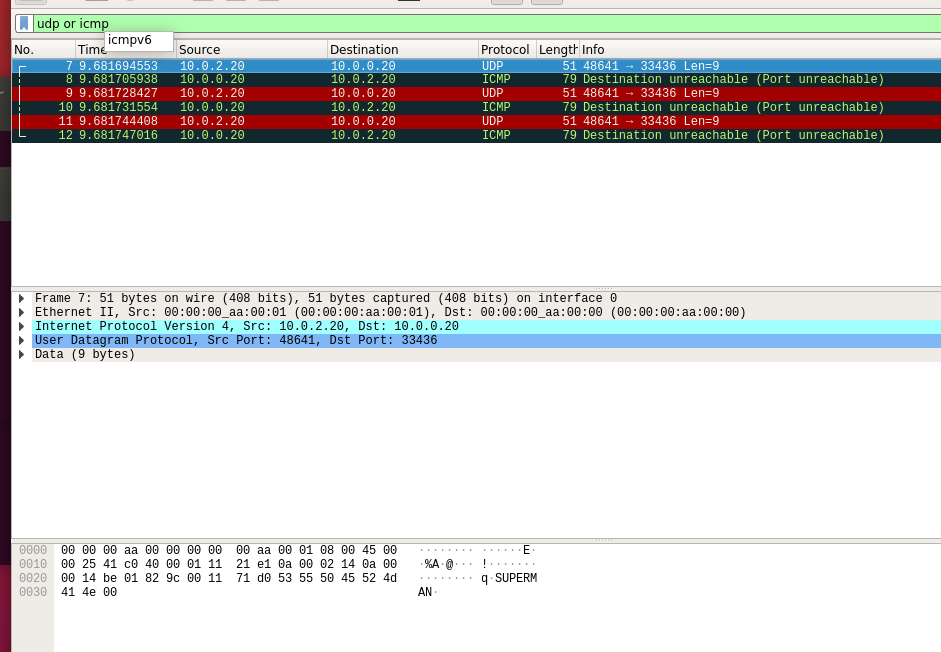
Вернемся к сети:



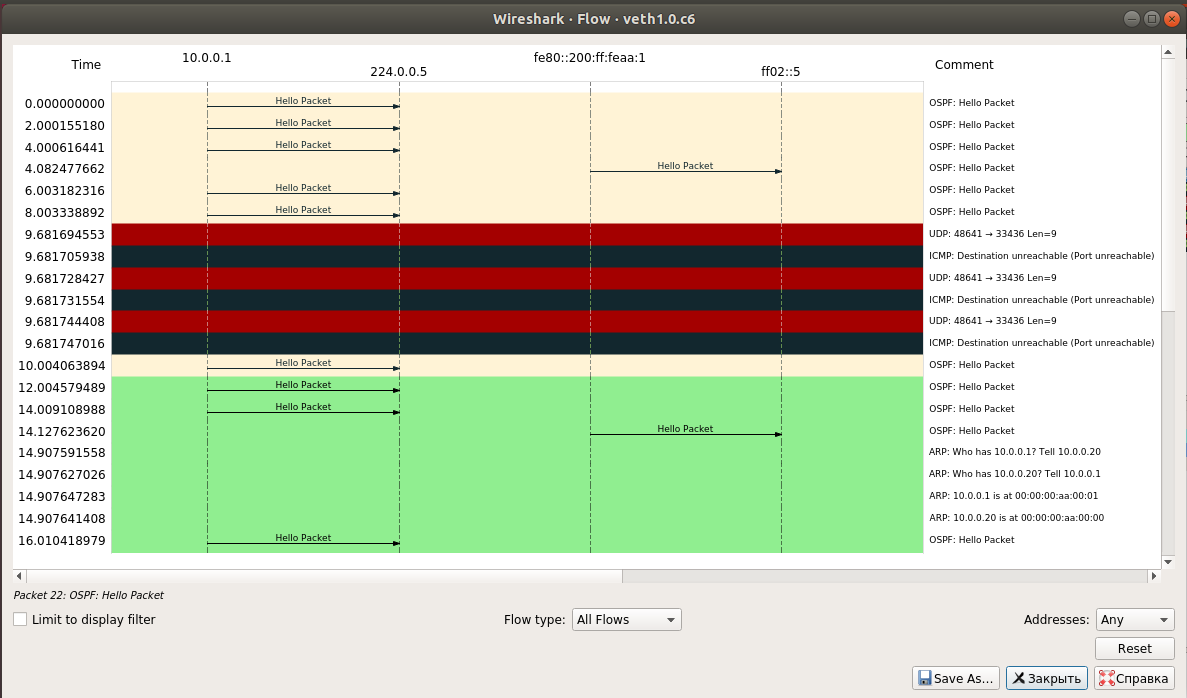
Запустим traceroute на n2:



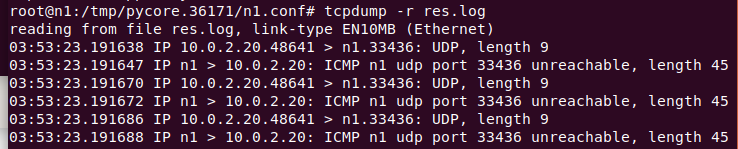
Применим фильтр вы Wireshark и увидим пакеты:



FlowGraph выглядит следующим образом:



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



Таким образом можно увидеть, что информация полностью сходится, однако в это же время в Wireshark мы можем увидеть и другую информацию, например, данные пересылаемых пакетов.