МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра вычислительных систем и технологий

Отчет по лабораторной работе №1

по дисциплине

"Сети и телекоммуникации"

РУКОВОДИТЕЛЬ:

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

Студенты группы 19-В-2:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Степушин С.В.

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

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

Нижний Новгород 2021

**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 MACадресу). 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.

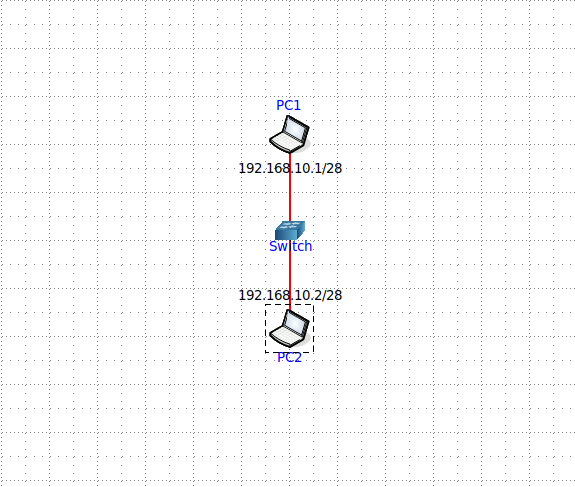
2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов возпользоваться утилитой ping. Результат сохранить в текстовый файл.

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.

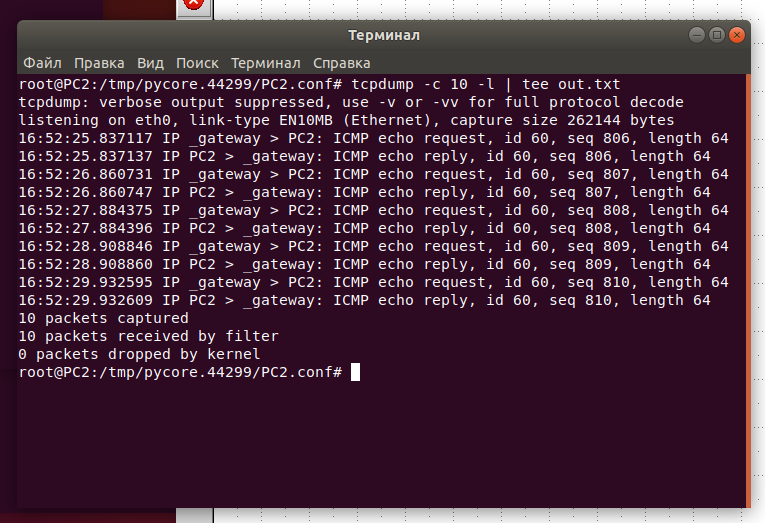
**Выполнение работы.**

Соберем схему:



**Работа с анализатором протоколов tcpdump.**

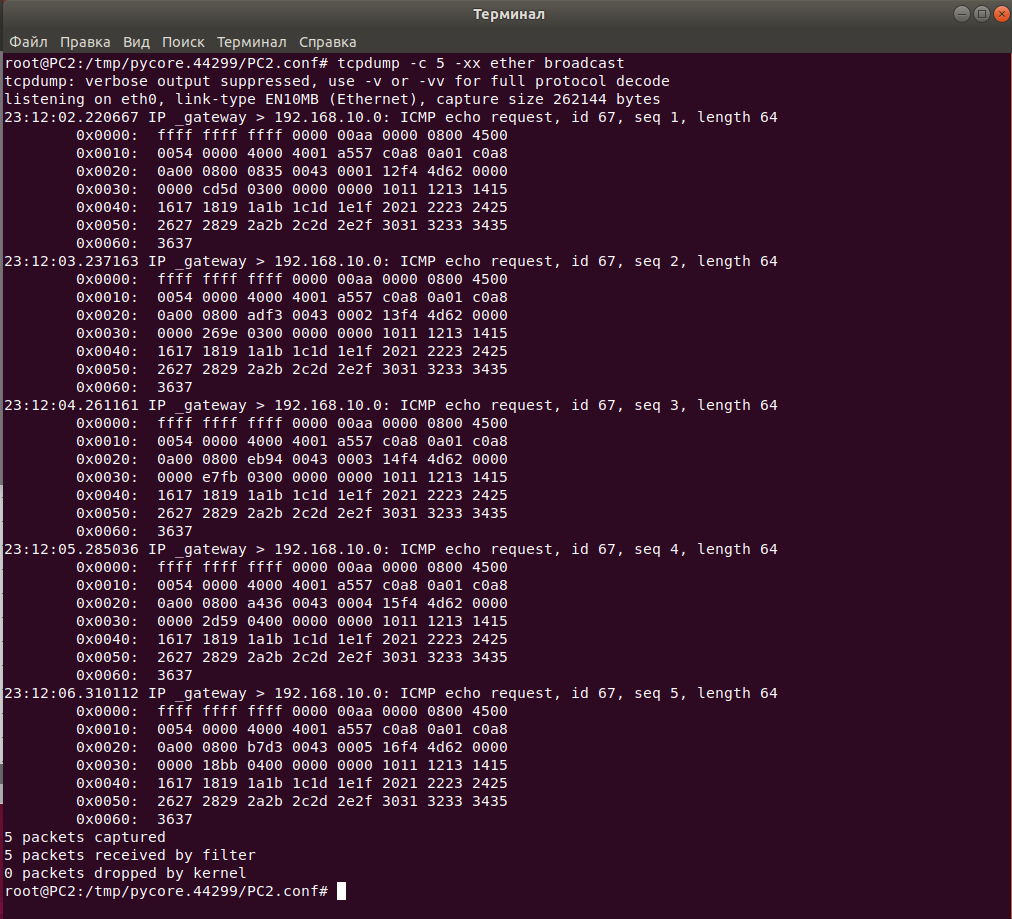
**1.** Запускаем на PC2 tcpdump, отлавливаем 10 пакетов и записываем в файл.



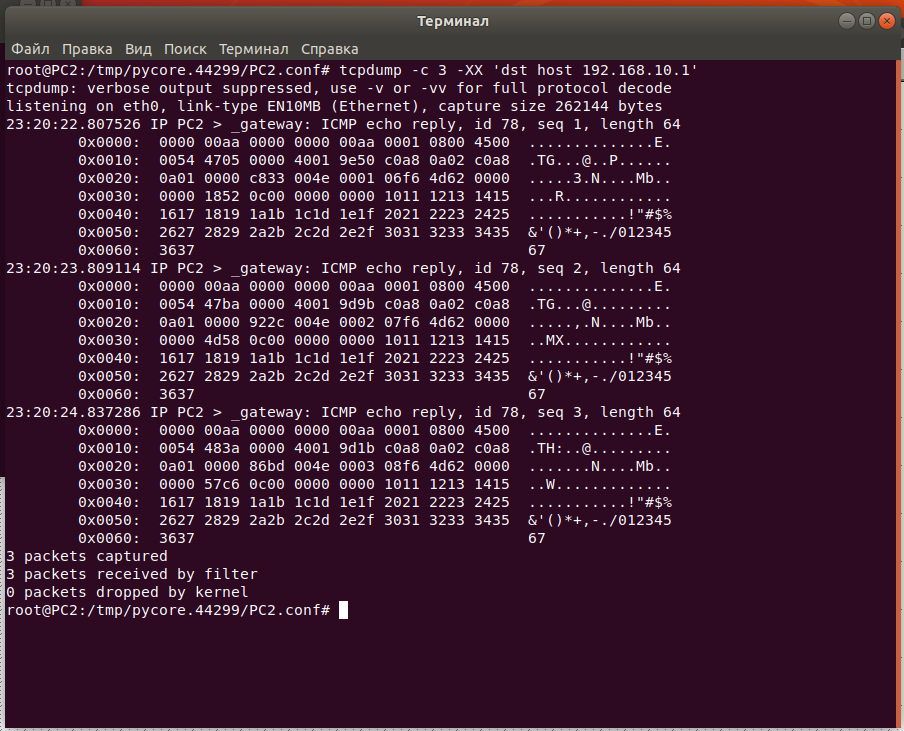
**2.** С PC1 отправляем широковещательный запрос.



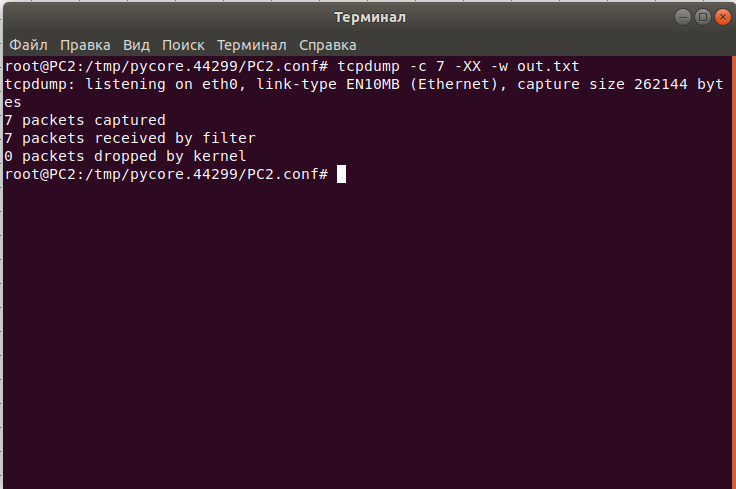
Затем на PC2 отлавливаем.



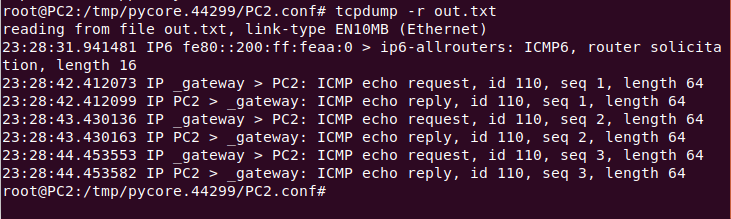
**3.** Запускаем на PC1 ping. А на PC2 отлавливаем только ICMP.

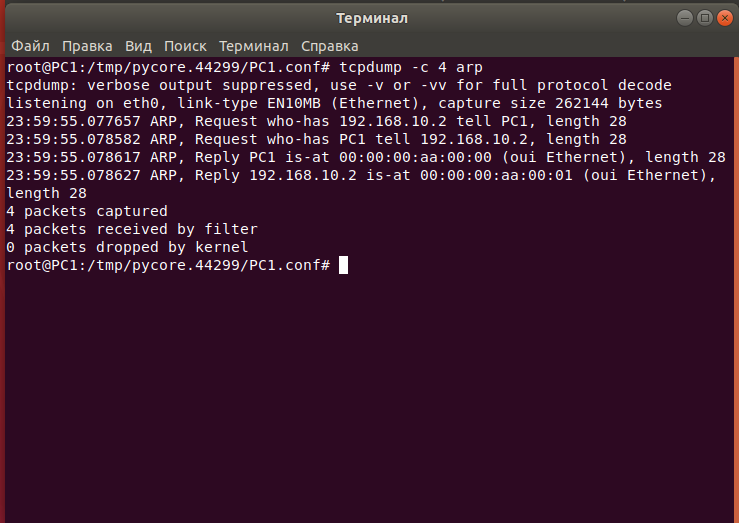


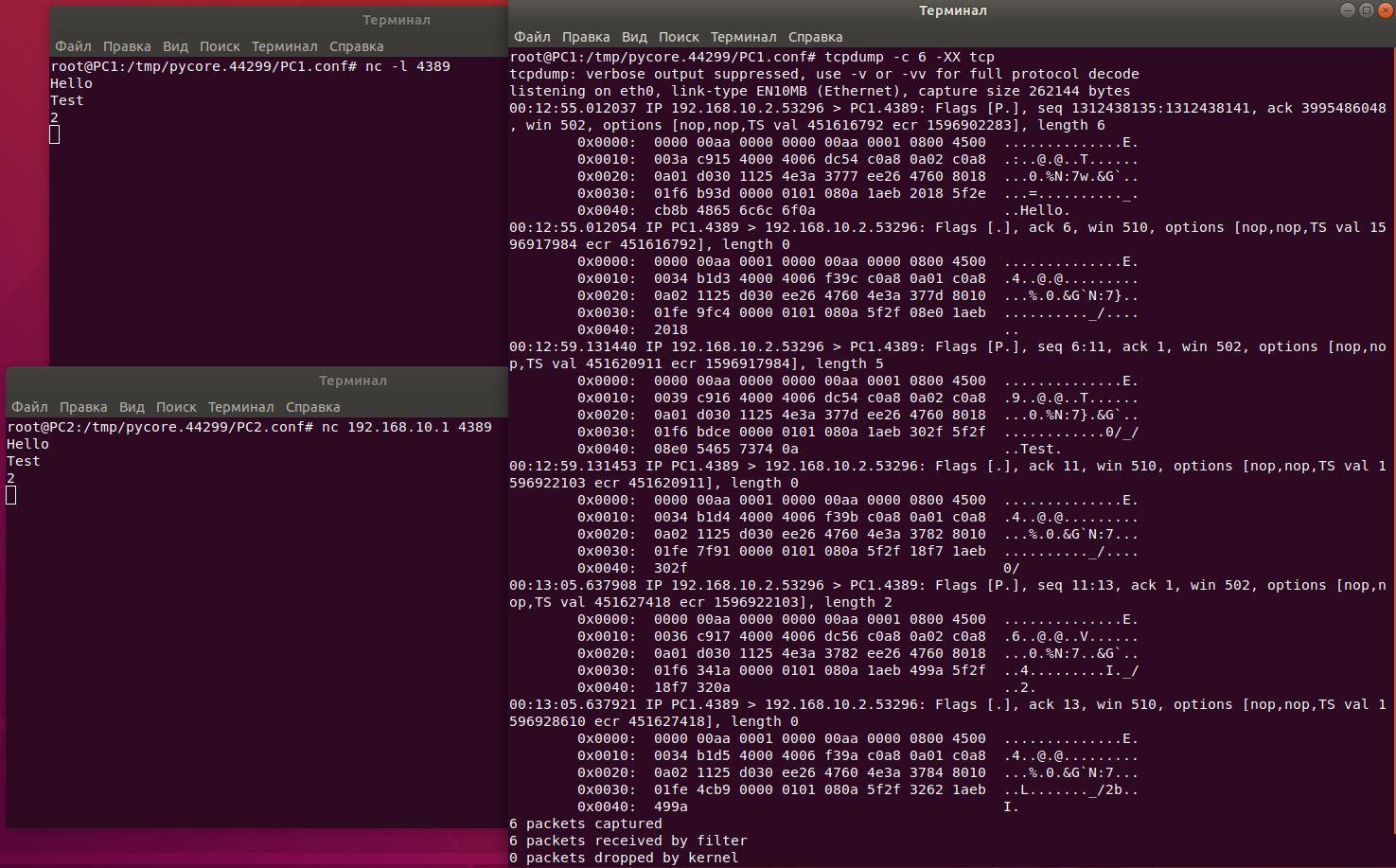
**4.** На PC2 запускаем tcpdump в режиме сохранения данных.



**5.** Здесь с помощью tcpdump читаем файл out.txt, который содержит сохраненные данные ранее.

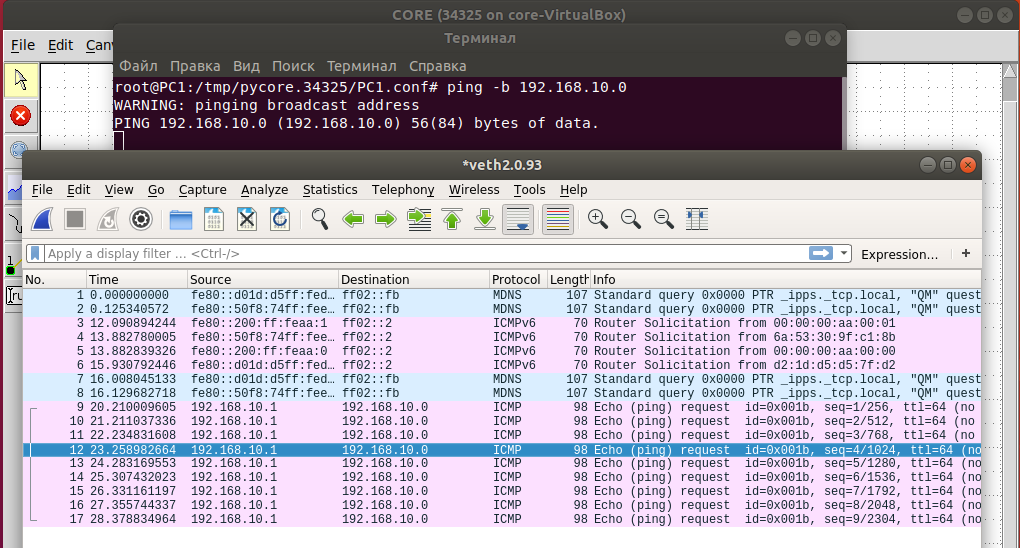


**6.** Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ARP, отправленные на определенный IP-адрес. Количество захватываемых пакетов ограничить 4. Для генерирования пакетов воспользоваться утилитой ping.  


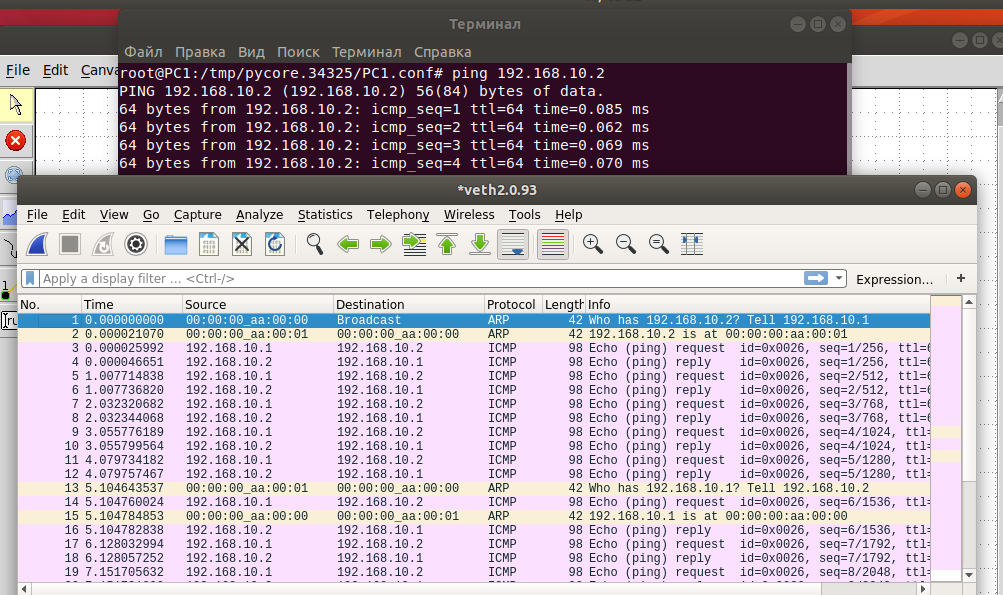
Запустить tcpdump так, чтобы он перехватывал только пакеты протокола TCP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 6. Для генерирования пакетов воспользоваться утилитой ping.  


**Работа с анализатором протоколов wireshark.**

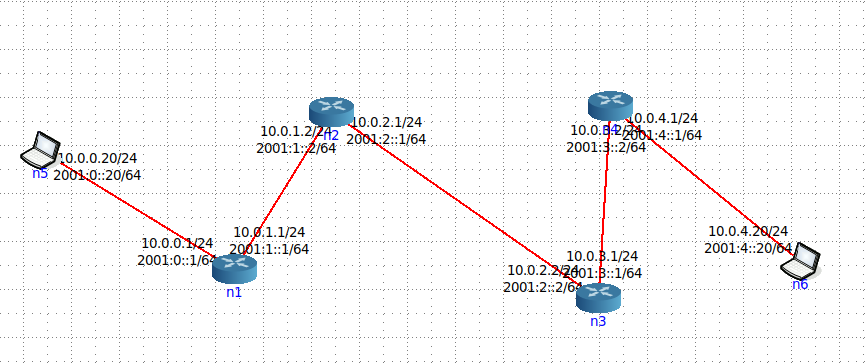
**1.** С PC1 создаем широковещательный трафик. На PC2 отлавливаем пакеты широковещательного трафика с помощью Wireshark.



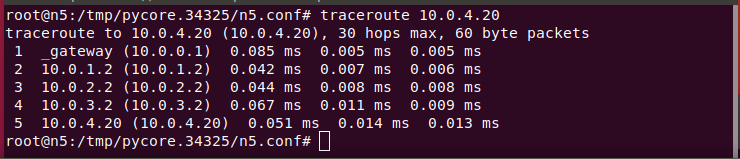
**2.** С PC1 запускаем ping на PC2. На PC2 отлавливаем пакеты ICMP.



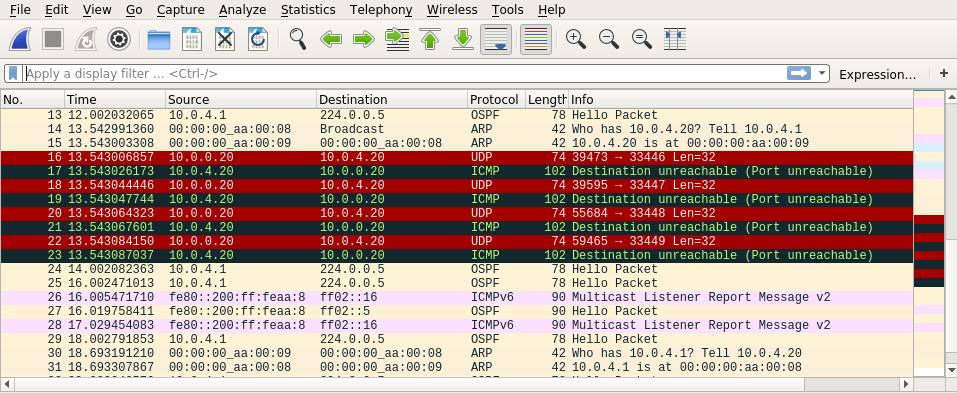
**3.** Соберем схему:

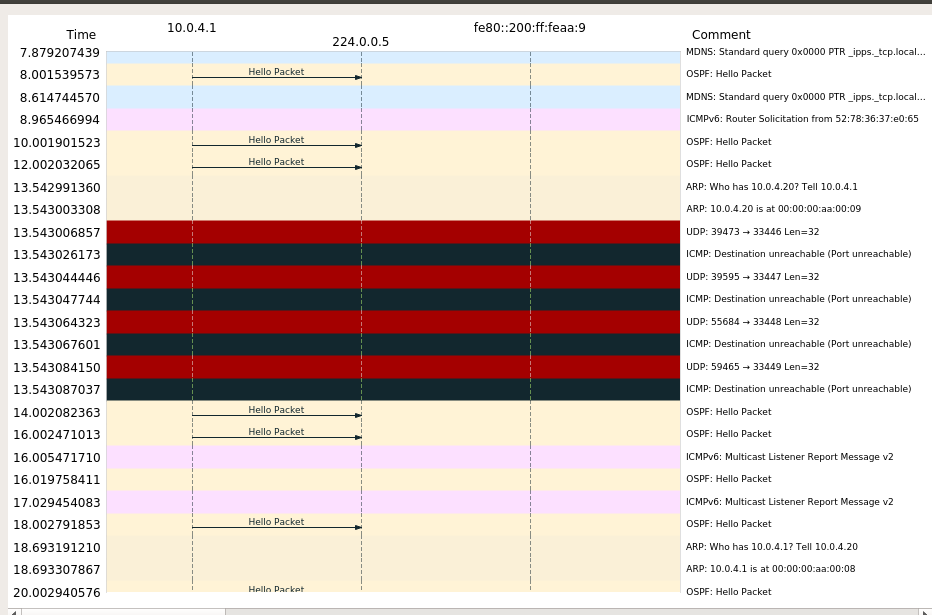
****

Запустим traceroute с n5.

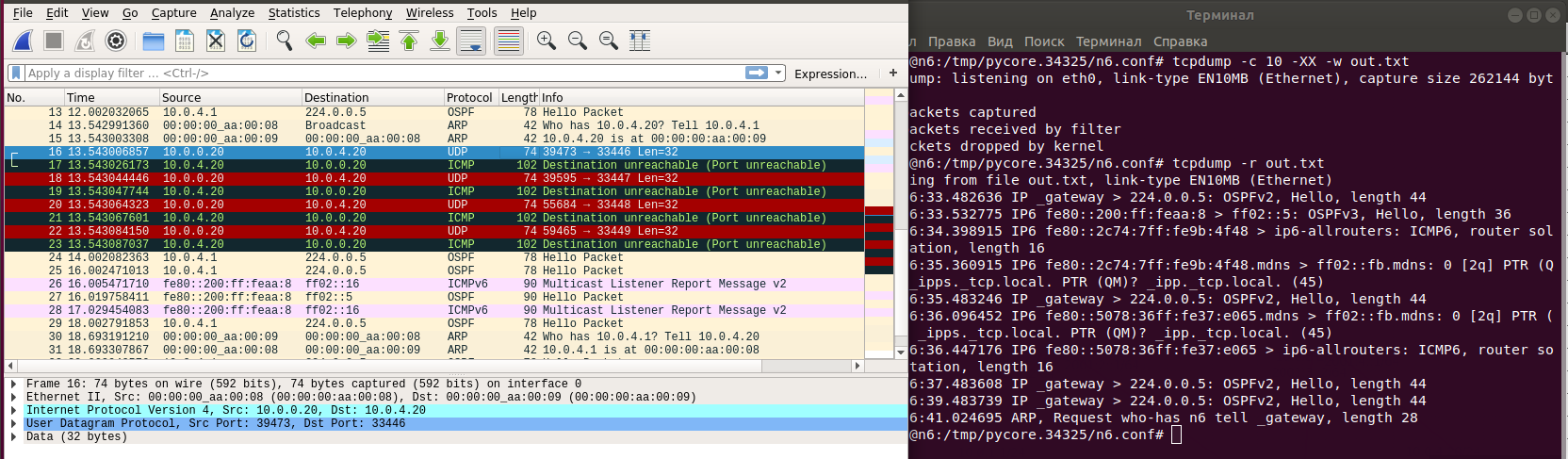


На n6 отлавливаем пакеты через Wireshark.

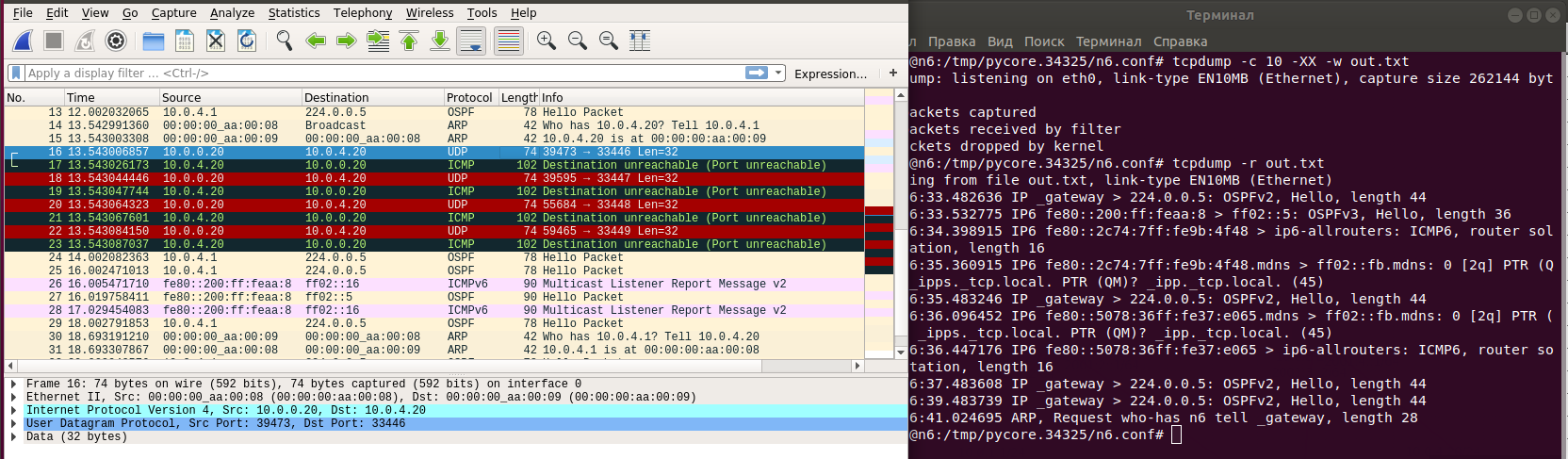




**4.** Рассмотрим данные сохраненные tcpdump.



Рассмотрим пакеты, которые получил Wireshark.



Как мы можем видеть информация совпадает, однако Wireshark предоставляет более детальную информацию.