МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

Кафедра информатики и систем управления

Лабораторная работа №5

ОТЧЕТ

по лабораторной работе

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

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

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Лосев Д. А.

(подпись) (фамилия, и.,о.)

19-АС

(шифр группы)

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

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

Нижний Новгород 2022

**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 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.

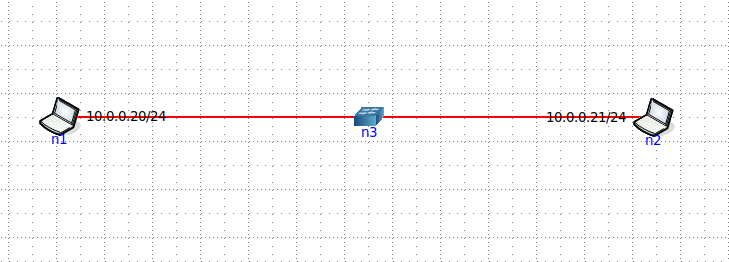
3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.

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

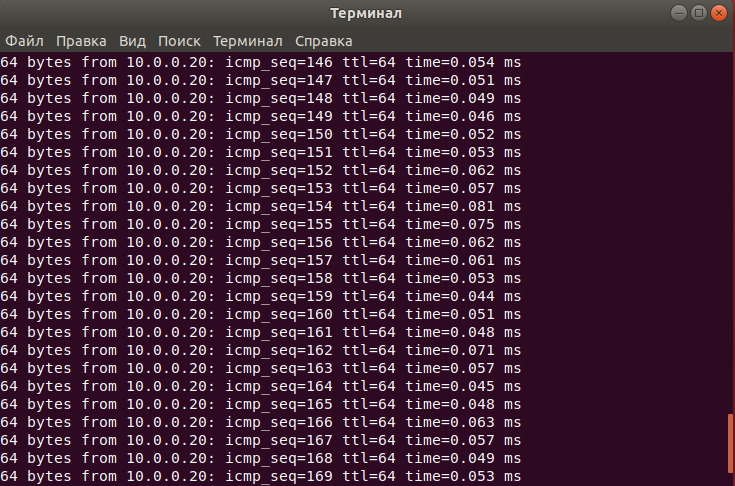
**Работа с анализатором протоколов tcpdump**

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

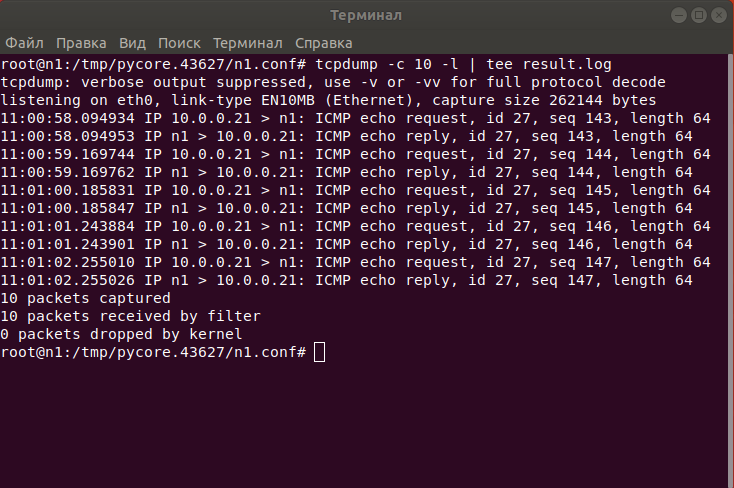
*Структура сети:*



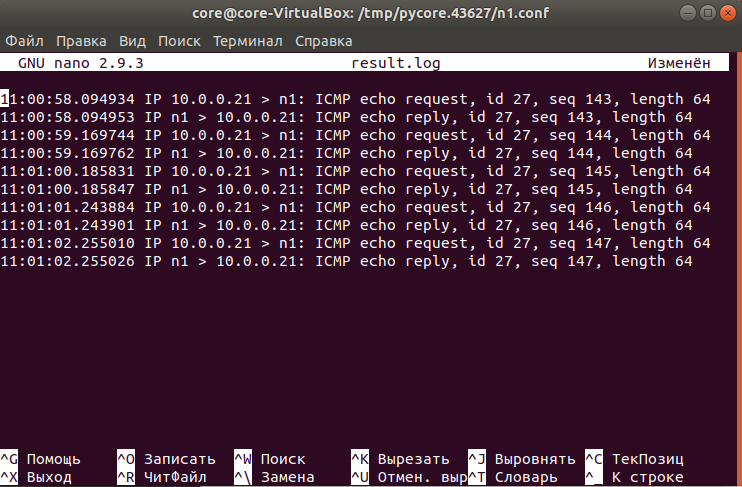
*Запускаем ping с PC2 на PC1:*



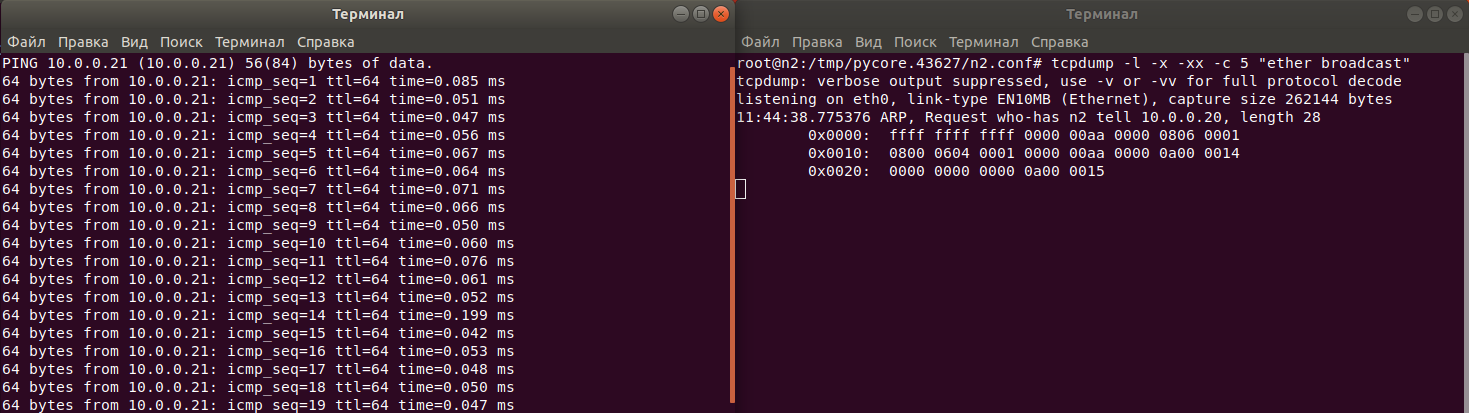
*На PC1 запускаем tcpdump с нужными параметрами:*



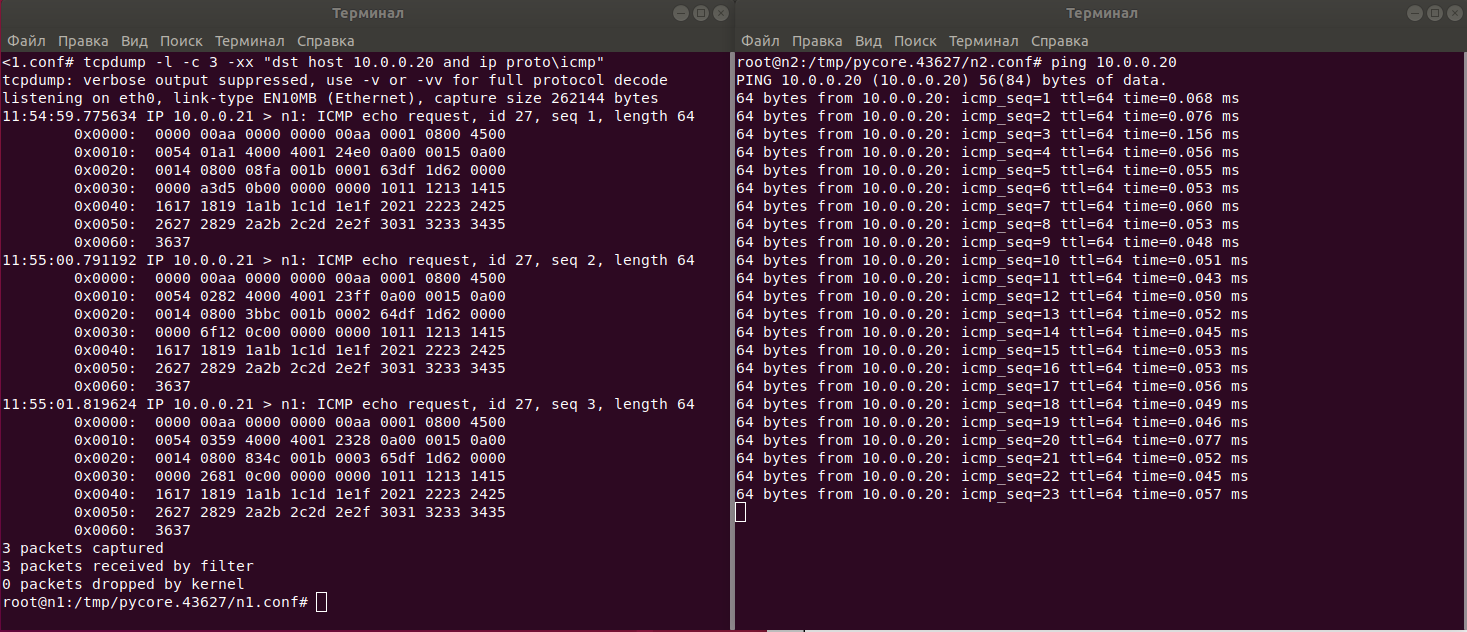
*Результаты в файле:*



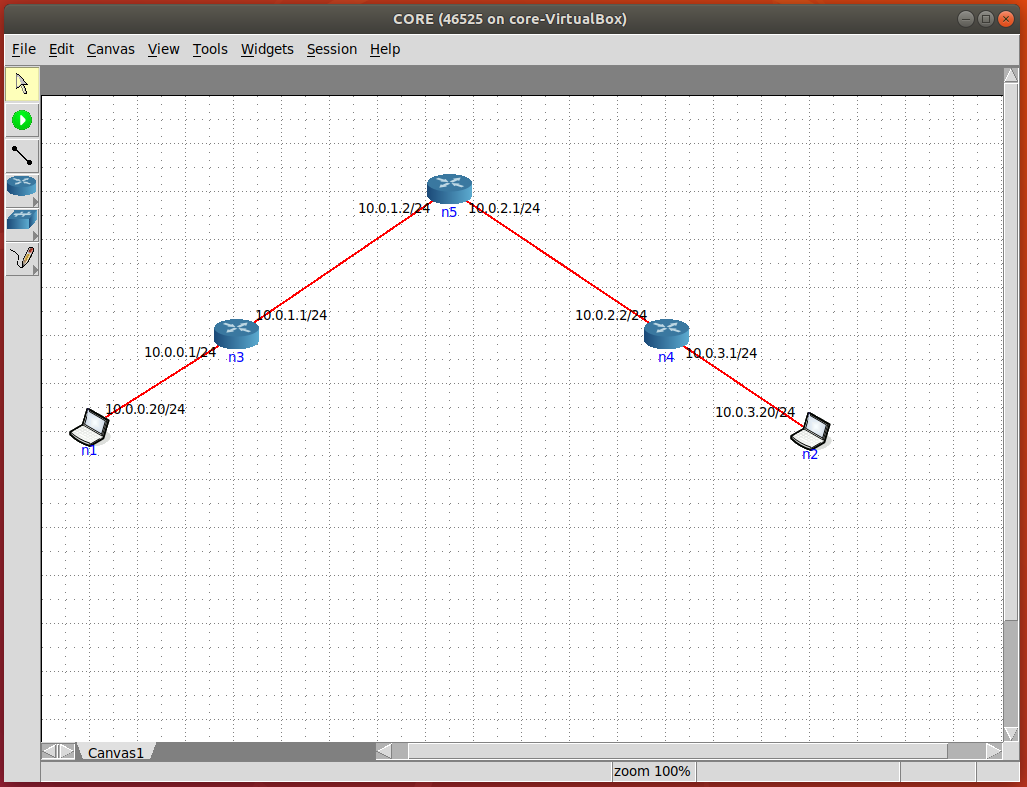
**#2.** Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

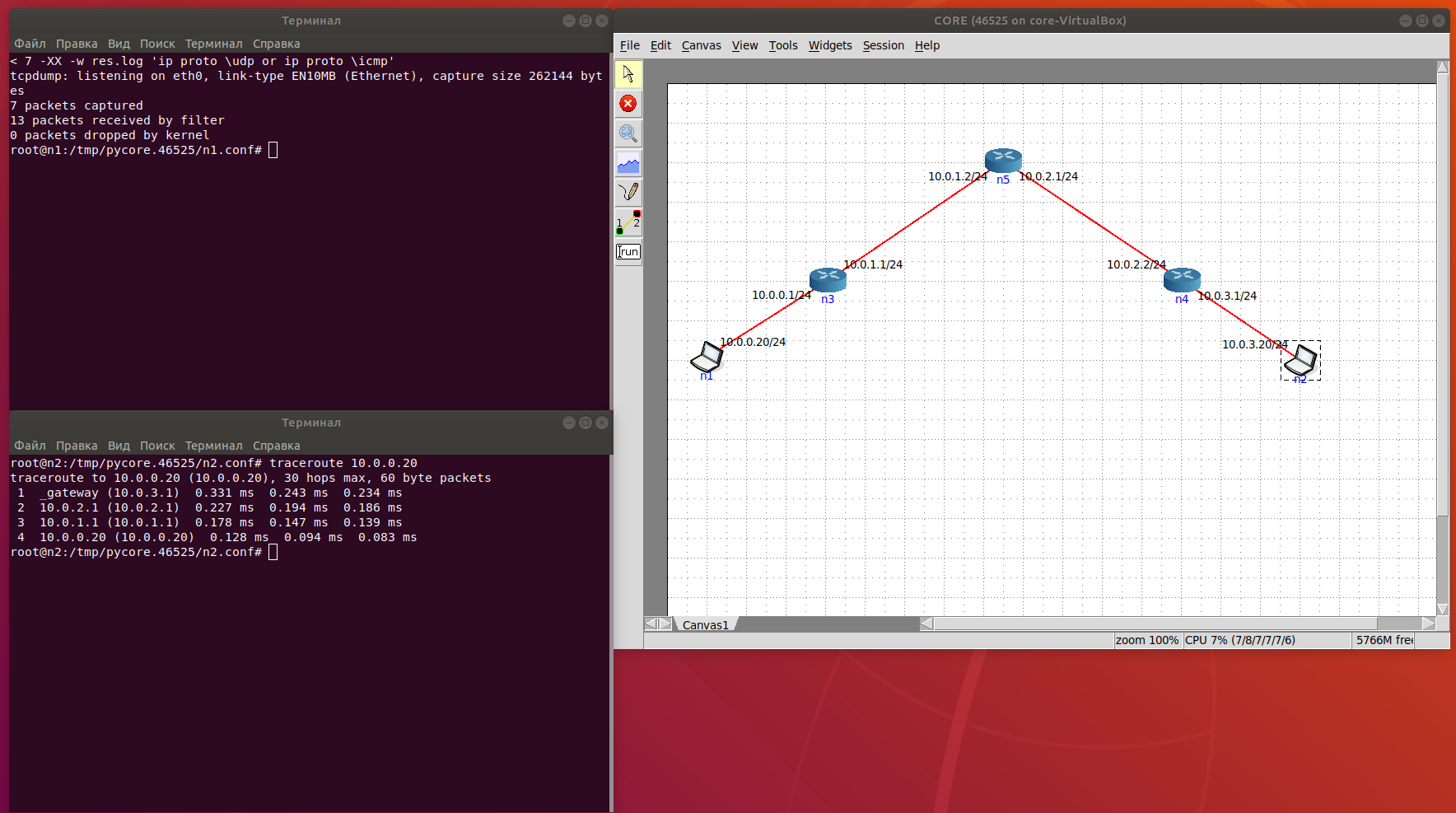


**#3.** Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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

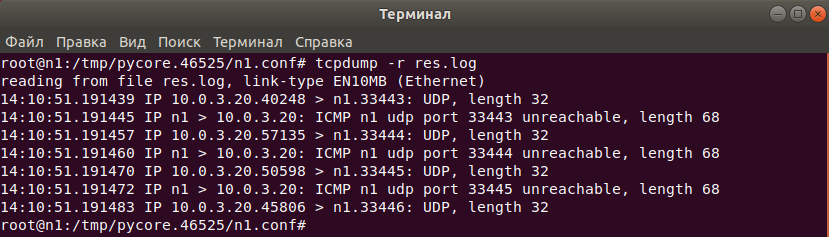


**#4.** Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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



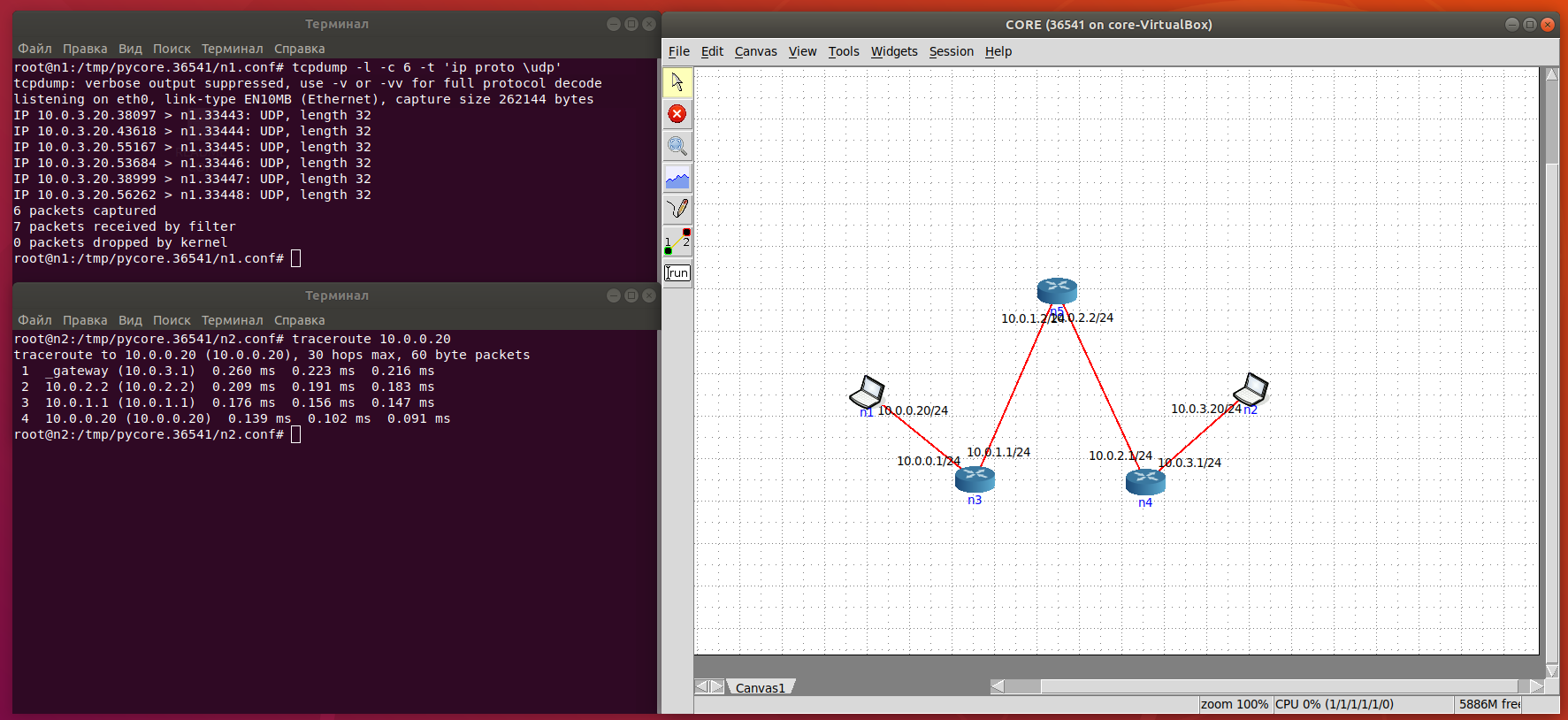


**#5.** Прочесть программой tcpdump созданный в предыдущем пункте файл.

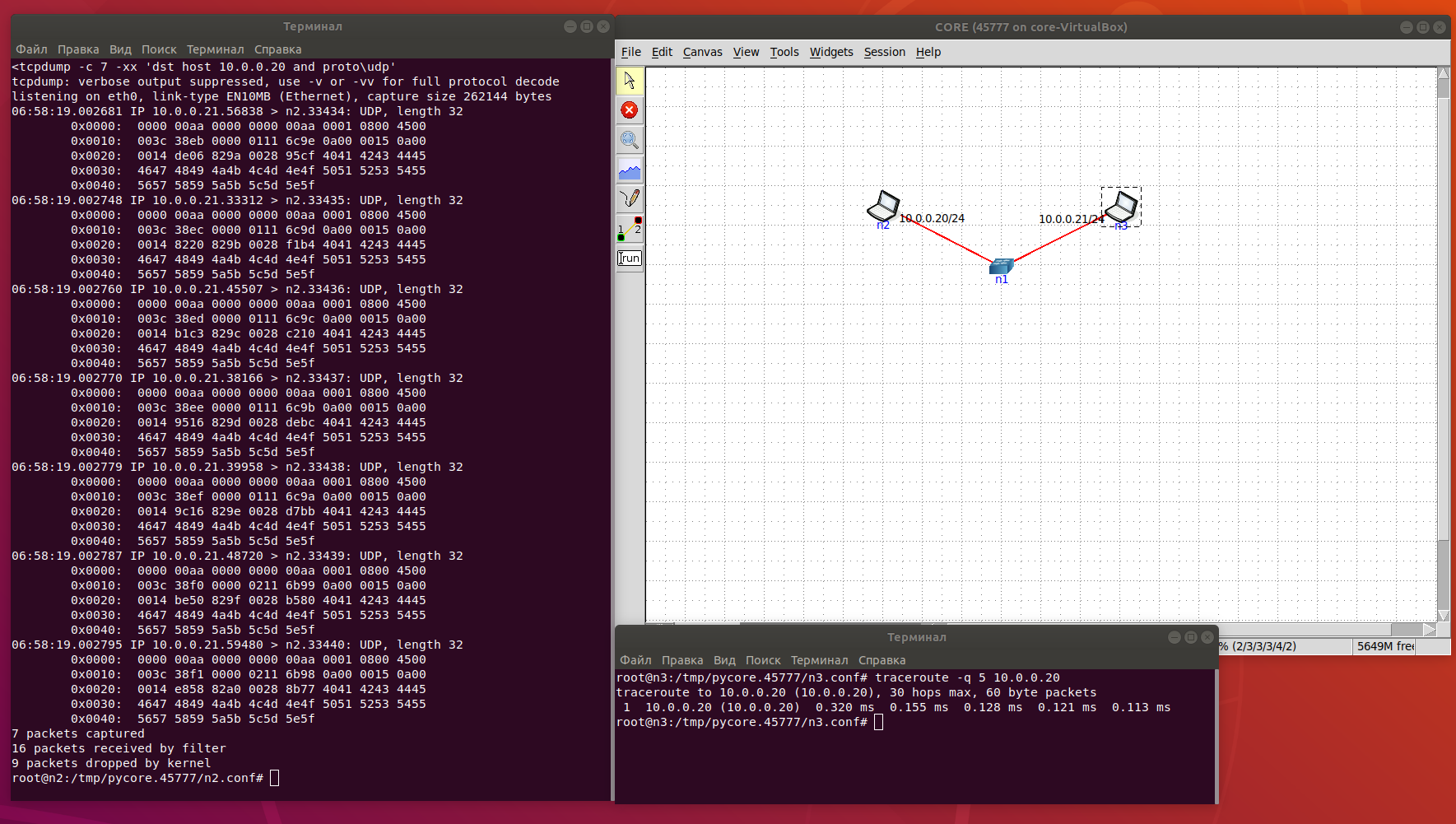


**#6.** Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP, ICMP

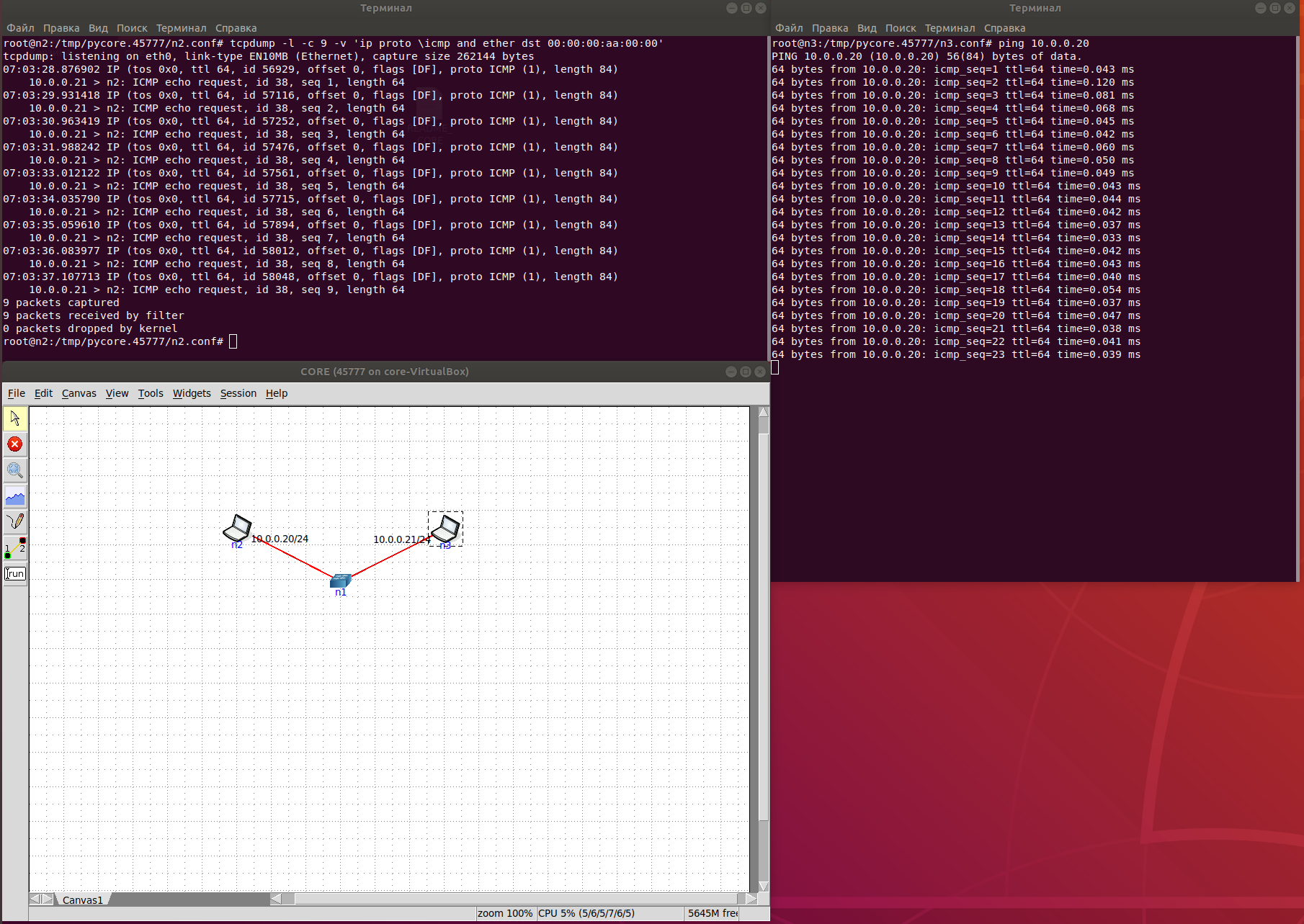
*1) Запустить tcpdump для перехвата данных протокола UDP. Не отображать метку времени в каждой строке. Количество захватываемых пакетов ограничить до 6.*

**

*2) Запустить tcpdump для перехвата пакетов протокола UDP. Включить распечатку пакета в шестнадцатеричной системе. Использовать утилиту traceroute. Количество захватываемых пакетов ограничить 7.*

**

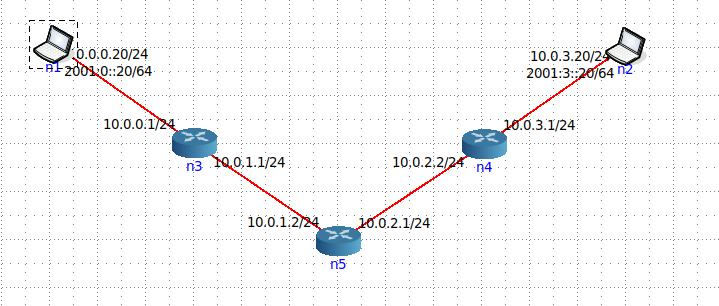
*3) Запустить tcpdump для перехвата пакетов протокола ICMP. Добавить фильтр на MAC-адрес получателя. Сделать подробный вывод информации. Для передачи использовать утилиту ping. Количество захватываемых пакетов ограничить до 9.*

**

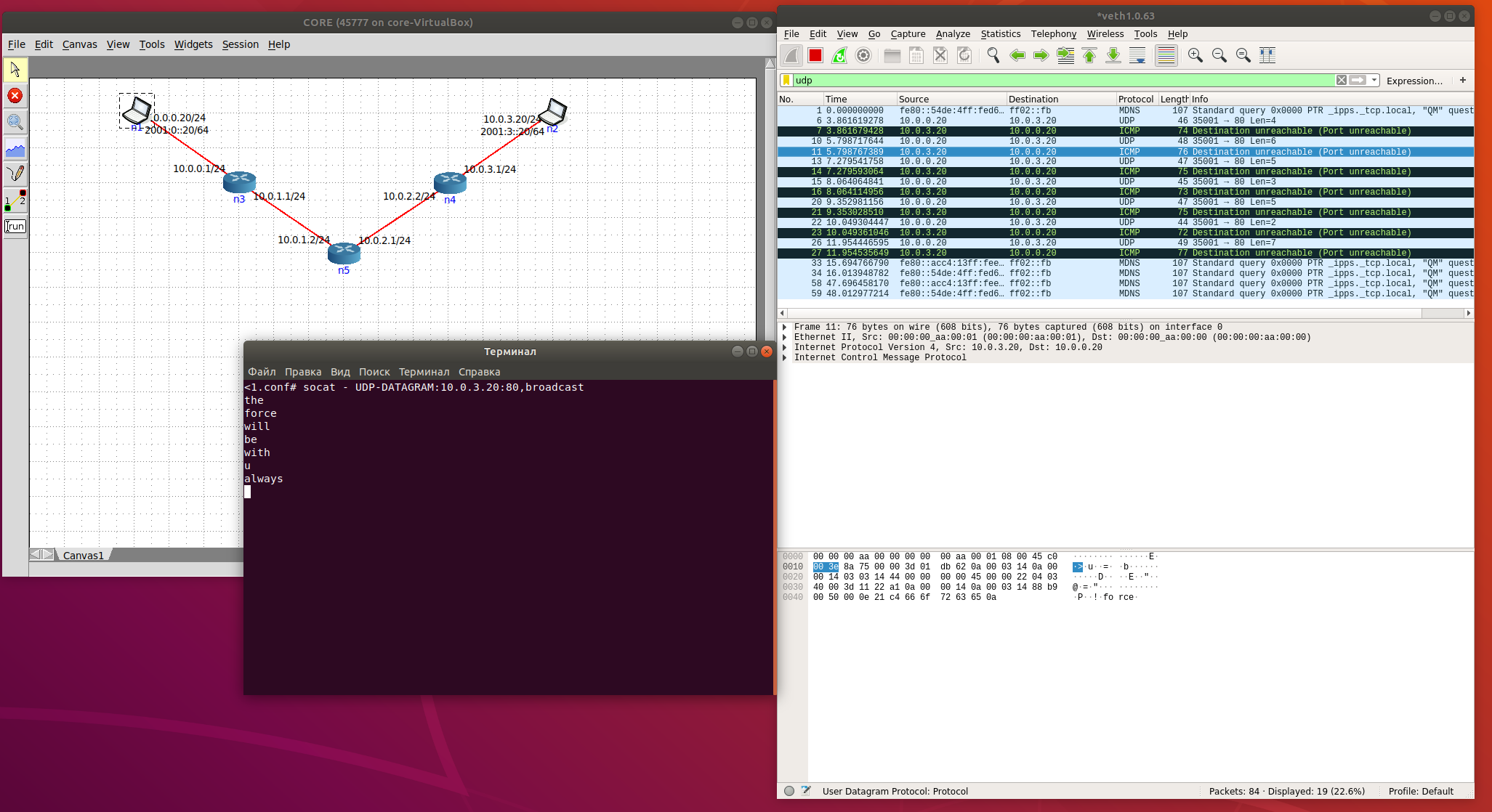
**Работа с анализатором протоколов wireshark**

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

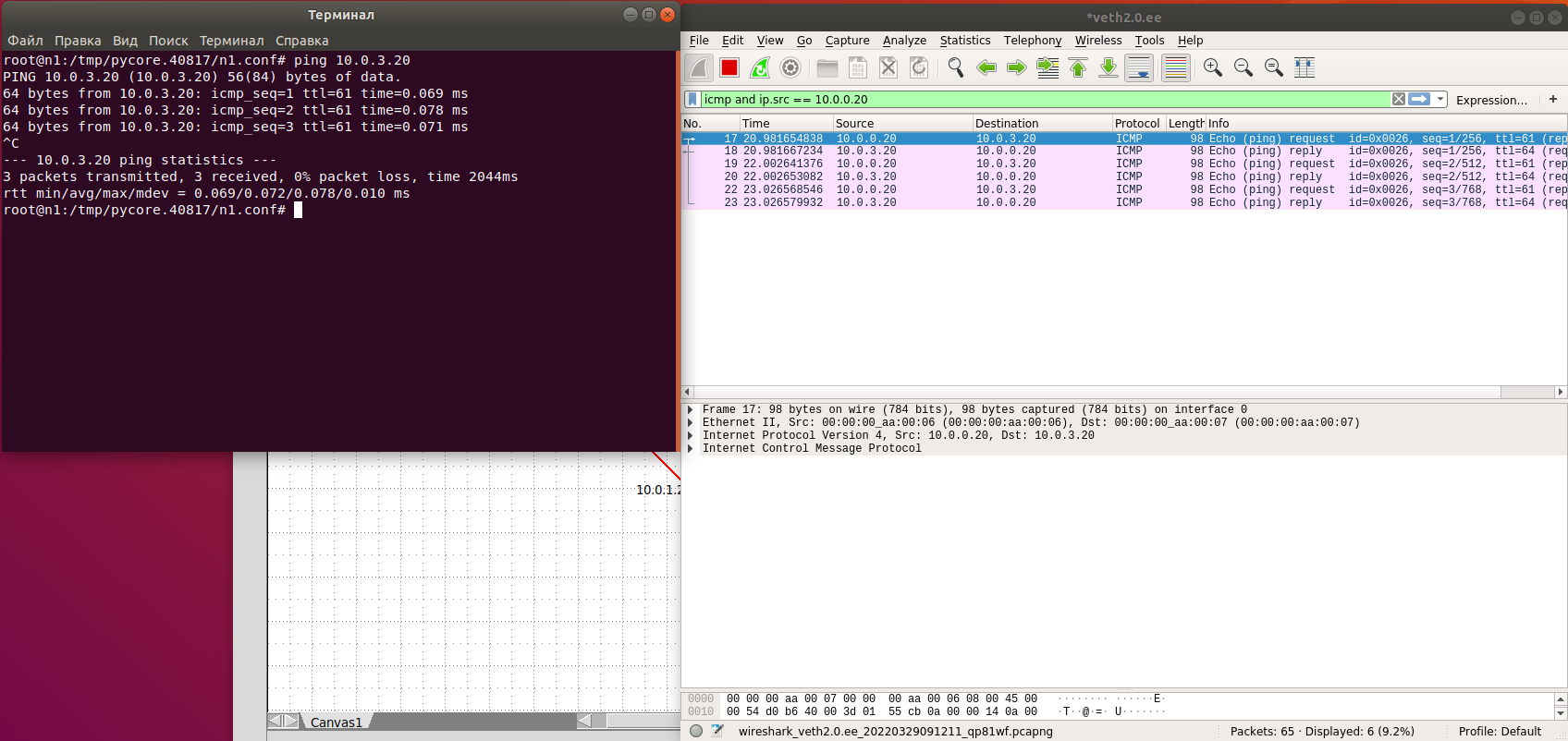
*Структура сети:*

**

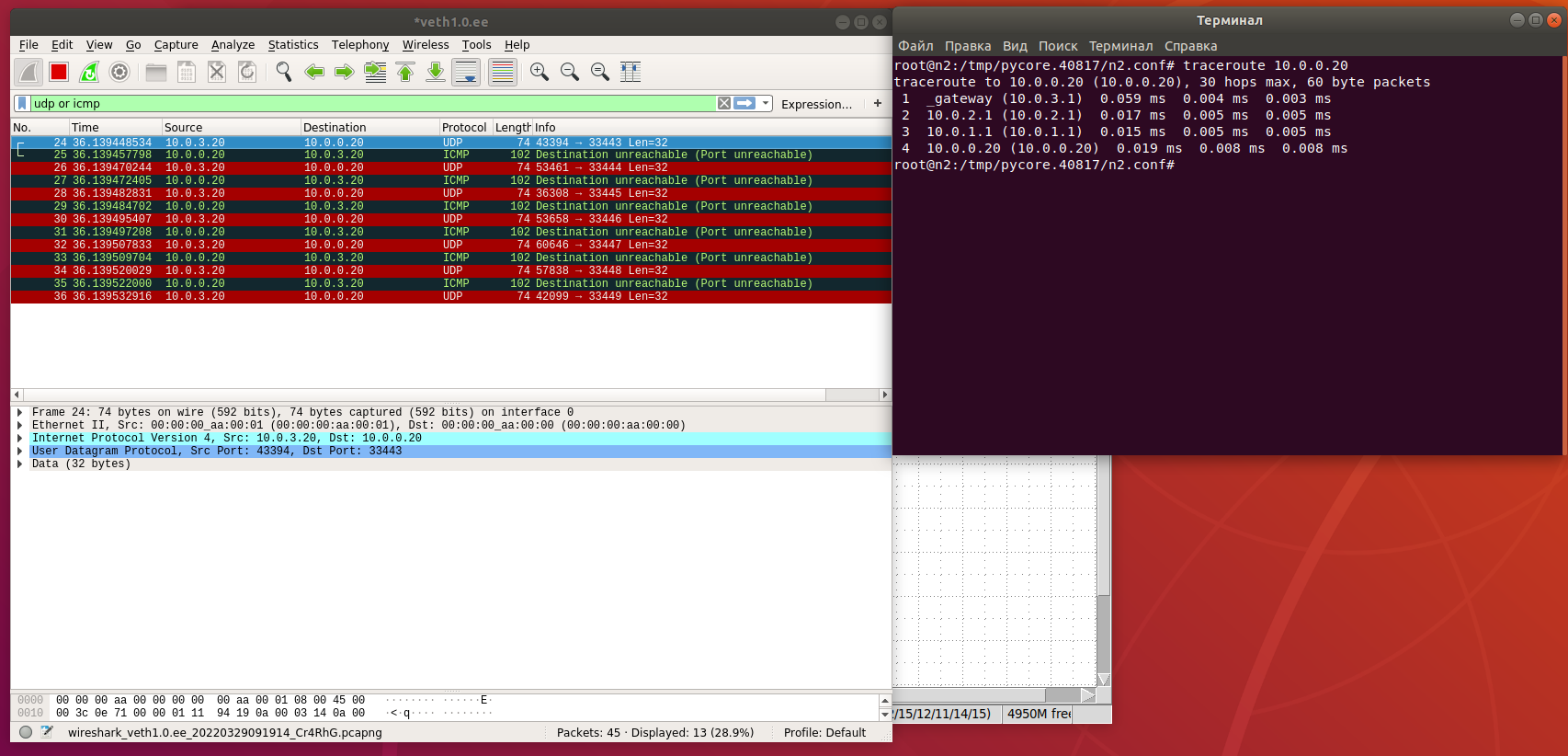
*Создаём широковещательный трафик на компьютере n2 и отправляем сообщения:*

**

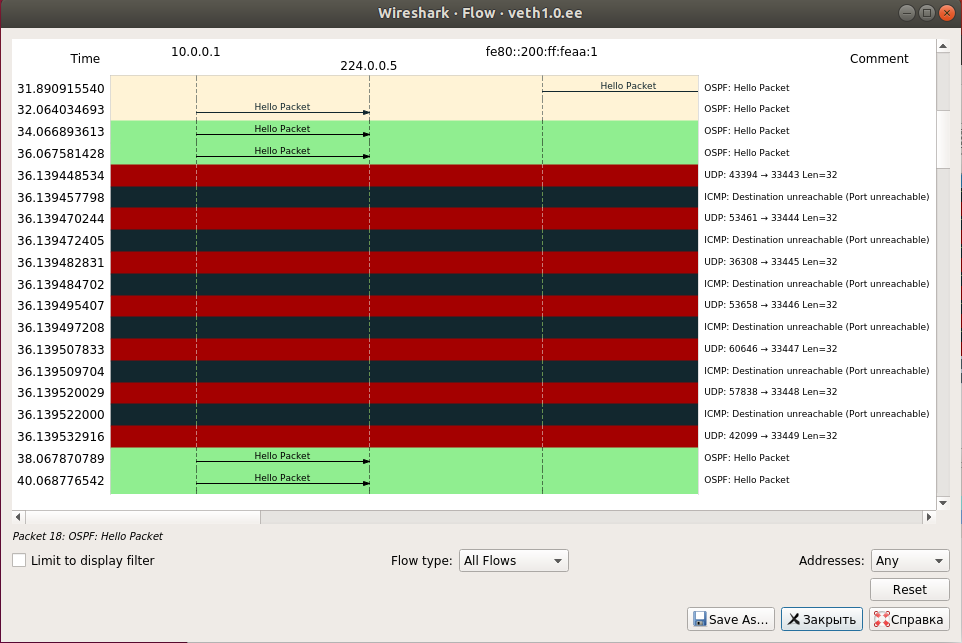
**#2.** Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов воспользоваться утилитой ping. Результат сохранить в текстовый файл.



**#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.



*Диаграмма:*

**

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

