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 №5 по предмету

«Сети и телекоммуникации»

РУКОВОДИТЕЛЬ:

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

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Храмов Е.А.

18-В-2

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

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

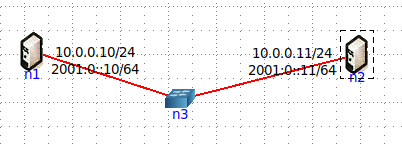
Нижний Новгород

2021 г.

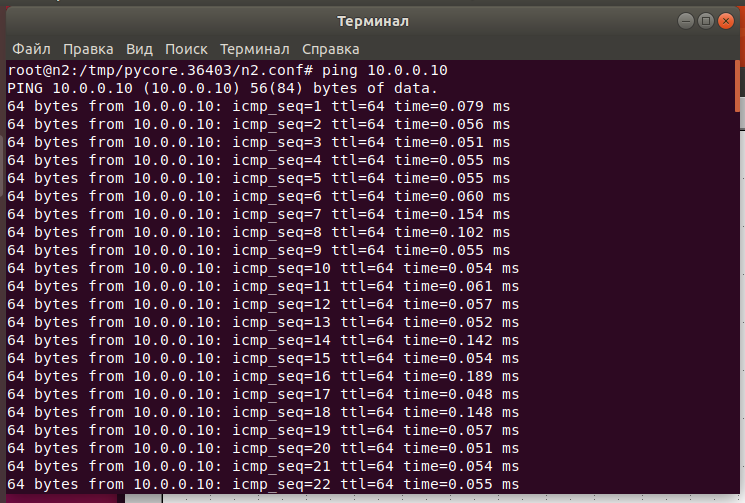
**Работа с анализатором протоколов tcpdump**

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

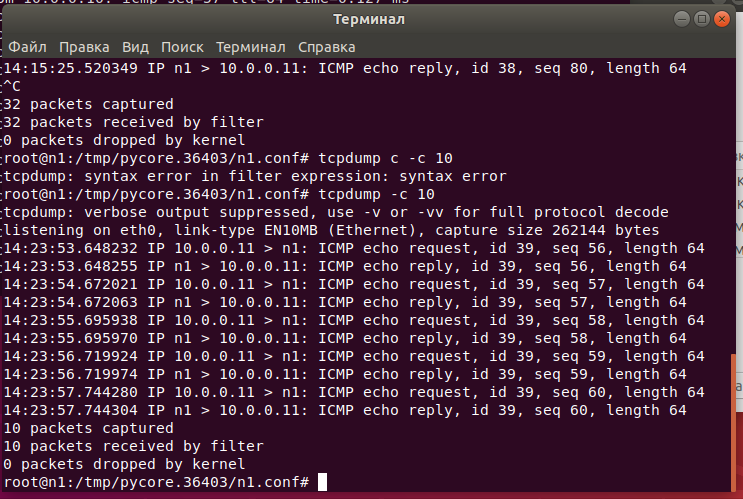
Создадим сеть из 2-х компьютеров.



Запустим генерацию ICMP пакетов с помощью ping на компьютере n2.

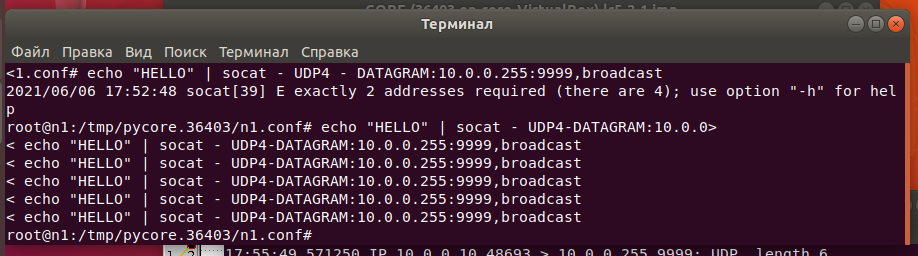


Запустим tcpdump на компьютере n1.

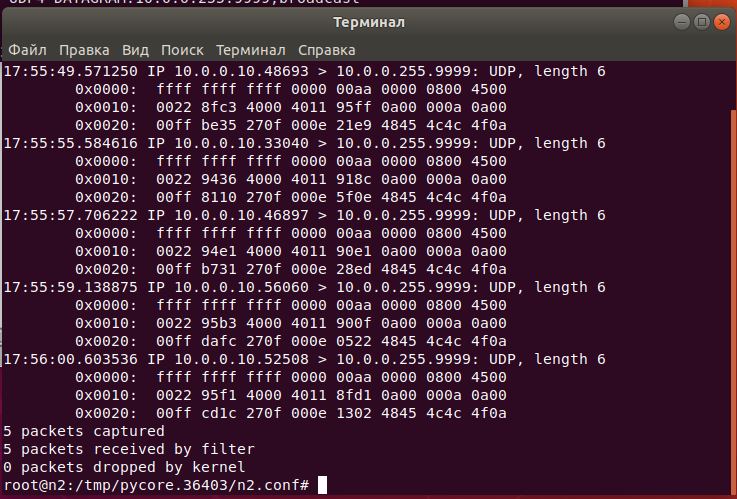


2. Запустить tcpdump в режиме перехвата широковещательного трафика (фильтр по MAC-адресу). Количество захватываемых пакетов ограничить 5. Включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).

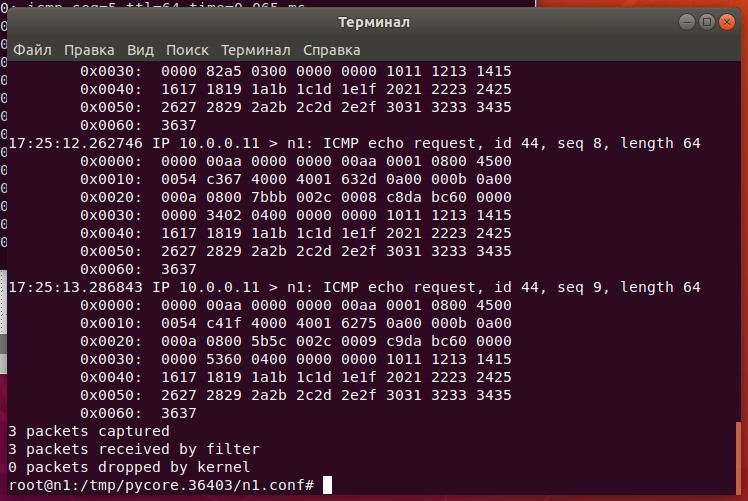
Генерируем широковещательный трафик.



Запускаем захват пакетов с помощью tcpdump.

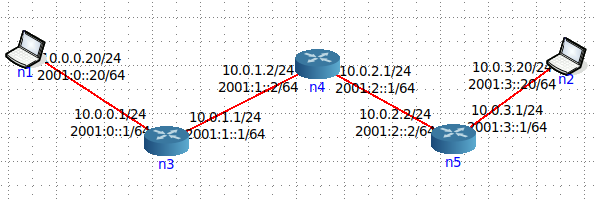


3. Запустить tcpdump так, чтобы он перехватывал только пакеты протокола ICMP, отправленные на определенный IP-адрес. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничить 3. Для генерирования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

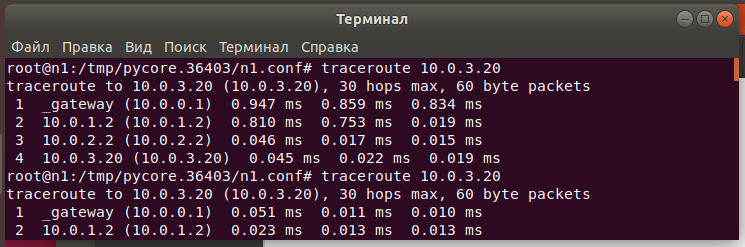


4. Запустить tcpdump в режиме сохранения данных в двоичном режиме так, чтобы он перехватывал пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включить распечатку пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество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

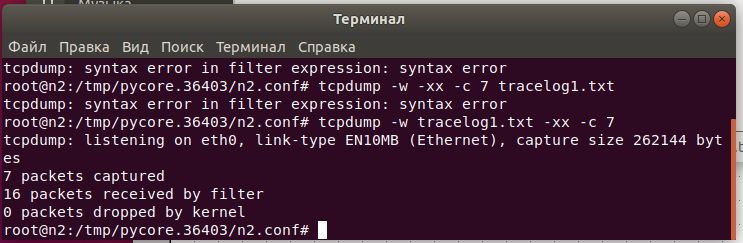
Изменим структуру сети следующим образом.



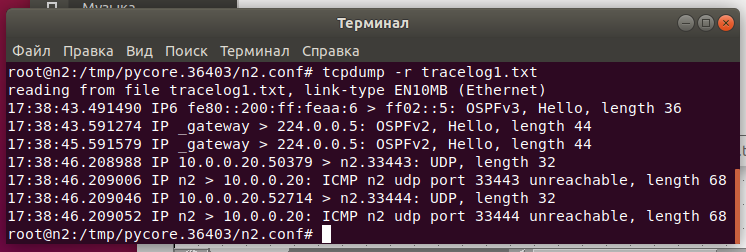
Запускаем на компьютере n1 traceroute.



Запускаем на компьютере n2 утилиту tcpdump, которая будет сохранять полученные данные в файл tracelog1.txt.



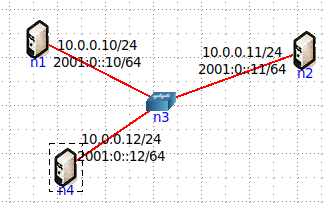
5. Прочесть программой tcpdump созданный в предыдущем пункте файл.



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

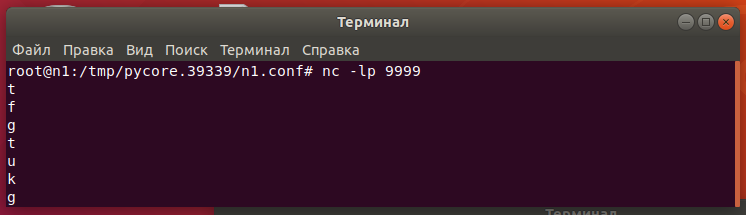
1. Захватить 4 пакета, идущих на порт 9999.

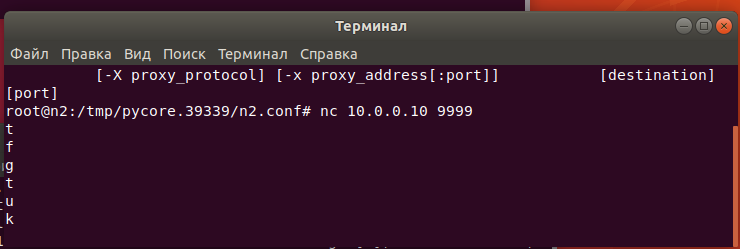
Схема сети.



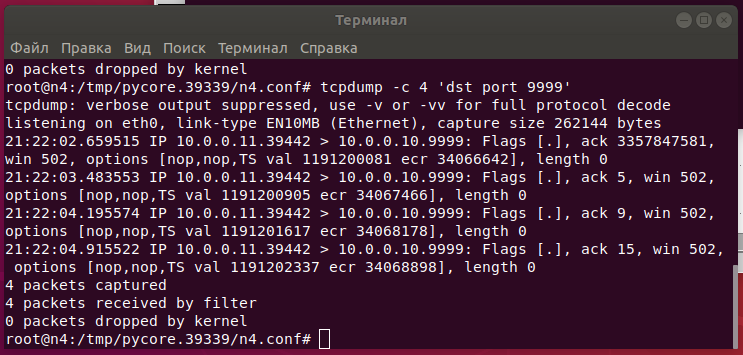
Запускаем на компьютере n1 tcp сервер и подключаемся через

n2.

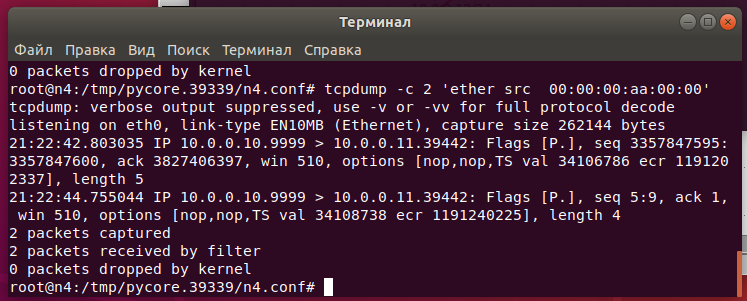




На n4 запускаем захват пакетов.

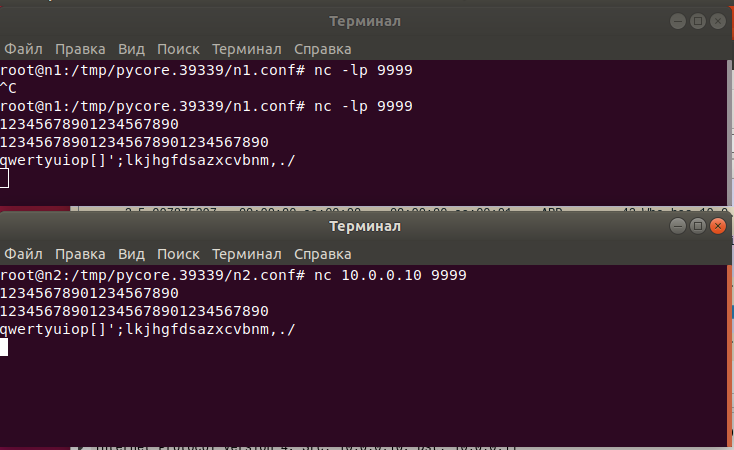


1. Захватить 2 пакета, для которых поле MAC-адреса отправителя содержит значение 00:00:00:aa:00:00.

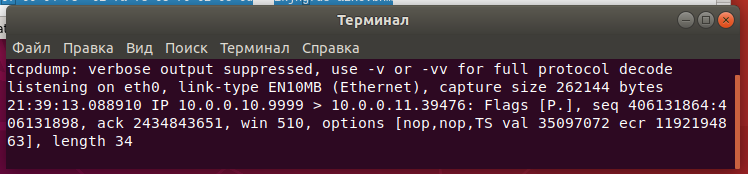


1. Захватить пакеты, размер которых больше 100байт.

Отправляем сообщения разной длительности.



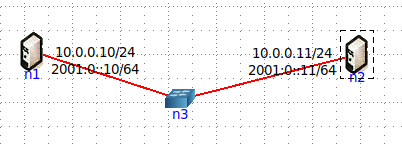
Запускаем tcpdump.

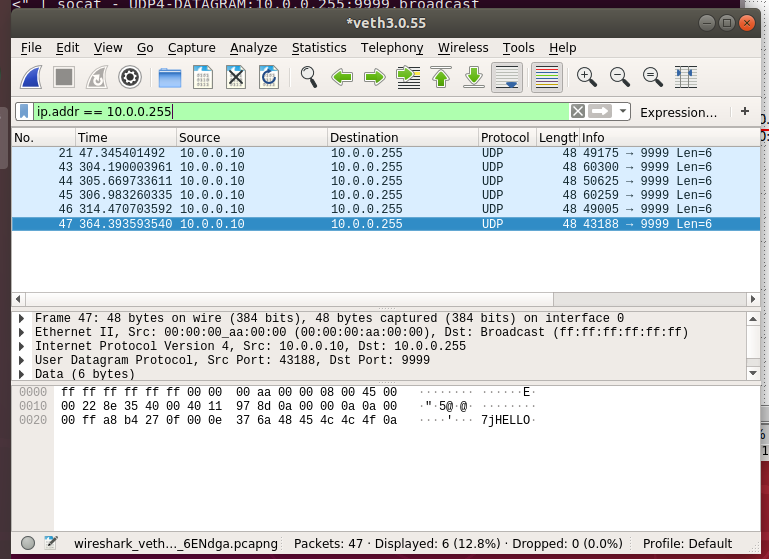


**Работа с анализатором протоколов wireshark**

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

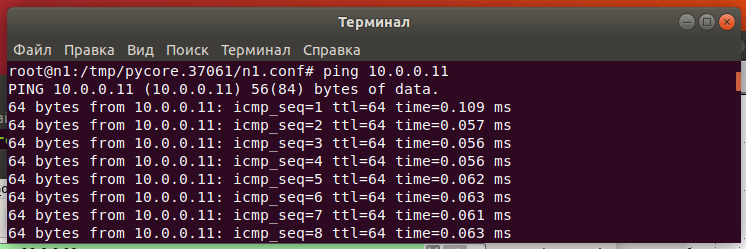
Схема сети.



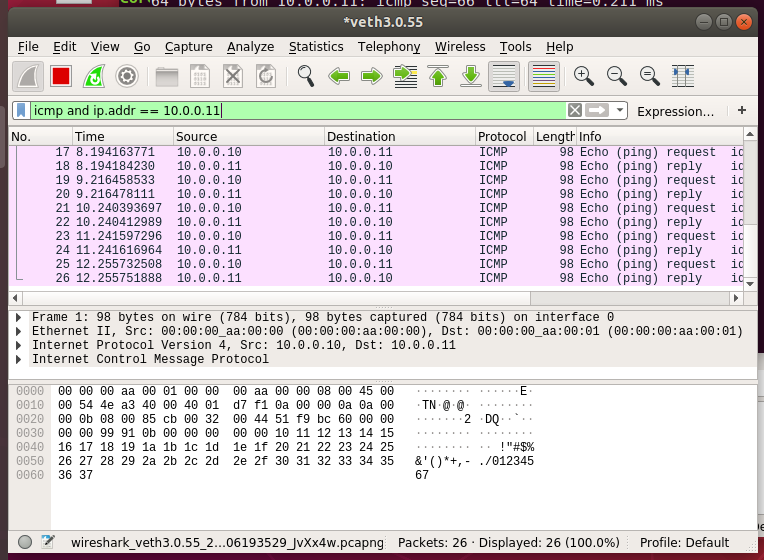


2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования пакетов возпользоваться утилитой ping. Результат сохранить в текстовый файл.

Запускаем утилиту ping на компьютере n1.

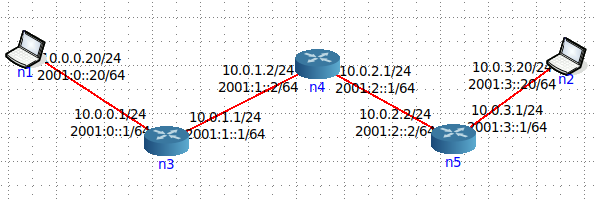


Захватываем пакеты, пришедшие на компьютер с именем n2.

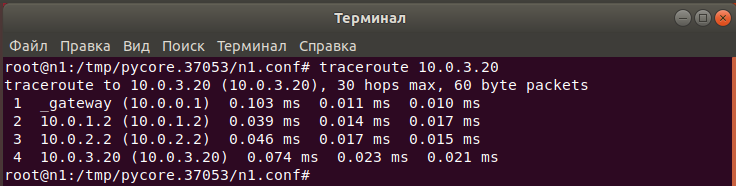


3. Перехватить пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. По результатам построить диаграмму Flow Graph. Диаграмму сохранить либо в виде текстового файла либо в виде изображения.

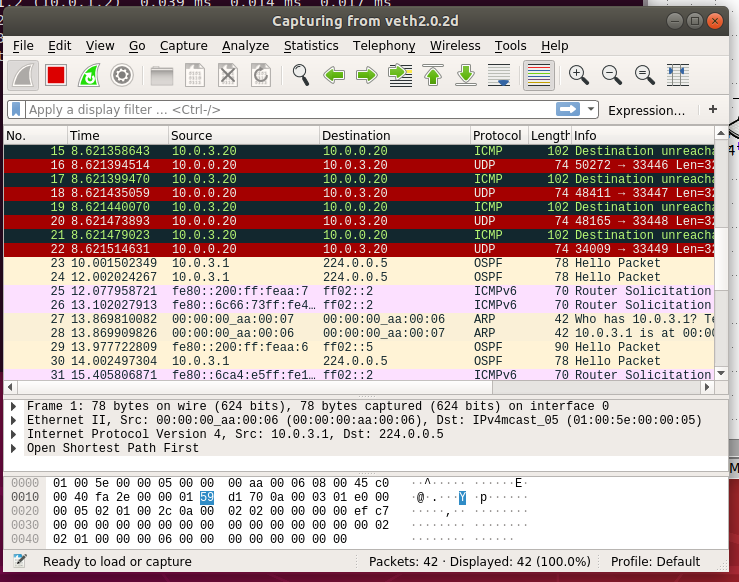
Схема сети.



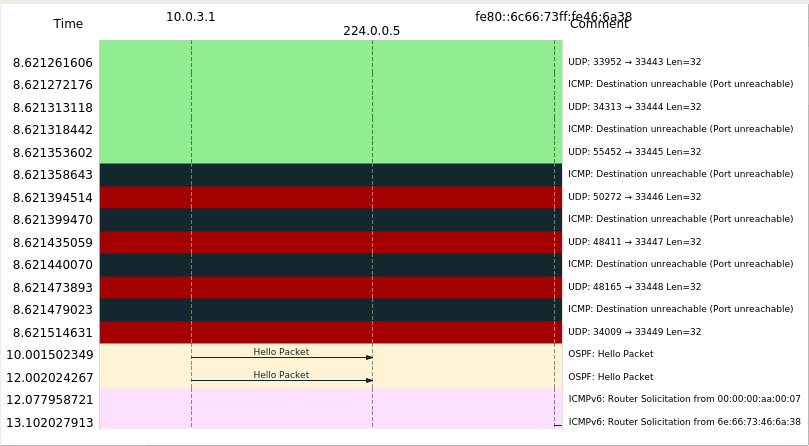
Запускаем traceroute на n1.



Запускаем Wireshark на n2.

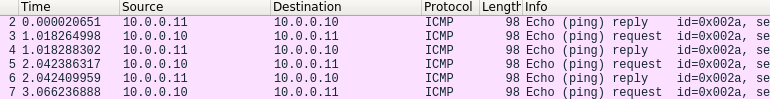


Flow Graph.



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

Wireshark.



Tcpdump.

