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.\_\_\_\_\_\_\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_Алексеева Е.А.\_\_

(подпись) (фамилия, и.,о.)

\_\_\_\_\_\_\_19-В-2\_\_\_\_\_\_\_\_\_

(шифр группы)

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

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

Нижний Новгород 2022

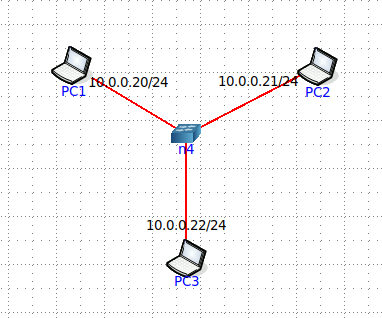
**Задание:**

**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 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

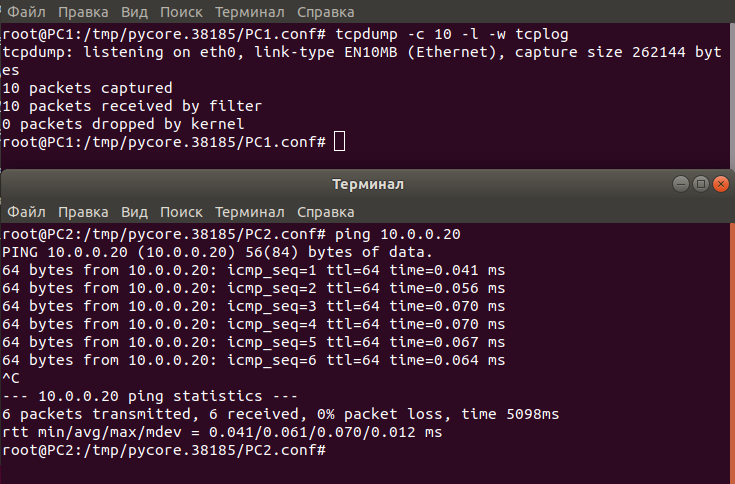
**Работа с анализатором протоколов wireshark**1. Захватить 5-7 пакетов широковещательного трафика (фильтр по IP-адресу). Результат  
сохранить в текстовый файл.  
2. Захватить 3-4 пакета ICMP, полученных от определенного узла. Для генерирования  
пакетов возпользоваться утилитой ping. Результат сохранить 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.

**Ход работы**

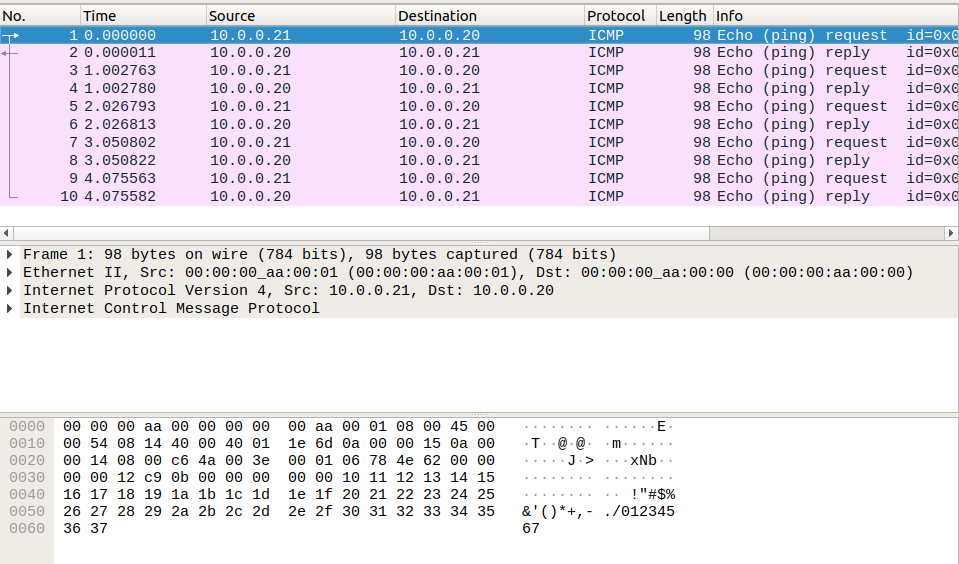
Для лабораторной работы создадим сеть из трёх компьютеров:



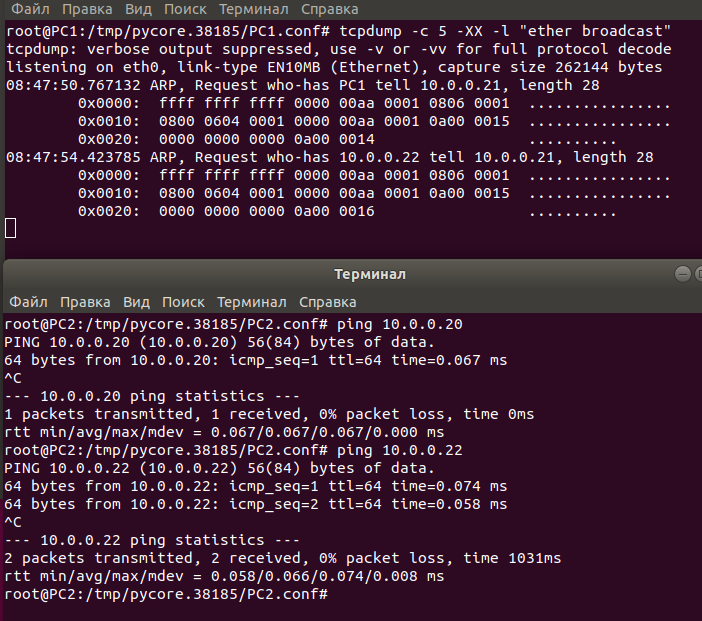
1. Режим захвата всех пакетов, проходящих по сети. Количество  
захватываемых пакетов ограничено 10. Результаты протоколированы в файл tcplog.



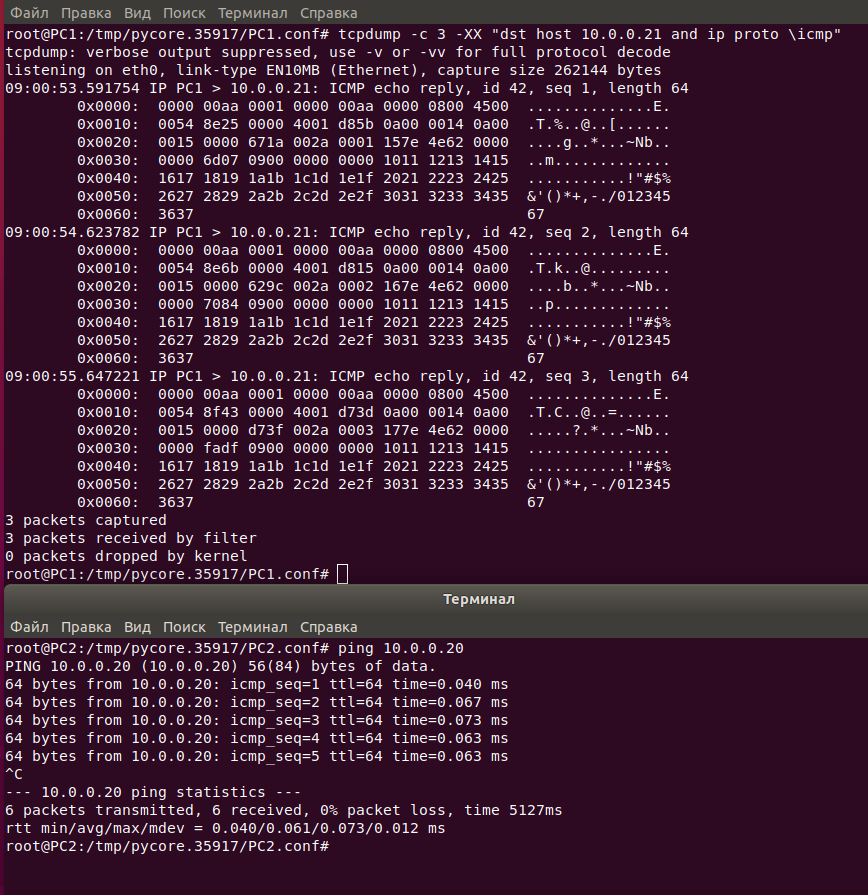
Файл можно прочитать через WireShark:



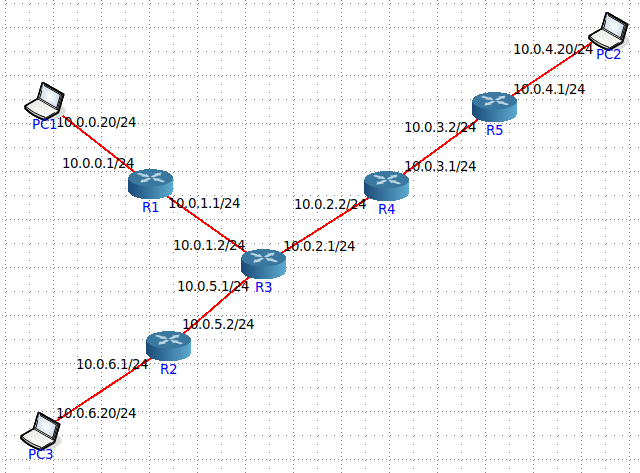
2. Режим перехвата широковещательного трафика (фильтр по MACадресу). Количество захватываемых пакетов ограничено 5. Включена распечатка пакета в шестнадцатеричной системе (включая заголовок канального уровня).



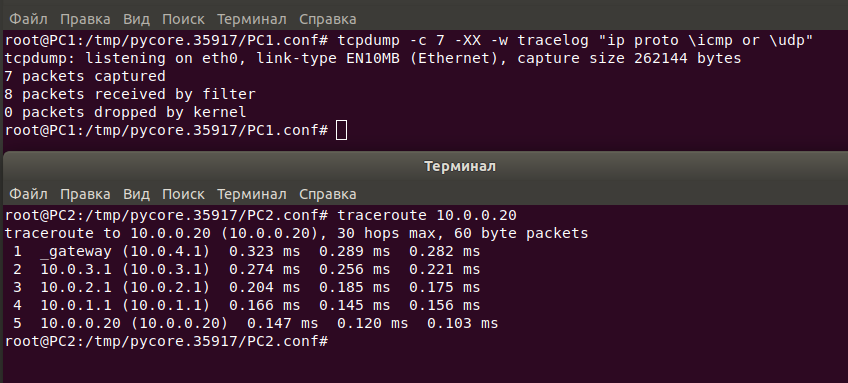
3. Режим перехвата пакетов протокола ICMP, отправленные на определенный IP-адрес. Включена распечатка пакета в шестнадцатеричной системе и ASCII формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничено 3.



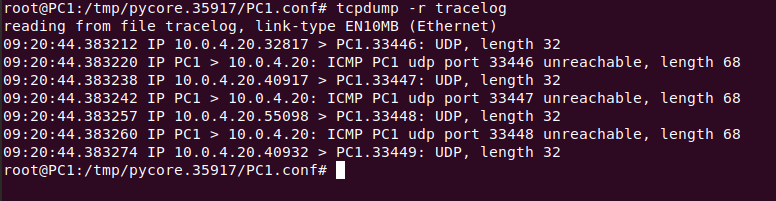
4. Для выполнения задания создадим новую схему:



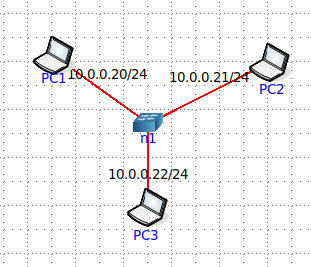
Режим сохранения данных в двоичном режиме так, чтобы перехватывались пакеты, созданные утилитой traceroute для определения маршрута к заданному в варианте узлу. Включена распечатка пакета в шестнадцатеричной системе и ASCII-формате (включая заголовок канального уровня). Количество захватываемых пакетов ограничено 7. Результат работы программы записаны в файл tracelog.



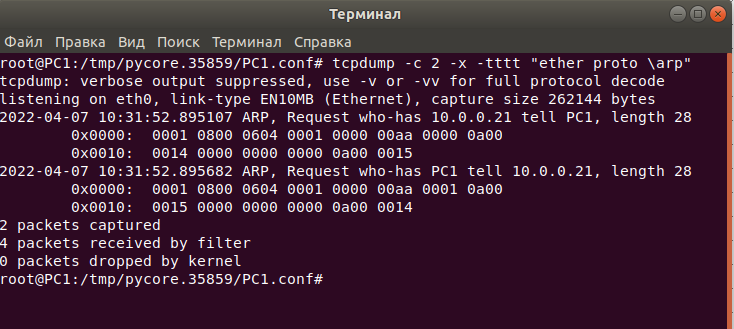
5. Прочесть программой tcpdump созданный в предыдущем пункте файл.



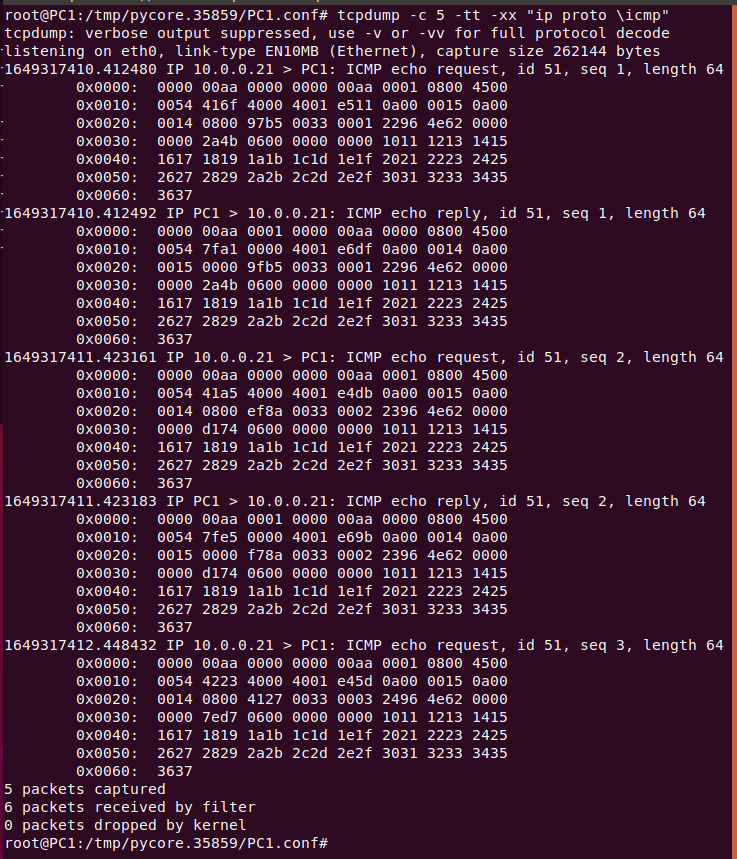
6. Придумать три задания для фильтрации пакетов на основе протоколов ARP, TCP, UDP,  
ICMP.



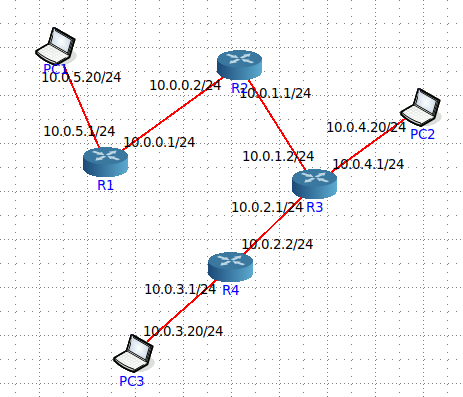
1. Перехват 2 пакетов ARP. Отобразить время вместе с датой. При этом включить распечатку пакета в шестнадцатеричной системе.



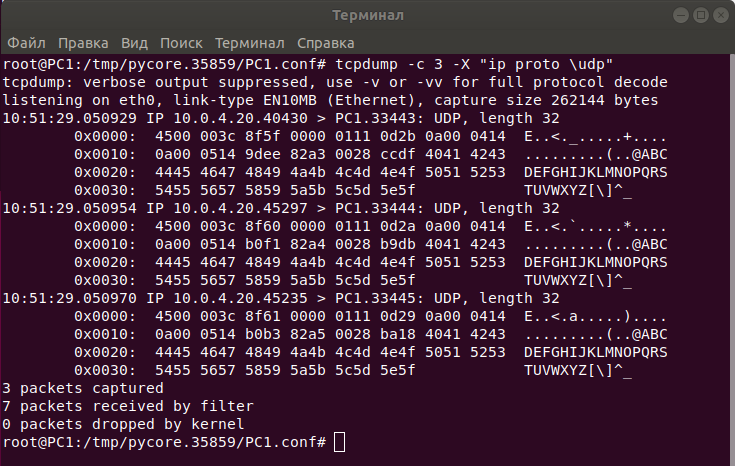
1. Перехват 5 пакетов ICMP. Отобразить неформатированную метку времени в каждой строке. При этом включить распечатку пакета в шестнадцатеричной системе (включая заголовок канального уровня).



1. Воспользуемся схемой:

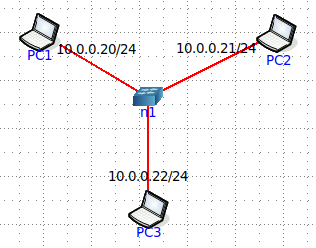
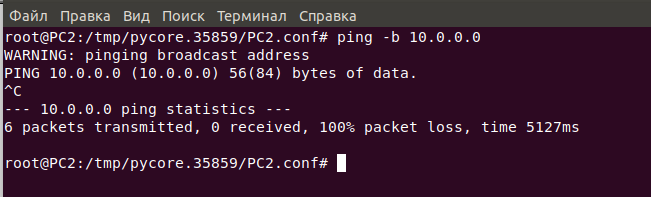


Перехват 3 пакетов UDP. При этом включить распечатку пакета в шестнадцатеричной системе и ASCII-формате.

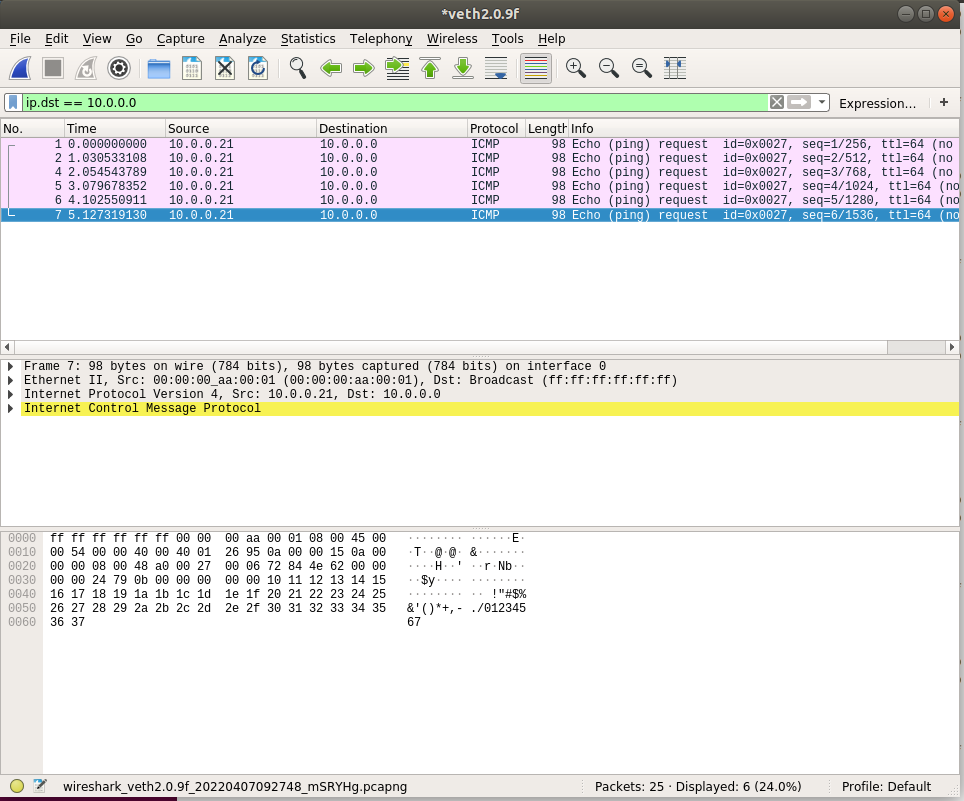


**Работа с анализатором протоколов wireshark**

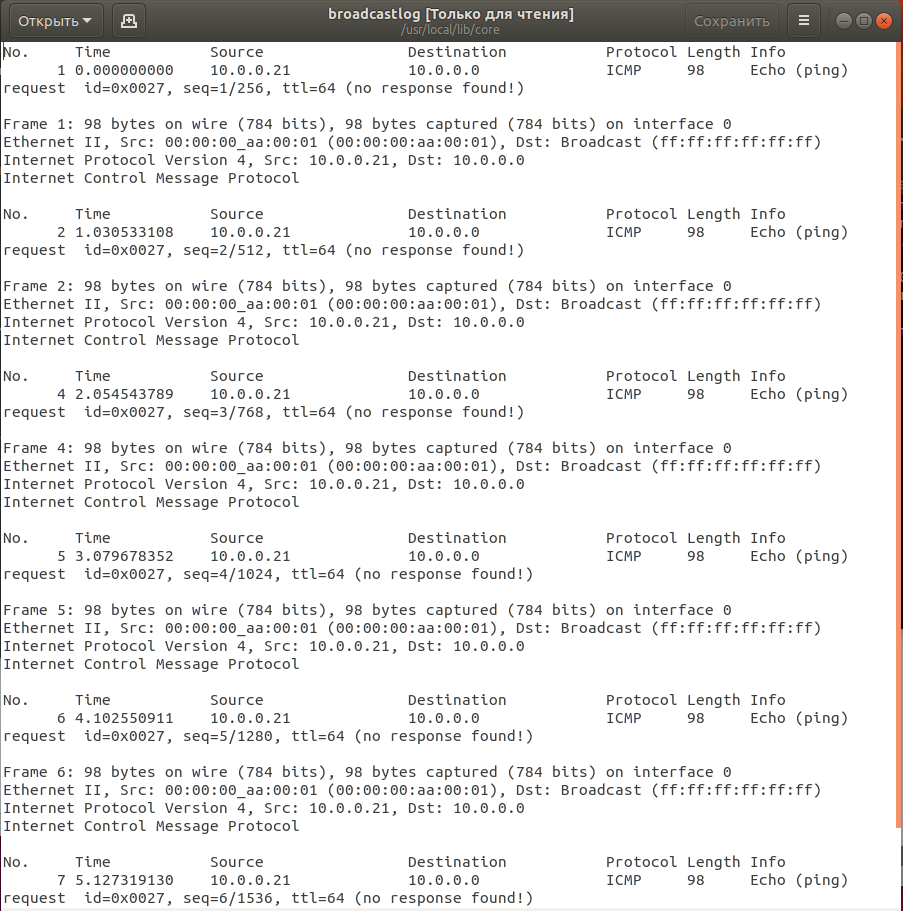
Создадим сеть, состоящую из трёх компьютеров:

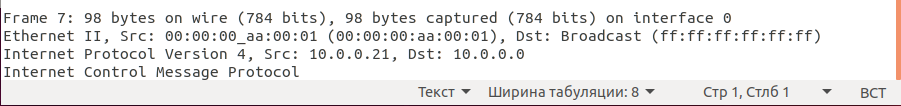
1. Захват 5-7 пакетов широковещательного трафика (фильтр по IP-адресу).   
Используем ping -b 10.0.0.0 на компьютере PC2:

Отфильтруем пакеты в WireShark на PC1:



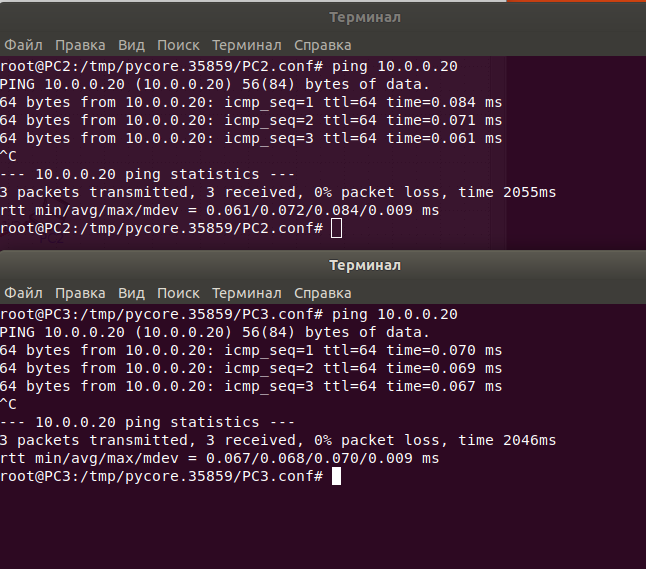
Результат сохранён в текстовый файл broadcastlog.txt.



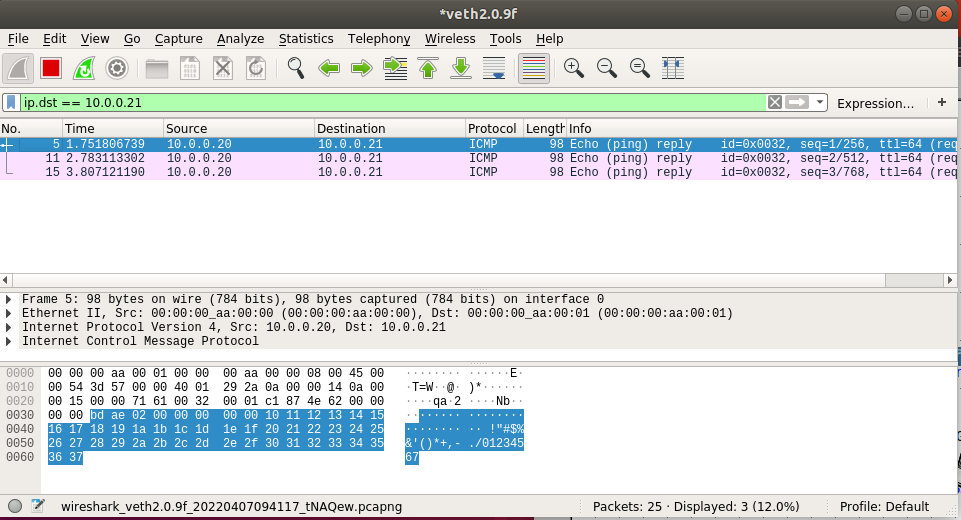


2. Захват 3-4 пакета ICMP, полученных от определенного узла. Для генерирования  
пакетов воcпользоваться утилитой ping.

Используем ping 10.0.0.20 на PC2 и PC3



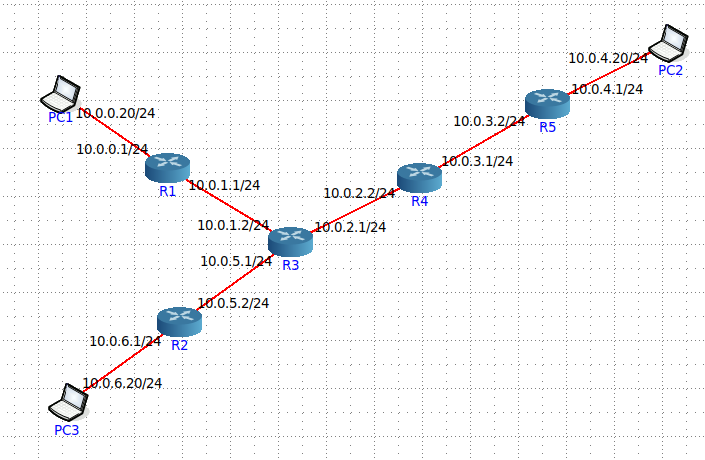
В WireShark на PC1 отфильтруем пакеты, полученные от PC2.



Результат сохранён в текстовый файл pclog.

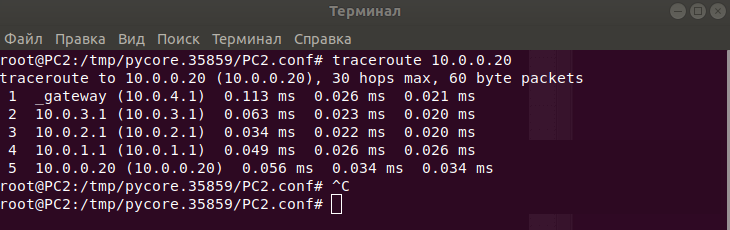


3. Создадим следующую схему:

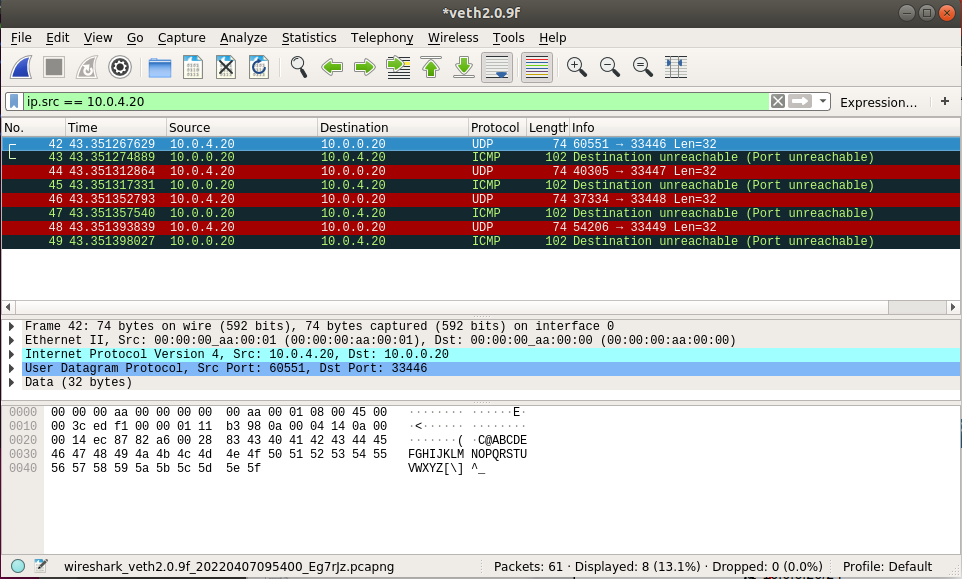


Перехват пакетов, созданных утилитой traceroute для определения маршрута к  
заданному в варианте узлу.

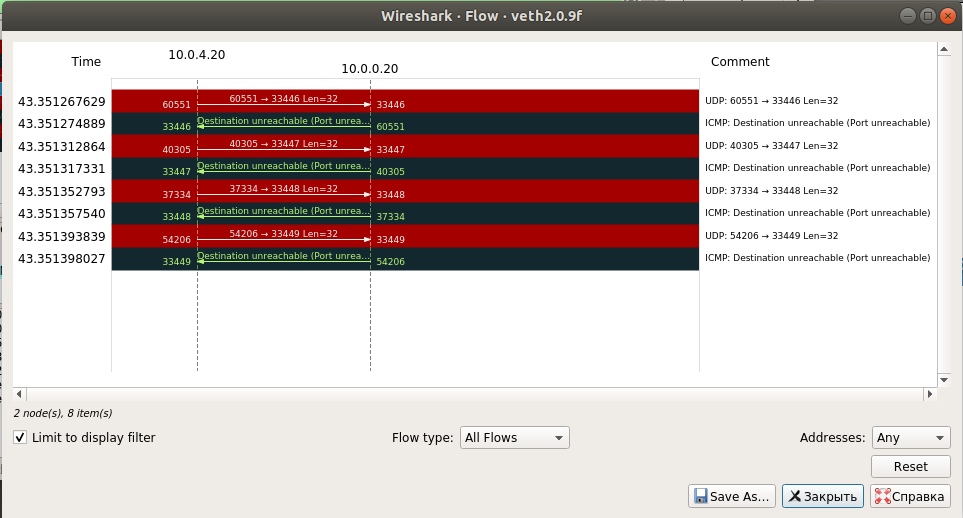
Используем traceroute 10.0.0.20 на PC2:



Откроем WireShark на PC1 и отфильтруем пакеты:



По результатам построим диаграмму Flow Graph:



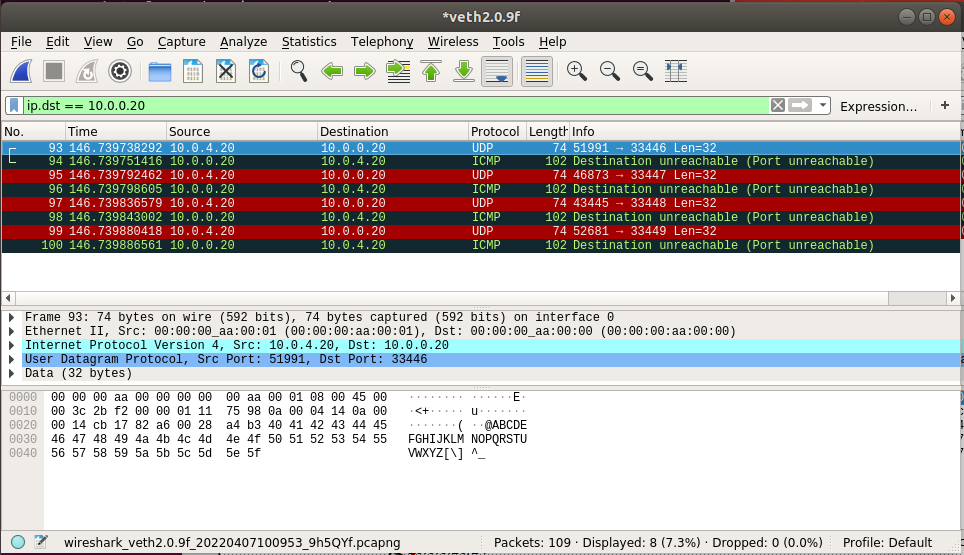
Диаграмму сохраним виде изображения traceflow.jpeg.



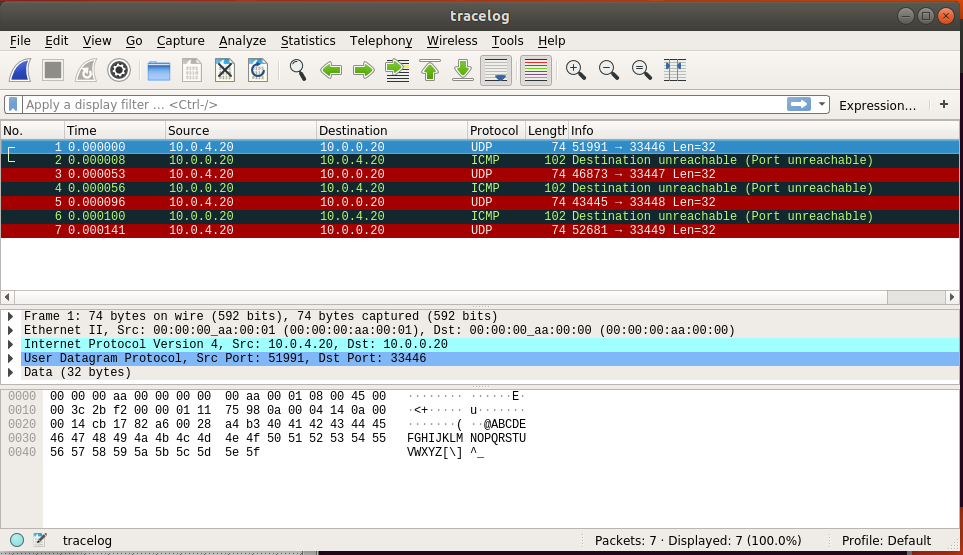
4. Прочесть файл, созданный программой tcpdump. Сравнить с тем, что было получено  
утилитой wireshark.

Воспользуемся файлами из заданий, связанных с утилитой traceroute.

WireShark:



Файл tracelog, созданный программой tcpdump:



Единственное отличие: в файле tracelog, созданном программой tcpdump на один пакет меньше, т.к. использовался параметр –c 7, который ограничил перехват пакетов.