МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ

УНИВЕРСИТЕТ им. Р.Е.АЛЕКСЕЕВА

Институт радиоэлектроники и информационных технологий

ОТЧЕТ

по лабораторной работе №3

по дисциплине

«Сети и телекоммуникации»

6 вариант

РУКОВОДИТЕЛЬ: Гай В.Е.

СТУДЕНТ : Варнашина А.А.

Группа 19-АС

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

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

Нижний Новгород 2021

**Задание:**

Для экспериментов использовать схему из первой лабораторной работы. Все ip-адреса (или маски) необходимо поменять так, чтобы адрес сети у всех компьютеров был один. Все действия должны быть выполнены в симуляторе сетей CORE.

**Часть 1. Формирование запроса и получение ответа**

1. Начать захват пакетов при помощи WireShark.

2. Сформировать кадр ARP-запроса с помощью утилиты PackETH и отправить его в сеть (компьютеры выбрать самостоятельно).

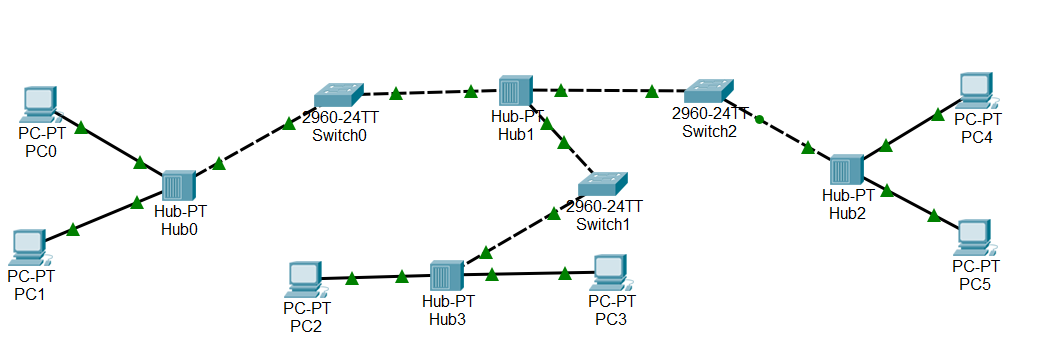
3. Убедиться, что был получен кадр ARP-ответа, соответствующий посланному запросу. Захваченные пакеты сохранить для отчета. Вывести arp таблицу (команда «arp»).

4. Прекратить захват пакетов.

**Часть 2. ARP-спуфинг**

1. Выделить на схеме и обозначить три компьютера: A, B, Сервер.

2. Подготовить кадр ARP-ответа, направляемый Сервером хосту А с помощью программы PackETH. Кадр должен быть составлен так, чтобы MAC-адресу Сервера соответствовал IP-адрес хоста В. Вывести arp таблицу на хосте А. Отправить сформированный пакет от Сервера хосту А.



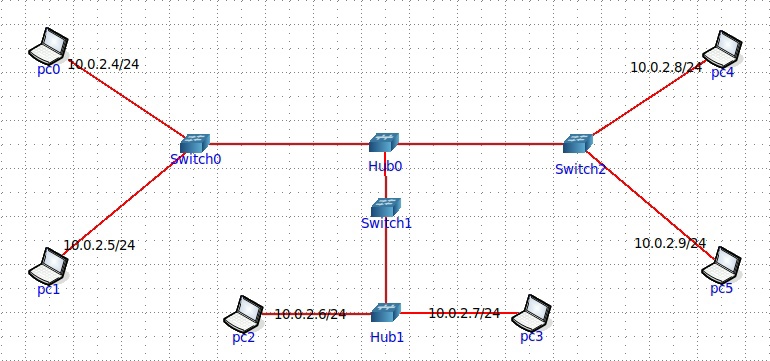
Компьютер PC2 имеет IP-адрес 10.0.1.5.

Компьютер PC1 имеет IP-адрес 10.0.2.5.

Компьютер PC4 имеет IP-адрес 10.0.64.1.

Компьютер PC3 имеет IP-адрес 192.168.1.1.

Задать IP-адреса PC0, PC5, создавая отличные от остальных ПК подсети

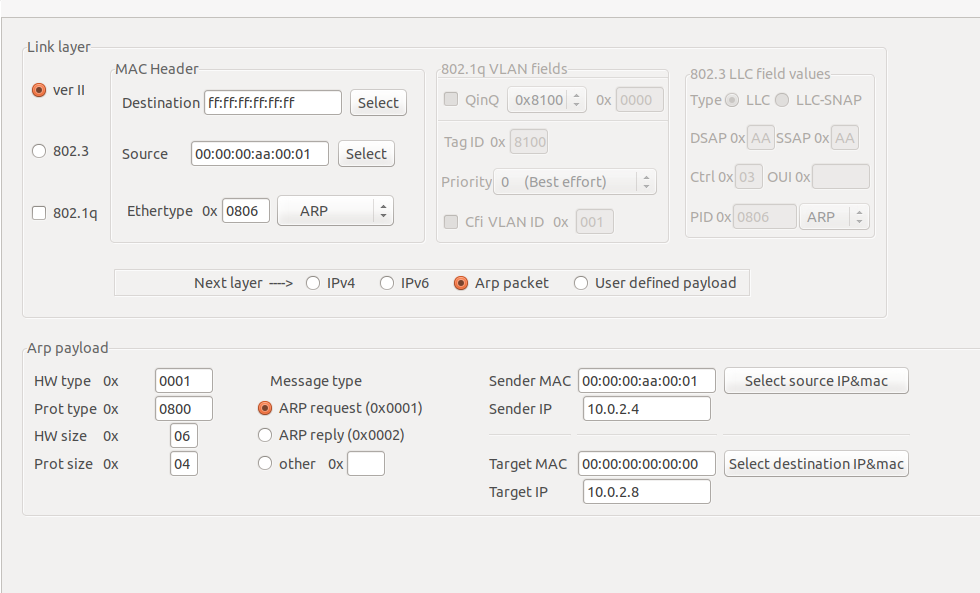


Часть 1

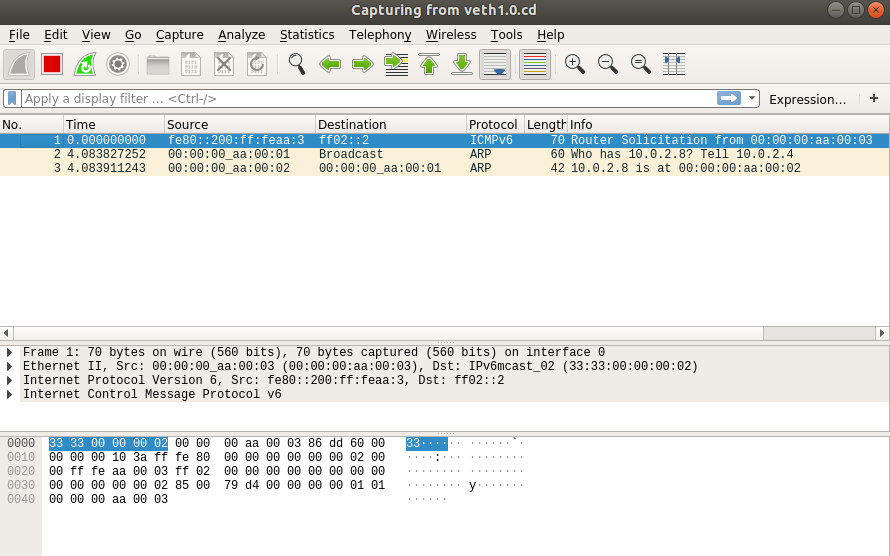
Сформировать кадр ARP-запроса с помощью утилиты PackETH и отправить его в сеть (компьютеры выбрать самостоятельно).

Для запуска packEth в консоли выполняем команду «xhost +», в консоли узла «DISPLAY=:0 packeth» или «DISPLAY=:0 packeth --sync». Разрешили подключаться к серверу с любых хостов командой xhost+

C:\Users\nastya\YandexDisk\Скриншоты\2021-12-02_21-02-56.png

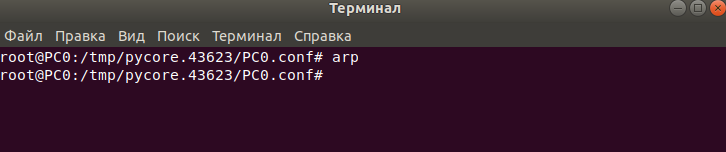


Ну и затем убедимся, что кадр ARP-ответа был получен после посланного запроса.

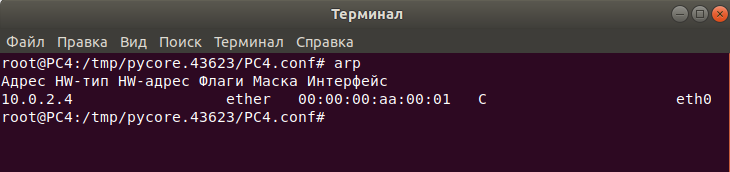


Вывести arp таблицу (команда «arp»)

PC0

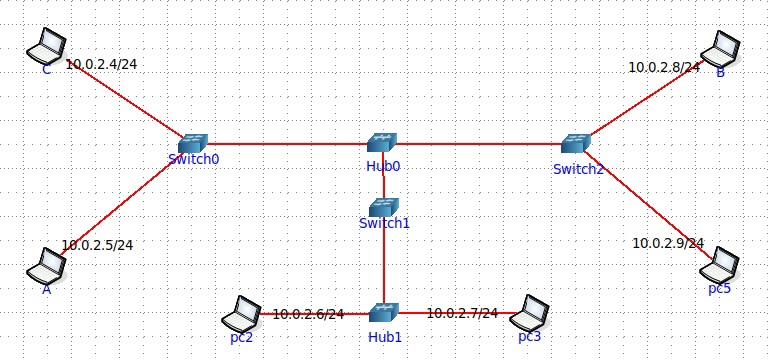


PC4

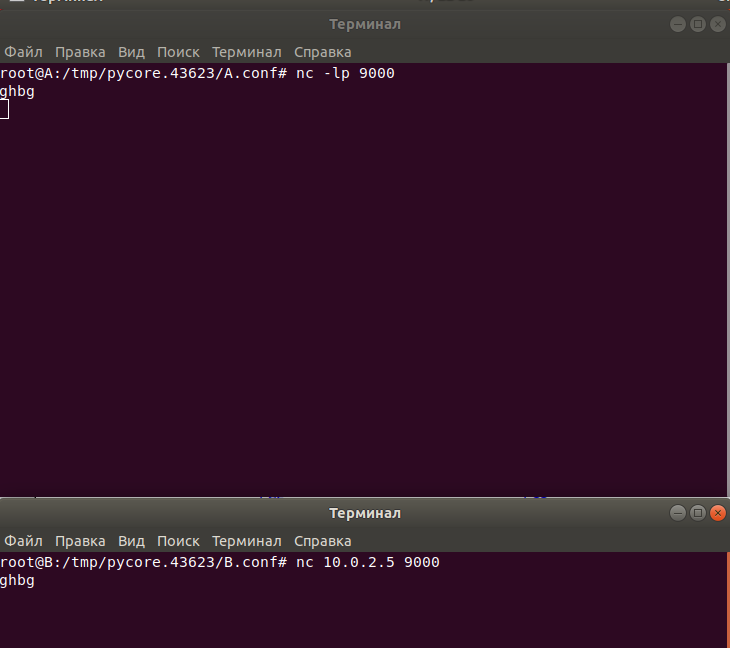


Часть 2

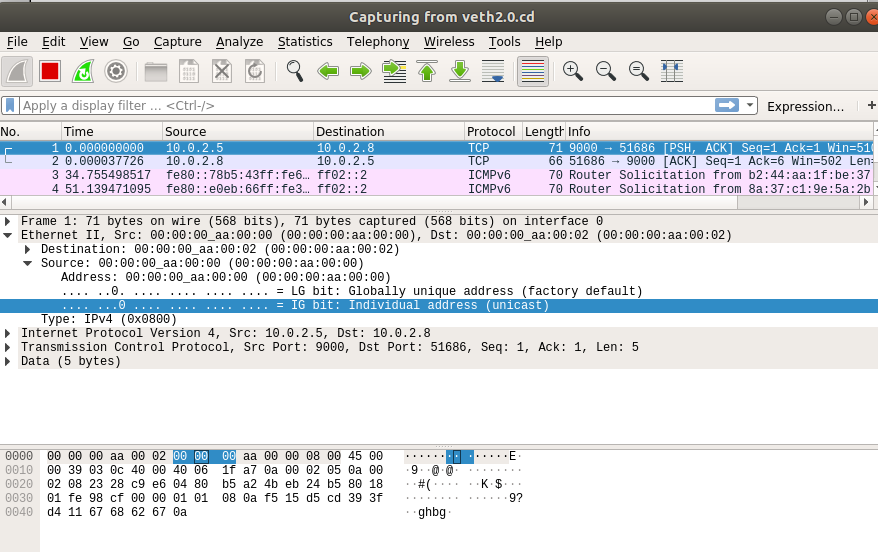
Выделить на схеме и обозначить три компьютера: A, B, Сервер.



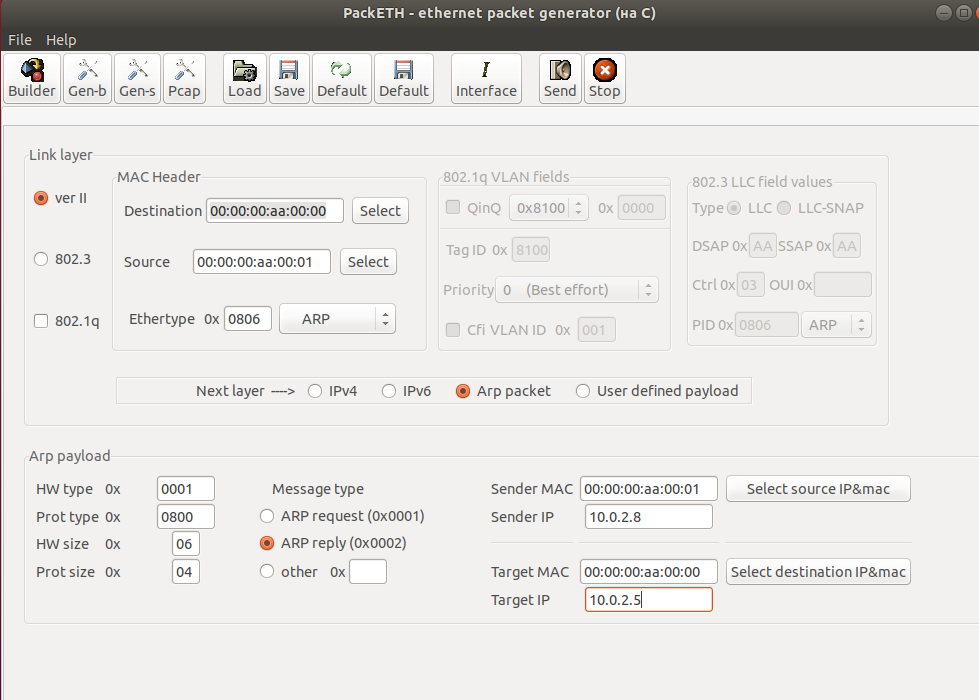
Для начала установим связь между А и В, используя команду утилиту netcat так, чтобы компьютер B начинал прослушивать порт 9000, а компьютер А передавал сообщения по ipадресу и порту 9000.



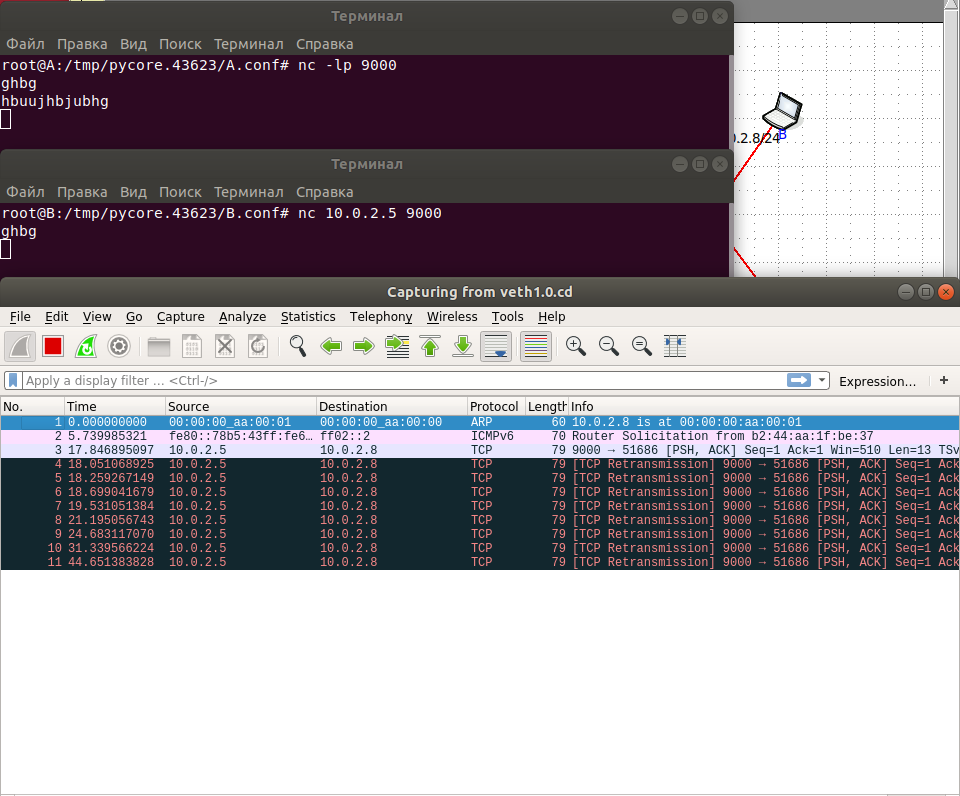
Если посмотреть wireshark PC(A) и найти TCP – пакет, который закрывает соединение, то в нём можно обнаружить текст сообщений, которые мы отсылали:



Следующим действием нам нужно произвести атаку на это соединение и перехватить пакеты. Т.е Сервер представится PC(A), как PC(B) и будет пропускать через себя пакеты, которые между ними шли. Для этого мы вновь используем программу PackETH, которая запускается на PC(C) – Сервере.



И если теперь наш PC(A) захочет отправить какое-нибудь сообщение PC(B), то оно до него не дойдет:



Чуть позже потерянные сообщения всё-таки дойдут до истинного адресата, потому что происходит перезапрос MAC-адреса хоста В и в последствии потерянные пакеты будут доставлены, но с задержкой.

