Минобрнауки России

Федеральное государственное бюджетное образовательное

учреждение высшего образования

**НИЖЕГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ**

**ИМ. Р.Е. АЛЕКСЕЕВА**

ИНСТИТУТ РАДИОЭЛЕКТРОНИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

|  |  |  |
| --- | --- | --- |
|  |  |  |

Курс “Сети и телекоммуникации”

**Отчет по лабораторной работе №3**

Выполнил: студент группы 18 В-1

Петров М.А.

Проверил: Гай В.Е.

Нижний Новгород 2020

**1. Задание на работу:**

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.

Для запуска packEth в консоли выполните команду «xhost +», в консоли узла «DISPLAY=:0 packeth» или «DISPLAY=:0 packeth --sync».

netcat (англ. net сеть + cat) — утилита Unix, позволяющая устанавливать соединения TCP и UDP, принимать оттуда данные и передавать их.

Организация чата между узлами с помощью netcat:

1. На первом узле (192.168.1.100):

$ nc -lp 9000

2. На втором узле:

$ nc 192.168.1.100 9000

3. Начать захват пакетов при помощи WireShark на Сервере.

4. Попытаться установить соединение между хостом А и хостом В с помощью программы netcat (А отправляет сообщения В). Убедиться, что запросы от хоста A, направленные хосту В поступают на Сервер.

5. Прекратить захват пакетов.

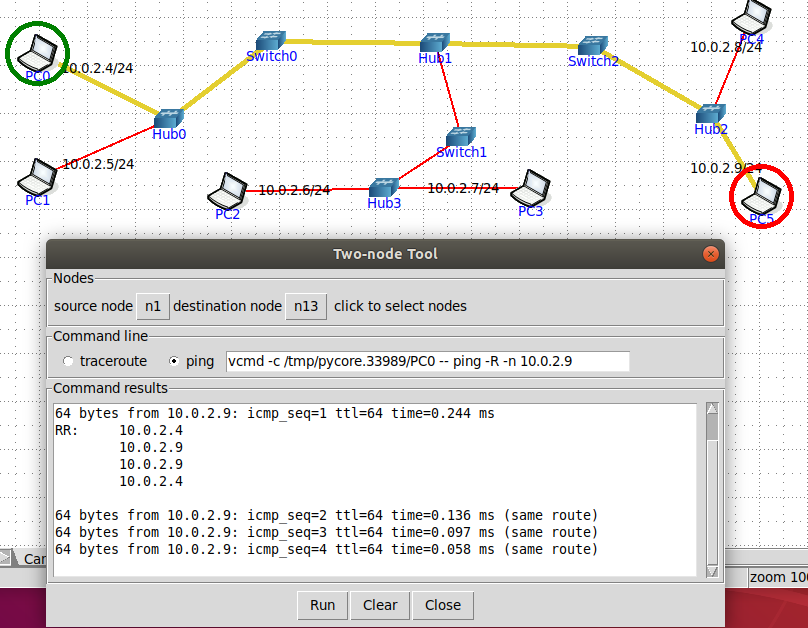
6. Сохранить для отчета отправленный кадр ARP-ответа и несколько перехваченных пакетов, переданных на Сервер, arp таблицу хоста А.

**2. Структура сети:**

Перед началом работы мне было необходимо переделать свою схему, точнее поменять ip-адреса так, чтобы адрес сети у всех компьютеров был один.

**3. Доказательства работы сети:**

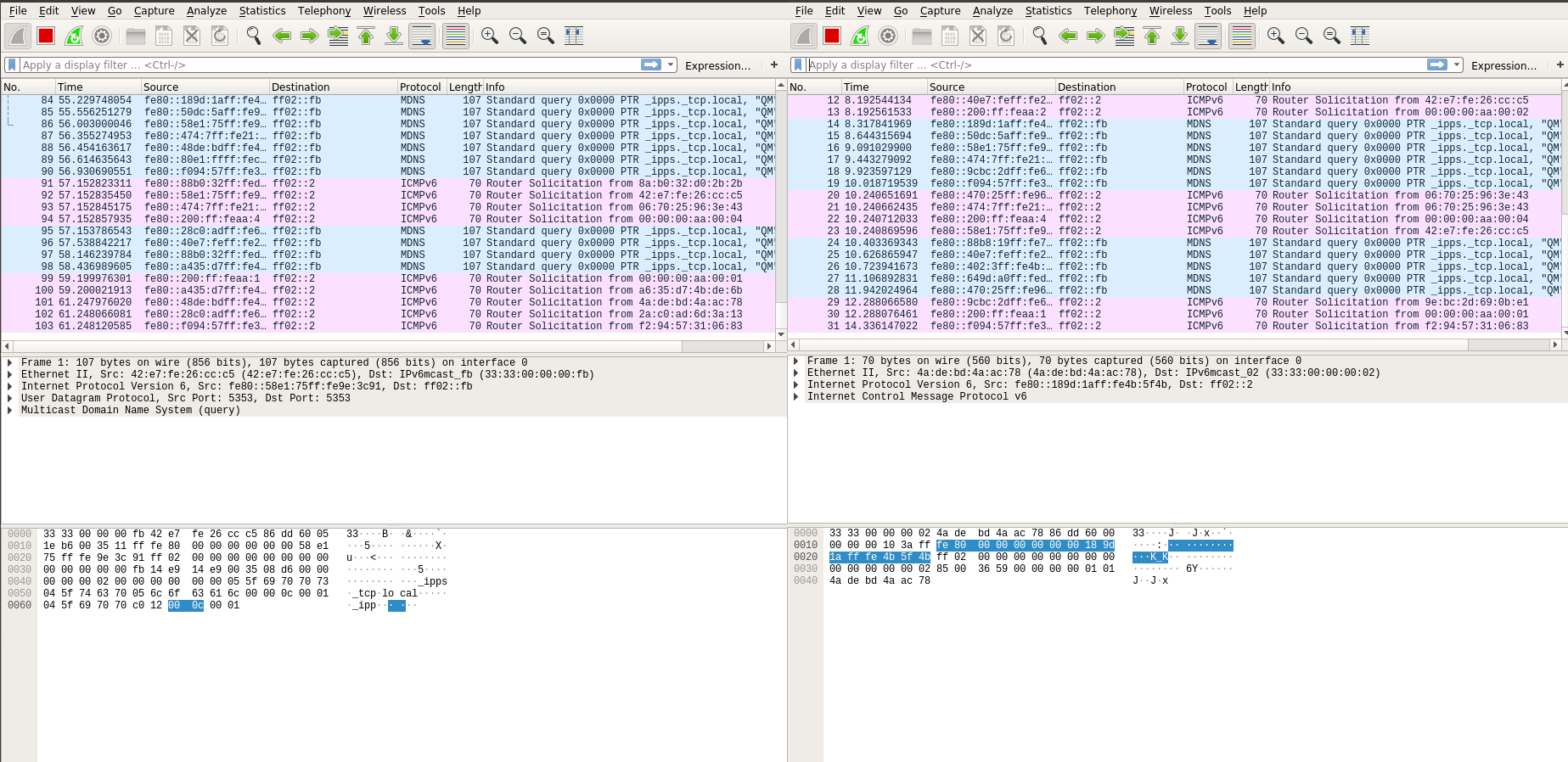
После смены айпи и образования одной сети, теперь каждый компьютер может пинговаться друг с другом. Вот пример:



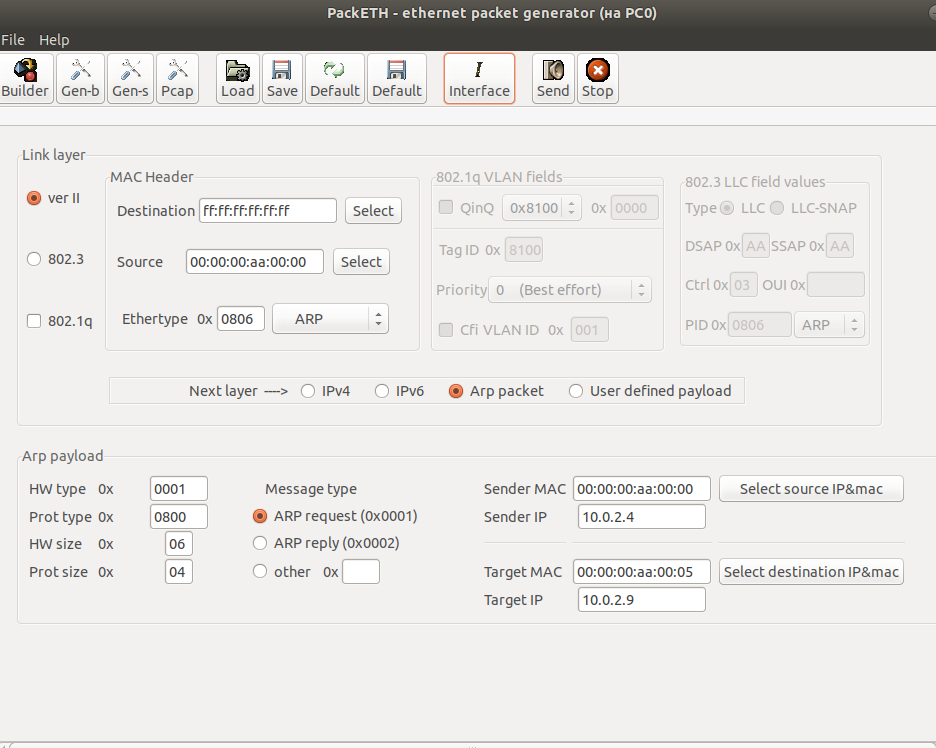
**4. Выполнение задания:**

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

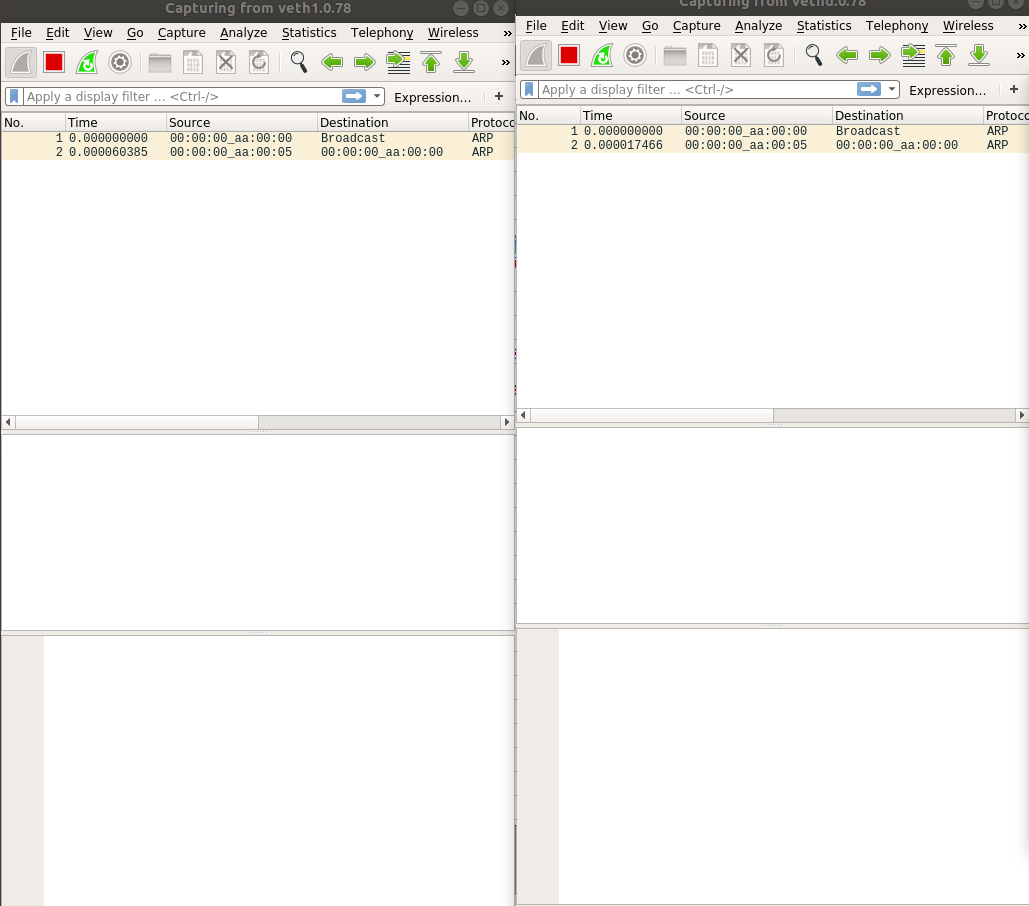
1) Дня начала запустим WireShark на двух компьютерах. Я выбрал PC0 и PC5



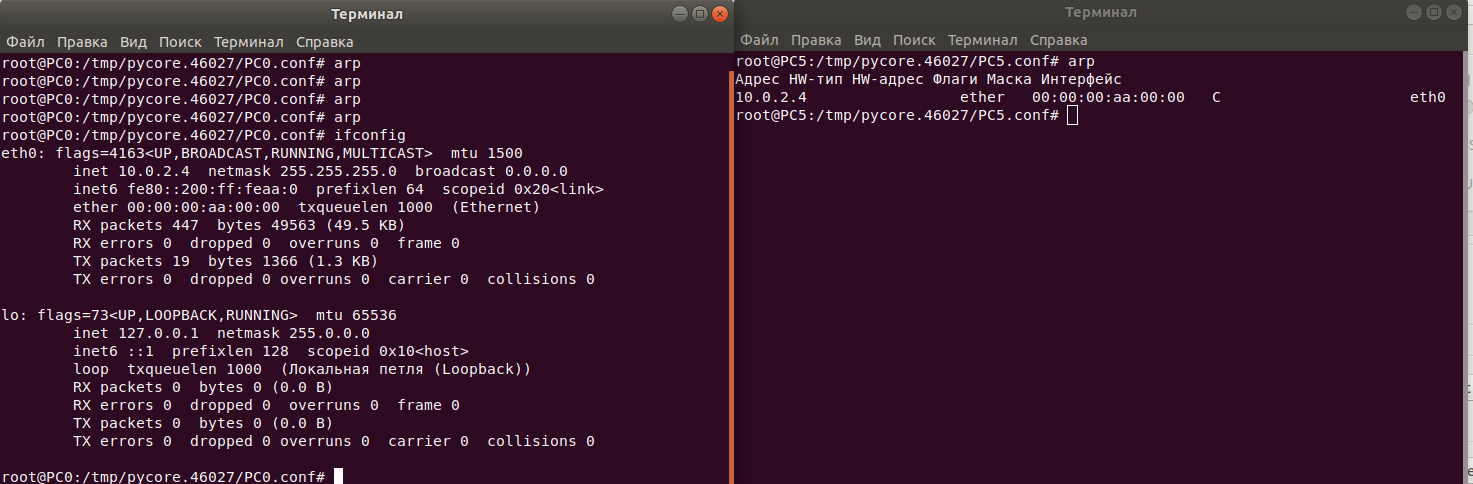
2) Затем запустим утилиту PackETH на PC0, с помощью которой сформируем кадр ARP-запроса и отправим его в сеть.



3) Ну и затем убедимся, что кадр ARP-ответа был получен после посланного запроса. Вывести arp таблицу (команда «arp»).

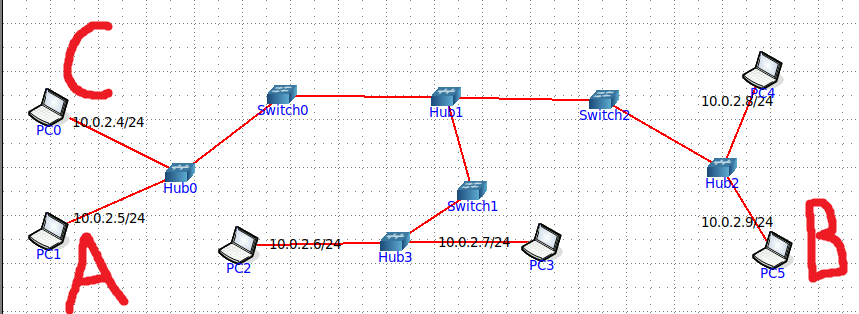


Также не забываем вывести ARP – таблицу, где будет показана связь между PC0 и PC5.



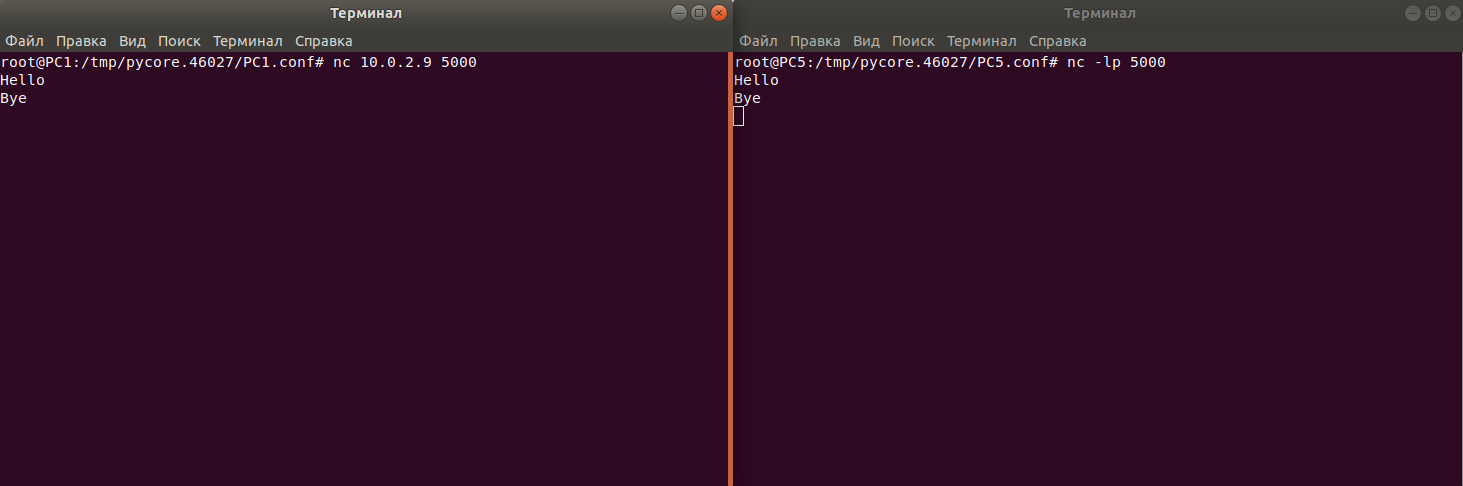
**Часть 2. ARP-спуфинг**

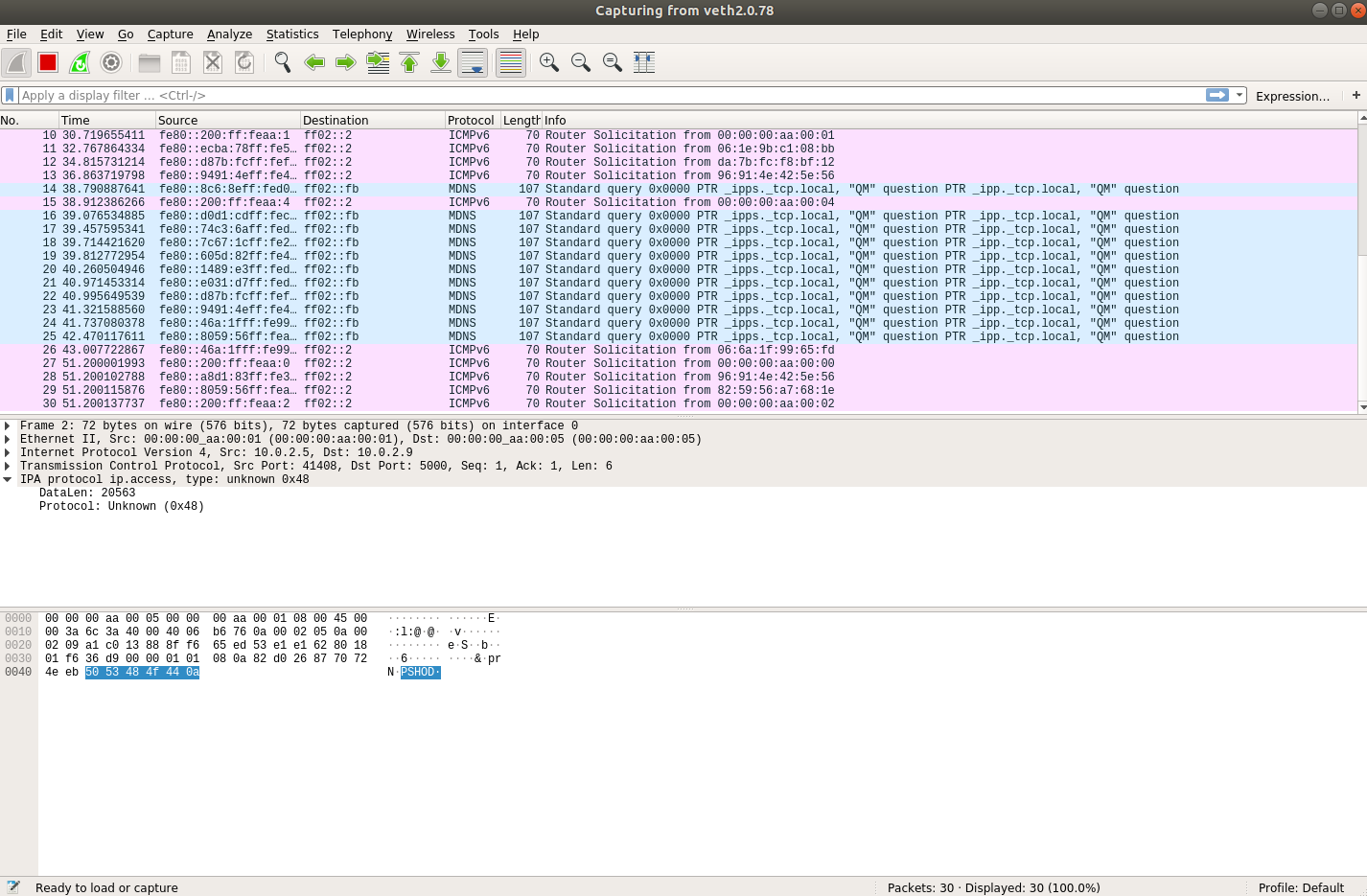
1) Для начала выделим на схеме три компьютера и обозначим их следующим образом:   
A – PC1 B – PC5 С – PC0



2) Наша задача состоит в том, чтобы перехватить информацию, которая проходит по пути из А в В. Для этого нам необходимо подготовить кадр ARP-ответа, который направляется Сервером хосту А с помощью программы PackETH. Получается так, что в результате у нас MAC-адресу Сервера будет соответствовать IP-адрес хоста В.

Для начала установим связь между А и В, используя команду утилиту netcat так, чтобы компьютер B начинал прослушивать порт 5000, а компьютер А передавал сообщения по ip-адресу и порту 5000.

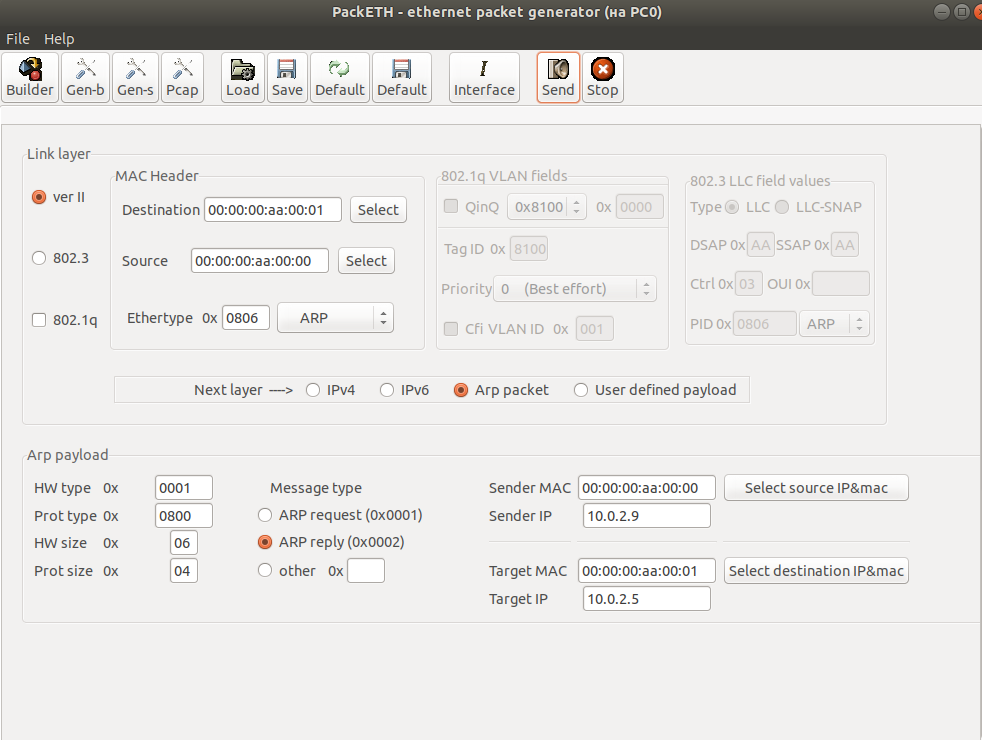


И затем, если открыть wireshark PC1 и найти TCP – пакет, который закрывает соединение, то в нём можно обнаружить текст сообщений, которые мы отсылали:  


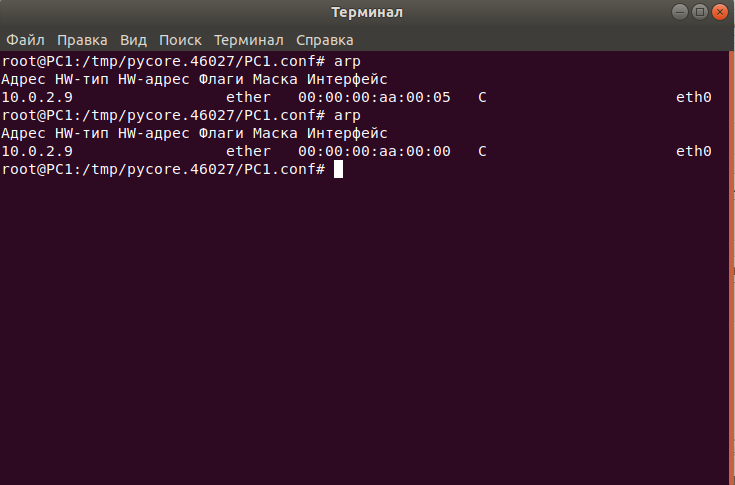
Тоже самое можно обнаружить в wireshark PC5, с которым мы непосредственно осуществляли передачу. В других же компьютерах подобного не найти.

Также, если вывести ARP - таблицу на хосте А, то там будет сказано, что он имеет контакт с хостом В.

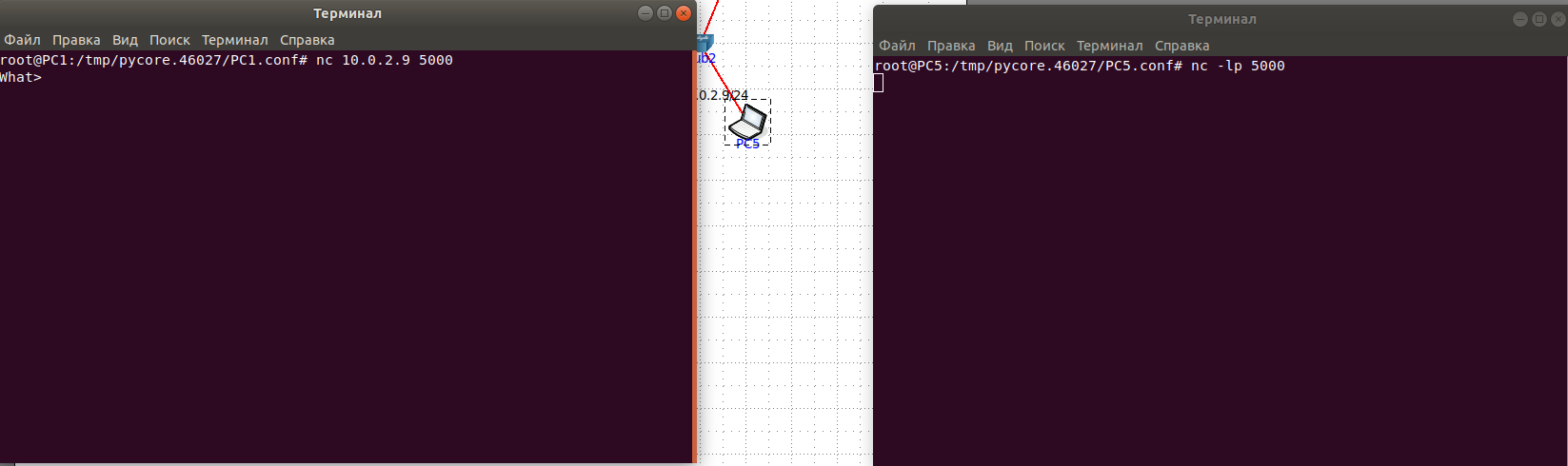
3) Следующим действием нам нужно произвести атаку на это соединение и перехватить пакеты. Т.е Сервер представится PC1, как PC5 и будет пропускать через себя пакеты, которые между ними шли. Для этого мы вновь используем программу PackETH, которая запускается на PC0 – Сервере.



Сразу после этого мы можем проверить, поменялся ли MAC – адрес в ARP таблице на хосте А:



И если теперь наш PC1 захочет отправить какое-нибудь сообщение PC5, то оно до него не дойдет:



Затем, нам необходимо открыть wireshark, то там мы увидим TCP запросы черного цвета, поскольку TCP пытается доставить пакет, но у него это не получается и генерируются пакеты, подсвеченные черным цветом. Это будет видно на компьютере A и C, а на В ничего.

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.

Если попробовать повторить снова тоже самое, то также будут появляться темные TCP – запросы и сообщения будут доходить с задержкой.