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

ОТЧЕТ

по лабораторной работе №3

по дисциплине

Сети и телекоммуникации

РУКОВОДИТЕЛЬ:

\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_Гай В.Е.\_\_

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_Егоров Д.А.\_

(подпись) (фамилия, и.,о.)

\_\_\_\_18-АС \_

(шифр группы)

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

* оценкой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

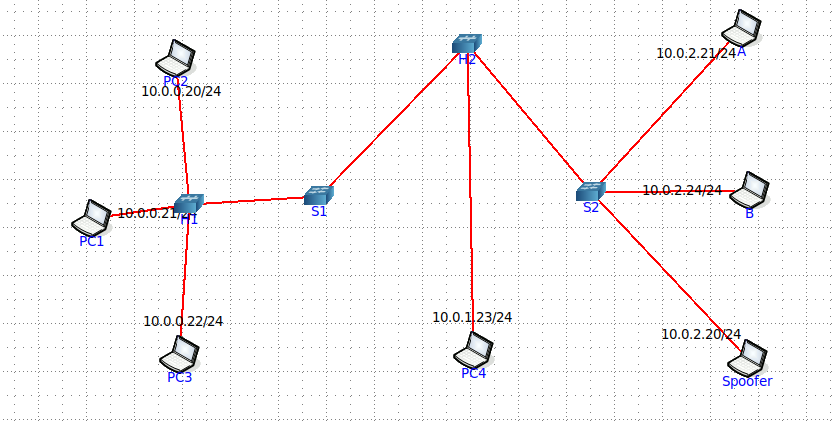
Нижний Новгород 2020

**Цель работы:**

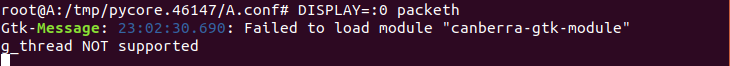
Осуществить перехват ARP пакетов используя принцип ARP Spoofing

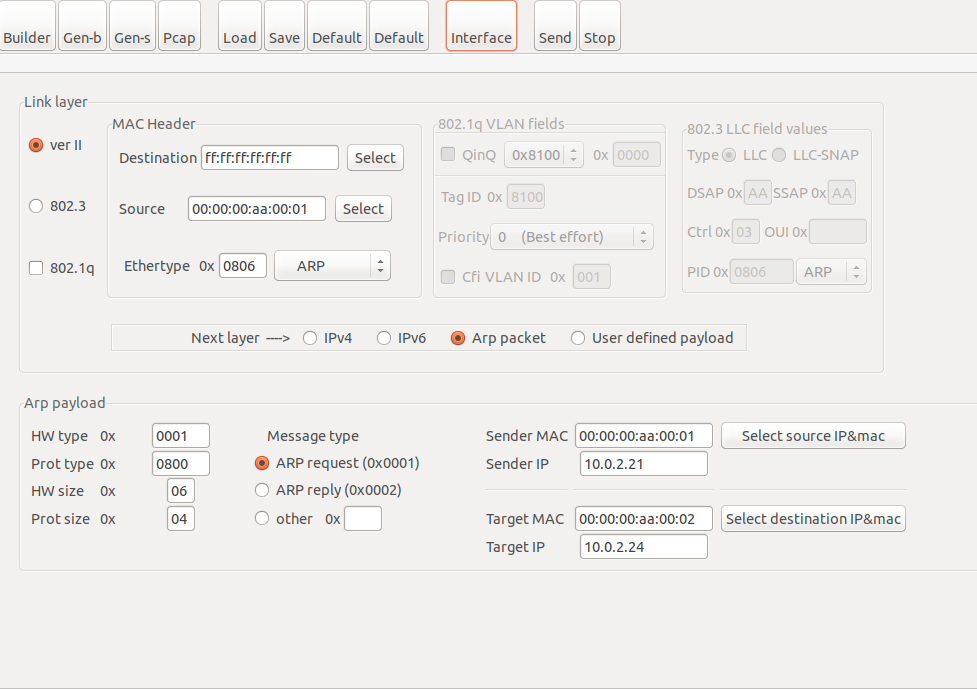
**Ход работы:**

1. В ранее созданную сеть были добавлены дополнительные ПК: Spoofer и А. PC5 был переименован в узел B для удобства обозначений. Схема выглядит следующим образом:



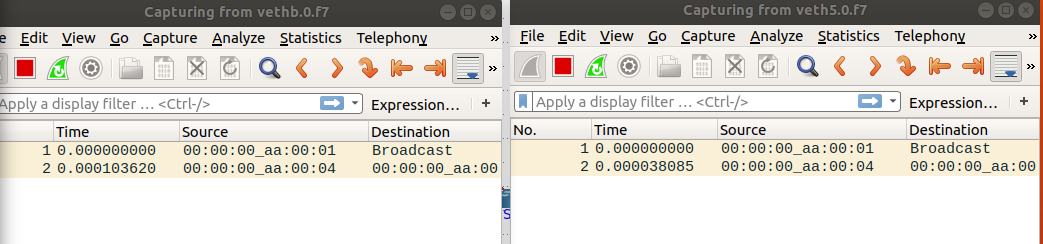
1. Запуск и проверка генератора пакетов packeth. Отправка ARP пакета с А на B:



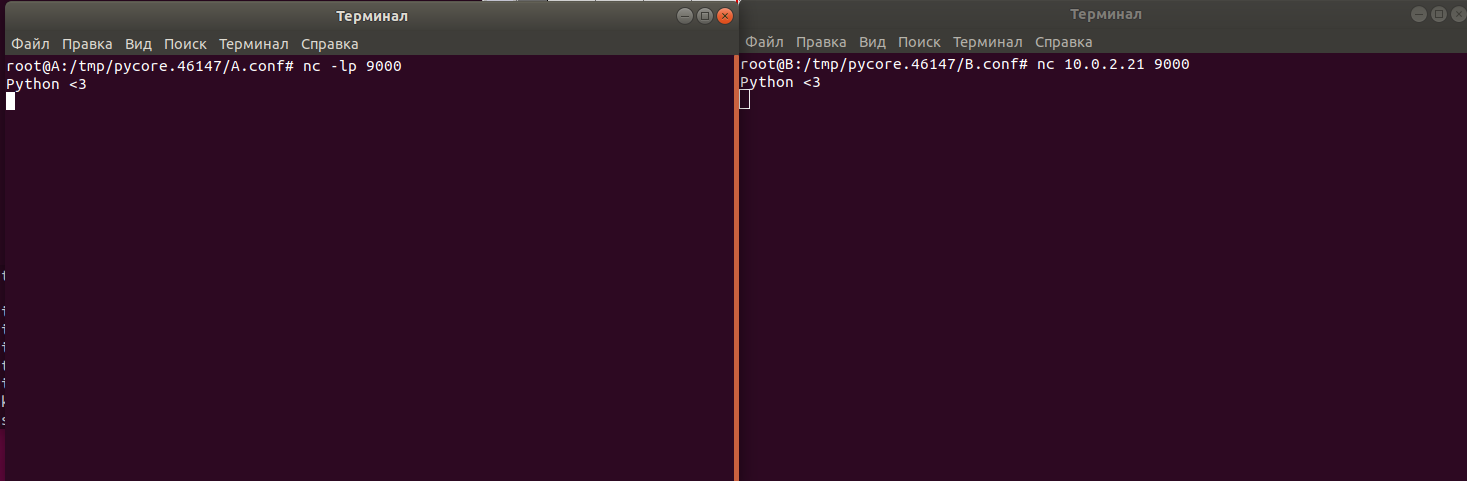


Запрос - широковещательный. В source указывается MAC-адрес А, в Sender MAC указывается MAC-адрес А, в Sender IP - IP-адрес A, в Target MAC - любой адрес, в Target IP - IP-адрес B. Выбирается интерфейс eth0.

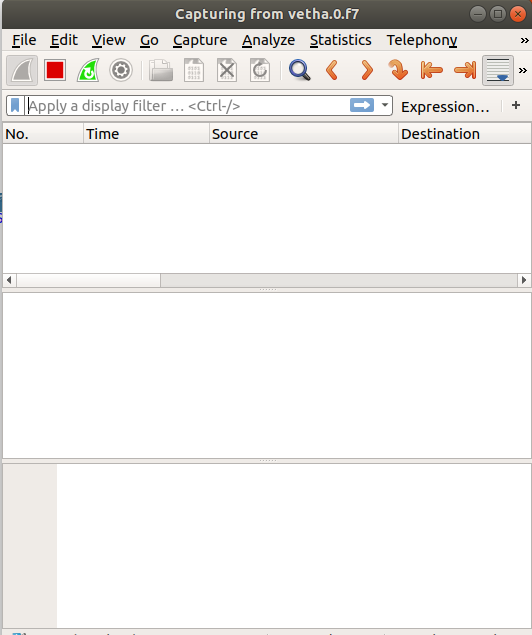
Результаты Wireshark:



1. Создание с помощью программы NetCat сервера, к которому будут подключены А и B:

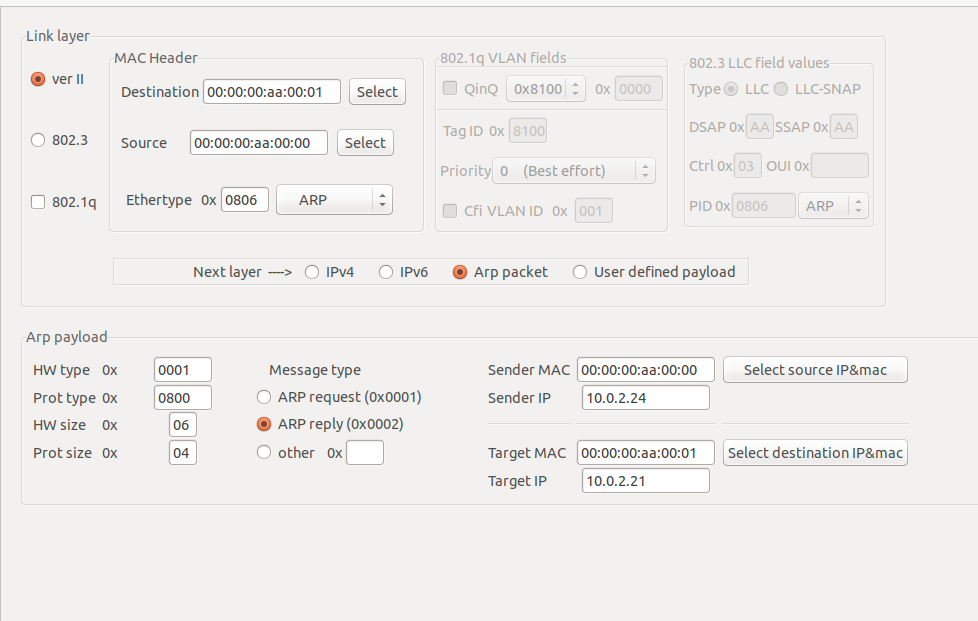


Spoofer же данные пакеты не получает:



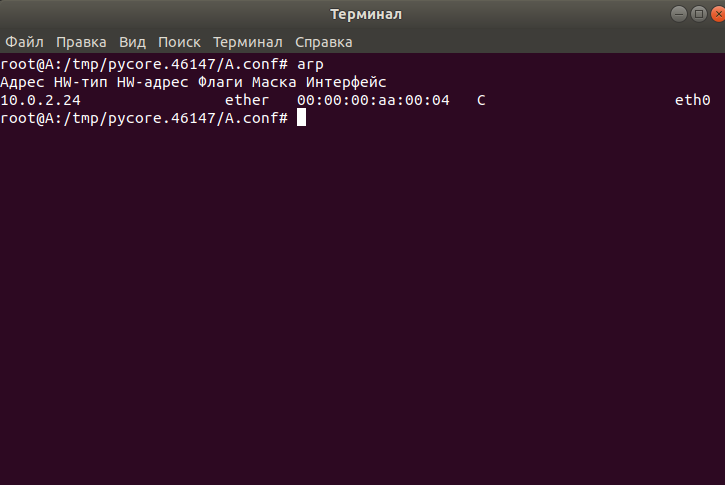
Теперь наша цель состоит в том, чтобы как-то перехватить пакеты, идущие от A к B

1. Сделаем так, чтобы сервер “представился” компьютеру А, как если бы он был компьютером B. Для этого сгенерируем еще один ARP пакет, на этот раз - reply:

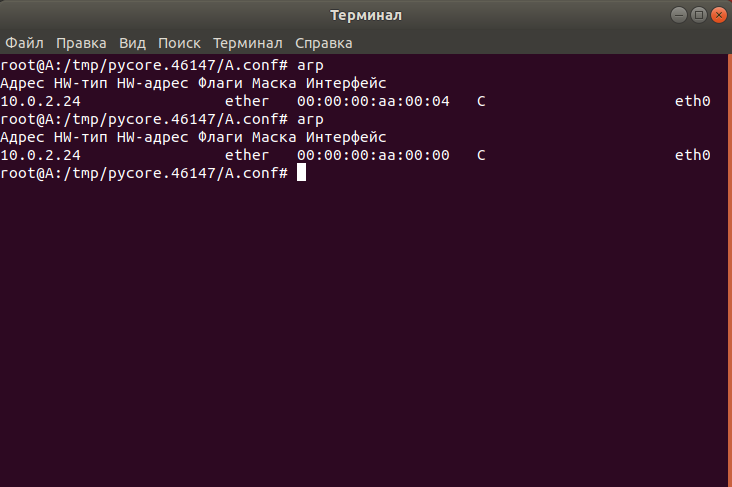


В Destination указывается MAC-адрес А. В source указывается MAC-адрес Spoofer, в Sender MAC указывается MAC-адрес Spoofer, в Sender IP - IP-адрес B (именно это и создает видимость, что пакет идет от узла B, хотя он идет от узла Spoofer), в Target MAC - MAC-адрес А, в Target IP - IP-адрес А. Выбирается интерфейс eth0.

Заранее проверим ARP таблицу A:

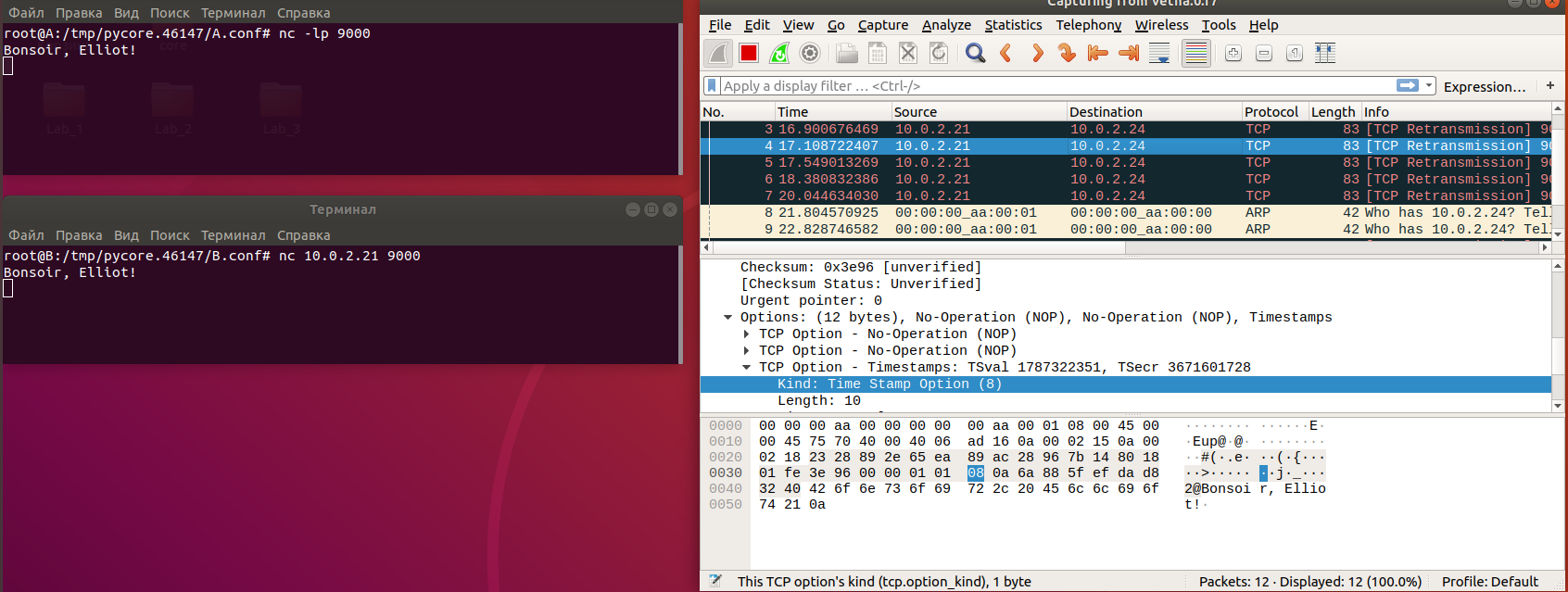


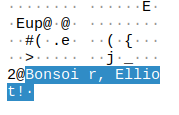
Отправим пакет из packeth и проверим таблицу еще раз:



Как мы видим, здесь числится уже MAC-адрес Spoofer, а не узла B.

1. Попробуем снова отправить сообщение с А на B, после проделанных манипуляций, предварительно запустив Wireshark на узле Spoofer:





Пакет от А к B доставился не мгновенно. Как видно из Wireshark, было несколько попыток перенаправления пакета (retransmission) и именно в этот момент Spoofer перехватил данные. Узел А отправлял ARP запросы, а после нескольких неудачных попыток он отправил широковещательный запрос, узнал MAC-адрес B и корректно отправил ему пакет. Сообщение было доставлено, но с задержкой в 6-7 секунд.

**Вывод по работе:**

В ходе проделанной работы я более подробно изучил способы передачи ARP пакетов. Был осуществлен перехват пакетов сторонним узлом сети.