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 №3  
 «сети и телекоммуникации»

РУКОВОДИТЕЛЬ:

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

(подпись) (фамилия, и.,о.)

СТУДЕНТ:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Панкратьев И.А

(подпись) (фамилия, и.,о.)

18-В1

(шифр группы)

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

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

Нижний Новгород 2020

**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.

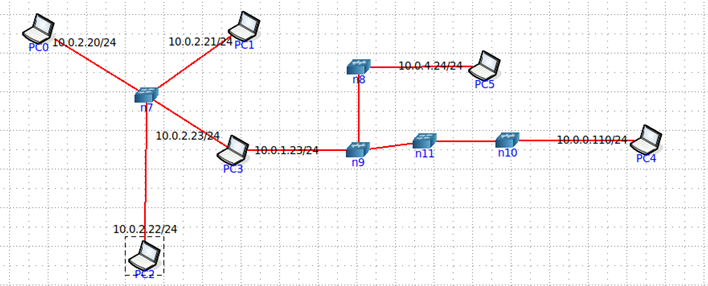
**Часть 2. ARP-спуфинг**

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

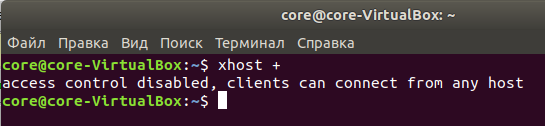
2. Подготовить кадр ARP-ответа, направляемый Сервером хосту А с помощью программы PackETH. Кадр должен быть составлен так, чтобы MAC-адресу Сервера соответствовал IP-адрес хоста В. Вывести arp таблицу на хосте А. Отправить сформированный пакет от Сервера хосту А.

**Ход работы:**

Схема из 1ЛР со всеми изменениями:

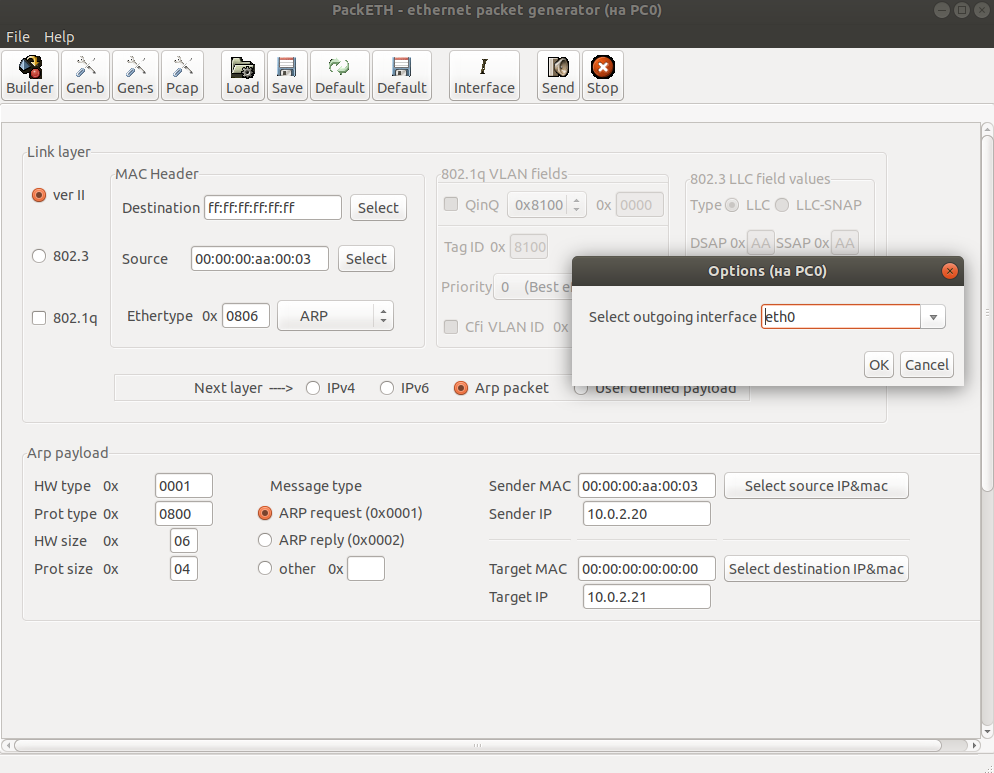


Для запуска PackETH в консоли выполняем команду «xhost +», тем самым разрешаем подключаться к серверу с любых хостов. Далее в консоли узла PC0 «DISPLAY=:0 packeth».



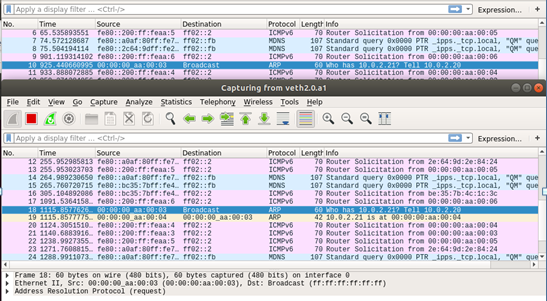
1. Удостоверимся, что «всё работает».

Запущенная на PC0 утилита PackETH

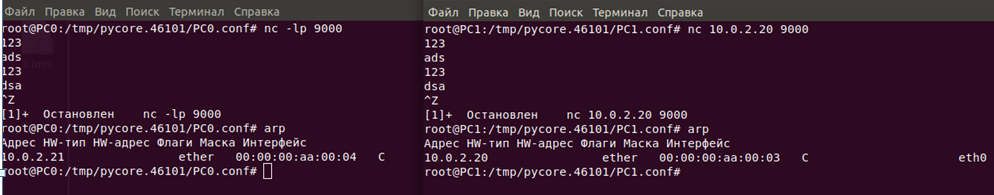


По широковещательному каналу отправляем сообщение, чтобы убедиться, что система работает исправно.

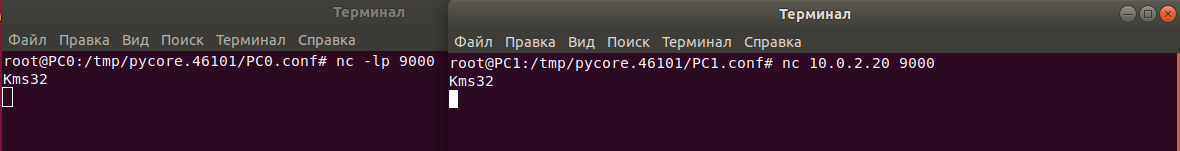
В Wireshark проверяем наличие сформированного arp-запроса



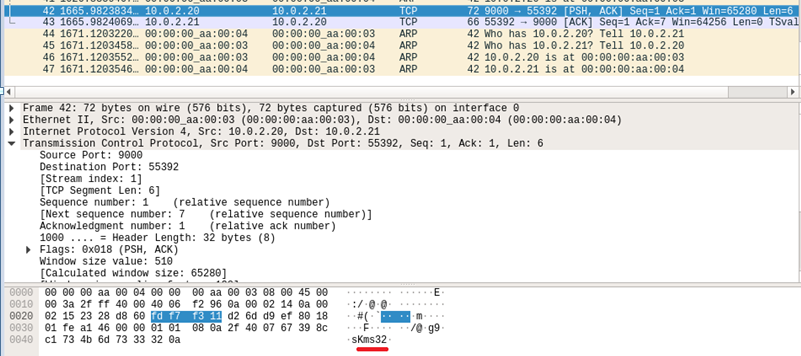
Выведем arp-таблицу и видим, что PC0 и PC1 «соединены»:

****

Подключённые через nightcat PC0 и PC1 и передача сообщений между ними

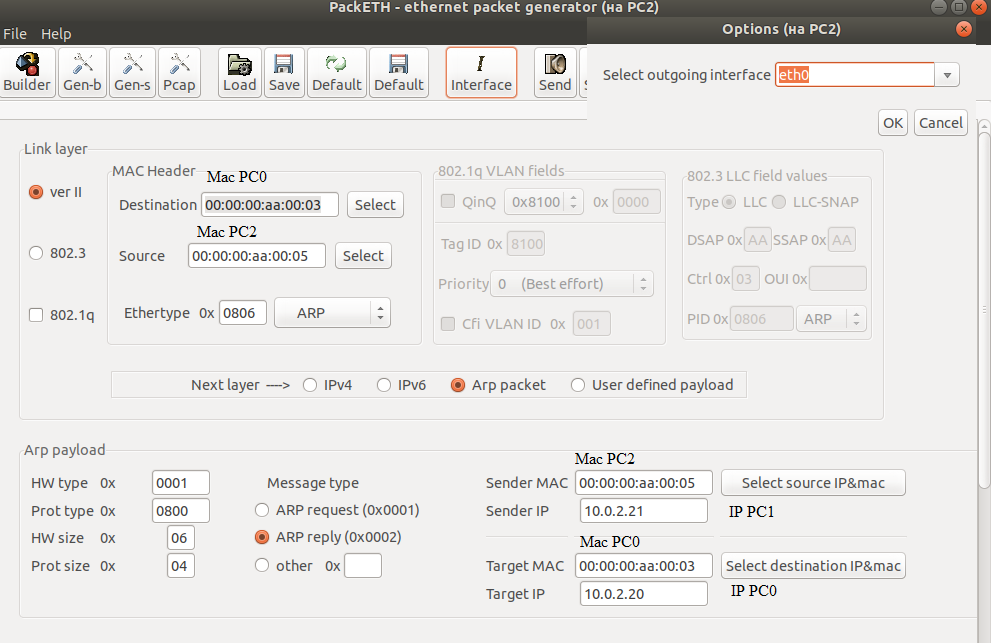


Отметим переданное сообщение и в wireshark



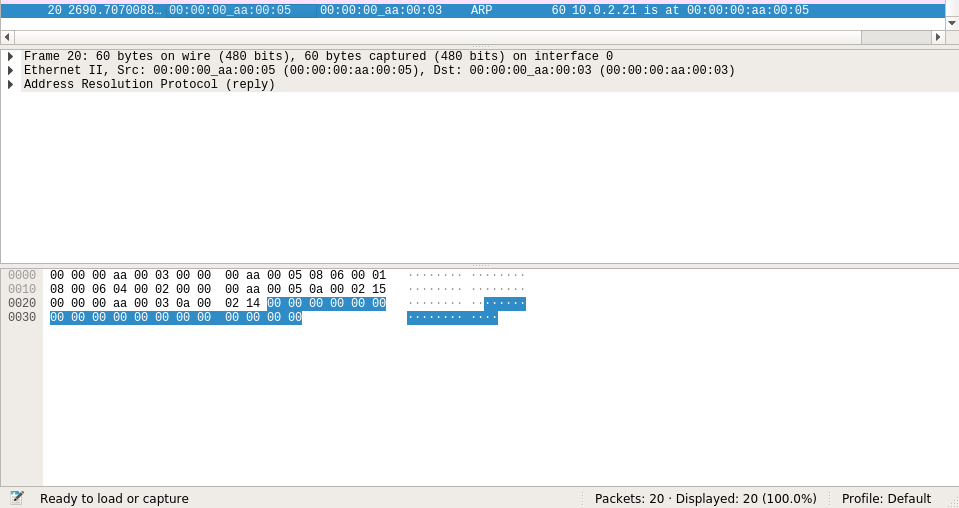
2)Начинаем производить атаку:

PackETH на PC2

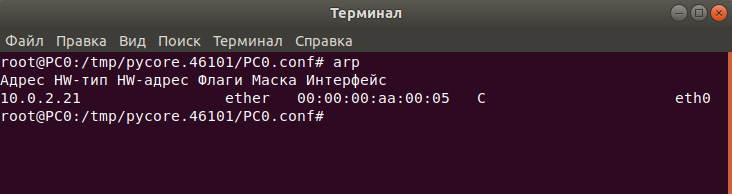


Говорим PC2 представляться как PC1 при их общении с PC0.

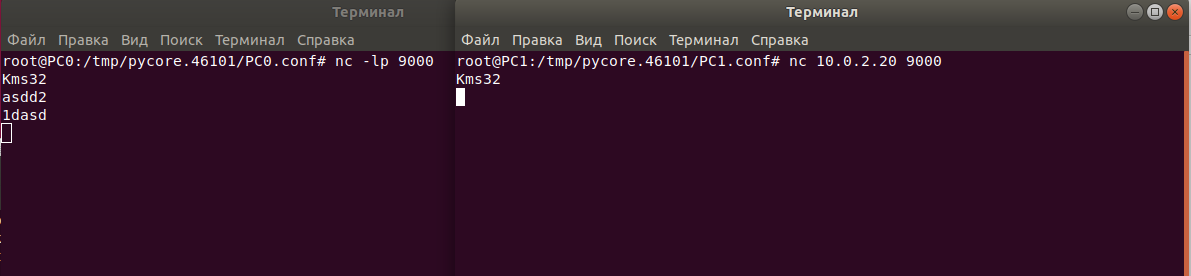
И отсылаем пакет:



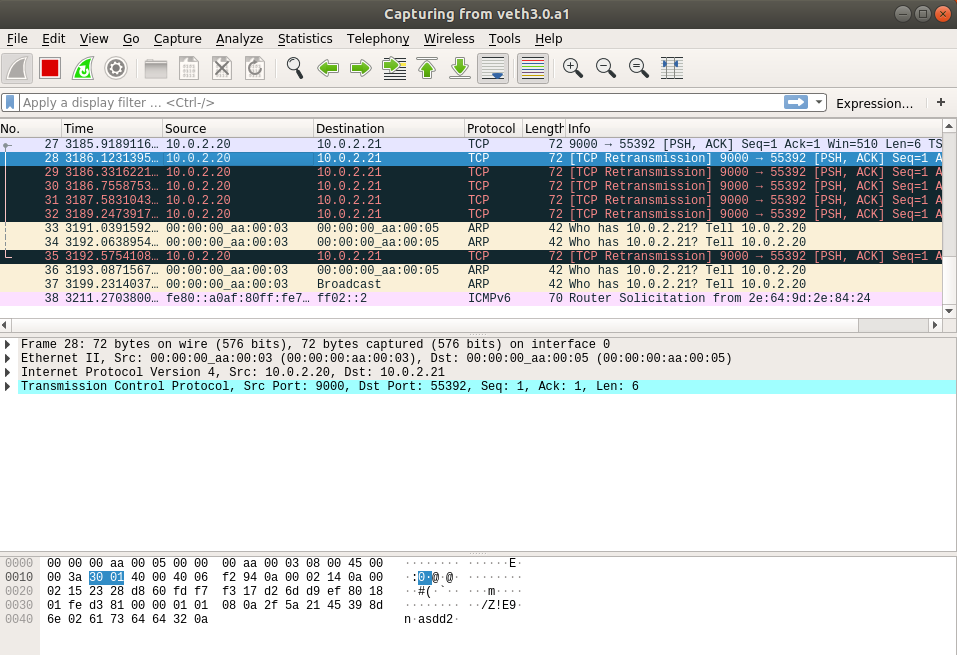
Изменённая таблица ARP на PC0:

****

Доходящие с задержкой сообщения:



Отметим эти сообщения в wireshark (они помечены тёмным цветом) с тэгом retransmission

****

**Вывод:** изучили подробнее arp протокол и провели простой вариант arp-спуфинга.