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: Федоров Н.А.

Группа: 19-В-2

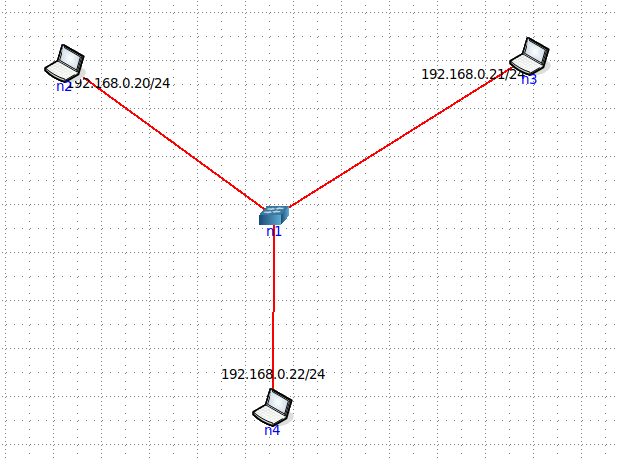
Проверил: Гай В.Е.

Нижний Новгород 2021

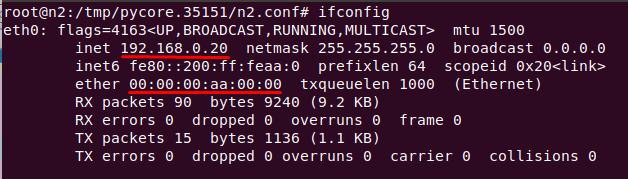
**Ход работы**

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

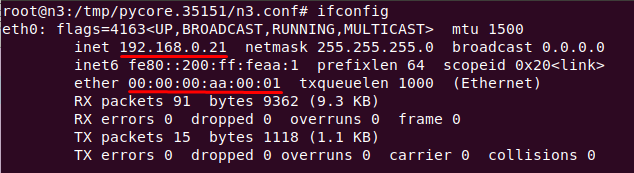
*Схема сети:*



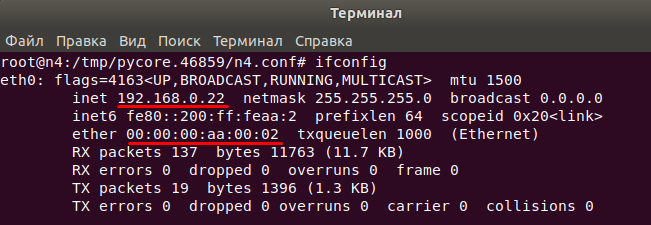
Сетевой интерфейс eth0 компьютера n2 - А:



Сетевой интерфейс eth0 компьютера n3 - В:

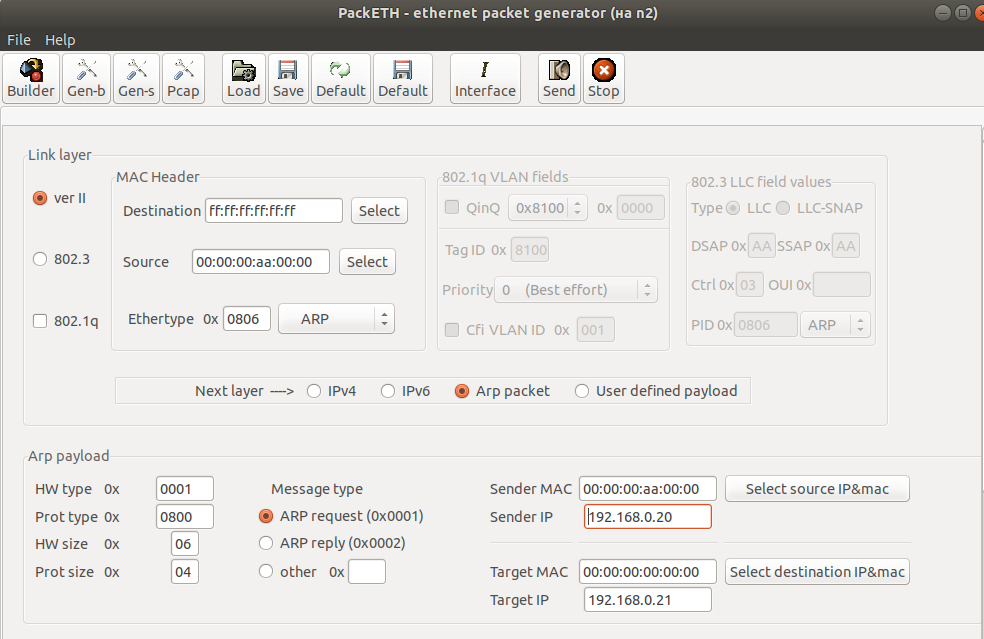


Сетевой интерфейс eth0 компьютера n4 - С:



Сформируем пакет ARP-запроса с помощью программы Packeth на компьютере n2:

* Destination – широковещательный MAC-адрес (ff:ff:ff:ff:ff:ff),
* Source – MAC-адрес источника n2 (00:00:00:aa:00:00)
* Sender MAC – MAC-адрес отправителя n2 (00:00:00:aa:00:00)
* Sender IP – IP-адрес отправителя n2 (192.168.0.20)
* Target MAC – MAC-адрес получателя n3, который пока неизвестен (00:00:00:00:00:00)
* Target IP – IP-адрес получателя n3 (192.168.0.21)
* Выберем интерфейс с которого будет посылаться пакет – eth0



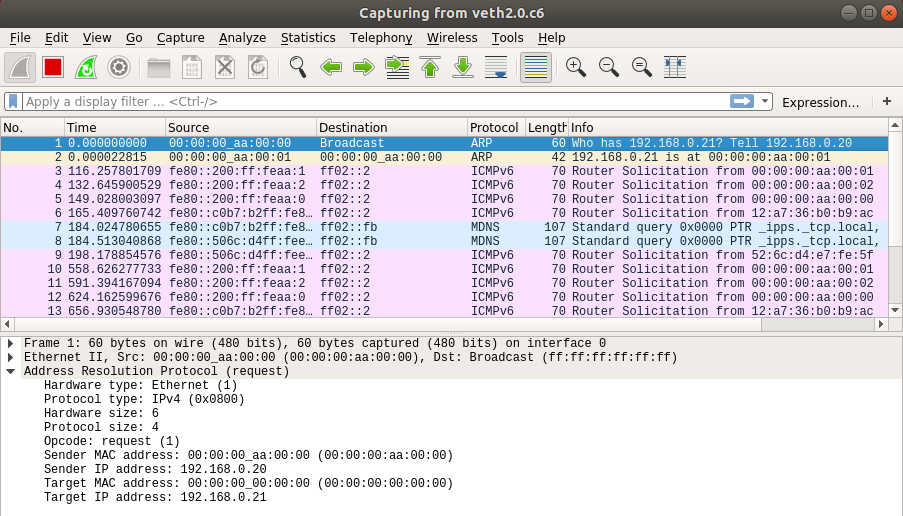
Выполним захват пакетов - запустим Wireshark на компьютере n2

Сформированный пакет был отправлен на коммутатор, который разослал аналогичные пакеты всем участникам сети:

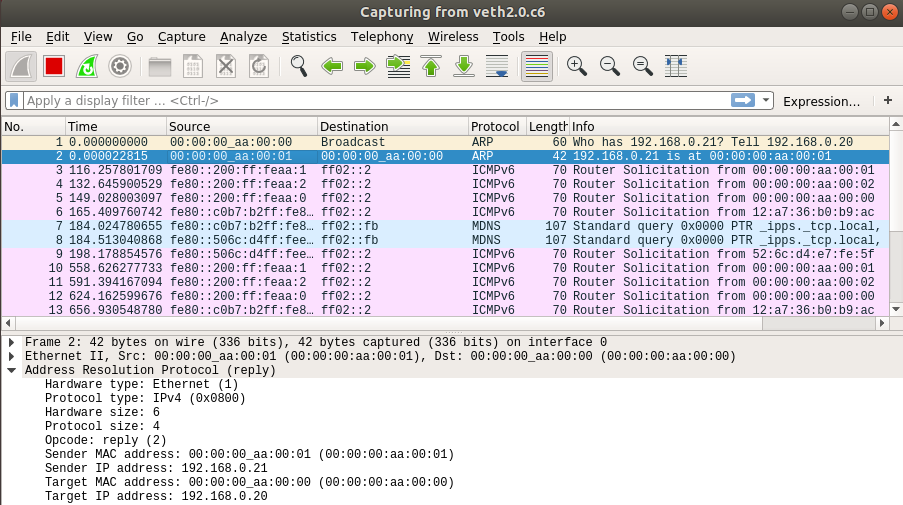
Broadcast ARP-запрос получат все хосты в сети, а ARP-ответ будет получен только хостом n2, который отправил ARP-запрос на получение MAC-адреса.

Результаты захвата пакетов на n3:

1 пакет – сформированный ARP-запрос на компьютере n2

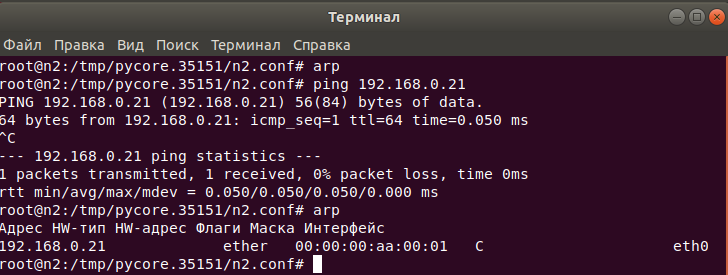


2 пакет – ARP-ответ от 192.168.0.21 с информацией о MAC адресе искомого хоста:

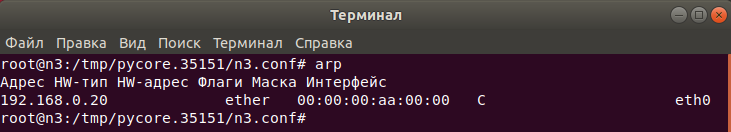


Вывод ARP-таблицы на хосте n2:

В силу особенности ручной генерации ARP-пакетов программой Packeth на хосте n2 после получения ответного пакета от n3 в arp таблице не появляется запись соотвествия MAC и IP адресов.



Вывод ARP-таблицы на хосте n3:



**Часть 2. ARP-спуфинг**

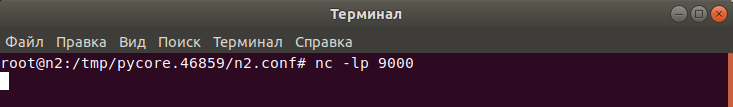
Под ARP-спуфингом понимается выдача злоумышленником своего MAC-адреса за MAC-адрес другого компьютера.

В нашем примере пакеты, отправляемые с n2 на IP-адрес n3, будут отправляться на хост n4, в результате реализации этой атаки.

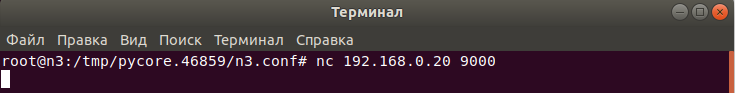
Нормальный обмен информацией между n2 и n3

Сгенерируем трафик между n2 и n3 с помощью программы netcat:

* n2 будет являться сервером



* n3 является клиентом



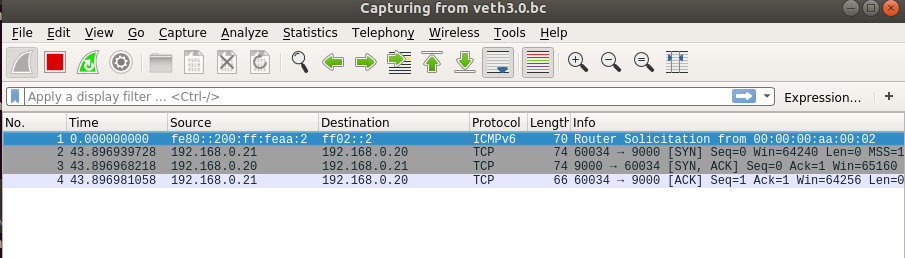
Выполним захват пакетов на n3:

Выполняется трёхшаговый процесс установки соединения между n2 и n3 по протоколу TCP:

1 пакет отправляется с n2 на n3 с предложением начать обмен данными

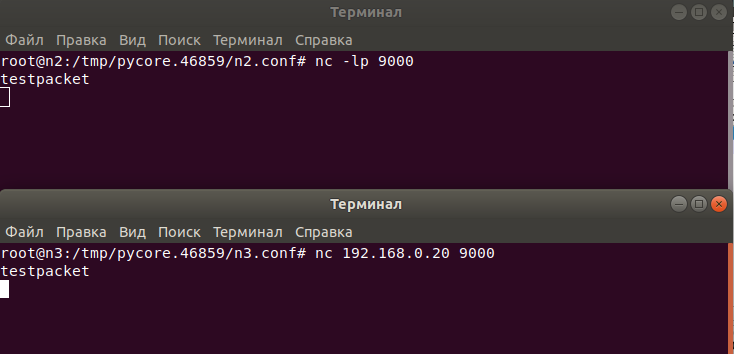
2 пакет отправляется с n3 на n2, в котором сообщается готовность n3 к обмену

3 пакет отправляется с n2 на n3 с подтверждением согласия



*Захват пакетов на n3*

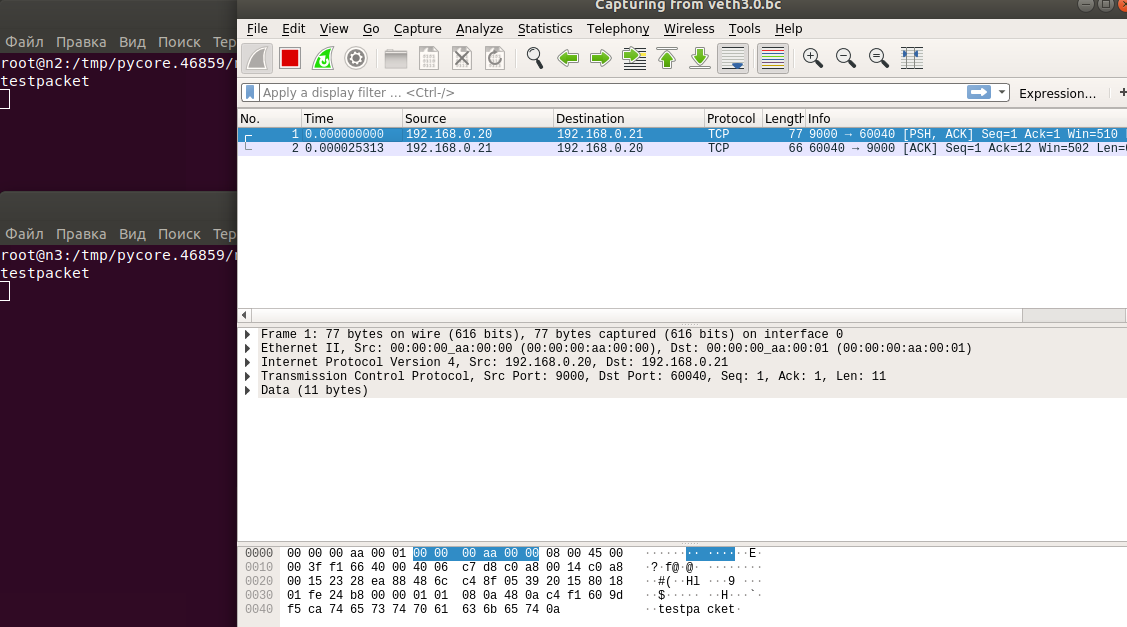
Начнем обмен данными между хостами:



*Обмен между n2 и n3*

1 пакет отправляется от n2 к n3 с данными

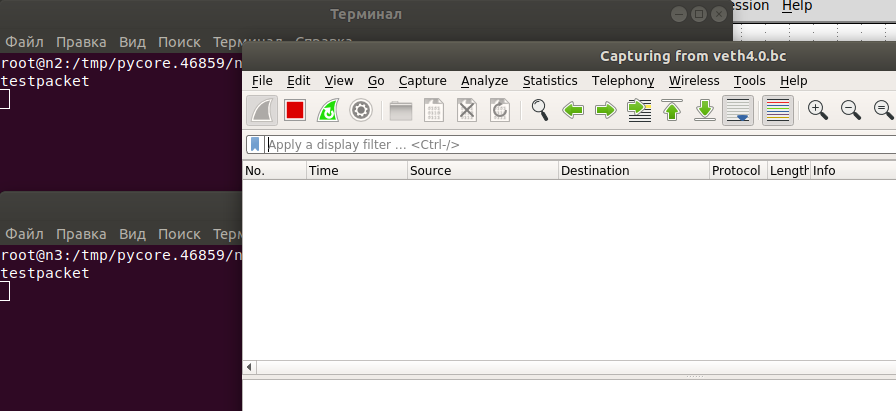
2 пакет отправляется от n3 к n2, в котором подтверждается получение предыдущего



*Захват пакетов на n3*

В случае если пакет с подтверждением не получен, идет повторная отправка пакета с данными.

Хост n4 не видит проходящий трафик между n2 и n3

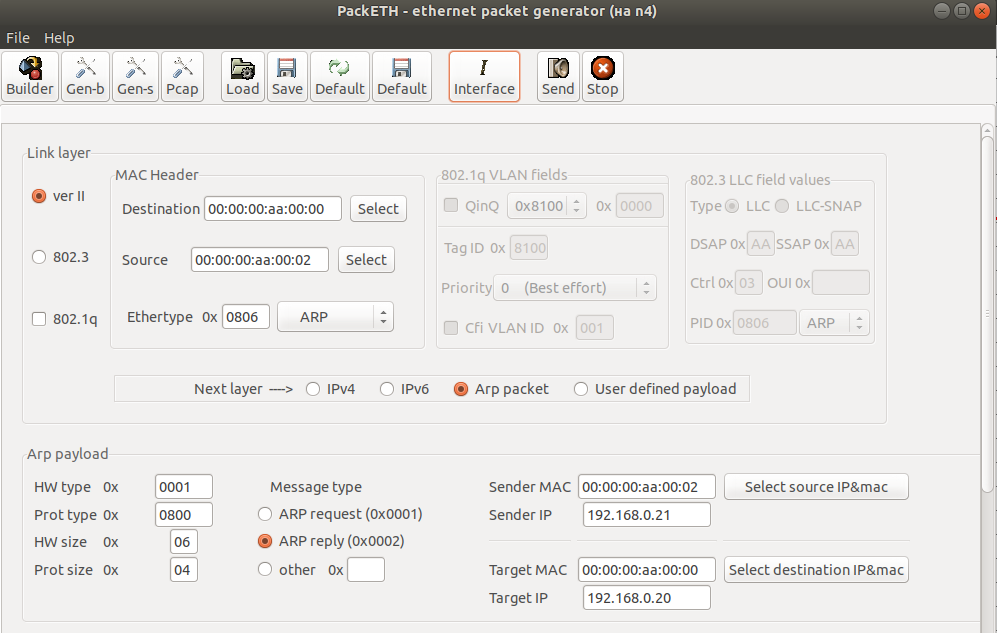


*Захват пакетов на n4*

Реализация ARP-спуфинга

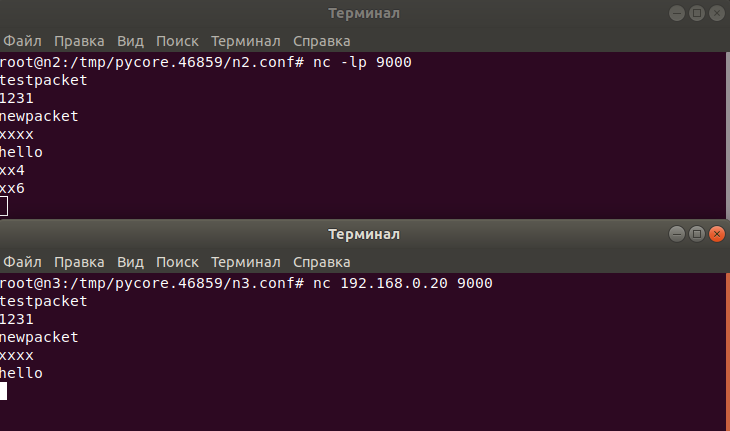
Сформируем ARP-ответ на хосте n4, в котором сообщим хосту n2, что MAC-адресу n4 соответствует IP-адрес хоста n3 – т.е:

* В поле Destination укажем MAC хоста n2 – 00:00:00:aa:00:00
* В поле Source укажем MAC хоста n4 – 00:00:00:aa:00:02
* В поле Sender MAC укажем MAC хоста n4 – 00:00:00:aa:00:02
* В поле Sender IP укажем IP хоста n3 – 192.168.0.21
* В поле Target MAC укажем MAC хоста n2 – 00:00:00:aa:00:00
* В поле Target IP укажем IP хоста n2 – 00:00:00:aa:00:00
* Выберем интерфейс, с которого отправляется пакет: eth0



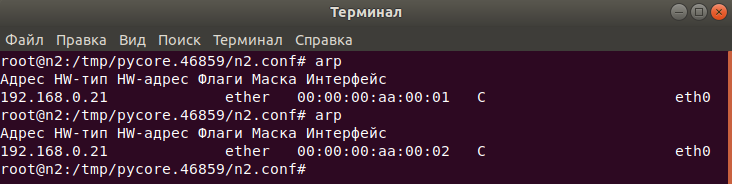
*Сформированный пакет ARP-ответа*

После отправки сообщения hello, с n4 был отослан сформированный ARP-ответ на n2, c «неправильным» соответствием IP и MAC адреса.



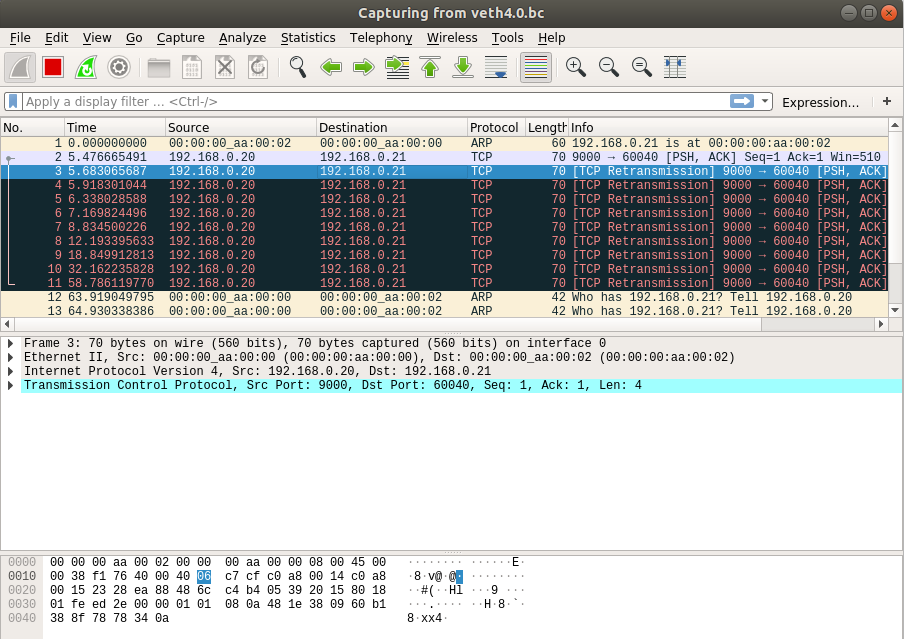
*n3 не получает отправленные сообщения*

После отправки такого пакета обновляется arp-таблица хоста n2, в результате чего IP-адресу n3 будет соответствовать MAC-адрес n4.



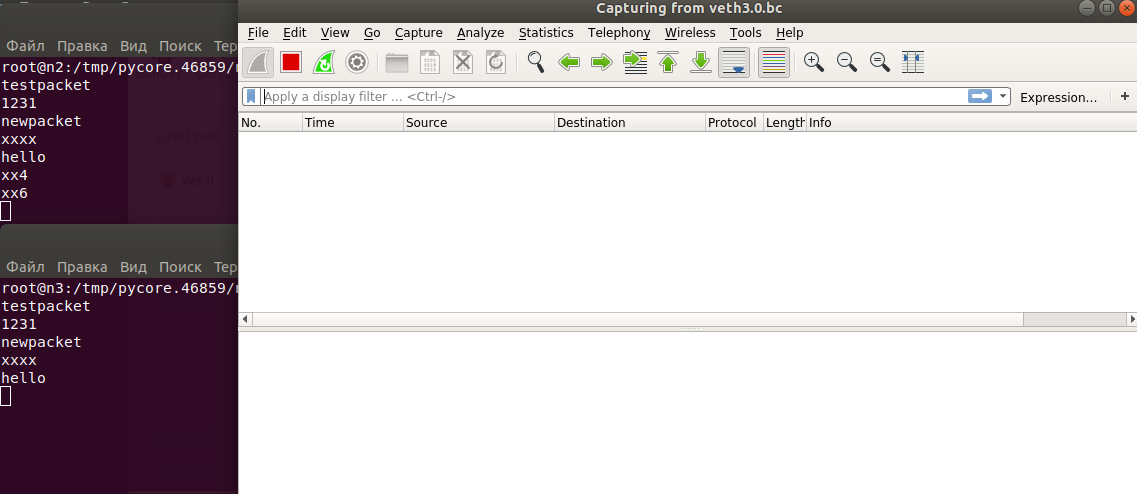
*Вывод ARP таблицы n2*

Поэтому, отправляя сообщение xx4 на IP 192.168.0.21, пакет придет на n4, и не получив подтверждение будет проводиться повторная отправка этого пакета (Retransmission).



*Захват пакетов на n4*

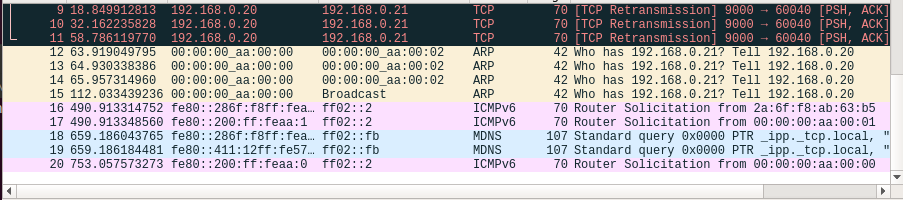
Подтверждение о получении пакета от 192.168.0.21 не было получено, т.к. хост n3 не видел этот пакет, этот пакет получил n4:



*Захват пакетов на n3*

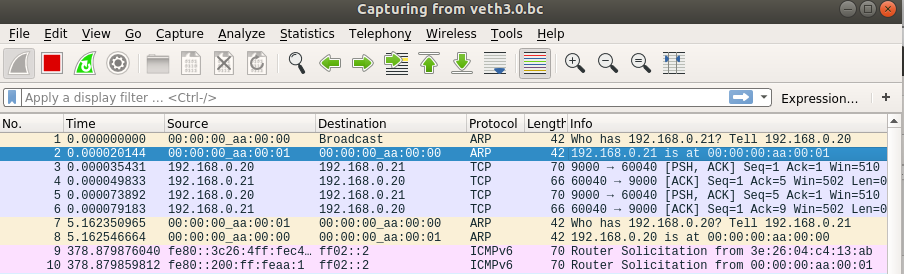
Хост n2 отправляет ARP-запросы на MAC n4 с целью узнать верный MAC-адрес (12-14 строки).

Т.к. он в течение некоторого времени не получил ответа от MAC n4 о том, что его IP – 192.168.0.21, n2 почти сразу начинает широковещательную рассылку с целью узнать верный MAC (15 строка).



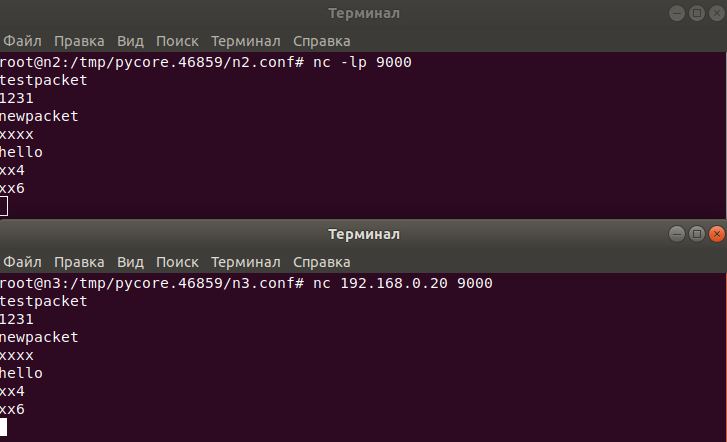
*Захват пакетов на n4*

Поскольку широковещательную рассылку видят все участники сети, n3 получает ARP-запрос с просьбой для хоста 192.168.0.21 отправить свой MAC(1 строка) и отправляет правильный MAC(2 строка).



*Захват пакетов на n3*

После чего возобновляется процесс передачи между n2 и n3, теперь n3 получает отправленные пакеты с n2:



*Возобновление передачи*