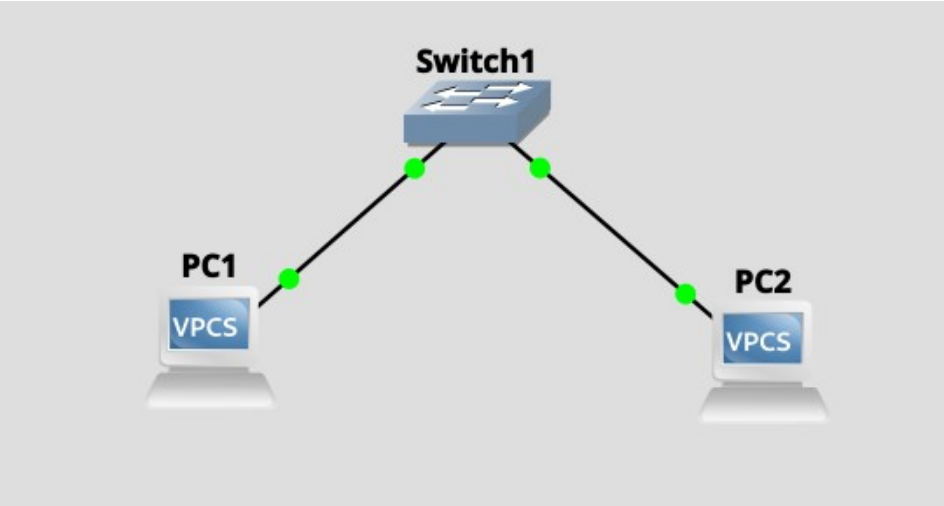
Лабораторная работа №1

Локальная сеть



Show IP

PC1:

```
NAME   IP/MASK              GATEWAY           MAC               LPORT  RHOST:PORT
PC1    192.168.0.3/24       192.168.0.1       00:50:79:66:68:00 20006  127.0.0.1:20007
       fe80::250:79ff:fe66:6800/64
```

PC2:

```
NAME   IP/MASK              GATEWAY           MAC               LPORT  RHOST:PORT
PC2    192.168.0.2/24       192.168.0.1       00:50:79:66:68:01 20004  127.0.0.1:20005
       fe80::250:79ff:fe66:6801/64
```

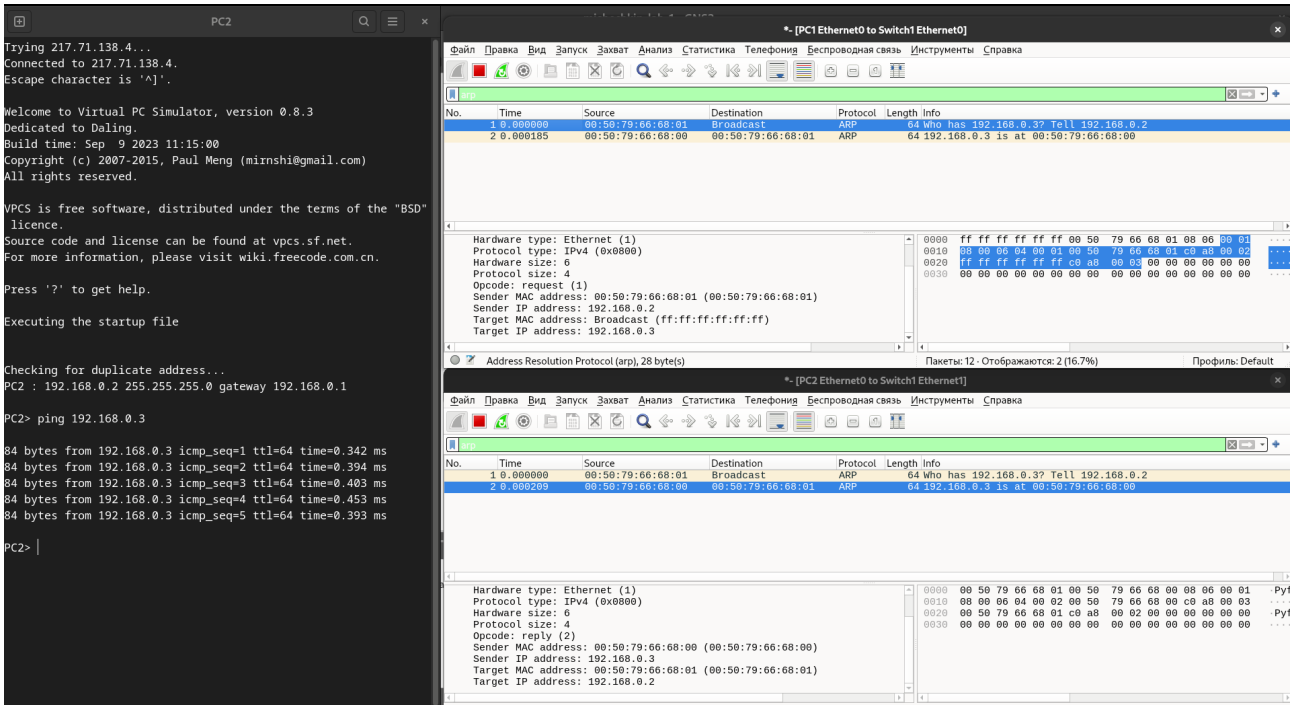
Поставил компьютерам одинаковую маску /24 (255.255.255.0) для того чтобы они находились в одной сети. Первый три октета определяют IP адрес сети, последний октет указывает на определенный хост в этой сети.

Перехватить трафик протокола arp

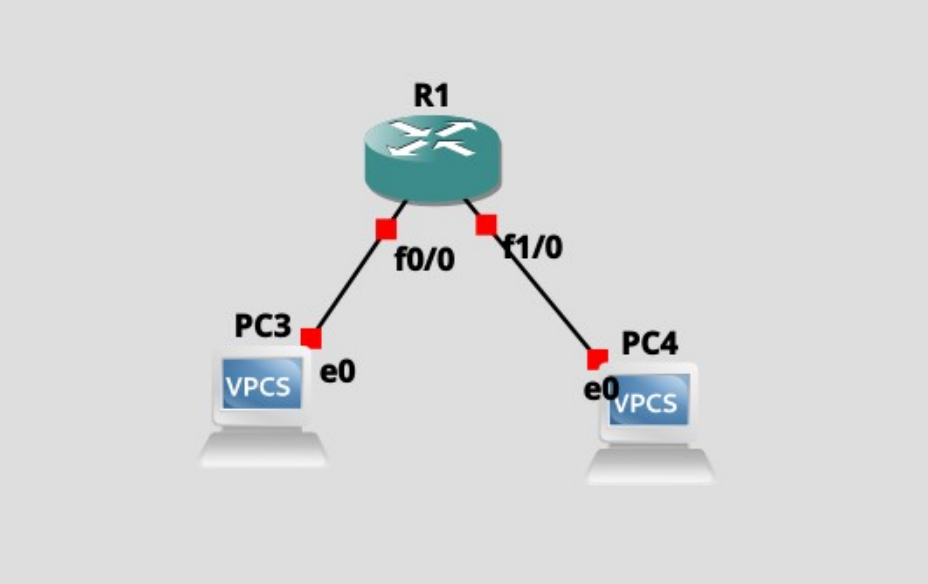
1) PC2 с MAC: 00:50:79:66:68:01 отправляет broadcast ARP запрос в заголовке которого указан MAC и IP самого отправителя, IP адрес хоста у которого мы хотим узнать MAC адрес.

2) PC1 с MAC: 00:50:79:66:68:00 получает broadcast ARP запрос и отвечает указывая свой MAC и IP, MAC и IP запросившего. Так же он записывает ARP таблицу MAC и IP запросившего

3) PC2 получает MAC и IP (PC1) и так же записывает в ARP таблицу



Сеть из маршрутизатора и двух подсетей



Перехват трафика протокола ARP и ICMP

Адрес указанный в команде ping, при выполнении хост понимает что адрес не находится в его сети и отправляет пакет на шлюз по умолчанию то есть на наш маршрутизатор. А так же перед этим ему нужен mac адрес если его нет в ARP таблице он делает ARP запрос и после этого только отправляет icmp запрос. Маршрутизатор принимаем этот запрос понимает в какую сеть нужно отправить с помощью таблицы маршрутизации и отправляет в нужную сеть.