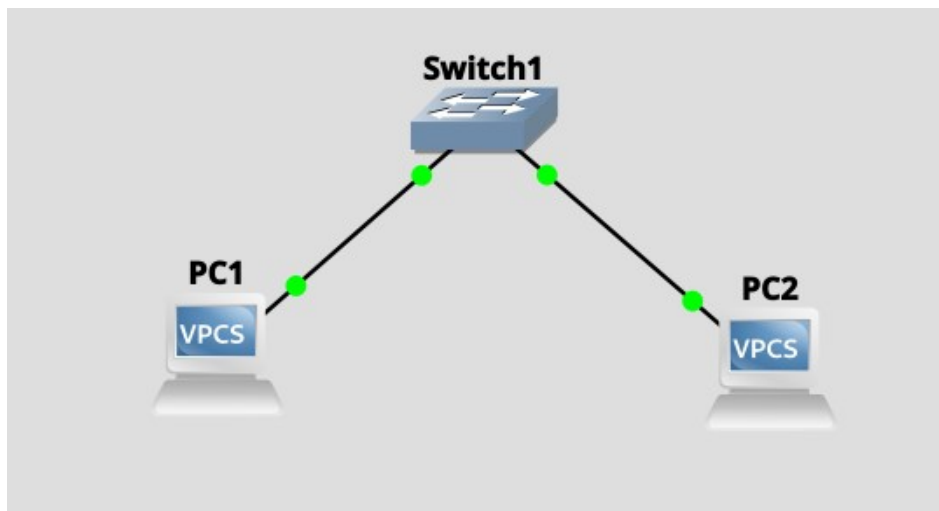


# Лабораторная работа №1

## Локальная сеть



## Show IP

PC1:

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

PC2:

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

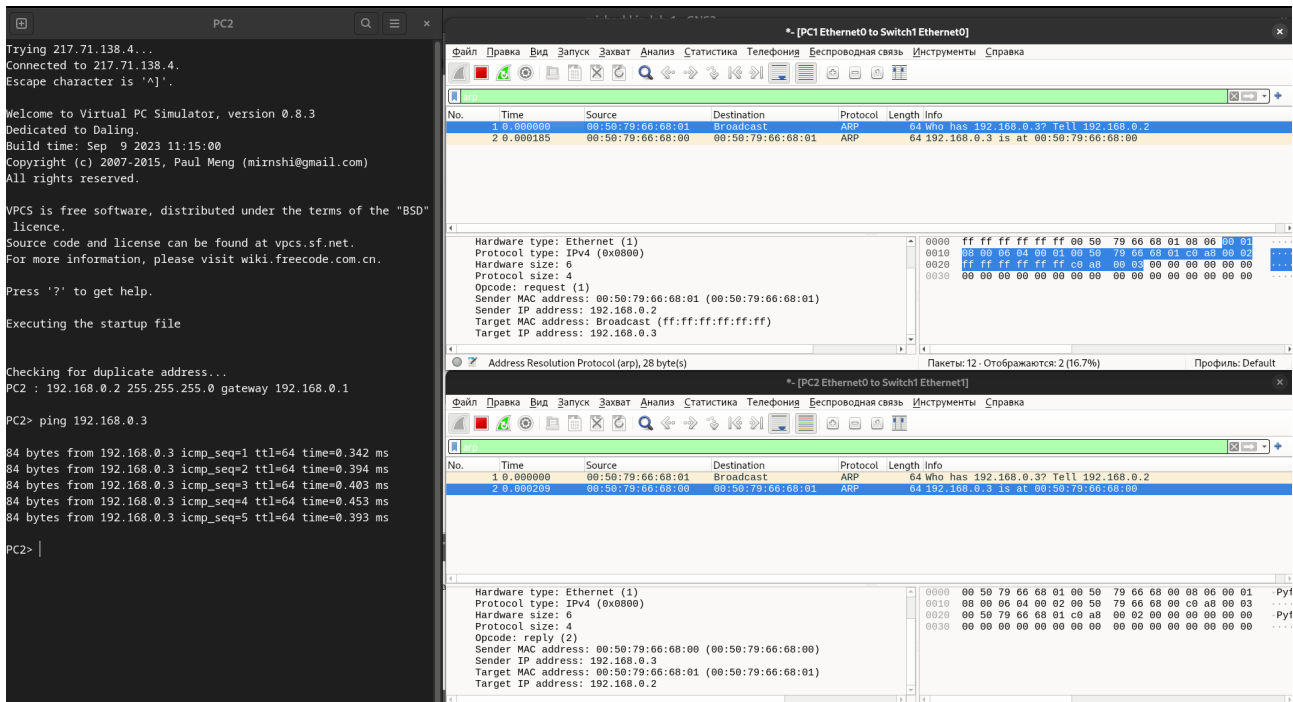
Поставил компьютерам одинаковую маску /24 (255.255.255.0) для того чтобы они находились в одной сети. Первый три октета определяют IP адрес сети, последний октет указывает на определенный хост в этой сети.

## Перехватить трафик протокола arp

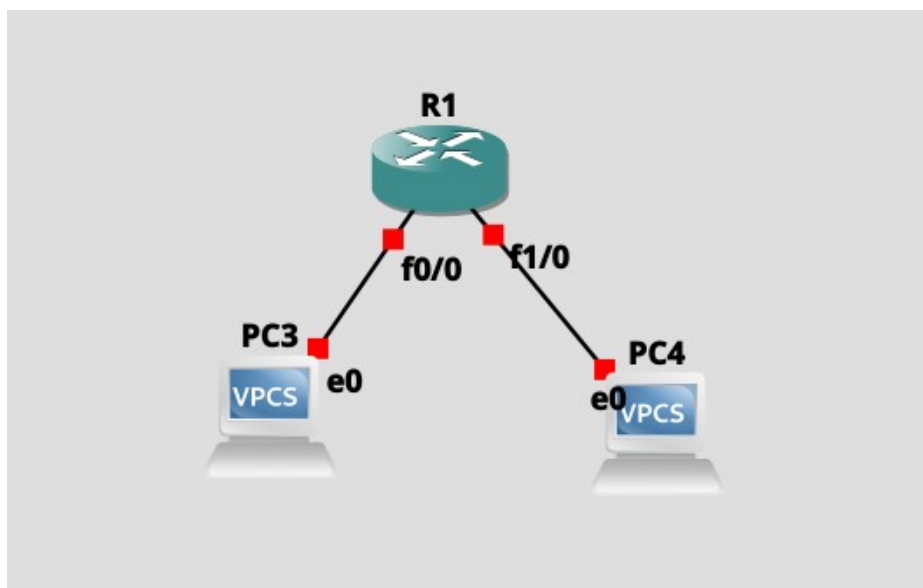
1) PC2 с MAC: 00:50:79:66:68:01 отправляет broadcast ARP запрос в заголовке которого указан MAC и IP самого отправителя, IP адрес хоста у которого мы хотим узнать MAC адрес.

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 тас адрес если его нет в ARP таблице он делает ARP запрос и после этого только отправляет icmp запрос. Маршрутизатор принимает этот запрос понимает в какую сеть нужно отправить с помощью таблицы маршрутизации и отправляет в нужную сеть.

The screenshot displays a network traffic capture in Wireshark, showing the interaction between a PC3 (192.168.1.1) and a router (192.168.2.2) during a ping operation. The capture is divided into two main sections: the top section shows the initial ARP request and reply, and the bottom section shows the subsequent ICMP echo request and reply.

**Top Section: ARP and ICMP Traffic**

No.	Time	Source	Destination	Protocol	Length	Info
38	323.455544	00:50:79:66:68:00	Broadcast	ARP	64	Who has 192.168.2.1? Tell 192.168.2.2
39	323.464081	cc:01:06:ec:00:00	00:50:79:66:68:00	ARP	60	192.168.2.1 is at cc:01:06:ec:00:00
40	323.465064	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) request id=0x98dd, seq=1/256, ttl=64 (reply in
41	323.494293	192.168.2.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0x98dd, seq=1/256, ttl=63 (request i
42	324.494781	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) request id=0x99dd, seq=2/512, ttl=64 (reply in
43	324.510483	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0x99dd, seq=2/512, ttl=63 (request i
44	325.510749	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) request id=0x9add, seq=3/768, ttl=64 (reply in
45	325.520531	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0x9add, seq=3/768, ttl=63 (request i
46	326.526747	192.168.2.2	192.168.1.2	TCP	98	Echo (ping) request id=0x9add, seq=3/768, ttl=64 (reply in

**Bottom Section: ICMP Traffic**

No.	Time	Source	Destination	Protocol	Length	Info
37	313.018101	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) request id=0x98dd, seq=1/256, ttl=63 (reply in
38	313.018202	00:50:79:66:68:02	Broadcast	ARP	64	Who has 192.168.1.1? Tell 192.168.1.2
39	313.020705	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0x98dd, seq=1/256, ttl=64 (request i
40	313.020785	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x99dd, seq=2/512, ttl=63 (request i
41	314.044350	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x99dd, seq=2/512, ttl=64 (request i
42	314.044425	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x9add, seq=3/768, ttl=63 (reply in
43	315.060392	192.168.2.2	192.168.1.2	ICMP	98	Echo (ping) reply id=0x9add, seq=3/768, ttl=64 (request i
44	315.060465	192.168.1.2	192.168.2.2	ICMP	98	Echo (ping) request id=0x9add, seq=3/768, ttl=64 (request i

The terminal on the left shows the PC3's command prompt with the following output:

```
PC3> ipconfig
Connected to 217.71.138.4...
Escape character is '^['.
ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=255 time=9.842 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=255 time=5.195 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=255 time=5.880 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=255 time=5.396 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=255 time=5.124 ms

PC3> arp
cc:01:06:ec:00:00 192.168.2.1 expires in 113 seconds
PC3> |
```