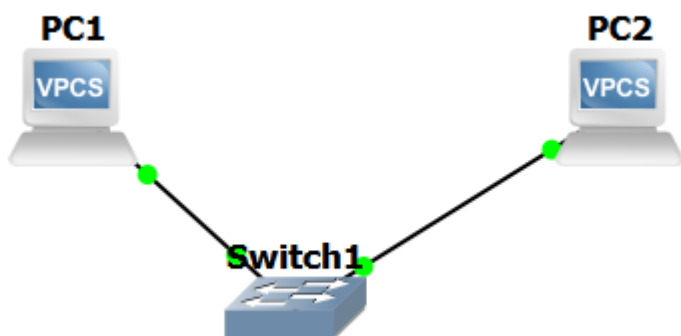


Лабораторная работа №1

Локальная сеть:



Show IP:

PC 1:

```
NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PORT
PC1       192.168.1.2/24  192.168.1.1  00:50:79:66:68:00  22286  127.0.0.1:22287
fe80::250:79ff:fe66:6800/64
```

PC 2:

```
NAME      IP/MASK      GATEWAY      MAC      LPORT  RHOST:PORT
PC2       192.168.1.3/24  192.168.1.1  00:50:79:66:68:01  22284  127.0.0.1:22285
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 IP адрес сети, последний октет указывает на определенный хост в этой сети.

Ping:

```
PC1> ping 192.168.1.3

84 bytes from 192.168.1.3 icmp_seq=1 ttl=64 time=0.139 ms
84 bytes from 192.168.1.3 icmp_seq=2 ttl=64 time=0.179 ms
84 bytes from 192.168.1.3 icmp_seq=3 ttl=64 time=0.210 ms
84 bytes from 192.168.1.3 icmp_seq=4 ttl=64 time=0.216 ms
84 bytes from 192.168.1.3 icmp_seq=5 ttl=64 time=0.174 ms
```

Перехватить трафик протокола arp:

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

The left screenshot shows a terminal window with the following output:

```
Welcome to Virtual PC Simulator, version 0.8.3
Dedicated to Galing.
Build time: Sep  9 2023 11:15:00
Copyright (c) 2007-2015, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1

PC1> ping 192.168.1.3

84 bytes from 192.168.1.3 icmp_seq=1 ttl=64 time=0.208 ms
84 bytes from 192.168.1.3 icmp_seq=2 ttl=64 time=0.132 ms
84 bytes from 192.168.1.3 icmp_seq=3 ttl=64 time=0.199 ms
84 bytes from 192.168.1.3 icmp_seq=4 ttl=64 time=0.208 ms
84 bytes from 192.168.1.3 icmp_seq=5 ttl=64 time=0.143 ms

PC1> arp
00:50:79:66:68:01 192.168.1.3 expires in 113 seconds

PC1> arp
00:50:79:66:68:01 192.168.1.3 expires in 70 seconds

PC1>
PC1> ping 192.168.1.3

84 bytes from 192.168.1.3 icmp_seq=1 ttl=64 time=0.147 ms
84 bytes from 192.168.1.3 icmp_seq=2 ttl=64 time=0.156 ms
84 bytes from 192.168.1.3 icmp_seq=3 ttl=64 time=0.169 ms
84 bytes from 192.168.1.3 icmp_seq=4 ttl=64 time=0.206 ms
84 bytes from 192.168.1.3 icmp_seq=5 ttl=64 time=0.139 ms

PC1>
```

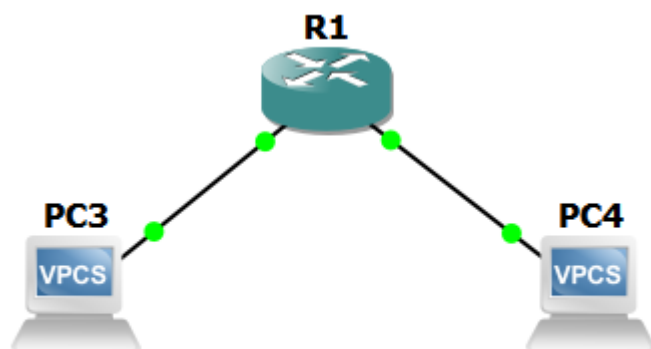
The right screenshot shows a packet capture window with the following table:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.3? [ttl 1]
2	0.000121	Private_66:68:01	Private_66:68:00	ARP	64	192.168.1.3 is at 00:50:79:66:68:00

Below the table, the packet details for Frame 1 are shown:

```
Frame 1: 64 bytes on wire (512 bits), 64 bytes captured on interface 0:00:00:00:00:00
Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: ff:ff:ff:ff:ff:ff (01:00:00:00:00:00)
Address Resolution Protocol (request)
```

Сеть маршрутизатора и 2 двух подсетей.



Конфигурация R1

#Назначаем IP - адрес на интерфейс f 0 / 0 R1(config)# int f0/0
#Указываем IP - адрес 192.168.2.1 с маской подсети 255.255.255.0

```
R1(config-if)# ip address 192.168.2.1 255.255.255.0
```

#Включаем интерфейс

```
R1(config-if)# no shut
```

```
R1(config-if)# exit #Назначаем IP - адрес на интерфейс f 1/0
```

```
R1(config)# int f1/0
```

#Указываем IP - адрес 192.168.1.1 с маской подсети 255.255.255.0

```
R1(config-if)# ip address 192.168.3.1 255.255.255.0
```

#Включаем интерфейс

```
R1(config-if)# no shut
```

```
R1(config-if)# exit
```

```
R1(config)# exit
```

Конфигурация PC3

```
#Назначаем IP - адрес 192.168.2.2 с маской подсети  
255.255.255.0 #Указываем шлюз по умолчанию  
192.168.2.1 PC3> ip 192.168.2.2/24 192.168.2.1
```

Конфигурация PC4

```
#Назначаем IP - адрес 192.168.1.2 с маской подсети  
255.255.255.0 #Указываем шлюз по умолчанию  
192.168.3.1 PC3> ip 192.168.3.2/24 192.168.3.1
```

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 принимая этот запрос понимает в какую сеть нужно отправить с помощью таблицы маршрутизации и отправляет в нужную сеть.

```

PC3 - PuTTY
PC3 : 192.168.2.2 255.255.255.0 gateway 192.168.2.1
PC3> ping 192.168.3.1
host (192.168.2.1) not reachable
PC3> enable
Bad command: "enable". Use ? for help.
PC3> arp
arp table is empty
PC3> show
NAME      IP/MASK      GATEWAY      MAC          IPORT  RHOST:PORT
PC3      192.168.2.2/24  192.168.2.1  00:50:79:66:68:02  22422  127.0.0.1:22423
fe80::250:79ff:fe66:6802/64
PC3> ping 192.168.3.2
host (192.168.2.1) not reachable
PC3> ping 192.168.3.2
host (192.168.2.1) not reachable
PC3> ping 192.168.3.2
192.168.3.2 icmp_seq=1 timeout
192.168.3.2 icmp_seq=2 timeout
84 bytes from 192.168.3.2 icmp_seq=3 ttl=63 time=19.499 ms
84 bytes from 192.168.3.2 icmp_seq=4 ttl=63 time=14.991 ms
84 bytes from 192.168.3.2 icmp_seq=5 ttl=63 time=14.680 ms
PC3> ping 192.168.3.2
84 bytes from 192.168.3.2 icmp_seq=1 ttl=63 time=16.138 ms
84 bytes from 192.168.3.2 icmp_seq=2 ttl=63 time=15.207 ms
84 bytes from 192.168.3.2 icmp_seq=3 ttl=63 time=14.510 ms
84 bytes from 192.168.3.2 icmp_seq=4 ttl=63 time=15.016 ms
84 bytes from 192.168.3.2 icmp_seq=5 ttl=63 time=14.871 ms
PC3> arp
cc:01:6c:6e:00:00 192.168.2.1 expires in 87 seconds
PC3>

```

Capturing from Standard input (R1 FastEthernet0/0 to PC3 Ethernet0)

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter: <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x0
2	0.016022	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0x0
3	1.017129	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x0
4	1.022133	cc:01:6c:6e:00:00	cc:01:6c:6e:00:00	LOOP	60	Reply
5	1.032228	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0x0
6	2.033109	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x0
7	2.047513	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0x0
8	3.048101	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x0
9	3.062997	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0x0
10	4.064839	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0x0
11	4.078795	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0x0

Frame 1: 98 bytes on wire (784 bits), 98 bytes captured on interface 0, 98 bytes from 192.168.2.2 to 192.168.3.2 on interface 0

Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: 01:00:00:00:00:00

Internet Protocol Version 4, Src: 192.168.2.2, Dst: 192.168.3.2

Internet Control Message Protocol

Standard input: <live capture in progress> Packets: 11 Profile: Default