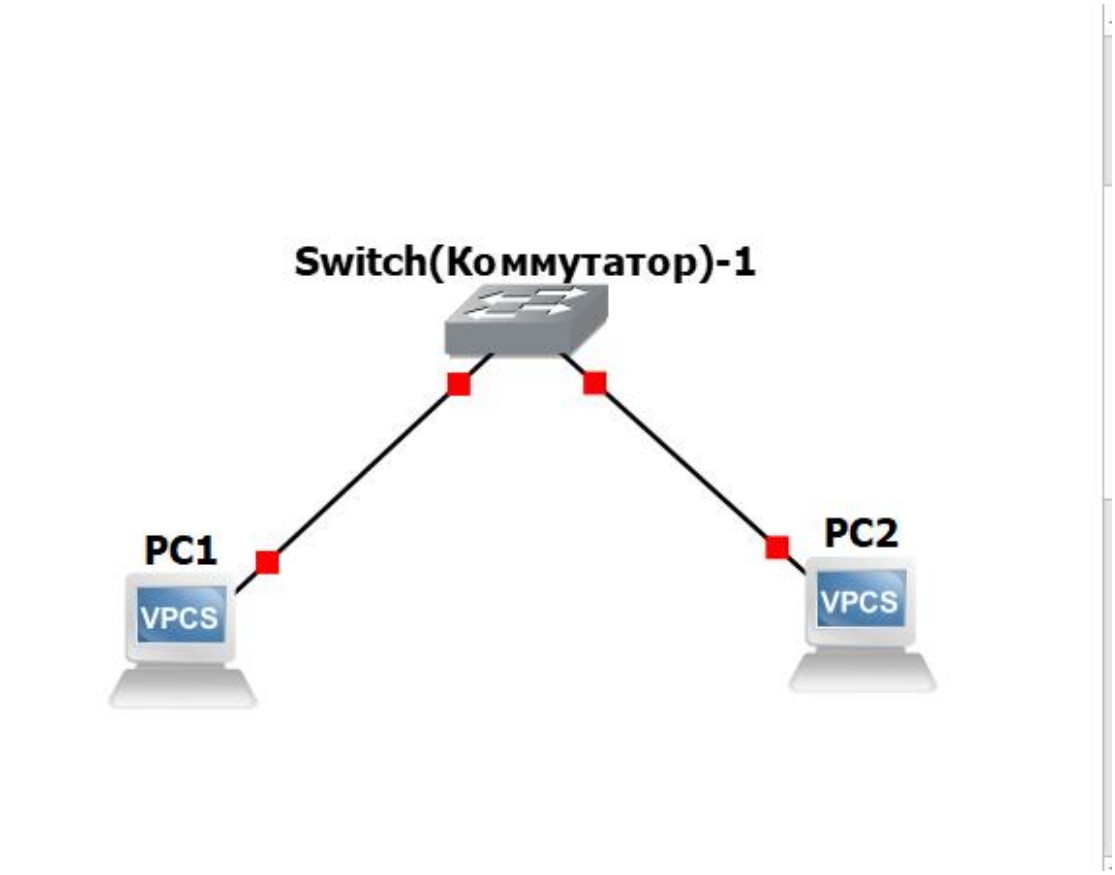
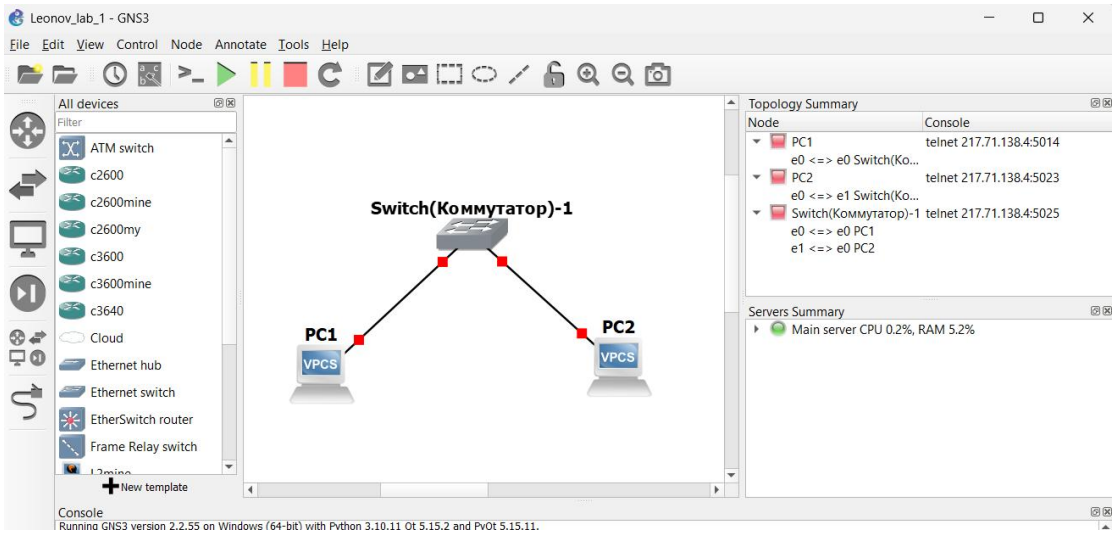
Добавление связей между ПК и Свичом





3) Запустить симуляцию, выполнить команду ping с одного из компьютеров, используя ip адрес второго компьютера

Правой кнопкой мыши -> console

```
PC1> show ip

NAME        : PC1[1]
IP/MASK     : 0.0.0.0/0
GATEWAY     : 0.0.0.0
DNS         :
MAC         : 00:50:79:66:68:01
LPORT       : 25265
RHOST:PORT  : 127.0.0.1:25266
MTU         : 1500
```

Адрес не настроен

На pc 1
ip 192.168.1.1/24

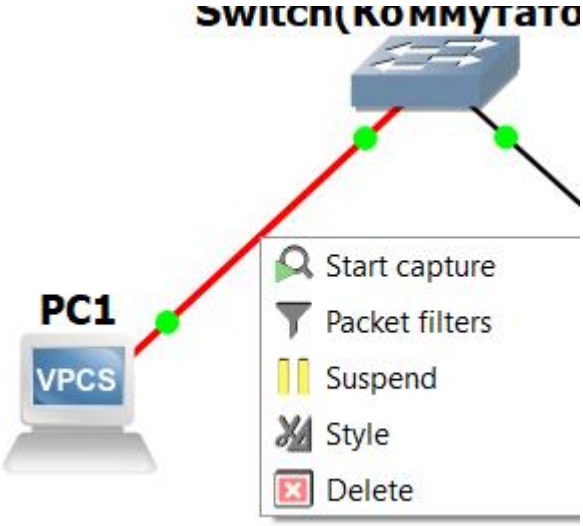
На pc 2
ip 192.168.1.2/24

Пингуем с пк 1:
ping 192.168.1.2

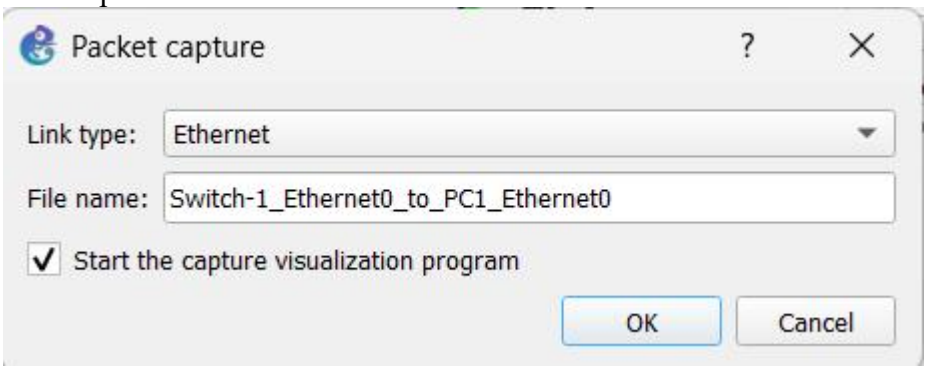
```
PC1> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=0.568 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=0.487 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=0.611 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=2.635 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=2.459 ms
```

4) Перехватить трафик протокола arp на всех линках(nb!), задокументировать и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark

clear arp (сбрасываем кэш, т.к. компы знают mac адреса друг друга)



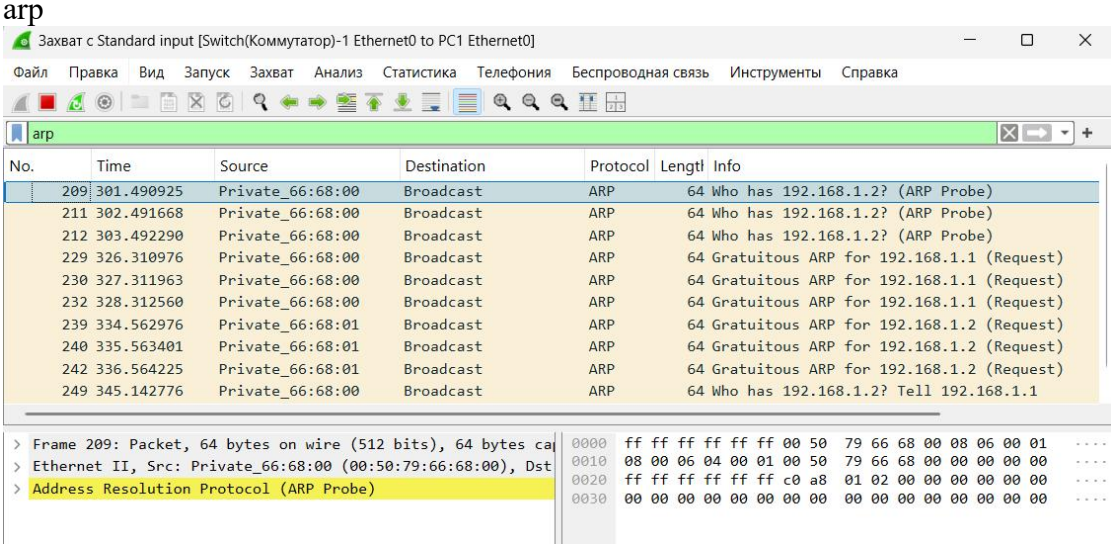
Start capture



Открывается wireshark

Выполняю на pc 1
ping 192.168.1.2

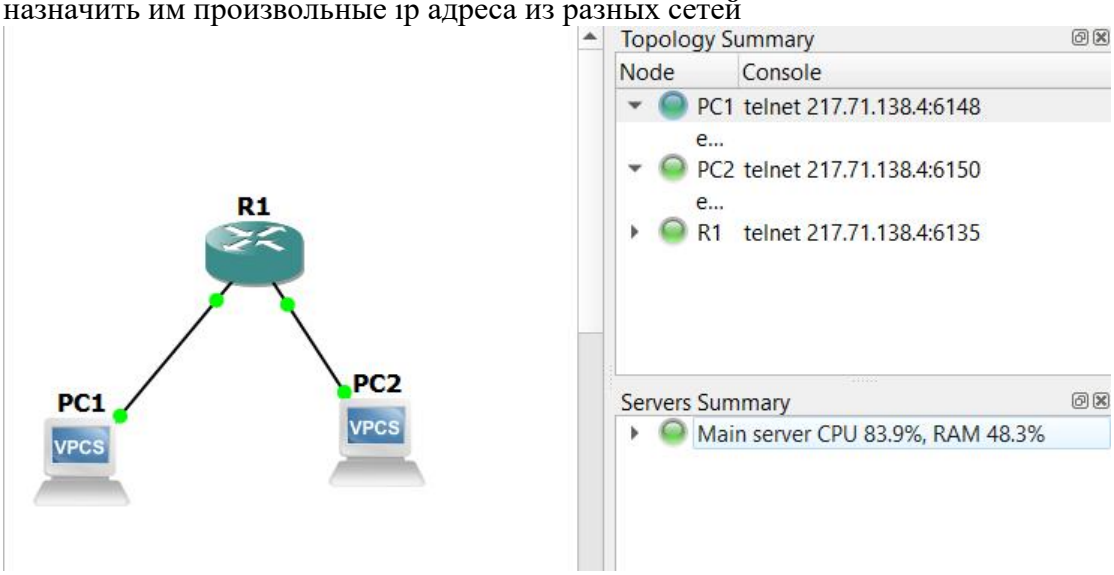
В верхней строке (строка фильтра):
arp



```
> Frame 209: Packet, 64 bytes on wire (512 bits), 64 bytes ca
v Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst
  > Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  > Source: Private_66:68:00 (00:50:79:66:68:00)
    Type: ARP (0x0806)
    [Stream index: 4]
    Padding: 000000000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
> Address Resolution Protocol (ARP Probe)
```

```
Address Resolution Protocol (ARP Probe)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  [Is probe: True]
  Sender MAC address: Private_66:68:00 (00:50:79:66:68:00)
  Sender IP address: 0.0.0.0
> Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
  Target IP address: 192.168.1.2
```

5) Создать простейшую сеть, состоящую из 1 маршрутизатора и 2 компьютеров, назначить им произвольные ip адреса из разных сетей



IP-адрес, затем Шлюз, затем маска
Pc 1 :
ip 192.168.10.2 192.168.10.1 24
Pc 2:
ip 192.168.20.2 192.168.20.1 24

Настройка роутера:
enable ! Переход в привилегированный режим
configure terminal ! Переход в режим конфигурации

! Настройка ЛЕВОГО интерфейса (смотрящего на PC1)
interface FastEthernet0/0 ! Введите имя вашего порта (f0/0, g0/0, e0/0)
ip address 192.168.10.1 255.255.255.0
no shutdown ! ВАЖНО: Включить интерфейс
exit

! Настройка ПРАВОГО интерфейса (смотрящего на PC2)
interface FastEthernet1/0 ! Введите имя второго порта
ip address 192.168.20.1 255.255.255.0
no shutdown ! Включить интерфейс
exit

6) Запустить симуляцию, выполнить команду ping с одного из компьютеров, используя ip адрес второго компьютера

Пинг с pc 1 на pc 2

```
PC1 : 192.168.10.2 255.255.255.0 gateway 192.168.10.1

PC1> ping 192.168.10.1

84 bytes from 192.168.10.1 icmp_seq=1 ttl=255 time=9.291 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=255 time=6.496 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=255 time=4.874 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=255 time=6.073 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=255 time=6.287 ms

PC1> ping 192.168.20.2

192.168.20.2 icmp_seq=1 timeout
84 bytes from 192.168.20.2 icmp_seq=2 ttl=63 time=12.914 ms
84 bytes from 192.168.20.2 icmp_seq=3 ttl=63 time=15.291 ms
84 bytes from 192.168.20.2 icmp_seq=4 ttl=63 time=16.132 ms
84 bytes from 192.168.20.2 icmp_seq=5 ttl=63 time=16.169 ms

PC1>
```

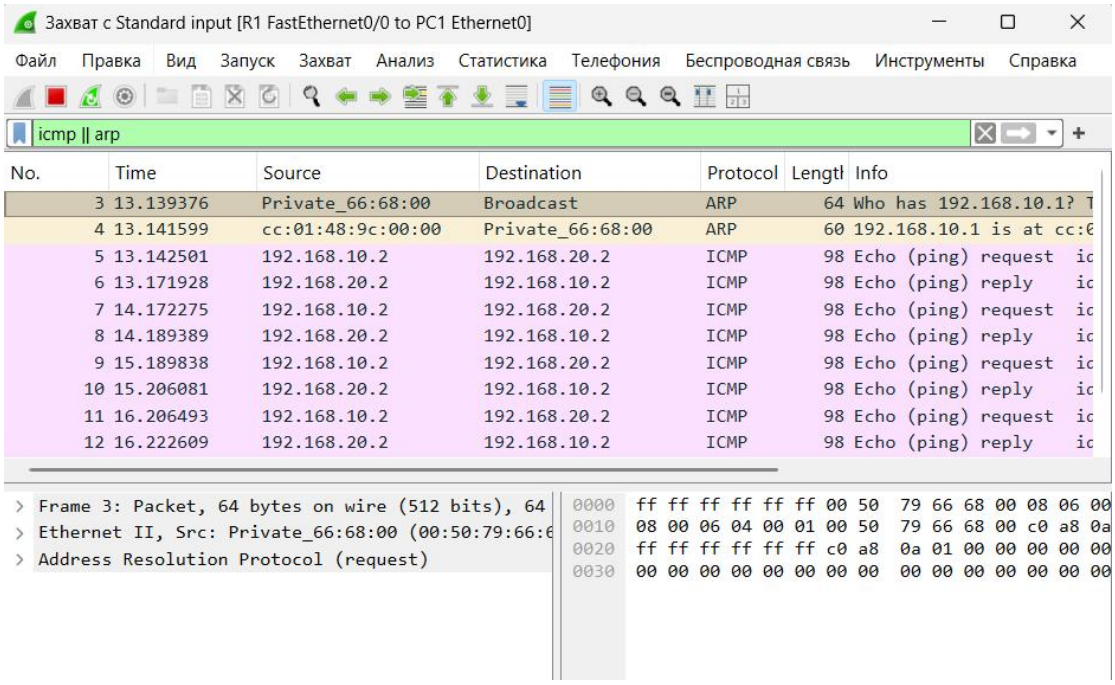
Пинг с pc 2 на pc 1:

```
PC2 : 192.168.20.2 255.255.255.0 gateway 192.168.20.1

PC2> ping 192.168.20.1

84 bytes from 192.168.20.1 icmp_seq=1 ttl=255 time=1.020 ms
84 bytes from 192.168.20.1 icmp_seq=2 ttl=255 time=5.797 ms
84 bytes from 192.168.20.1 icmp_seq=3 ttl=255 time=6.302 ms
84 bytes from 192.168.20.1 icmp_seq=4 ttl=255 time=6.992 ms
84 bytes from 192.168.20.1 icmp_seq=5 ttl=255 time=6.551 ms

PC2> ping 192.168.10.2

84 bytes from 192.168.10.2 icmp_seq=1 ttl=63 time=20.136 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=63 time=16.671 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=63 time=16.924 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=63 time=16.381 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=63 time=16.295 ms

PC2>
```

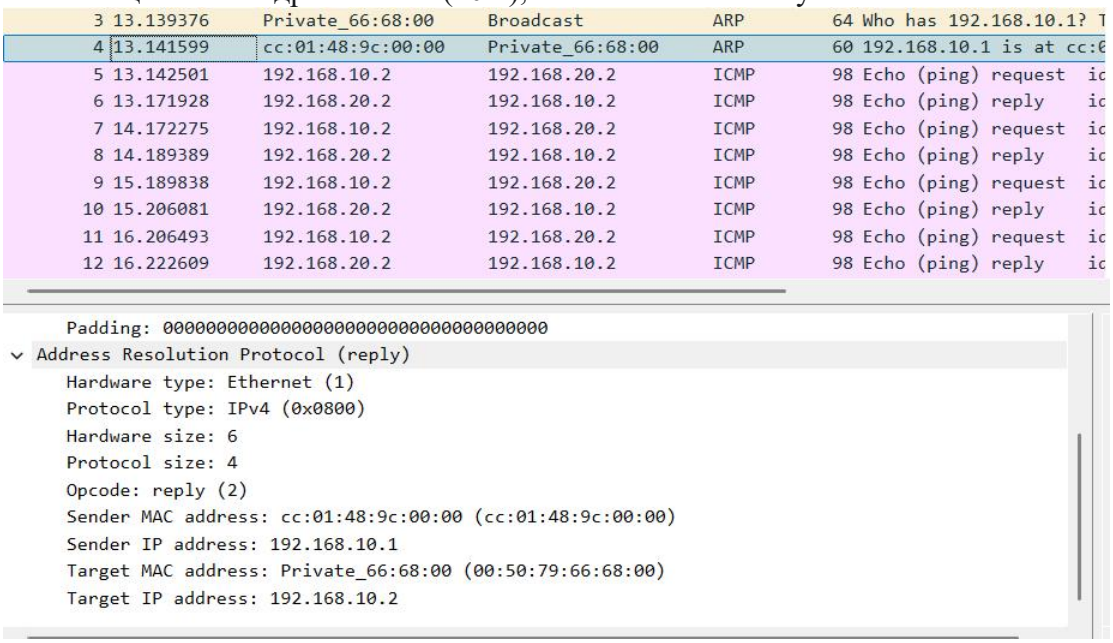
7) Перехватить трафик протокола arp и icmp на всех линках(nb!), задокументировать и проанализировать заголовки пакетов в программе Wireshark, для фильтрации трафика, относящегося к указанному протоколу использовать фильтры Wireshark

На обоих пк:
clear arp

На пк 1:
ping 192.168.20.2



1. PC1 ищет MAC-адрес шлюза (10.1), а не конечного получателя.

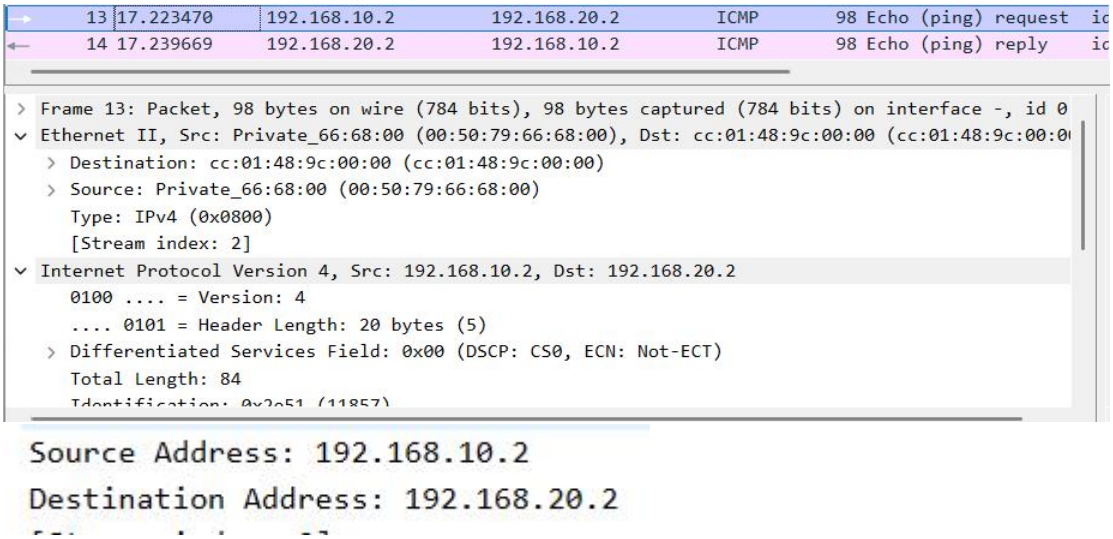


3	13.139376	Private_66:68:00	Broadcast	ARP	64 Who has 192.168.10.1? T
4	13.141599	cc:01:48:9c:00:00	Private_66:68:00	ARP	60 192.168.10.1 is at cc:0
5	13.142501	192.168.10.2	192.168.20.2	ICMP	98 Echo (ping) request id
6	13.171928	192.168.20.2	192.168.10.2	ICMP	98 Echo (ping) reply id
7	14.172275	192.168.10.2	192.168.20.2	ICMP	98 Echo (ping) request id
8	14.189389	192.168.20.2	192.168.10.2	ICMP	98 Echo (ping) reply id
9	15.189838	192.168.10.2	192.168.20.2	ICMP	98 Echo (ping) request id
10	15.206081	192.168.20.2	192.168.10.2	ICMP	98 Echo (ping) reply id
11	16.206493	192.168.10.2	192.168.20.2	ICMP	98 Echo (ping) request id
12	16.222609	192.168.20.2	192.168.10.2	ICMP	98 Echo (ping) reply id

```
    Padding: 00000000000000000000000000000000
Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: cc:01:48:9c:00:00 (cc:01:48:9c:00:00)
    Sender IP address: 192.168.10.1
    Target MAC address: Private_66:68:00 (00:50:79:66:68:00)
    Target IP address: 192.168.10.2
```

Нашел mac-адрес шлюза

2. ICMP Request



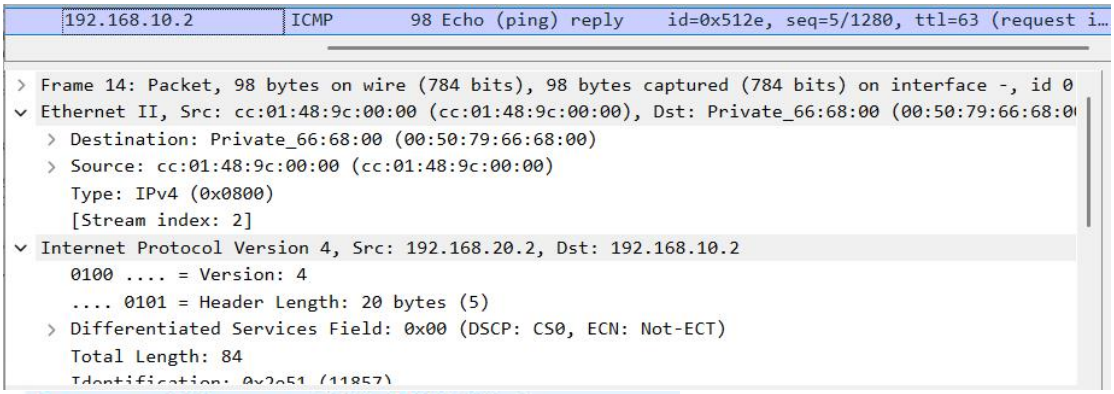
13	17.223470	192.168.10.2	192.168.20.2	ICMP	98 Echo (ping) request id
14	17.239669	192.168.20.2	192.168.10.2	ICMP	98 Echo (ping) reply id

```
> Frame 13: Packet, 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
v Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: cc:01:48:9c:00:00 (cc:01:48:9c:00:0
  > Destination: cc:01:48:9c:00:00 (cc:01:48:9c:00:00)
  > Source: Private_66:68:00 (00:50:79:66:68:00)
    Type: IPv4 (0x0800)
    [Stream index: 2]
v Internet Protocol Version 4, Src: 192.168.10.2, Dst: 192.168.20.2
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x2e51 (11857)
```

```
Source Address: 192.168.10.2
Destination Address: 192.168.20.2
```

Time to live (TTL) = 64

3. ICMP Reply



Source Address: 192.168.20.2

Destination Address: 192.168.10.2

Time to live (TTL) = 63

Ответ пришел от далекого PC2, но физически провод, по которому он прилетел к PC1, подключен к Роутеру. Поэтому отправителем на уровне "железа" (MAC) числится Роутер.