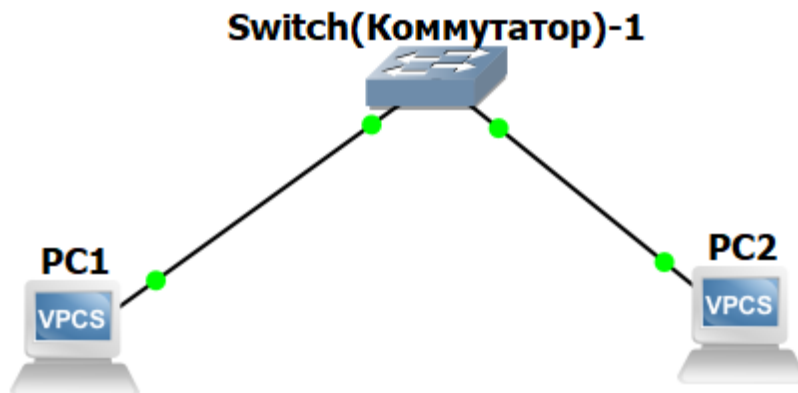


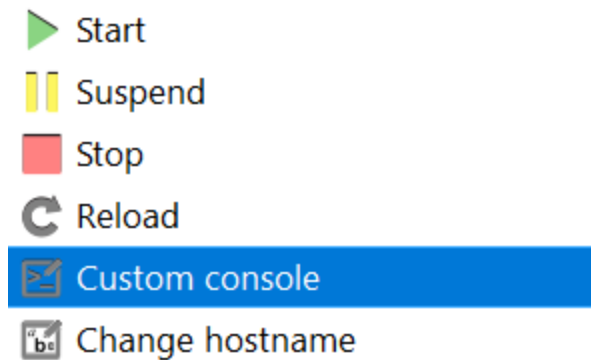
Лабораторная работа №1

Тема: Освоение инструментария для выполнения работ, построение простой сети

- 1) Устанавливаем и настраиваем эмулятор GNS3.
- 2) Создаём простейшую сеть, состоящую из 1 коммутатора и 2 компьютеров.



2.1) Назначаем им произвольные ip адреса из одной сети. Для этого кликаем по PC1 и выбираем Custom console. Для PC2 аналогично.



2.3) Пишем команды:

Для PC 1: *ip 192.168.0.1/24*

Для PC 2: *ip 192.168.0.2/24*

3) Запускаем симуляцию, выполняем команду ping с одного из компьютеров, используя ip адрес второго компьютера

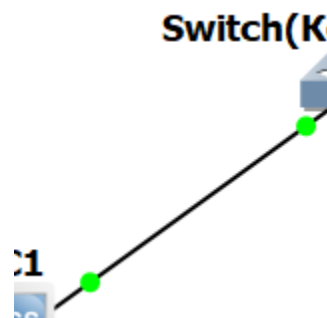
Пишем с PC1 *ping 192.168.0.2*

```
PC1> ping 192.168.0.2

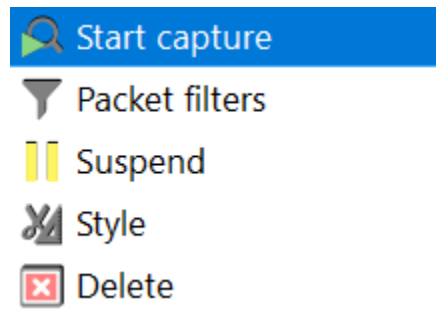
84 bytes from 192.168.0.2: icmp_seq=1 ttl=64 time=7.384 ms
84 bytes from 192.168.0.2: icmp_seq=2 ttl=64 time=6.713 ms
84 bytes from 192.168.0.2: icmp_seq=3 ttl=64 time=8.109 ms
84 bytes from 192.168.0.2: icmp_seq=4 ttl=64 time=4.383 ms
84 bytes from 192.168.0.2: icmp_seq=5 ttl=64 time=1.718 ms
```

4) Перехватим трафик протокола arp на всех линках, проанализируем заголовки пакетов в программе Wireshark.

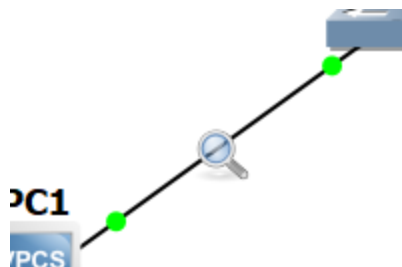
4.1) Открываем Wireshark между PC1 и коммутатором. Для этого кликаем по каналу между PC1 и коммутатором.



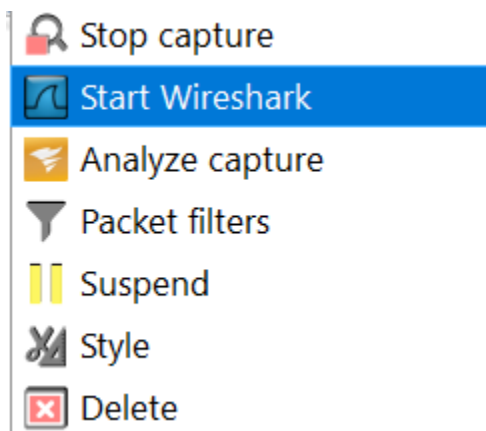
4.2) Выбираем Start capture.



4.3) На канале появляется значок лупы.



4.4) Снова кликаем на канал и жмём Start Wireshark. Для канала между PC2 и коммутатором аналогично.



4.5) Ещё раз пропируем, чтобы Wireshark захватил нужные пакеты.

```
PC1> ping 192.168.0.2
84 bytes from 192.168.0.2 icmp_seq=1 ttl=64 time=7.301 ms
84 bytes from 192.168.0.2 icmp_seq=2 ttl=64 time=0.660 ms
84 bytes from 192.168.0.2 icmp_seq=3 ttl=64 time=14.412 ms
84 bytes from 192.168.0.2 icmp_seq=4 ttl=64 time=0.806 ms
84 bytes from 192.168.0.2 icmp_seq=5 ttl=64 time=5.821 ms
```

4.6) Пойманные ARP PC1. Разберём подробнее:

441: PC1 спрашивает всех (широковещательная рассылка), кто имеет IP-адрес 192.168.0.2 (IP-адрес PC2), и ждёт ответа.

442: PC1 получил ответ от IP-адреса 192.168.0.2 – MAC-адрес 192.168.0.2.

Захват с Standard input [PC1 Ethernet0 to Switch(Коммутатор)-1 Ethernet0]

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

arp

No.	Time	Source	Destination	Protocol	Length	Info
441	636.005618	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.0.2? Tell 192.168.0.1
442	636.011301	Private_66:68:01	Private_66:68:00	ARP	64	192.168.0.2 is at 00:50:79:66:68:01

4.7) Пойманные ARP PC2. Разберём подробнее:

314: PC2 получил сообщение, в котором ждут ответа от устройства с его IP-адресом (то есть, от него).

315: PC2 отправляет ответ. Однако если вопрос PC1 отправлял широковещательной рассылкой, так как не знал, где находится PC2, то PC2 знает, от кого пришло сообщение, и, соответственно, отправляет ответ со своим MAC-адресом именно на этот адрес.

Захват с Standard input [PC2 Ethernet0 to Switch(Коммутатор)-1 Ethernet1]

Файл Правка Вид Запуск Захват Анализ Статистика Телефония Беспроводная связь Инструменты Справка

arp

No.	Time	Source	Destination	Protocol	Length	Info
314	452.033674	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.0.2? Tell 192.168.0.1
315	452.033772	Private_66:68:01	Private_66:68:00	ARP	64	192.168.0.2 is at 00:50:79:66:68:01

4.8) Более подробный вид пакета 441 номера PC1 (ARP-запрос). Здесь дата и время, когда этот пакет был получен (Arrival Time и UTC Arrival Time), номер пакета (Frame Number), длина пакета (Frame Length).

Ниже указан адрес отправления (Destination). Как видим указана широковещательная рассылка, так как PC1 не знает MAC-адрес PC2.

В адресе источника (Source) указан PC1.

Тип протокола (Type) – ARP.

Ниже (Address Resolution Protocol) указано, что для пересылки используется Ethernet, IPv4, MAC-адрес и IP-адрес источника – MAC-адрес и IP-адрес PC1, IP-адрес отправления – IP-адрес PC2 и MAC-адрес отправления – широковещательная рассылка.

```
▼ Frame 441: Packet, 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
    Section number: 1
    ▶ Interface id: 0 (-)
        Encapsulation type: Ethernet (1)
        Arrival Time: Dec  4, 2025 16:50:07.652778000 Новосибирское стандартное время
        UTC Arrival Time: Dec  4, 2025 09:50:07.652778000 UTC
        Epoch Arrival Time: 1764841807.652778000
        [Time shift for this packet: 0.000000000 seconds]
        [Time delta from previous captured frame: 102.307000 milliseconds]
        [Time since reference or first frame: 10 minutes, 36.005618000 seconds]
        Frame Number: 441
        Frame Length: 64 bytes (512 bits)
        Capture Length: 64 bytes (512 bits)
        [Frame is marked: False]
        [Frame is ignored: False]
        [Protocols in frame: eth:ethertype:arp]
        Character encoding: ASCII (0)
        [Coloring Rule Name: ARP]
        [Coloring Rule String: arp]
▼ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
    ▶ 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: 000000000000000000000000000000000000000000000000
        Frame check sequence: 0x00000000 [unverified]
        [FCS Status: Unverified]
▼ Address Resolution Protocol (request)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    Sender MAC address: Private_66:68:00 (00:50:79:66:68:00)
    Sender IP address: 192.168.0.1
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.0.2
```

4.9) Остальные пакеты ARP схожи, поэтому разберём только их различия. Рассмотрим 442 номер PC1 (ARP-ответ).

```

▼ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)
  ► Destination: Private_66:68:00 (00:50:79:66:68:00)
  ► Source: Private_66:68:01 (00:50:79:66:68:01)
    Type: ARP (0x0806)
    [Stream index: 5]
    Padding: 000000000000000000000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Private_66:68:01 (00:50:79:66:68:01)
  Sender IP address: 192.168.0.2
  Target MAC address: Private_66:68:00 (00:50:79:66:68:00)

```

Теперь MAC-адрес отправления принадлежит PC1, а MAC-адрес источника – PC2. IP-адрес источника так же принадлежит PC2.

4.10) 314 пакет PC2.

```
▼ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ▶ Source: Private_66:68:00 (00:50:79:66:68:00)
    Type: ARP (0x0806)
    [Stream index: 3]
    Padding: 00000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Private_66:68:00 (00:50:79:66:68:00)
  Sender IP address: 192.168.0.1
  Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
  Target IP address: 192.168.0.2
```

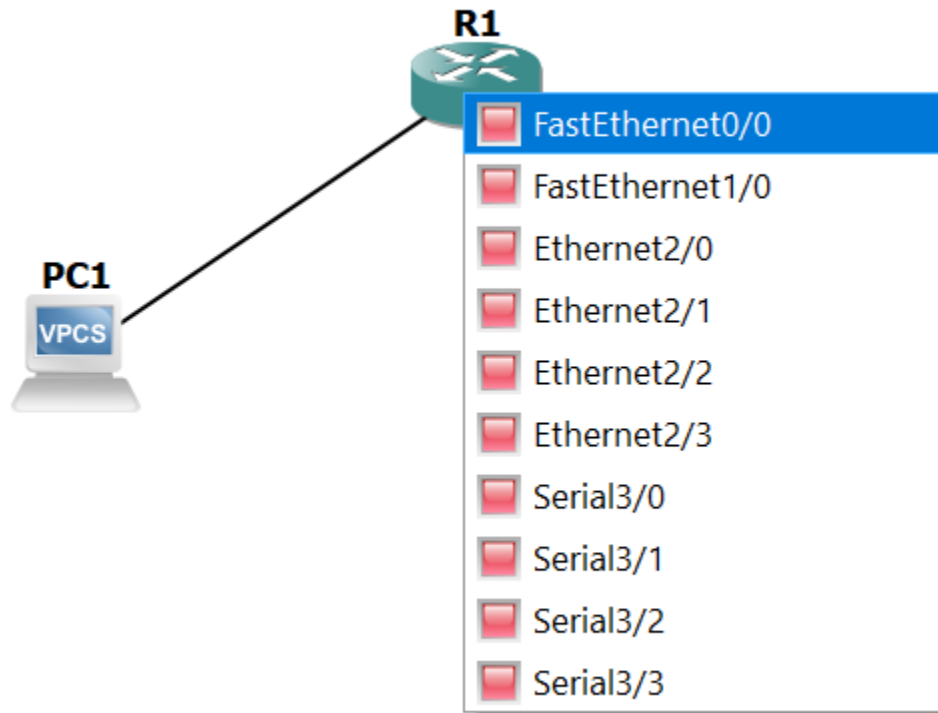
MAC-адрес отправления – широковещательная рассылка. IP-адрес источника – 192.168.0.1 (PC1). IP-адрес отправления – 192.168.0.2 (PC2).

4.11) 315 пакет PC2.

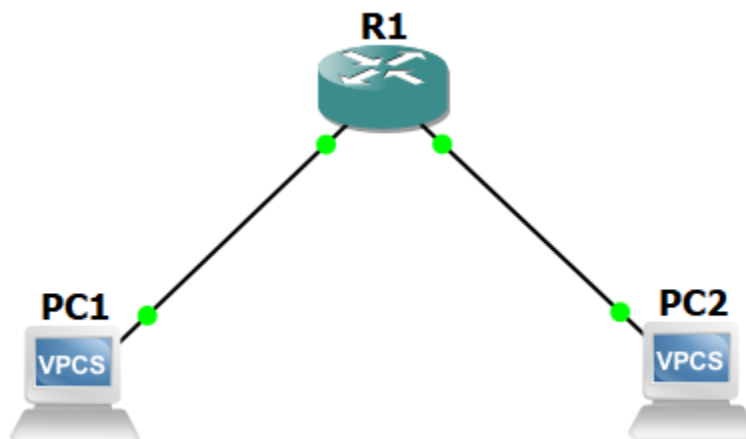
```
▼ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)
  ▶ Destination: Private_66:68:00 (00:50:79:66:68:00)
  ▶ Source: Private_66:68:01 (00:50:79:66:68:01)
    Type: ARP (0x0806)
    [Stream index: 4]
    Padding: 00000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
▼ Address Resolution Protocol (reply)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: reply (2)
  Sender MAC address: Private_66:68:01 (00:50:79:66:68:01)
  Sender IP address: 192.168.0.2
  Target MAC address: Private_66:68:00 (00:50:79:66:68:00)
  Target IP address: 192.168.0.1
```

MAC-адрес отправления – MAC-адрес PC1. MAC-адрес источника – PC2. IP-адрес источника – 192.168.0.2 (PC2). IP-адрес отправителя – 192.168.0.1 (PC1).

5) Создаём простейшую сеть, состоящую из 1 маршрутизатора и 2 компьютеров, соединяем PC1 с R1 с помощью FastEthernet 0/0. PC2 – FastEthernet 1/0 соответственно.



Получившаяся сеть:



5.1) Настраиваем маршрутизатор. Используем данные команды:

Заходим в режим конфигурации: *config terminal*

Заходим на интерфейс, к которому подключён PC1: *int FastEthernet 0/0*

Назначаем этому интерфейсу IP-адрес: *ip address 192.168.1.1 255.255.255.0*

Выходим: *no shutdown*

exit

Заходим на интерфейс, к которому подключён PC2: *int FastEthernet 1/0*

Назначаем этому интерфейсу IP-адрес: *ip address 192.168.2.1 255.255.255.0*

Выходим: *no shutdown*

exit

```
R1#confug
Translating "confug"

Translating "confug"
% Unknown command or computer name, or unable to find computer address
R1#config
Configuring from terminal, memory, or network [terminal]? terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#int FastEthernet 0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar 1 00:01:54.515: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to up
*Mar 1 00:01:55.515: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
R1(config)#int FastEthernet 1/0
R1(config-if)#ip address 192.168.2.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#
*Mar 1 00:03:01.639: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar 1 00:03:02.639: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R1(config)#ip routing
R1(config)#end
```

5.2) Назначаем PC1 и PC2 произвольные ip адреса из разных сетей. Пишем команды:

Для PC 1: *ip 192.168.1.10/24 192.168.1.1*

```
PC1> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.10 255.255.255.0 gateway 192.168.1.1
```

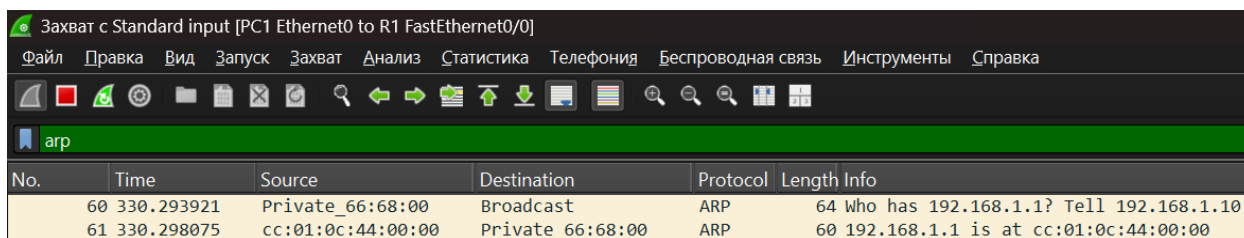
Для PC 2: *ip 192.168.2.20/24 192.168.2.1*


```
PC2> ip 192.168.2.20/24 192.168.2.1
Checking for duplicate address...
PC2 : 192.168.2.20 255.255.255.0 gateway 192.168.2.1
```

6) Запускаем симуляцию, выполняем команду с PC1: *ping 192.168.2.20*

7) Перехватим трафик протоколов на всех линках, проанализируем заголовки пакетов в программе Wireshark.

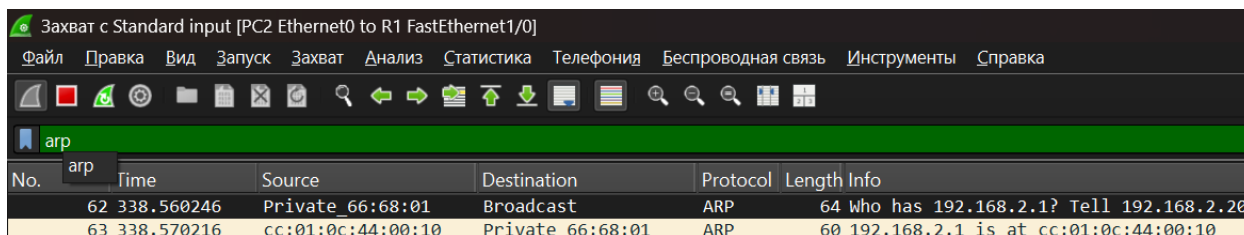
7.1) Протоколы ARP на PC1.



No.	Time	Source	Destination	Protocol	Length	Info
60	330.293921	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.1? Tell 192.168.1.10
61	330.298075	cc:01:0c:44:00:00	Private_66:68:00	ARP	60	192.168.1.1 is at cc:01:0c:44:00:00

Казалось бы, мы пинговали PC2, который имеет IP-адрес 192.168.2.20, а в ARP-запросе PC1 спрашивает 192.168.1.1 – IP-адрес интерфейса маршрутизатора, к которому подключён. Дело в том, что так как PC1 и PC2 находятся в разных сетях, то PC1 отправляет свой запрос маршрутизатору, который связывает его с другими сетями. Соответственно, так как PC1 и PC2 находятся в разных сетях, то и ответ PC1 получит не от PC2, как в предыдущем случае, а от маршрутизатора, что мы и видим в информации 61 пакета.

7.2) Протоколы ARP на PC2.



No.	Time	Source	Destination	Protocol	Length	Info
62	338.560246	Private_66:68:01	Broadcast	ARP	64	Who has 192.168.2.1? Tell 192.168.2.20
63	338.570216	cc:01:0c:44:00:10	Private_66:68:01	ARP	60	192.168.2.1 is at cc:01:0c:44:00:10

Так как PC1 и PC2 находятся в разных сетях, то напрямую ARP-запрос PC2 (и любое оконечное устройство другой сети) от PC1 получить не может. PC2 получает ARP-запрос от PC1 с помощью маршрутизатора. Маршрутизатор получил на свой интерфейс с IP-адресом 192.168.1.1 ARP-запрос и передал

его по всем остальным своим интерфейсам (широковещательная рассылка), среди которых оказался интерфейс с IP-адресом 192.168.2.1, к которому подключён PC2. Соответственно, PC2 отправляет свой MAC-адрес обратно интерфейсу маршрутизатора, из которого к нему пришёл запрос.

7.3) Более подробная информация о пакете 60 PC1.

```
▼ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ▸ 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: 00000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Private_66:68:00 (00:50:79:66:68:00)
  Sender IP address: 192.168.1.10
  Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
  Target IP address: 192.168.1.1
```

MAC-адрес отправления – широковещательная рассылка. MAC-адрес источника – PC1. IP-адрес источника – 192.168.1.10 (PC1). IP-адрес отправления – 192.168.1.1 (интерфейс FastEthernet 0/0 маршрутизатора).

7.4) Более подробная информация о пакете 61 PC1.

```
▼ Ethernet II, Src: cc:01:0c:44:00:00 (cc:01:0c:44:00:00), Dst: Private_66:68:00 (00:50:79:66:68:00)
  ▸ Destination: Private_66:68:00 (00:50:79:66:68:00)
  ▸ Source: cc:01:0c:44:00:00 (cc:01:0c:44:00:00)
    Type: ARP (0x0806)
    [Stream index: 2]
    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:01:0c:44:00:00 (cc:01:0c:44:00:00)
  Sender IP address: 192.168.1.1
  Target MAC address: Private_66:68:00 (00:50:79:66:68:00)
  Target IP address: 192.168.1.10
```

MAC-адрес отправления – PC1. MAC-адрес источника – PC2. IP-адрес источника – 192.168.1.1 (интерфейс FastEthernet 0/0 маршрутизатора). IP-адрес отправления – 192.168.1.10 (PC1).

7.5) Более подробная информация о пакете 62 РС2.

```

▼ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
  ↳ Destination: Broadcast (ff:ff:ff:ff:ff:ff)
  ↳ Source: Private_66:68:01 (00:50:79:66:68:01)
    Type: ARP (0x0806)
    [Stream index: 4]
    Padding: 0000000000000000000000000000000000000000000000000000000000000000
    Frame check sequence: 0x00000000 [unverified]
    [FCS Status: Unverified]
▼ Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Private_66:68:01 (00:50:79:66:68:01)
  Sender IP address: 192.168.2.20
  Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
  Target IP address: 192.168.2.1

```

MAC-адрес отправления – широковещательная рассылка. MAC-адрес источника – PC1. IP-адрес источника – 192.168.2.20 (PC2). IP-адрес отправления – 192.168.2.1 (интерфейс FastEthernet 1/0 маршрутизатора).

7.6) Более подробная информация о пакете 62 РС2.

```
▼ Ethernet II, Src: cc:01:0c:44:00:10 (cc:01:0c:44:00:10), Dst: Private_66:68:01 (00:50:79:66:68:01)
    ▶ Destination: Private_66:68:01 (00:50:79:66:68:01)
    ▶ Source: cc:01:0c:44:00:10 (cc:01:0c:44:00:10)
      Type: ARP (0x0806)
      [Stream index: 2]
      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:01:0c:44:00:10 (cc:01:0c:44:00:10)
    Sender IP address: 192.168.2.1
    Target MAC address: Private_66:68:01 (00:50:79:66:68:01)
    Target IP address: 192.168.2.20
```

MAC-адрес отправления – PC1. MAC-адрес источника – PC2. IP-адрес источника – 192.168.2.1 (интерфейс FastEthernet 1/0 маршрутизатора). IP-адрес отправления – 192.168.2.20 (PC2).

7.7) Протоколы ICMP на PC1.

271	1403.273079	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x3d6d, seq=1/256, ttl=64 (reply in 273)
273	1403.302574	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x3d6d, seq=1/256, ttl=63 (request in 271)
274	1404.302955	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x3e6d, seq=2/512, ttl=64 (reply in 275)
275	1404.319077	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x3e6d, seq=2/512, ttl=63 (request in 274)
276	1405.320053	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x3f6d, seq=3/768, ttl=64 (reply in 277)
277	1405.335302	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x3f6d, seq=3/768, ttl=63 (request in 276)
278	1406.336108	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x416d, seq=4/1024, ttl=64 (reply in 279)
279	1406.351834	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x416d, seq=4/1024, ttl=63 (request in 278)
280	1407.352149	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x426d, seq=5/1280, ttl=64 (reply in 281)
281	1407.368633	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x426d, seq=5/1280, ttl=63 (request in 280)

ICMP-запрос от PC1 (с которого пинговали) PC2. На него ICMP-ответ от PC2.

7.8) Протоколы ICMP на PC2.

259	1396.811481	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x3d6d, seq=1/256, ttl=63 (reply in 262)
262	1396.822245	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x3d6d, seq=1/256, ttl=64 (request in 259)
264	1397.838070	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x3e6d, seq=2/512, ttl=63 (reply in 265)
265	1397.838162	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x3e6d, seq=2/512, ttl=64 (request in 264)
266	1398.854273	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x3f6d, seq=3/768, ttl=63 (reply in 267)
267	1398.854389	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x3f6d, seq=3/768, ttl=64 (request in 266)
268	1399.870818	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x416d, seq=4/1024, ttl=63 (reply in 269)
269	1399.870910	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x416d, seq=4/1024, ttl=64 (request in 268)
270	1400.887598	192.168.1.10	192.168.2.20	ICMP	98 Echo (ping) request	id=0x426d, seq=5/1280, ttl=63 (reply in 271)
271	1400.887672	192.168.2.20	192.168.1.10	ICMP	98 Echo (ping) reply	id=0x426d, seq=5/1280, ttl=64 (request in 270)

7.9) Более подробный вид пакета ICMP-request от PC1.

```
▼ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: cc:01:0c:44:00:00 (cc:01:0c:44:00:00)
  ▶ Destination: cc:01:0c:44:00:00 (cc:01:0c:44:00:00)
  ▶ Source: Private_66:68:00 (00:50:79:66:68:00)
  Type: IPv4 (0x0800)
  [Stream index: 2]
▼ Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.2.20
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▶ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x6d3d (27965)
  ▶ 0000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0x88fd [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.10
  Destination Address: 192.168.2.20
  [Stream index: 0]
```

MAC-адрес отправления – PC2. MAC-адрес источника – PC1. IP-адрес источника – 192.168.1.10 (PC1). IP-адрес отправления – 192.168.2.20 (PC2).

7.10) Более подробный вид пакета ICMP-reply от PC1.

```

▼ Ethernet II, Src: cc:01:0c:44:00:00 (cc:01:0c:44:00:00), Dst: Private_66:68:00 (00:50:79:66:68:00)
  ▸ Destination: Private_66:68:00 (00:50:79:66:68:00)
  ▸ Source: cc:01:0c:44:00:00 (cc:01:0c:44:00:00)
  Type: IPv4 (0x0800)
  [Stream index: 2]
▼ Internet Protocol Version 4, Src: 192.168.2.20, Dst: 192.168.1.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x6d3d (27965)
  ▸ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 63
  Protocol: ICMP (1)
  Header Checksum: 0x89fd [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.2.20
  Destination Address: 192.168.1.10
  [Stream index: 0]

```

MAC-адрес отправления – PC1. MAC-адрес источника – PC2. IP-адрес источника – 192.168.2.20 (PC2). IP-адрес отправления – 192.168.1.10 (PC1).

7.11) Более подробный вид пакета ICMP-request от PC2.

```

▼ Ethernet II, Src: cc:01:0c:44:00:10 (cc:01:0c:44:00:10), Dst: Private_66:68:01 (00:50:79:66:68:01)
  ▸ Destination: Private_66:68:01 (00:50:79:66:68:01)
  ▸ Source: cc:01:0c:44:00:10 (cc:01:0c:44:00:10)
  Type: IPv4 (0x0800)
  [Stream index: 2]
▼ Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.2.20
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  Total Length: 84
  Identification: 0x6d3d (27965)
  ▸ 000. .... = Flags: 0x0
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 63
  Protocol: ICMP (1)
  Header Checksum: 0x89fd [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 192.168.1.10
  Destination Address: 192.168.2.20
  [Stream index: 0]

```

MAC-адрес отправления – PC1. MAC-адрес источника – PC2. IP-адрес источника – 192.168.1.10 (PC1). IP-адрес отправления – 192.168.2.20 (PC2).

7.12) Более подробный вид пакета ICMP-reply от PC2.

```

▼ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: cc:01:0c:44:00:10 (cc:01:0c:44:00:10)
  ▸ Destination: cc:01:0c:44:00:10 (cc:01:0c:44:00:10)
  ▸ Source: Private_66:68:01 (00:50:79:66:68:01)
    Type: IPv4 (0x0800)
    [Stream index: 2]
▼ Internet Protocol Version 4, Src: 192.168.2.20, Dst: 192.168.1.10
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  ▸ Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 84
    Identification: 0x6d3d (27965)
  ▸ 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 64
    Protocol: ICMP (1)
    Header Checksum: 0x88fd [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.2.20
    Destination Address: 192.168.1.10
    [Stream index: 0]

```

MAC-адрес отправления – PC2. MAC-адрес источника – PC1. IP-адрес источника – 192.168.2.20 (PC2). IP-адрес отправления – 192.168.1.10 (PC1).