

Лабораторная работа №1

Модуль 4

Глазунов Кирилл

Тема: Освоение инструментария для выполнения работ, построение простой сети

Проект на сервере: GKD1

nb! - отметка в тексте, "обратите особое внимание"

- 1) Установить и настроить эмулятор GNS3
- 2) Создать простейшую сеть, состоящую из 1 коммутатора и 2 компьютеров, назначить им произвольные ip адреса из одной сети
- 3) Запустить симуляцию, выполнить команду ping с одного из компьютеров, используя ip адрес второго компьютера
- 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
- 5) Создать простейшую сеть, состоящую из 1 маршрутизатора и 2 компьютеров, назначить им произвольные ip адреса из разных сетей
- 6) Запустить симуляцию, выполнить команду ping с одного из компьютеров, используя ip адрес второго компьютера
- 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

Выполнение

1) Сделано

2)

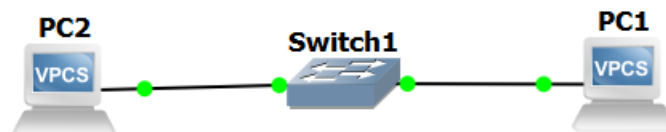


Рис.1 сеть из 1 коммутатора и 2 компьютеров

Для назначения ip адресов компьютерам необходимо ввести команды в консоли каждого пк:

PC1: «ip 192.168.0.1 255.255.255.0» (ip <адрес> <маска подсети>)

PC2: «ip 192.168.0.2 255.255.255.0»

3)

В консоли PC1 выполним следующую команду :

«ping 192.168.0.2» (ping <ip PC2>)

```
PC1> ping 192.168.0.2

84 bytes from 192.168.0.2 icmp_seq=1 ttl=64 time=0.170 ms
84 bytes from 192.168.0.2 icmp_seq=2 ttl=64 time=0.335 ms
84 bytes from 192.168.0.2 icmp_seq=3 ttl=64 time=0.355 ms
84 bytes from 192.168.0.2 icmp_seq=4 ttl=64 time=0.347 ms
84 bytes from 192.168.0.2 icmp_seq=5 ttl=64 time=0.301 ms
```

Рис.2 Результат работы ping

4)

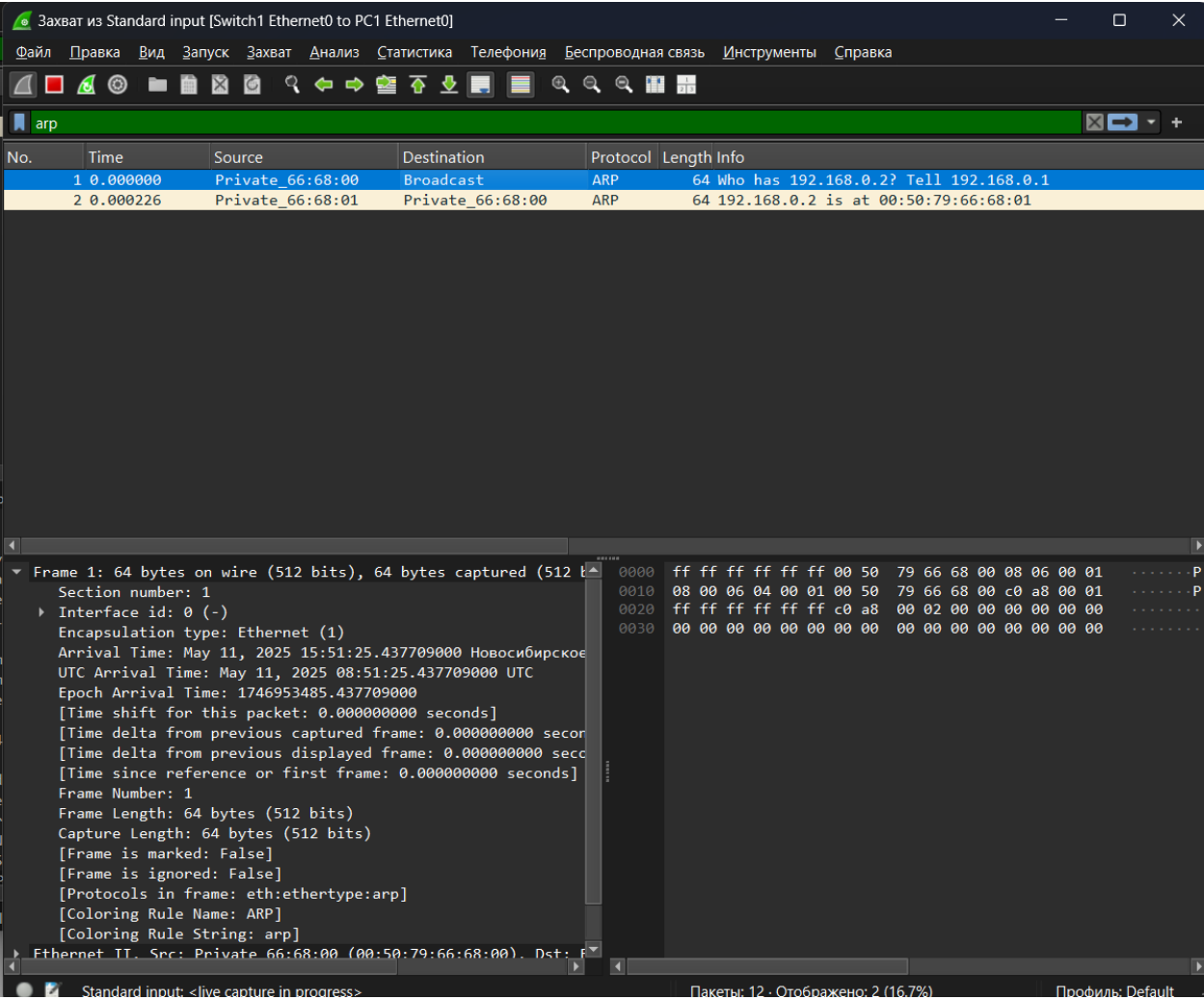
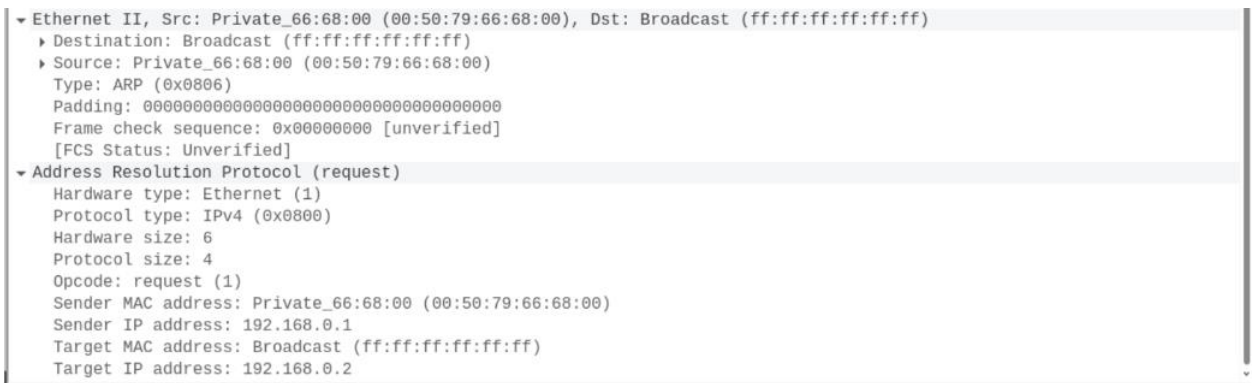


рис.3 перехваченный трафик протокола arp на линке PC1 — Switch



В кадр Ethernet II входят:

1. Мас адрес назначения 6 байтов — широковещательный канал (broadcast)
2. MAC адрес отправителя 6 байтов
3. Тип заголовка протокола лежащего внутри сообщения 2 байта — ARP (0x0806)
4. Выравнивание и контрольная сумма — 18 + 4 байтов нулей

Заголовок ARP:

1. Тип оборудования – 1 для Ethernet 2 байта
2. Тип протокола – протокол, используемый на сетевом уровне IPv4 2 байта.
3. Длина аппаратного адреса—длина в байтах, поэтому для Ethernet она равна 6.
4. Длина адреса протокола – Его значение составляет 4 байта.
5. Ор код указывает, что пакет представляет собой запрос ARP (1) или ответ ARP (2). 2байта
6. Аппаратный адрес отправителя – аппаратный (MAC) адрес исходного узла 6 байтов.
7. Адрес протокола отправителей — ip адрес исходного узла 4 байта.
8. Аппаратный адрес – аппаратный адрес назначения- широковещательный канал 6 байтов
9. Ip адрес узла которому послан запрос 4 байта

широковещательный домен PC1 отправляет запрос: «Кто имеет такой-то ip адрес?»

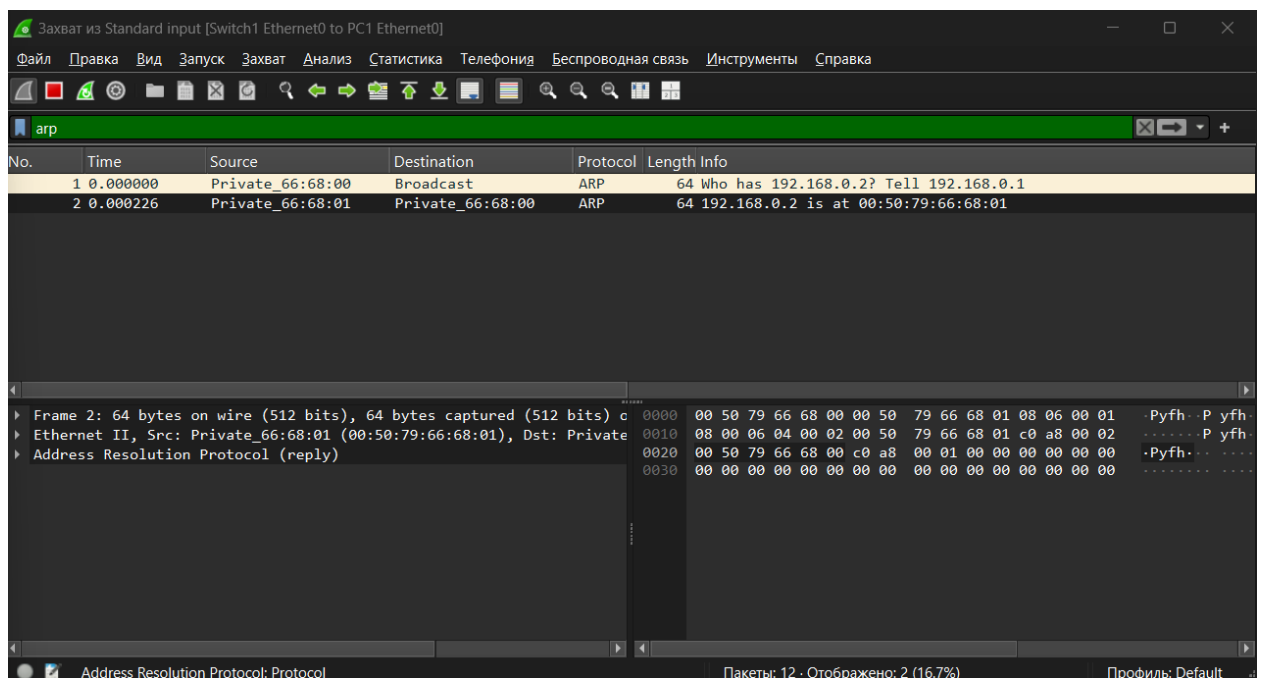


рис.4 2ое сообщение — ответ на arp запрос на линке PC1 — Switch

```

▼ 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)
  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)
  Target IP address: 192.168.0.1

```

Типы заголовков не изменились.

Изменения в содержании:

Аппартные адреса отправителя (PC2) и назначения (PC1);

Opcode: ответ (2) (был запрос)

IP адреса назначения (PC1), отправителя (PC2),

Аппартный адрес отправителя (PC2) и назначения (PC1)

Линк pc2-switch

Первый кадр — arp запрос без изменений относительно pc1-switch

Второй кадр — ответ на arp запрос без изменений относительно pc1-switch

5) Построим сеть из одного маршрутизатора C2600 и двух компьютеров:

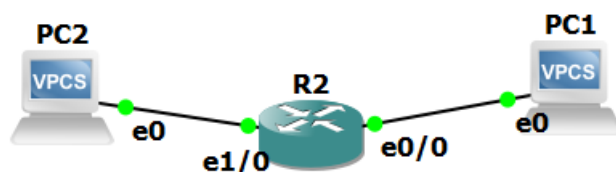


рис. 5 сеть, состоящая из 1 маршрутизатора и 2 компьютеров

Настройка маршрутизатора:

В слоты необходимо добавить сетевой модуль NM-4E для возможности подключения

компьютеров к маршрутизатору по интерфейсу ethernet

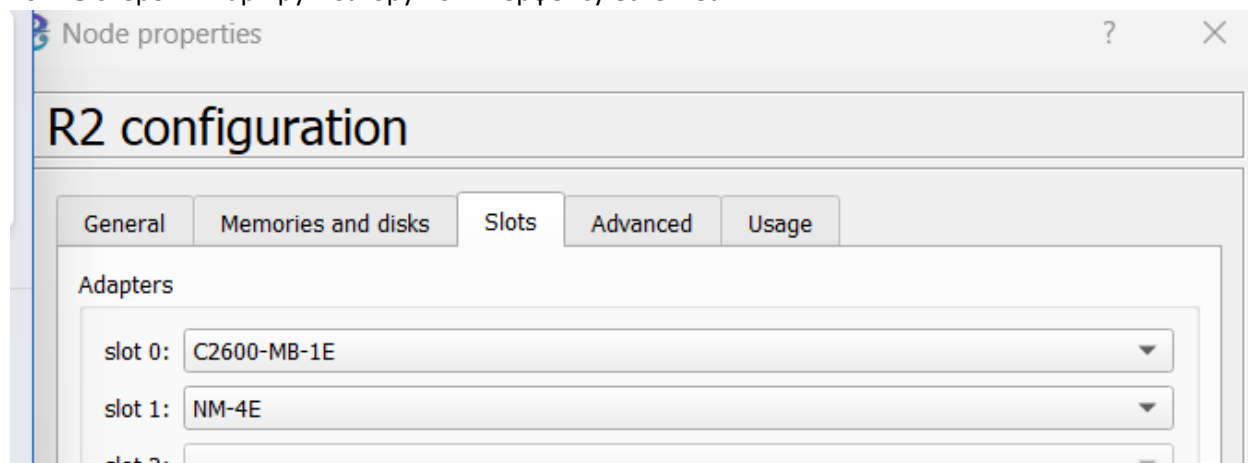


рис.6 вкладка Slots R2 configuration

Конфигурирование маршрутизатора в консоли:

R2:

```

R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface Ethernet0/0
R2(config-if)#ip address 192.168.1.1 255.255.255.0
^
% Invalid input detected at '^' marker.

R2(config-if)#ip address 192.168.1.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
*Mar 1 00:01:58.987: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Mar 1 00:01:59.988: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R2(config-if)#exit
R2(config)#interface Ethernet1/0
R2(config-if)#ip address 192.168.5.1 255.255.255.0
R2(config-if)#no shutdown
R2(config-if)#
*Mar 1 00:02:40.687: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Mar 1 00:02:41.689: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to up
R2(config-if)#exit
R2(config)#ip
% Incomplete command.

R2(config)#exit
R2#ip
*Mar 1 00:03:02.723: %SYS-5-CONFIG_I: Configured from console by console
R2#ip
Translating "ip"

Translating "ip"
% Unknown command or computer name, or unable to find computer address
R2#ip
Translating "ip"

Translating "ip"
% Unknown command or computer name, or unable to find computer address
R2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.5.0/24 is directly connected, Ethernet1/0
C    192.168.1.0/24 is directly connected, Ethernet0/0
R2#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Protocol
Ethernet0/0	192.168.1.1	YES	manual	up	up
Ethernet1/0	192.168.5.1	YES	manual	up	up
Ethernet1/1	unassigned	YES	unset	administratively down	down
Ethernet1/2	unassigned	YES	unset	administratively down	down
Ethernet1/3	unassigned	YES	unset	administratively down	down

```

R2#

```

рис. 7 Настройка маршрутизатора

- interface Ethernet0/0
- ip address 192.168.1.1 255.255.255.0
- no shutdown
- exit
- interface Ethernet1/0
- ip address 192.168.5.1 255.255.255.0

- no shutdown
- exit
- exit

Для проверки настройки:

- show ip route
- show ip interface brief

Настройка компьютеров

PC1:

ip 192.168.1.5 255.255.255.0 192.168.1.1 (ip <ip adr> <mask> <gateway(шлюз)>)

PC2:

ip 192.168.5.5 255.255.255.0 192.168.5.1

6) Выполним команду ping от PC1 до PC2

PC1> ping 192.168.5.5

```
PC1> ping 192.168.5.5

192.168.5.5 icmp_seq=1 timeout
84 bytes from 192.168.5.5 icmp_seq=2 ttl=63 time=20.982 ms
84 bytes from 192.168.5.5 icmp_seq=3 ttl=63 time=16.089 ms
84 bytes from 192.168.5.5 icmp_seq=4 ttl=63 time=15.672 ms
84 bytes from 192.168.5.5 icmp_seq=5 ttl=63 time=16.547 ms
```

рис. 8 результат команды ping

7) С помощью wireshark перехватим пакеты трафика на всех линках

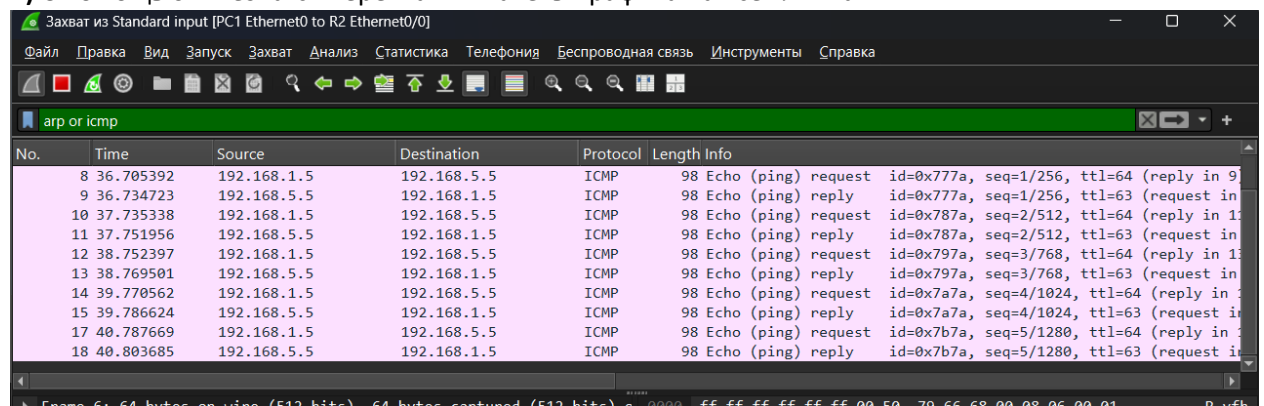


рис. 9 трафик линка PC1 — R2

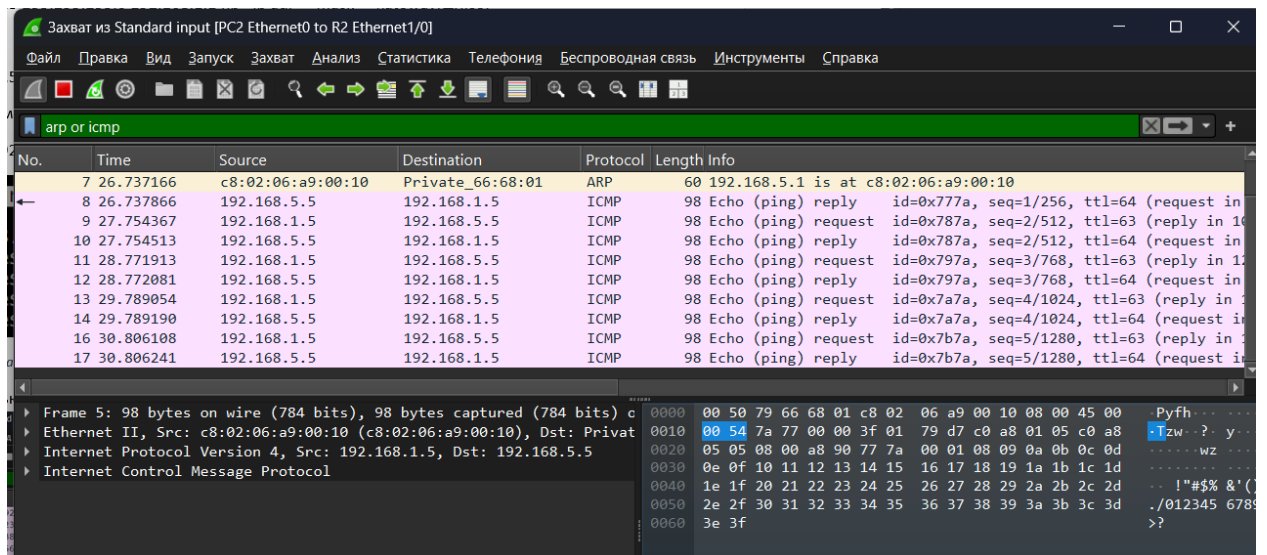


рис. 10 трафик линка PC2 — R2

Логика общения:

- PC1 отправляет arp запрос, чтобы узнать аппаратный адрес шлюза e0/0
 - R2 с e0/0 отвечает PC1 на arp запрос и сообщает ему аппаратный адрес
 - PC1 посылает icmp (ping) запрос, посылает его через шлюз, ip адрес назначения — адрес PC2
 - R2 пересылает с интерфейса e1/0 PC2 icmp запрос
 - PC2 не знает аппаратный адрес своего шлюза (e1/0), поэтому посылает по широковещательному каналу arp запрос, по ip адресу шлюза e1/0.
 - R2 отвечает на arp запрос, сообщая PC2 свой MAC адрес
 - PC2 отвечает на icmp запрос, отсылая сообщение до PC1 через R2 (свой шлюз e1/0)
 - R2 пересылает ответ icmp запроса к PC1 с e0/0
- Т.е.

- icmp запрос PC1 — R2 e0/0__R2 e1/0 — PC2;
- ответ на icmp запрос PC2 — R2 e1/0__R2 e0/0 — PC1;
- так еще 3 раза

Анализ заголовков пакетов

ARP PC1 — R2 request

Заголовок ARP

1. Тип оборудования – 1 для Ethernet 2 байт
2. Тип протокола – протокол, используемый на сетевом уровне IPv4 2 байта.
3. Длина аппаратного адреса–длина в байтах, поэтому для Ethernet она равна 6.
4. Длина адреса протокола – Его значение составляет 4 байта.
5. Оп код указывает, что пакет представляет собой запрос ARP (1) или ответ ARP (2). 2байта
6. Аппаратный адрес отправителя – аппаратный (MAC) адрес исходного узла (PC3) 6 байтов.

7. Адрес протокола отправителей — ip адрес PC1 исходного узла 4 байта.
8. Адрес протокола отправителей — ip адрес PC1 исходного узла 4 байта.
9. Target Адрес протокола – Ip адрес узла R2 e0/0 которому послан запрос ARP 4 байта

ICMP запрос линк PC1 — R2

Заголовок 2 уровня:

1. Аппаратный адрес назначения (R2 e0/0) 6 байтов
2. Аппаратный адрес источника (PC1) 6 байтов
3. Протокол, лежащий внутри IPv4 2байта

Заголовок IPv4:

1. 1. Версия IP: 4, 4 бита
2. Длина заголовка (0101 = 20байтов) 4 бита
3. Тип обслуживания 1 байт
4. Общая длина (84 байта) 2 байта
5. Идентификация фрагмента 2 байта (для сборки пакетов)
6. Флаги 3 бита для управления фрагментацией пакетов.
7. Смещение фрагмента 13 бит
8. Время жизни 1 байт 64раз - максимальное количество переходов через маршрутизаторы, после чего пакет будет отброшен.
9. Протокол 1 байт: 1 — ICMP
10. Контрольная сумма заголовка 2 байта
11. IP-адрес источника 4 байта (PC1)
12. IP-адрес назначения 4 байта (PC2)

Заголовок протокола ICMP:

1. Тип: 8 — ping запрос 1байт
2. Код: 0 1байт
3. Контрольная сумма 2байта
4. Идентификатор: 2байта
5. Номер последовательности 2 байта
6. Данные, 56 байтов

Заголовки на другом линке и в обратном сообщении аналогичны с изменения адресов логических и физических, типов сообщений и тд.