Лабораторная работа №1
Модуль 4
Долгих Вячеслав

Проект на сервере: Dolgikh_Lab1

Тема: Освоение инструментария для выполнения работ, построение простой сети

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

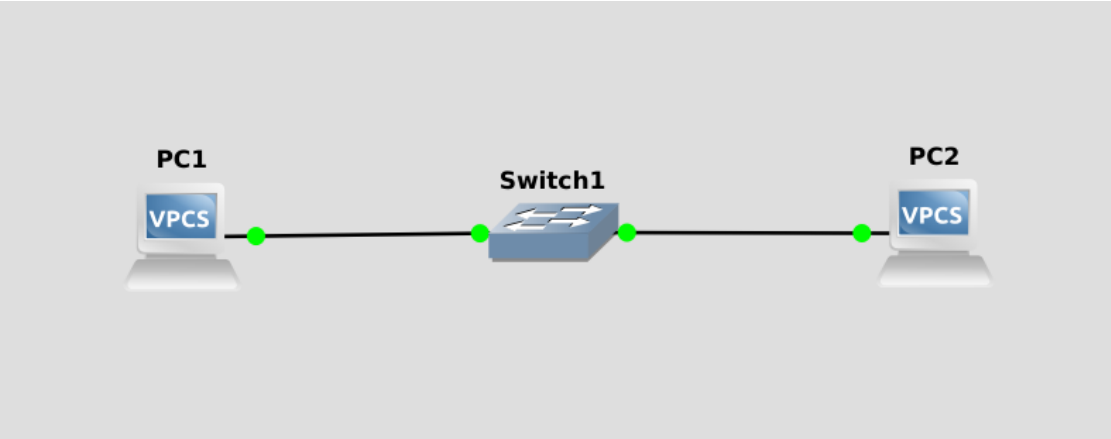

рис. 1 сеть состоящая из 1 коммутатора и 2 компьютеров

Для назначения ip адресов компьютерам необходимо ввести команды в консоли каждого компьютера:
PC1: «ip 192.168.0.1 255.255.255.0» (ip <адрес> <маска подсети>)
PC2: «ip 192.168.0.2 255.255.255.0»
В файлах лаб. Работы приложены конфигурации для PC1 и PC2 в которых выставлены ip адреса.

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=0.368 ms
84 bytes from 192.168.0.2 icmp_seq=2 ttl=64 time=0.333 ms
84 bytes from 192.168.0.2 icmp_seq=3 ttl=64 time=0.346 ms
84 bytes from 192.168.0.2 icmp_seq=4 ttl=64 time=0.458 ms
84 bytes from 192.168.0.2 icmp_seq=5 ttl=64 time=0.395 ms
```

рис.2 результат команды ping

С помощью программы Wireshark перехватим трафик протокола arp на всех линиях связи:

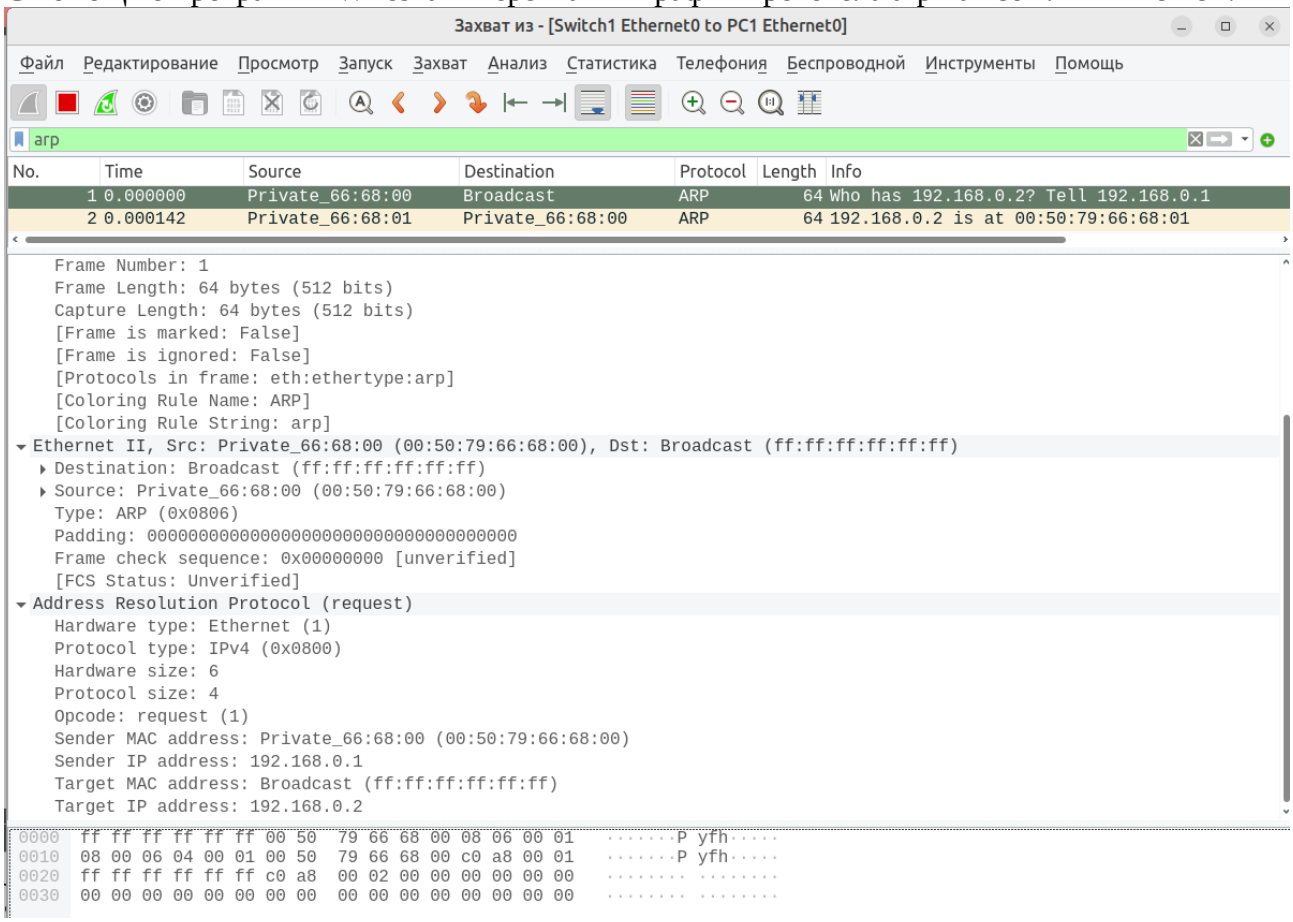

рис.3 перехваченный трафик протокола arp на линке PC1 — Switch

В кадр Ethernet II входят:

1. Mac 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. Хвост и контрольная сумма — 18 + 4 байтов нулей

Заголовок ARP

1. Тип оборудования – 1 для Ethernet 2 байта
2. Тип оборудования – 1 для Ethernet 2 байтТип 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. Орегакод 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 уровня 3 исходного узла 4 байта.

8. Target Аппаратный адрес – аппаратный адрес назначения- широковещательный канал 6 байтов
9. Target Адрес протокола – Ip адрес узла которому послан запрос ARP 4 байта

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

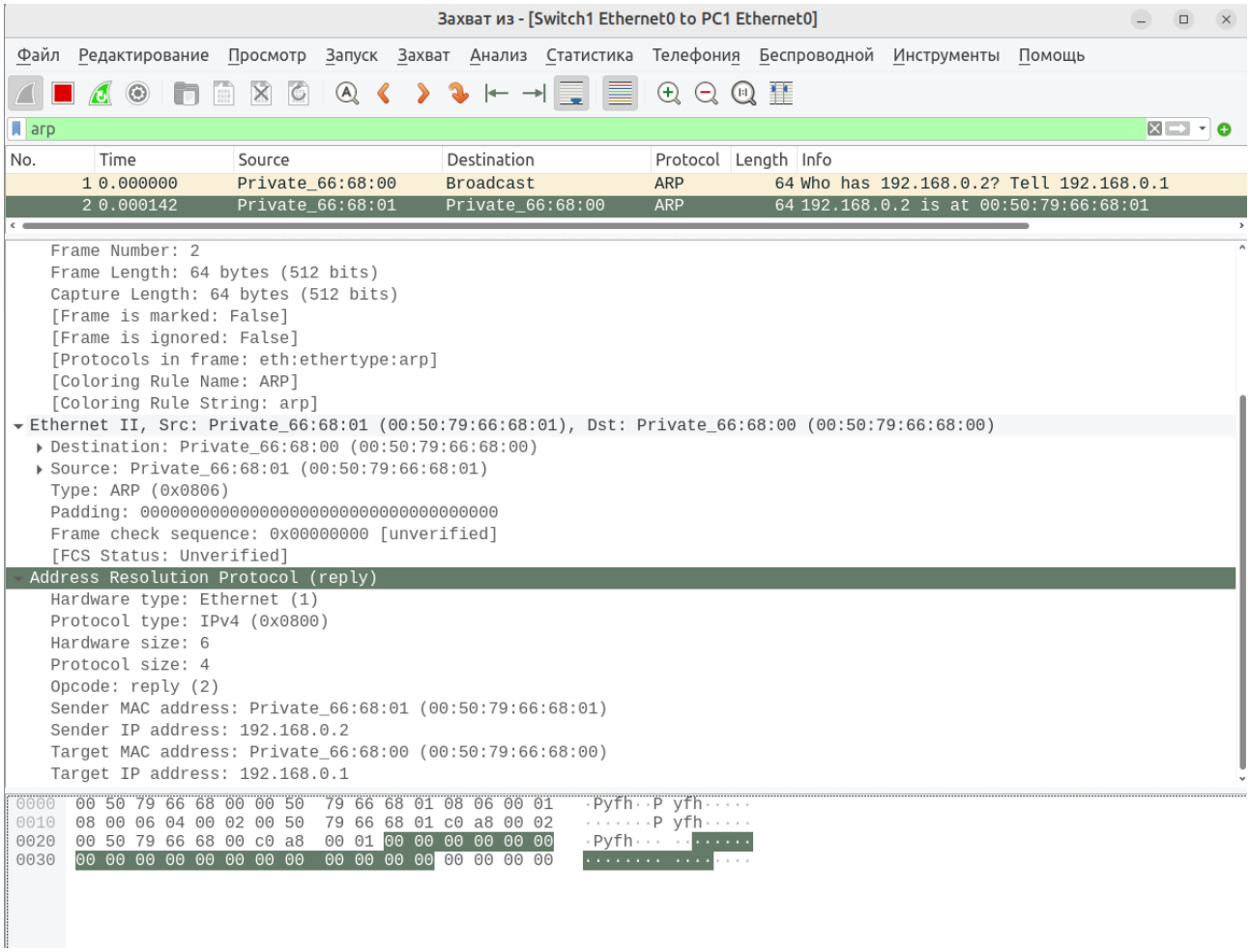

рис.4 2ое сообщение — ответ на arp запрос на линке PC1 — Switch

Сообщение имеет следующий тип — «PC2 отвечает :такой ip адрес имею я, держи мой MAC адрес»

Типы заголовков не изменились.
Изменения в содержании:
Аппартные адреса отправителя (PC2) и назначения (PC1);
Oprcode: ответ (2) (был запрос)
Ip адреса назначения(PC1), отправителя (PC2),
Аппаратный адрес отправителя (PC2) и назначения (PC1)
Файл с пакетами: «pc1-sw».

Линк pc2-sw
Первый кадр — arp запрос без изменений относительно pc1-sw
Второй кадр — ответ на arp запрос без изменений относительно pc1-sw
Файл с пакетами: «pc2-sw»

Построим сеть из одного маршрутизатора C2600 и двух компьютеров:

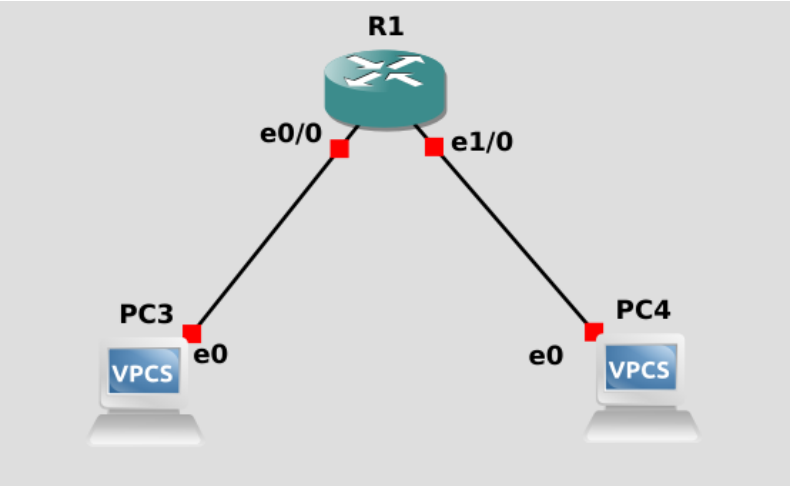

рис. 5 сеть состоящая из 1 маршрутизатора и 2 компьютеров

Настройка маршрутизатора:
В слоты необходимо добавить сетевой модуль NM-4E для возможности подключения компьютеров к маршрутизатору по интерфейсу ethernet

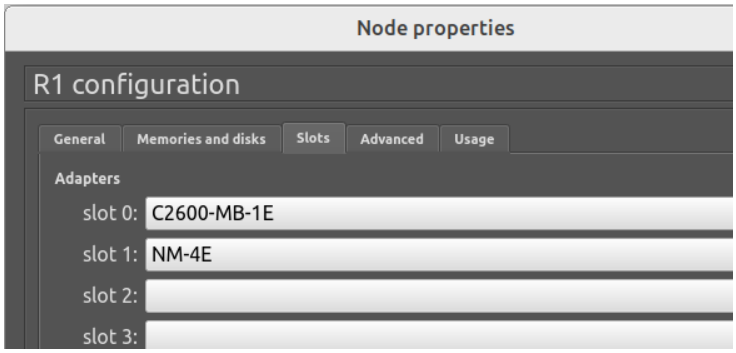

рис.6 вкладка Slots R1 configuration

Конфигурирование маршрутизатора в консоли:
R1:
- enable
- configure terminal
- 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

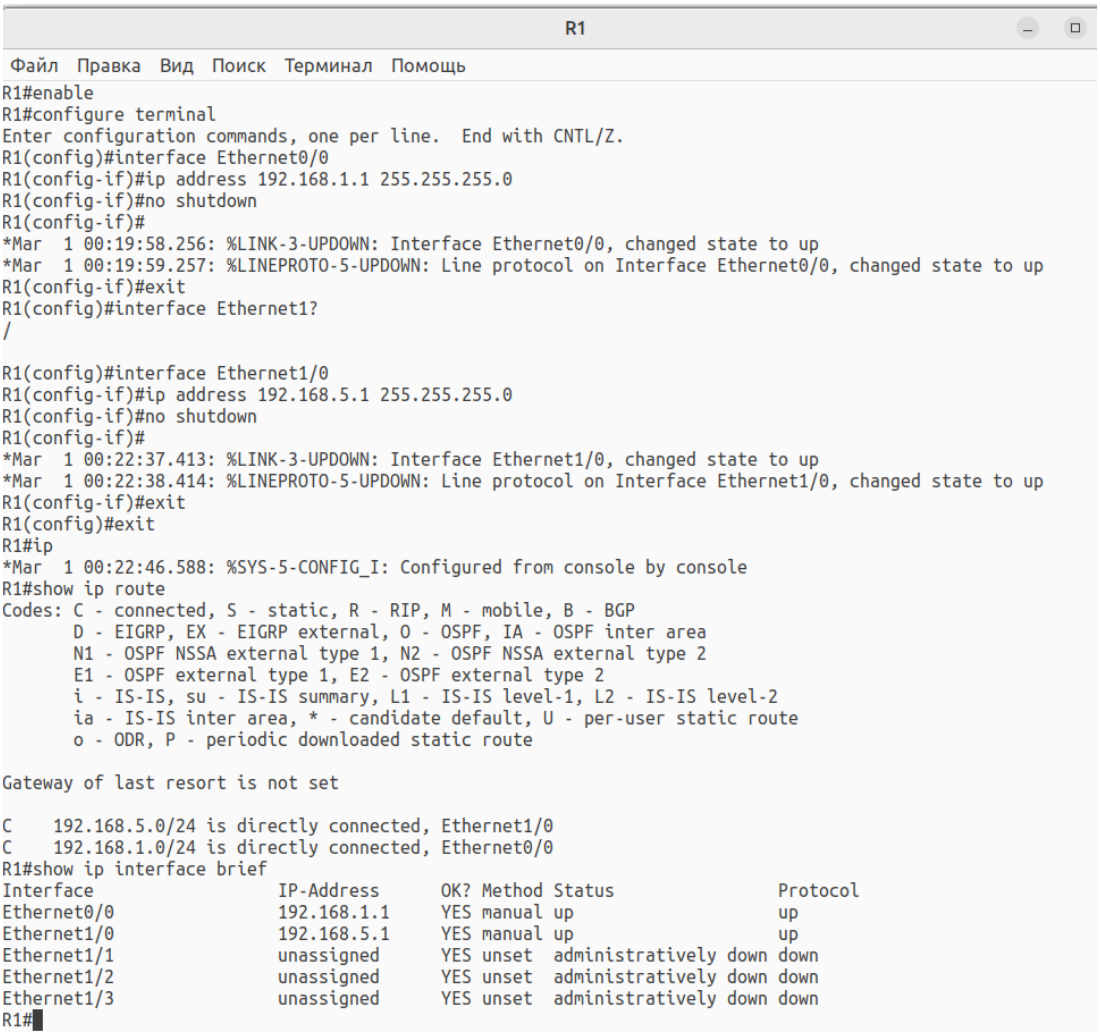

рис. 7 Настройка маршрутизатора по представленным командам

Настройка компьютеров
PC3:
- ip 192.168.1.5 255.255.255.0 192.168.1.1 (ip <ip adr> <mask> <gateway(шлюз)>

PC4:
- ip 192.168.5.5 255.255.255.0 192.168.5.1

Выполним команду ping от PC3 до PC4
PC3 > ping 192.168.5.5

```
PC3> ping 192.168.5.5

84 bytes from 192.168.5.5 icmp_seq=1 ttl=63 time=29.218 ms
192.168.5.5 icmp_seq=2 timeout
84 bytes from 192.168.5.5 icmp_seq=3 ttl=63 time=13.010 ms
84 bytes from 192.168.5.5 icmp_seq=4 ttl=63 time=16.059 ms
84 bytes from 192.168.5.5 icmp_seq=5 ttl=63 time=16.744 ms
```

рис. 8 результат команды ping

С помощью wiresharck перехватим пакеты трафика на всех линках

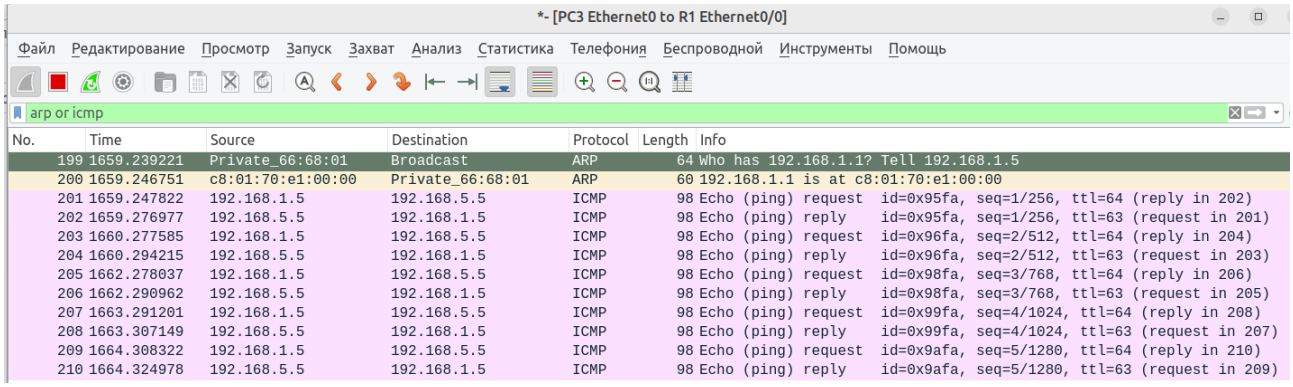

рис. 9 трафик линка PC3 — R1

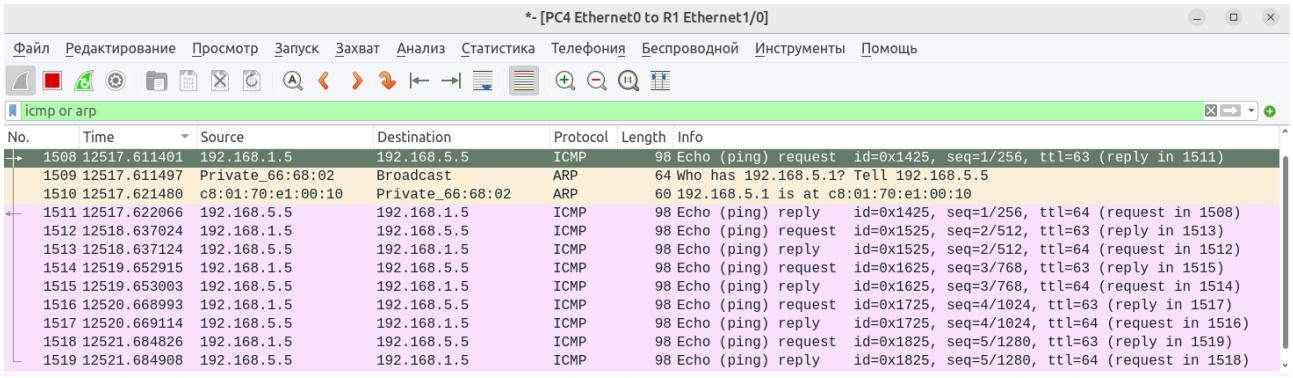

рис. 10 трафик линка PC4 — R1

Логика общения:
- PC3 отправляет arp запрос, чтобы узнать аппаратный адрес шлюза e0/0
- R1 с e0/0 отвечает PC3 на arp запрос и сообщает ему аппаратный адрес
- PC3 посылает icmp (ping) запрос, посылает его через шлюз, ip адрес назначения — адрес PC4
- R1 пересылает с интерфейса e1/0 PC4 icmp запрос
- PC4 не знает аппаратный адрес своего шлюза (e1/0), поэтому посылает по широковещательному каналу arp запрос, по ip адресу шлюза e1/0.
- R1 отвечает на arp запрос, сообщая PC4 свой MAC адрес
- PC4 отвечает на icmp запрос, отсылая сообщение до PC3 через R1 (свой шлюз e1/0)
- R1 пересылает ответ icmp запроса к PC3 с e0/0

- icmp запрос PC3 — R1 e0/0__R1 e1/0 — PC4;
- ответ на icmp запрос PC4 — R1 e1/0__R1 e0/0 — PC3;
.. так еще 3 раза..

Анализ заголовков пакетов
ARP PC3 — R1 request

Заголовок 2 уровня:

1. Тип оборудования – 1 для Ethernet 2 байта
2. Тип оборудования – 1 для Ethernet 2 байт
3. Тип протокола – протокол, используемый на сетевом уровне IpV4 2 байта.

Заголовок ARP

1. Длина аппаратного адреса–длина в байтах, поэтому для Ethernet она равна 6.
2. Длина адреса протокола – Его значение составляет 4 байта.
3. Орегакод указывает, что пакет представляет собой запрос ARP (1) или ответ ARP (2). 2байта
4. Аппаратный адрес отправителя – аппаратный (MAC) адрес исходного узла (PC3) 6 байтов.
5. Адрес протокола отправителей — ip адрес PC3 уровня 3 исходного узла 4 байта.
6. Target Аппаратный адрес – аппаратный адрес назначения широковещательный канал 6 байтов
7. Target Адрес протокола – Ip адрес узла R1 e0/0 которому послан запрос ARP 4 байта

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

ICMP запрос линк PC3 — R1
Заголовок 2 уровня:

1. Аппаратный адрес назначения (R1 e0/0) 6 байтов
2. Аппаратный адрес источника (PC3) 6 байтов
3. Протокол лежащий внутри IPv4 2байта

Заголовок IPv4:

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 (PC3)
12. IP-адрес назначения 4 байта (R1 e0/0)

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 переменная длина, здесь 56 байтов

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

При отправке ICMP например от PC3 до PC4 адреса IPv4 источника и назначения не изменяются, аппаратные же адреса отправителя и назначения постоянно изменяются от сетевого узла к узлу.

Перехваченный трафик приложен в файлах pc3-r1, pc4-r1