

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

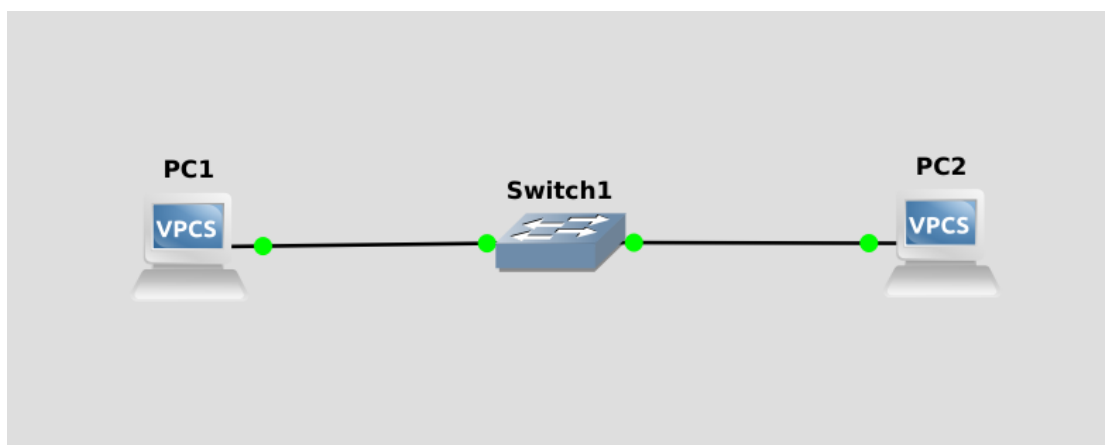


рис. 1 сеть состоящая из 1 коммутатора и 2 компьютеров

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:

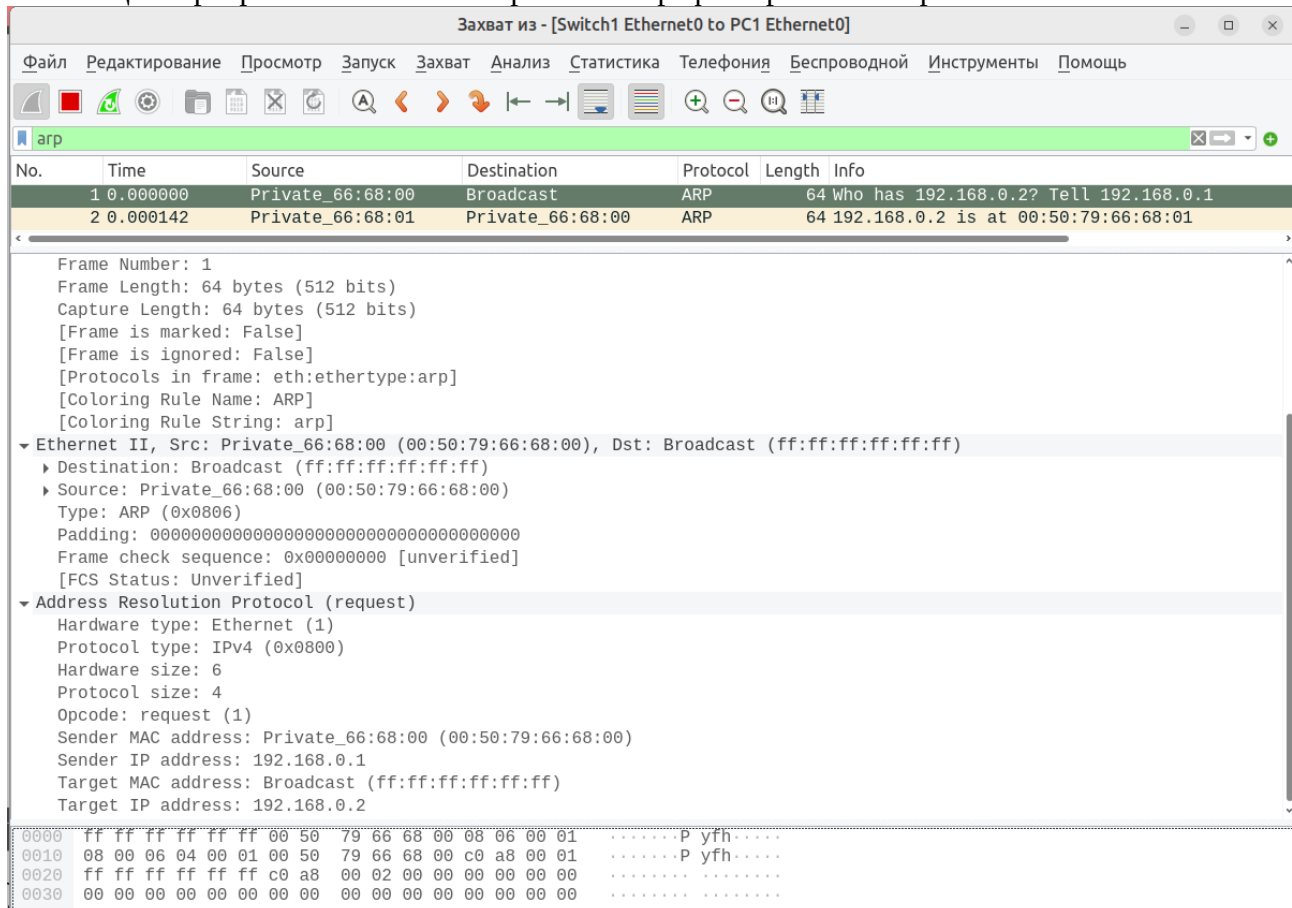


рис.3 перехваченный трафик протокола arp на линке PC1 — Switch

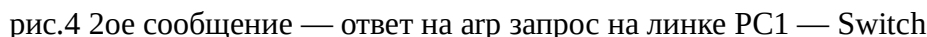
В кадр Ethernet II входят:

1. 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. 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 байта 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. Операционный 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 уровня 3 исходного узла 4 байта.

- В широковещательный домен РС1 отправляет запрос: «Кто имеет такой-то ip адрес?»



Файл с пакетами: «рс2-sw»

Построим сеть из одного маршрутизатора C2600 и двух компьютеров:

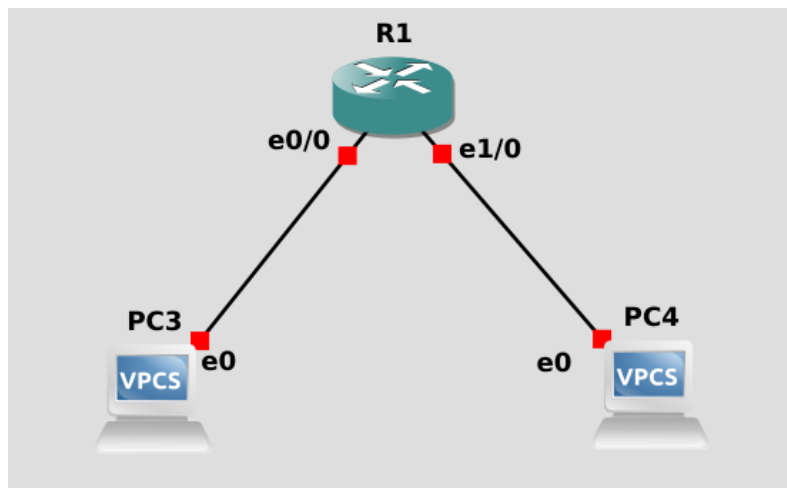


рис. 5 сеть состоящая из 1 маршрутизатора и 2 компьютеров

Настройка маршрутизатора:

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

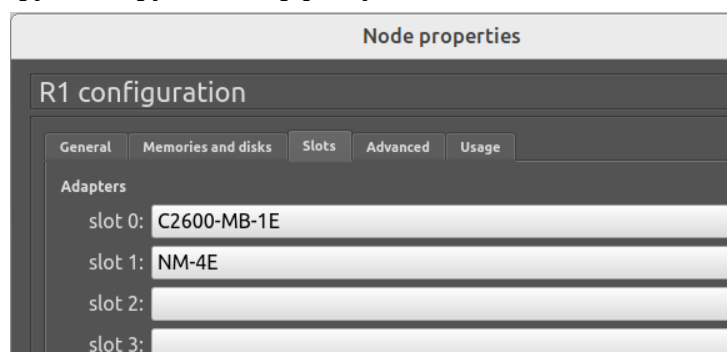


рис.6 вкладка Slots R1 configuration

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

```
R1
Файл Правка Вид Поиск Терминал Помощь
R1#enable
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#interface Ethernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:19:58.256: %LINK-3-UPDOWN: Interface Ethernet0/0, changed state to up
*Mar 1 00:19:59.257: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up
R1(config-if)#exit
R1(config)#interface Ethernet1?
/

R1(config)#interface Ethernet1/0
R1(config-if)#ip address 192.168.5.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#
*Mar 1 00:22:37.413: %LINK-3-UPDOWN: Interface Ethernet1/0, changed state to up
*Mar 1 00:22:38.414: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet1/0, changed state to up
R1(config-if)#exit
R1(config)#exit
R1#ip
*Mar 1 00:22:46.588: %SYS-5-CONFIG_I: Configured from console by console
R1#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
R1#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
R1#
```

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 wireshark перехватим пакеты трафика на всех линках

Wireshark capture on link PC3 to R1 Ethernet0/0. Filter: arp or icmp. The capture shows an ARP request from PC3 to the broadcast address, followed by several ICMP Echo (ping) requests and replies between PC3 and R1.

No.	Time	Source	Destination	Protocol	Length	Info
199	1659.239221	Private_66:68:01	Broadcast	ARP	64	Who has 192.168.1.1? Tell 192.168.1.5
200	1659.246751	c8:01:70:e1:00:00	Private_66:68:01	ARP	60	192.168.1.1 is at c8:01:70:e1:00:00
201	1659.247822	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x95fa, seq=1/256, ttl=64 (reply in 202)
202	1659.276977	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x95fa, seq=1/256, ttl=63 (request in 201)
203	1660.277585	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x96fa, seq=2/512, ttl=64 (reply in 204)
204	1660.294215	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x96fa, seq=2/512, ttl=63 (request in 203)
205	1662.278037	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x98fa, seq=3/768, ttl=64 (reply in 206)
206	1662.290962	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x98fa, seq=3/768, ttl=63 (request in 205)
207	1663.291201	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x99fa, seq=4/1024, ttl=64 (reply in 208)
208	1663.307149	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x99fa, seq=4/1024, ttl=63 (request in 207)
209	1664.308322	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x9afa, seq=5/1280, ttl=64 (reply in 210)
210	1664.324978	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x9afa, seq=5/1280, ttl=63 (request in 209)

рис. 9 трафик линка PC3 — R1

Wireshark capture on link PC4 to R1 Ethernet1/0. Filter: icmp or arp. The capture shows an ICMP Echo (ping) request from PC4 to R1, followed by an ARP request from PC4 to the broadcast address, and then several ICMP Echo (ping) requests and replies between PC4 and R1.

No.	Time	Source	Destination	Protocol	Length	Info
1508	12517.611461	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x1425, seq=1/256, ttl=63 (reply in 1511)
1509	12517.611497	Private_66:68:02	Broadcast	ARP	64	Who has 192.168.5.1? Tell 192.168.5.5
1510	12517.621480	c8:01:70:e1:00:10	Private_66:68:02	ARP	60	192.168.5.1 is at c8:01:70:e1:00:10
1511	12517.622066	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x1425, seq=1/256, ttl=64 (request in 1508)
1512	12518.637024	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x1525, seq=2/512, ttl=63 (reply in 1513)
1513	12518.637124	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x1525, seq=2/512, ttl=64 (request in 1512)
1514	12519.652915	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x1625, seq=3/768, ttl=63 (reply in 1515)
1515	12519.653003	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x1625, seq=3/768, ttl=64 (request in 1514)
1516	12520.668993	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x1725, seq=4/1024, ttl=63 (reply in 1517)
1517	12520.669114	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x1725, seq=4/1024, ttl=64 (request in 1516)
1518	12521.684826	192.168.1.5	192.168.5.5	ICMP	98	Echo (ping) request id=0x1825, seq=5/1280, ttl=63 (reply in 1519)
1519	12521.684908	192.168.5.5	192.168.1.5	ICMP	98	Echo (ping) reply id=0x1825, seq=5/1280, ttl=64 (request in 1518)

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