

Туртугешев А.В.

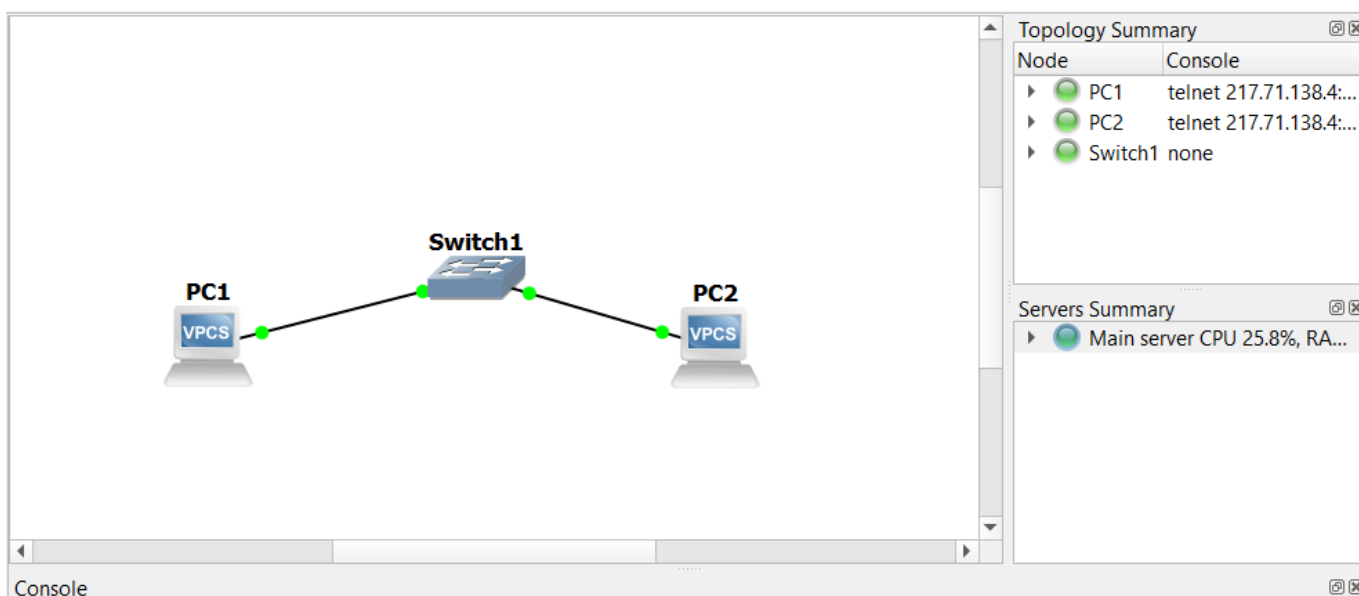
Лабораторная работа №1

1) Установить и настроить эмулятор GNS3

Установка и настройка GNS3 была выполнена по инструкции из файла gns3 lab.pdf.

2) Создать простейшую сеть, состоящую из 1 коммутатора и 2 компьютеров, назначить им произвольные ip адреса из одной сети

- Схема сети.



- Заданы ip адреса для PC1 и PC2.

```
PC1> show ip
NAME       : PC1[1]
IP/MASK    : 192.168.1.7/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 20676
RHOST:PORT : 127.0.0.1:20677
MTU        : 1500
PC1>

PC2> show ip
NAME       : PC2[1]
IP/MASK    : 192.168.1.8/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:01
LPORT      : 20678
RHOST:PORT : 127.0.0.1:20679
MTU        : 1500
PC2>
```

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

```
PC1> ping 192.168.1.8

84 bytes from 192.168.1.8 icmp_seq=1 ttl=64 time=0.246 ms
84 bytes from 192.168.1.8 icmp_seq=2 ttl=64 time=0.260 ms
84 bytes from 192.168.1.8 icmp_seq=3 ttl=64 time=0.251 ms
84 bytes from 192.168.1.8 icmp_seq=4 ttl=64 time=0.241 ms
84 bytes from 192.168.1.8 icmp_seq=5 ttl=64 time=0.234 ms

PC1> █
```

```
PC2> ping 192.168.1.7

84 bytes from 192.168.1.7 icmp_seq=1 ttl=64 time=0.189 ms
84 bytes from 192.168.1.7 icmp_seq=2 ttl=64 time=0.235 ms
84 bytes from 192.168.1.7 icmp_seq=3 ttl=64 time=0.259 ms
84 bytes from 192.168.1.7 icmp_seq=4 ttl=64 time=0.223 ms
84 bytes from 192.168.1.7 icmp_seq=5 ttl=64 time=0.254 ms

PC2> █
```

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

Отображения всех ARP пакетов.

arp						
No.	Time	Source	Destination	Protocol	Leng	Info
1	0.000000	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.8? Tell 192.168.1.7
2	0.000123	Private_66:68:01	Private_66:68:00	ARP	64	192.168.1.8 is at 00:50:79:66:68:01

- ARP запрос.

> Frame 1: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface

> Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadcast

▼ 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: 192.168.1.7

Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)

Target IP address: 192.168.1.8

0000	ff ff ff ff ff ff 00 50	79 66 68 00 08 06 00 01P yfh....
0010	08 00 06 04 00 01 00 50	79 66 68 00 c0 a8 01 07	P yfh....
0020	ff ff ff ff ff c0 a8	01 08 00 00 00 00 00 00	P yfh....
0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	P yfh....

- ARP ответ.

> Frame 2: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on i	0000	00 50 79 66 68 00 00 50	79 66 68 01 08 06 00 01	Pyfh...P yfh...
> Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66	0010	08 00 06 04 00 02 00 50	79 66 68 01 c0 a8 01 08P yfh...
✓ Address Resolution Protocol (reply)	0020	00 50 79 66 68 00 c0 a8	01 07 00 00 00 00 00 00	Pyfh... ..
Hardware type: Ethernet (1)	0030	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00
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: 192.168.1.8				
Target MAC address: Private_66:68:00 (00:50:79:66:68:00)				
Target IP address: 192.168.1.7				

В результате перехвата трафика и анализа заголовков пакетов были выявлены следующие события:

ARP-запрос:

- 1) Отправитель: PC1 (MAC: 00:50:79:66:68:00, IP: 192.168.1.7)
- 2) Назначение: Широковещательный адрес (ff:ff:ff:ff:ff:ff)
- 3) Содержание запроса: "who has 192.168.1.8 ip? Сообщите устройству с IP 192.168.1.7"

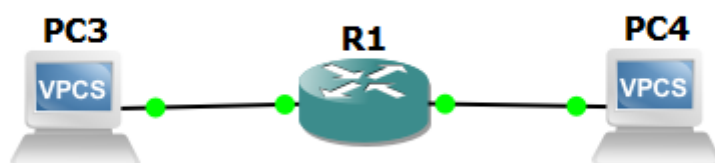
Устройство PC1 отправило широковещательный ARP-запрос, чтобы определить MAC-адрес устройства с IP-адресом 192.168.1.8.

ARP-ответ:

- 1) Отправитель: PC2 (MAC: 00:50:79:66:68:01, IP: 192.168.1.8)
- 2) Назначение: PC1 (MAC: 00:50:79:66:68:00)
- 3) Содержание ответа: "IP-адрес 192.168.1.8 принадлежит MAC-адресу 00:50:79:66:68:01"

Устройство PC2 ответило на ARP-запрос, предоставив свой MAC-адрес.

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



- Настройки компьютеров

<pre> PC3> ip 192.168.1.7 255.255.255.0 gateway 192.168.1.1 Checking for duplicate address... PC3 : 192.168.1.7 255.255.255.0 gateway 192.168.1.1 PC3> show ip NAME : PC3[1] IP/MASK : 192.168.1.7/24 GATEWAY : 192.168.1.1 DNS : MAC : 00:50:79:66:68:02 LPORT : 20676 RHOST:PORT : 127.0.0.1:20677 MTU : 1500 PC3> </pre>	<pre> PC4> ip 192.168.2.8 255.255.255.0 gateway 192.168.2.1 Checking for duplicate address... PC4 : 192.168.2.8 255.255.255.0 gateway 192.168.2.1 PC4> show ip NAME : PC4[1] IP/MASK : 192.168.2.8/24 GATEWAY : 192.168.2.1 DNS : MAC : 00:50:79:66:68:03 LPORT : 20678 RHOST:PORT : 127.0.0.1:20679 MTU : 1500 PC4> </pre>
---	---

- Настройки маршрутизатора

```

R1
R1(config)#interface FastEthernet0/0
R1(config-if)#ip address 192.168.1.1 255.255.255.0
R1(config-if)#no shutdown
R1(config-if)#exit
R1(config)#interface FastEthernet0/1
^
% Invalid input detected at '^' marker.

R1(config)#
R1#
*Mar  1 00:14:17.011: %SYS-5-CONFIG_I: Configured from console by console
R1#conf
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
R1(config)#interface FastEthernet1/0
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 00:15:20.147: %LINK-3-UPDOWN: Interface FastEthernet1/0, changed state to up
*Mar  1 00:15:21.147: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet1/0, changed state to up
R1(config)#show ip interface brief
^
% Invalid input detected at '^' marker.

R1(config)#exit
R1#configure terminal
*Mar  1 00:16:05.367: %SYS-5-CONFIG_I: Configured from console by console
R1#show ip interface brief

```

Interface	IP-Address	OK?	Method	Status	Prot
FastEthernet0/0	192.168.1.1	YES	manual	up	up
FastEthernet1/0	192.168.2.1	YES	manual	up	up
Ethernet2/0	unassigned	YES	unset	administratively down	down

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

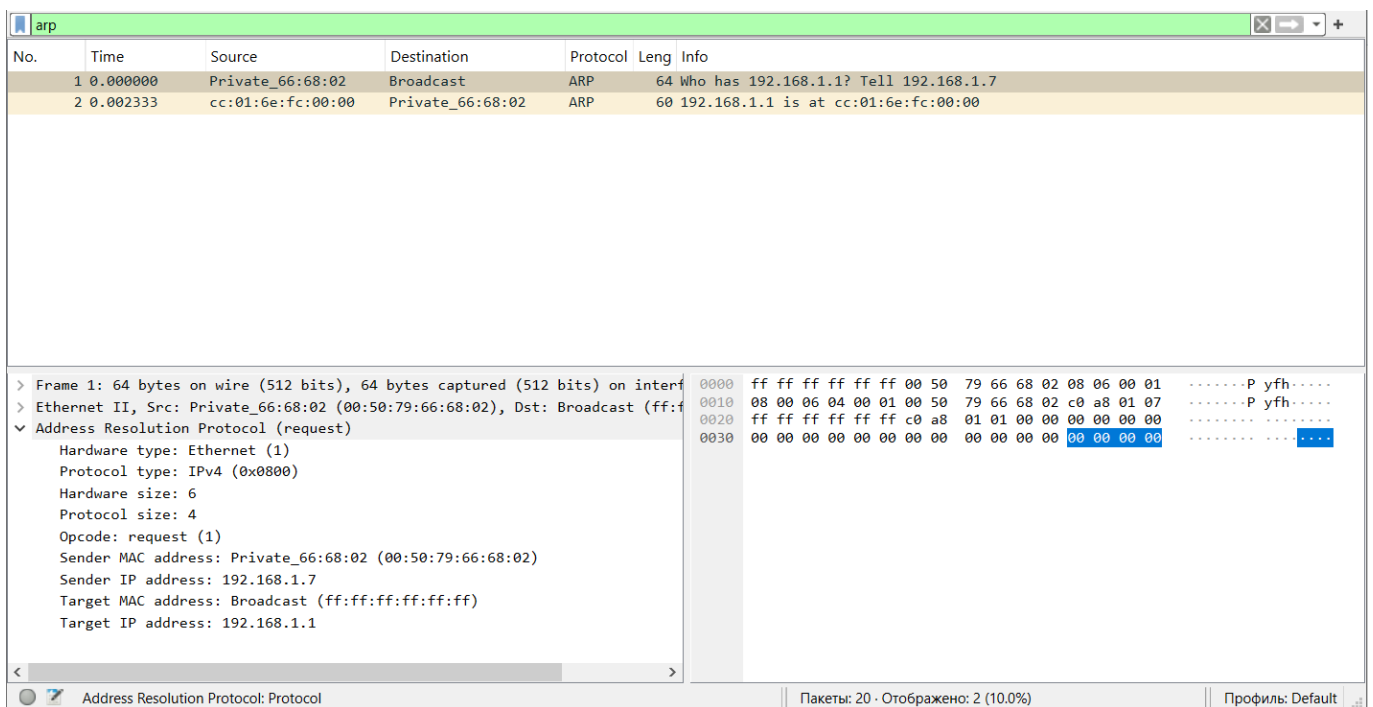
```
PC3> ping 192.168.2.8

84 bytes from 192.168.2.8 icmp_seq=1 ttl=63 time=14.441 ms
84 bytes from 192.168.2.8 icmp_seq=2 ttl=63 time=15.489 ms
84 bytes from 192.168.2.8 icmp_seq=3 ttl=63 time=15.293 ms
84 bytes from 192.168.2.8 icmp_seq=4 ttl=63 time=15.985 ms
84 bytes from 192.168.2.8 icmp_seq=5 ttl=63 time=14.635 ms

PC3> █
```

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

- ARP



- icmp

No.	Time	Source	Destination	Protocol	Leng	Info
3	0.003197	192.168.1.7	192.168.2.8	ICMP	98	Echo (ping) request id=0x5ab9, seq=1/256, ttl=64 (reply in 4)
4	0.032554	192.168.2.8	192.168.1.7	ICMP	98	Echo (ping) reply id=0x5ab9, seq=1/256, ttl=63 (request in 3)
5	1.032727	192.168.1.7	192.168.2.8	ICMP	98	Echo (ping) request id=0x5bb9, seq=2/512, ttl=64 (reply in 6)
6	1.048310	192.168.2.8	192.168.1.7	ICMP	98	Echo (ping) reply id=0x5bb9, seq=2/512, ttl=63 (request in 5)
8	2.048689	192.168.1.7	192.168.2.8	ICMP	98	Echo (ping) request id=0x5cb9, seq=3/768, ttl=64 (reply in 9)
9	2.064391	192.168.2.8	192.168.1.7	ICMP	98	Echo (ping) reply id=0x5cb9, seq=3/768, ttl=63 (request in 8)
10	3.064672	192.168.1.7	192.168.2.8	ICMP	98	Echo (ping) request id=0x5db9, seq=4/1024, ttl=64 (reply in 11)
11	3.080516	192.168.2.8	192.168.1.7	ICMP	98	Echo (ping) reply id=0x5db9, seq=4/1024, ttl=63 (request in 10)
12	4.081573	192.168.1.7	192.168.2.8	ICMP	98	Echo (ping) request id=0x5eb9, seq=5/1280, ttl=64 (reply in 13)
13	4.096159	192.168.2.8	192.168.1.7	ICMP	98	Echo (ping) reply id=0x5eb9, seq=5/1280, ttl=63 (request in 12)

> Ethernet II, Src: Private_66:68:02 (00:50:79:66:68:02), Dst: cc:01:6e:fc:1a:3e > Internet Protocol Version 4, Src: 192.168.1.7, Dst: 192.168.2.8 > Internet Control Message Protocol Type: 8 (Echo (ping) request) Code: 0 Checksum: 0xc551 [correct] [Checksum Status: Good] Identifier (BE): 23225 (0x5ab9) Identifier (LE): 47450 (0xb95a) Sequence Number (BE): 1 (0x0001) Sequence Number (LE): 256 (0x0100) [Response frame: 4] Data (56 bytes)		<pre> 0000 cc 01 6e fc 00 00 00 50 79 66 68 02 08 00 45 00 ..n...P yfh...E- 0010 00 54 b9 5a 00 00 40 01 3c ef c0 a8 01 07 c0 a8 .T.Z..@. <..... 0020 02 08 08 00 c5 51 5a b9 00 01 08 09 0a 0b 0c 0d QZ..... 0030 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 0040 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c 2d ..!"#\$%&'()*+,- 0050 2e 2f 30 31 32 33 34 35 36 37 38 39 3a 3b 3c 3d ./012345 6789:;<= 0060 3e 3f >? </pre>
---	--	--

ARP-запрос отправляет устройство с IP-адресом 192.168.1.7 для получения MAC-адреса устройства с IP-адресом 192.168.1.1. Этот запрос широковещательный (Broadcast), так как отправляется всем устройствам в сети. Запрос ответы содержат соответствующие MAC-адреса.

Для icmp каждый Echo request отображается соответствующим Echo reply, подтверждающий успешную доставку пакета.