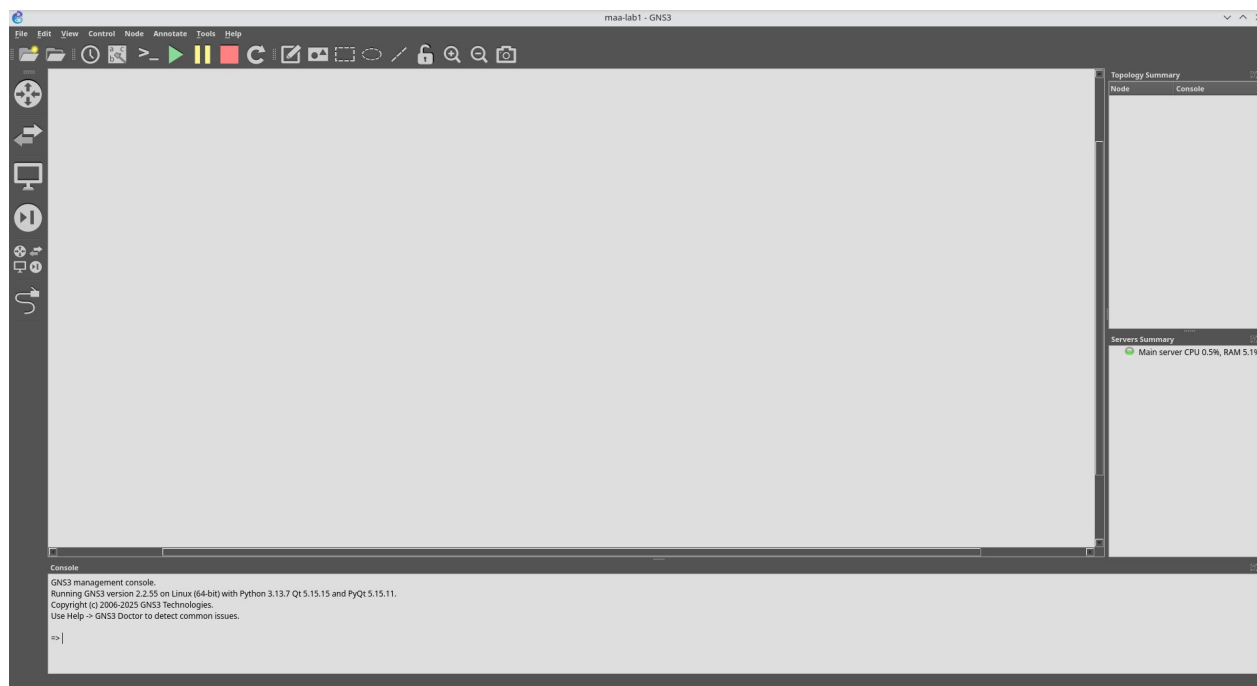


Лабораторная работа №1

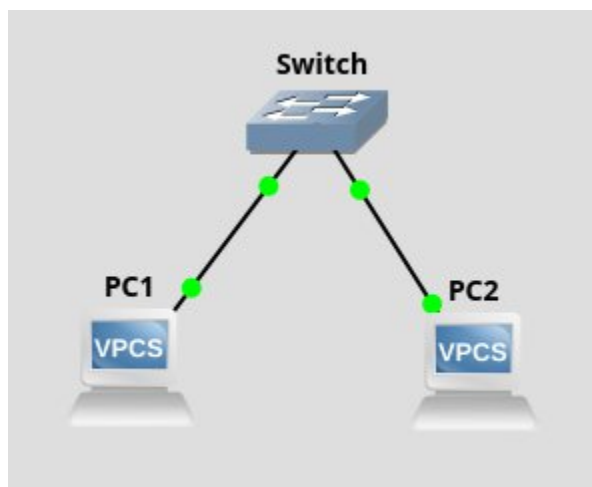
Пункт 1

Эмулятор GNS3 был установлен и настроен



Пункт 2

Далее была создана простейшая сеть, состоящая из 1 коммутатора и 2 компьютеров с адресами из сети «192.168.1.0/24».



Для первого компьютера был назначен адрес «192.168.1.1/24», для второго «192.168.1.2/24»:

(PC1)

ip 192.168.1.1 /24

(PC2)

ip 192.168.1.2 /24

Пункт 3

Далее была выполнена команда «ping» с компьютера «PC1» с адресом «192.168.1.1/24» на компьютер «PC2» с адресом «192.168.1.2/24»:

(PC1)

ping 192.168.1.2

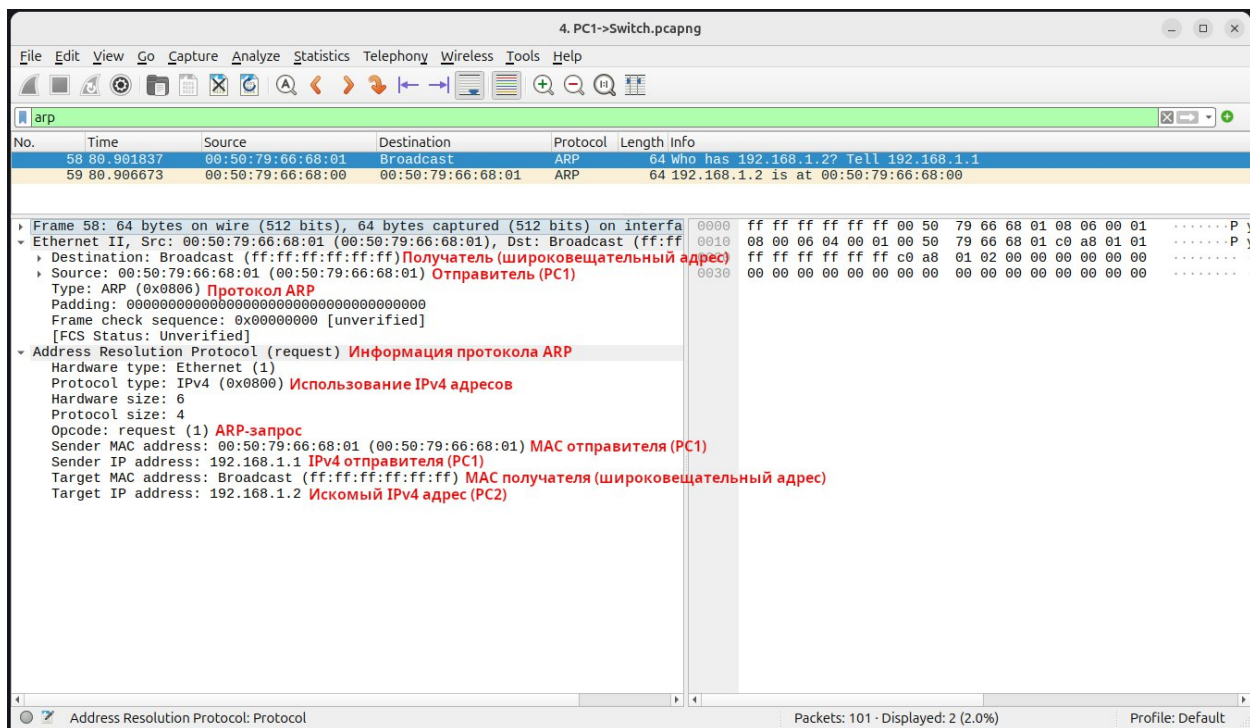
```
PC1> ping 192.168.1.2

84 bytes from 192.168.1.2 icmp_seq=1 ttl=64 time=1.484 ms
84 bytes from 192.168.1.2 icmp_seq=2 ttl=64 time=0.627 ms
84 bytes from 192.168.1.2 icmp_seq=3 ttl=64 time=3.880 ms
84 bytes from 192.168.1.2 icmp_seq=4 ttl=64 time=0.617 ms
84 bytes from 192.168.1.2 icmp_seq=5 ttl=64 time=3.219 ms
```

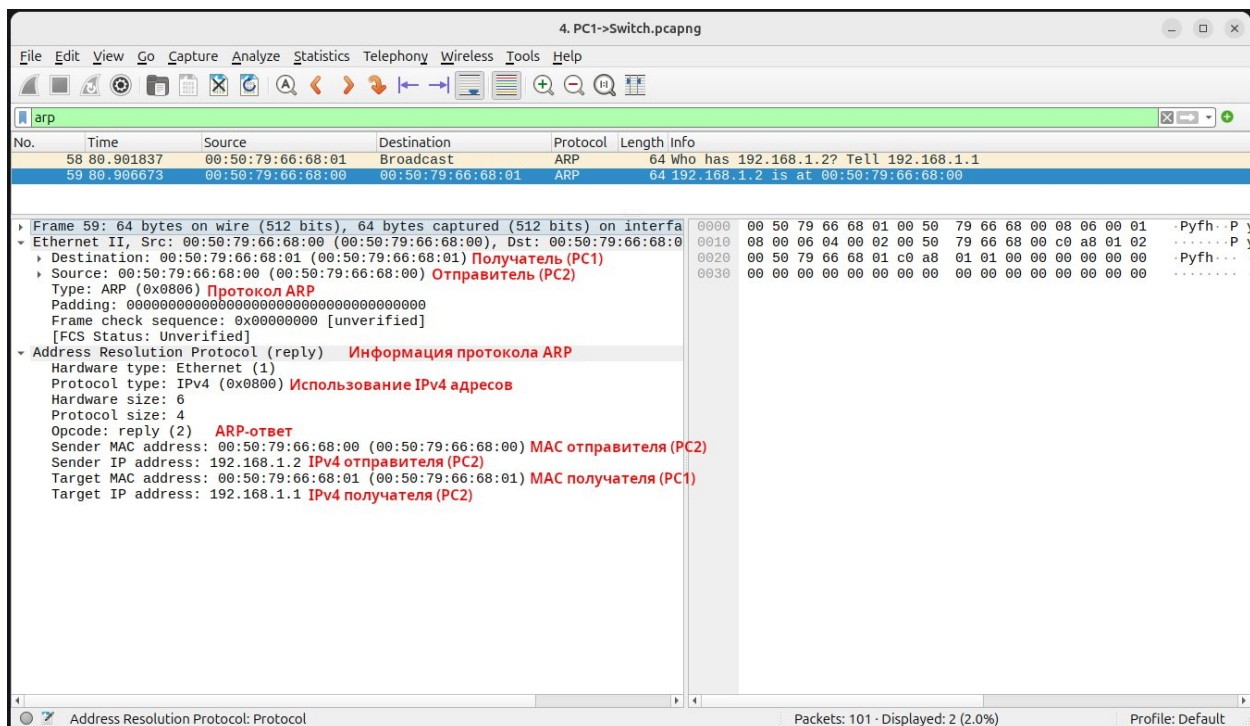
Пункт 4

Используя средства GNS3, был перехвачен трафик на всех линках (PC1<->Switch, PC2<->Switch), после чего полученный трафик был отфильтрован по протоколу «ARP» и проанализирован в программе «Wireshark».

Анализ ARP-запроса на линке PC1 <-> Switch:



Анализ ARP-ответа на линке PC1 <-> Switch:

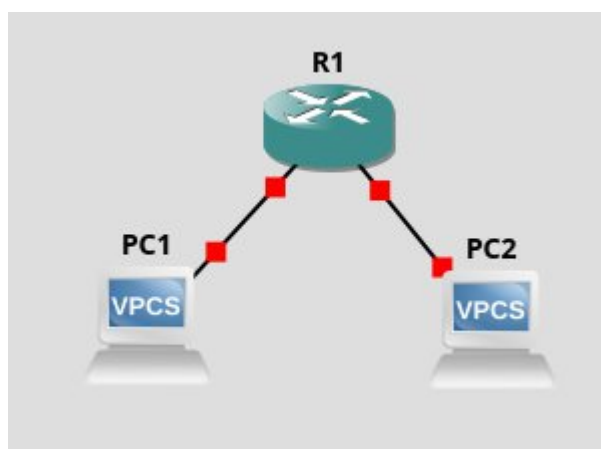


На линке PC2 <-> Switch были захвачены те же самые пакеты:

4. PC2->Switch.pcapng						
No.	Time	Source	Destination	Protocol	Length	Info
29	36.680641	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.1.2? Tell 192.168.1.1
30	36.680706	00:50:79:66:68:00	00:50:79:66:68:01	ARP	64	192.168.1.2 is at 00:50:79:66:68:00

Пункт 5

Далее была создана простейшая сеть, состоящая из 1 маршрутизатора и 2 компьютеров с адресами из разных сетей – «192.168.2.0/24» и «192.168.3.0/24».



Для первого компьютера был назначен адрес «192.168.2.2/24» и шлюз «192.168.2.1», для второго адрес «192.168.3.2/24» и шлюз «192.168.3.1»:

(PC1)

```
ip 192.168.2.2 /24 192.168.2.1
```

(PC2)

```
ip 192.168.3.2 /24 192.168.3.1
```

Для маршрутизатора был назначен адрес «192.168.2.1/24» в сети с PC1 и адрес «192.168.3.1» в сети с PC2.

(R1)

```
enable
```

```
configure terminal
```

```
interface FastEthernet 0/0
```

```
ip address 192.168.2.1 255.255.255.0
```

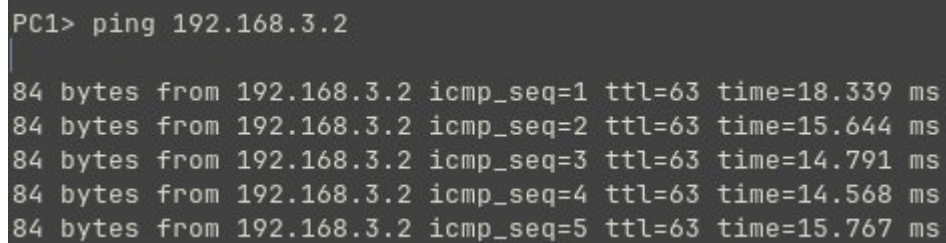
```
no shutdown  
end  
configure terminal  
interface FastEthernet 1/0  
ip address 192.168.3.1 255.255.255.0  
no shutdown  
end
```

Пункт 6

Далее была выполнена команда «ping» с компьютера «PC1» с адресом «192.168.2.2/24» на компьютер «PC2» с адресом «192.168.3.2/24»:

(PC1)

```
ping 192.168.3.2
```



```
PC1> ping 192.168.3.2  
84 bytes from 192.168.3.2 icmp_seq=1 ttl=63 time=18.339 ms  
84 bytes from 192.168.3.2 icmp_seq=2 ttl=63 time=15.644 ms  
84 bytes from 192.168.3.2 icmp_seq=3 ttl=63 time=14.791 ms  
84 bytes from 192.168.3.2 icmp_seq=4 ttl=63 time=14.568 ms  
84 bytes from 192.168.3.2 icmp_seq=5 ttl=63 time=15.767 ms
```

Пункт 7

Используя средства GNS3, был перехвачен трафик на всех линках (PC1<->R1, PC2<->R1), после чего полученный трафик был отфильтрован по протоколам «ARP» и «ICMP», и проанализирован в программе «Wireshark».

Анализ ARP-запроса на линке PC1 <-> R1 (запрос от PC1, определение MAC-адреса шлюза):

7. PC1->R1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp || icmp

No.	Time	Source	Destination	Protocol	Length	Info
3	38.136210	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.3.2? Tell 0.0.0.0
4	39.136286	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.3.2? Tell 0.0.0.0
6	40.136768	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.3.2? Tell 0.0.0.0
8	70.492221	00:50:79:66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.2.2 (Request)
9	71.492858	00:50:79:66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.2.2 (Request)
10	72.493177	00:50:79:66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.2.2 (Request)
13	118.216195	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.2.1? Tell 192.168.2.2
14	118.222109	cc:01:32:a1:00:00	00:50:79:66:68:01	ARP	60	192.168.2.1 is at cc:01:32:a1:00:00
15	118.222574	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc380, seq=1/256, ttl=64 (no response...)
16	120.223361	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc580, seq=2/512, ttl=64 (reply in 17)

Frame 13: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface 0

Ethernet II, Src: 00:50:79:66:68:01 (00:50:79:66:68:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff) **Получатель (широковещательный адрес)**

Source: 00:50:79:66:68:01 (00:50:79:66:68:01) **Отправитель (PC1)**

Type: ARP (0x0806) **Протокол ARP**

Padding: 00000000000000000000000000000000

Frame check sequence: 0x00000000 [unverified]

[FCS Status: Unverified]

Address Resolution Protocol (request) **Информация протокола ARP**

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800) **Использование IPv4 адресов**

Hardware size: 6

Protocol size: 4

Opcode: request (1) **ARP-запрос**

Sender MAC address: 00:50:79:66:68:01 (00:50:79:66:68:01) **MAC отправителя (PC1)**

Sender IP address: 192.168.2.2 **IPv4 отправителя (PC1)**

Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff) **MAC получателя (широковещательный адрес)**

Target IP address: 192.168.2.1 **Искомый IPv4 адрес (R1)**

7. PC1->R1.pcapng

Packets: 39 · Displayed: 17 (43.6%)

Profile: Default

Анализ ARP-ответа на линке PC1 <-> R1 (ответ от R1):

7. PC1->R1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp || icmp

No.	Time	Source	Destination	Protocol	Length	Info
3	38.136210	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.3.2? Tell 0.0.0.0
4	39.136286	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.3.2? Tell 0.0.0.0
6	40.136768	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.3.2? Tell 0.0.0.0
8	70.492221	00:50:79:66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.2.2 (Request)
9	71.492858	00:50:79:66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.2.2 (Request)
10	72.493177	00:50:79:66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.2.2 (Request)
13	118.216195	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.2.1? Tell 192.168.2.2
14	118.222109	cc:01:32:a1:00:00	00:50:79:66:68:01	ARP	60	192.168.2.1 is at cc:01:32:a1:00:00
15	118.222574	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc380, seq=1/256, ttl=64 (no response...)
16	120.223361	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc580, seq=2/512, ttl=64 (reply in 17)

Frame 14: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0

Ethernet II, Src: cc:01:32:a1:00:00 (cc:01:32:a1:00:00), Dst: 00:50:79:66:68:01 (00:50:79:66:68:01) **Получатель (PC1)**

Source: cc:01:32:a1:00:00 (cc:01:32:a1:00:00) **Отправитель (R1)**

Type: ARP (0x0806) **Протокол ARP**

Padding: 00000000000000000000000000000000

Address Resolution Protocol (reply) **Информация протокола ARP**

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800) **Использование IPv4 адресов**

Hardware size: 6

Protocol size: 4

Opcode: reply (2) **ARP-ответ**

Sender MAC address: cc:01:32:a1:00:00 (cc:01:32:a1:00:00) **MAC отправителя (R1)**

Sender IP address: 192.168.2.1 **IPv4 отправителя (R1)**

Target MAC address: 00:50:79:66:68:01 (00:50:79:66:68:01) **MAC получателя (PC1)**

Target IP address: 192.168.2.2 **IPv4 получателя (PC1)**

7. PC1->R1.pcapng

Packets: 39 · Displayed: 17 (43.6%)

Profile: Default

На линке PC2 <-> R1 был произведен аналогичный обмен, но инициатором был маршрутизатор R1 – он произвел ARP-запрос (поиск MAC-адреса PC2), PC2 ответил своим MAC-адресом:

7. PC2->R1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp || icmp

No.	Time	Source	Destination	Protocol	Length	Info
5	85.464644	00:50:79:66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.3.2 (Request)
6	86.465517	00:50:79:66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.3.2 (Request)
7	87.466304	00:50:79:66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.3.2 (Request)
9	102.944624	cc:01:32:a1:00:10	Broadcast	ARP	60	Who has 192.168.3.2? Tell 192.168.3.1
10	102.944707	00:50:79:66:68:00	cc:01:32:a1:00:10	ARP	60	192.168.3.2 is at 00:50:79:66:68:00
11	104.945822	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc580, seq=2/512, ttl=63 (reply in 12)
12	104.945905	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0xc580, seq=2/512, ttl=64 (request in 11)
13	105.961799	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc680, seq=3/768, ttl=63 (reply in 14)
14	105.961873	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0xc680, seq=3/768, ttl=64 (request in 13)
15	106.977586	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc780, seq=4/1024, ttl=63 (reply in 16)
16	106.977682	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0xc780, seq=4/1024, ttl=64 (request in 15)
17	107.993043	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc880, seq=5/1280, ttl=63 (reply in 18)
18	107.993144	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0xc880, seq=5/1280, ttl=64 (request in 17)

Далее проанализируем пакеты протокола ICMP, команда ping была запущена с PC1 (192.168.2.2/24) на PC2 (192.168.3.2/24) и прошла через шлюз R1.

Анализ ICMP-запроса на линке PC2 <-> R1:

7. PC2->R1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp || icmp

No.	Time	Source	Destination	Protocol	Length	Info
10	102.944707	00:50:79:66:68:00	cc:01:32:a1:00:10	ARP	60	192.168.3.2 is at 00:50:79:66:68:00
11	104.945822	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc580, seq=2/512, ttl=63 (reply in 12)
12	104.945905	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0xc580, seq=2/512, ttl=64 (request in ...)
13	105.961799	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc680, seq=3/768, ttl=63 (reply in 14)

Frame 11: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 00:50:79:66:68:00

Ethernet II, Src: cc:01:32:a1:00:10 (cc:01:32:a1:00:10), Dst: 00:50:79:66:68:00 (00:50:79:66:68:00) **MAC получателя (PC2)**

Source: cc:01:32:a1:00:10 (cc:01:32:a1:00:10) **MAC отправителя (шлюз R1 (не PC1))**

Type: IPv4 (0x0800) **Протокол IPv4**

Internet Protocol Version 4, Src: 192.168.2.2, Dst: 192.168.3.2 **Данные IP-пакета**

0100 = Version: 4

.... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 84

Identification: 0x80c4 (32964)

0000 = Flags: 0x0

...0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 63

Protocol: ICMP (1)

Header Checksum: 0x7490 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.2.2 **IPv4 адрес отправителя (PC1)**

Destination Address: 192.168.3.2 **IPv4 адрес получателя (PC2)**

Internet Control Message Protocol **Данные ICMP-пакета**

Type: 8 (Echo (ping) request) **ICMP ping запрос**

Code: 0

Checksum: 0x5a89 [correct]

[Checksum Status: Good]

Identifier (BE): 59560 (0xc580)

Identifier (LE): 32965 (0x80c5)

Sequence Number (BE): 2 (0x0002) **Номер ping в последовательности**

Sequence Number (LE): 512 (0x0200)

Response frame: 12

Data (56 bytes) **Данные, которые нужно отправить обратно**

Internet Control Message Protocol: Protocol

Packets: 35 · Displayed: 13 (37.1%)

Profile: Default

Анализ ICMP-ответа на линке PC2 <-> R1:

7. PC2->R1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp | icmp

No.	Time	Source	Destination	Protocol	Length	Info
10	102.944707	00:50:79:66:68:00	cc:01:32:a1:00:10	ARP	60	192.168.3.2 is at 00:50:79:66:68:00
11	104.945822	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc580, seq=2/512, ttl=63 (reply in 12)
12	104.945905	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0xc580, seq=2/512, ttl=64 (request in ...)

Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface 0

Ethernet II, Src: 00:50:79:66:68:00 (00:50:79:66:68:00), Dst: cc:01:32:a1:00:10 (cc:01:32:a1:00:10) **MAC получателя (шлюза R1 (не PC1))**

Source: 00:50:79:66:68:00 (00:50:79:66:68:00) **MAC отправителя (PC2)**

Type: IPv4 (0x0800) **Протокол IPv4**

Internet Protocol Version 4, Src: 192.168.3.2, Dst: 192.168.2.2 **Данные IP-пакета**

0100 = Version: 4

... 0101 = Header Length: 20 bytes (5)

Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)

Total Length: 84

Identification: 0x80c4 (32964)

0000 = Flags: 0x0

... 0 0000 0000 0000 = Fragment Offset: 0

Time to Live: 64

Protocol: ICMP (1)

Header Checksum: 0x7390 [validation disabled]

[Header checksum status: Unverified]

Source Address: 192.168.3.2 **IPv4 адрес отправителя (PC2)**

Destination Address: 192.168.2.2 **IPv4 адрес получателя (PC1)**

Internet Control Message Protocol **Данные ICMP-пакета**

Type: 0 (Echo (ping) reply) **ICMP ping ответ**

Code: 0

Checksum: 0x6289 [correct]

[Checksum Status: Good]

Identifier (BE): 50560 (0xc580)

Identifier (LE): 32965 (0x80c5)

Sequence Number (BE): 2 (0x0002)

Sequence Number (LE): 512 (0x0200) **Номер ping в последовательности**

[Request frame: 11]

[Response time: 0.083 ms]

Data (56 bytes) **Данные, которые были отправлены обратно**

Internet Control Message Protocol: Protocol

Packets: 35 · Displayed: 13 (37.1%)

Profile: Default

На линке PC1 <-> R1 можно наблюдать аналогичную ситуацию (за исключением загадочной потери 1-го ICMP-запроса):

7. PC1->R1.pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp | icmp

No.	Time	Source	Destination	Protocol	Length	Info
13	118.216195	00:50:79:66:68:01	Broadcast	ARP	64	Who has 192.168.2.1? Tell 192.168.2.2
14	118.222109	cc:01:32:a1:00:00	00:50:79:66:68:01	ARP	60	192.168.2.1 is at cc:01:32:a1:00:00
15	118.222574	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc380, seq=1/256, ttl=64 (no response...)
16	120.223361	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc580, seq=2/512, ttl=64 (reply in 17)
17	120.243481	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0xc580, seq=2/512, ttl=63 (request in ...)
18	121.244643	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc680, seq=3/768, ttl=64 (reply in 19)
19	121.259382	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0xc680, seq=3/768, ttl=63 (request in ...)
20	122.259692	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc780, seq=4/1024, ttl=64 (reply in 2...)
21	122.275228	192.168.3.2	192.168.2.2	ICMP	98	Echo (ping) reply id=0xc780, seq=4/1024, ttl=63 (request in ...)
22	123.275642	192.168.2.2	192.168.3.2	ICMP	98	Echo (ping) request id=0xc880, seq=5/1280, ttl=64 (reply in 2...)