Простые сети в GNS3. Анализ трафика

Абд эль хай мохамад

19.10.2023

РУДН, Москва, Российская Федерация

Введение

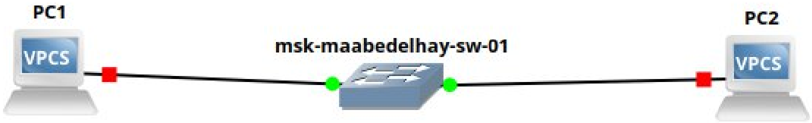
Построение простейших моделей сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, анализ трафика посредством Wireshark.

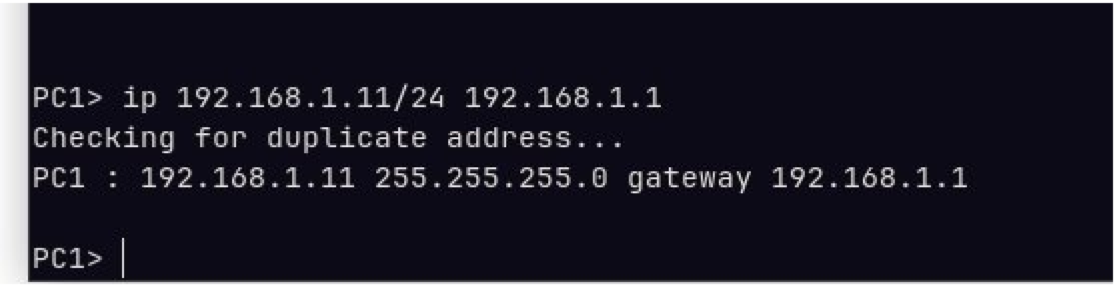
Задачи

- Моделирование простейшей сети на базе коммутатора в GNS3
- Анализ трафика в GNS3 посредством Wireshark
- Моделирование простейшей сети на базе маршрутизатора FRR в GNS3
- Моделирование простейшей сети на базе маршрутизатора VyOS в GNS3

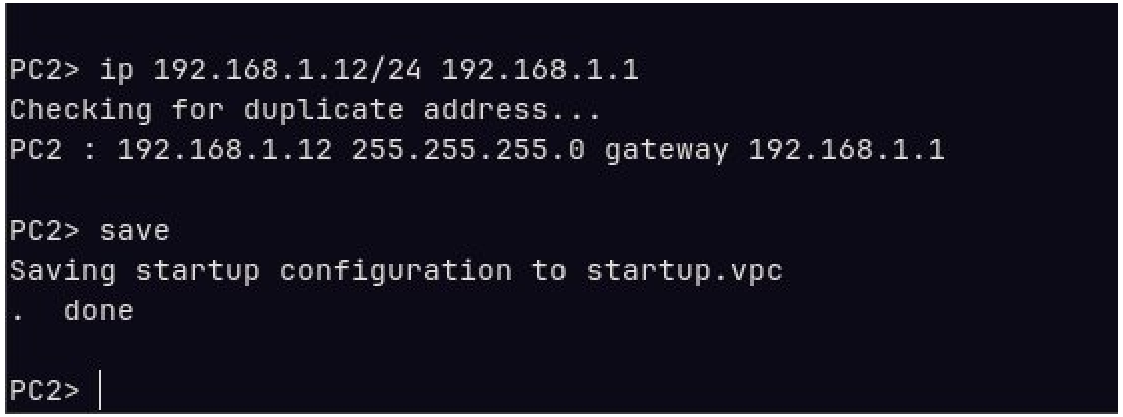
1. Моделирование простейшей сети на базе коммутатора в GNS3

Настроил IP-адресацию для PC1 и PC2, затем проверил соединение с помощью команды ping.

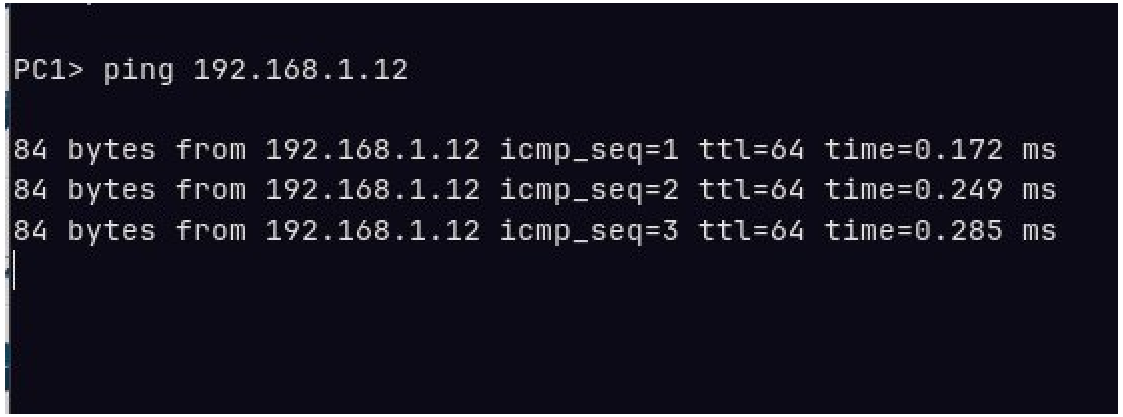




```
PC1> ip 192.168.1.11/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.11 255.255.255.0 gateway 192.168.1.1

PC1>
```



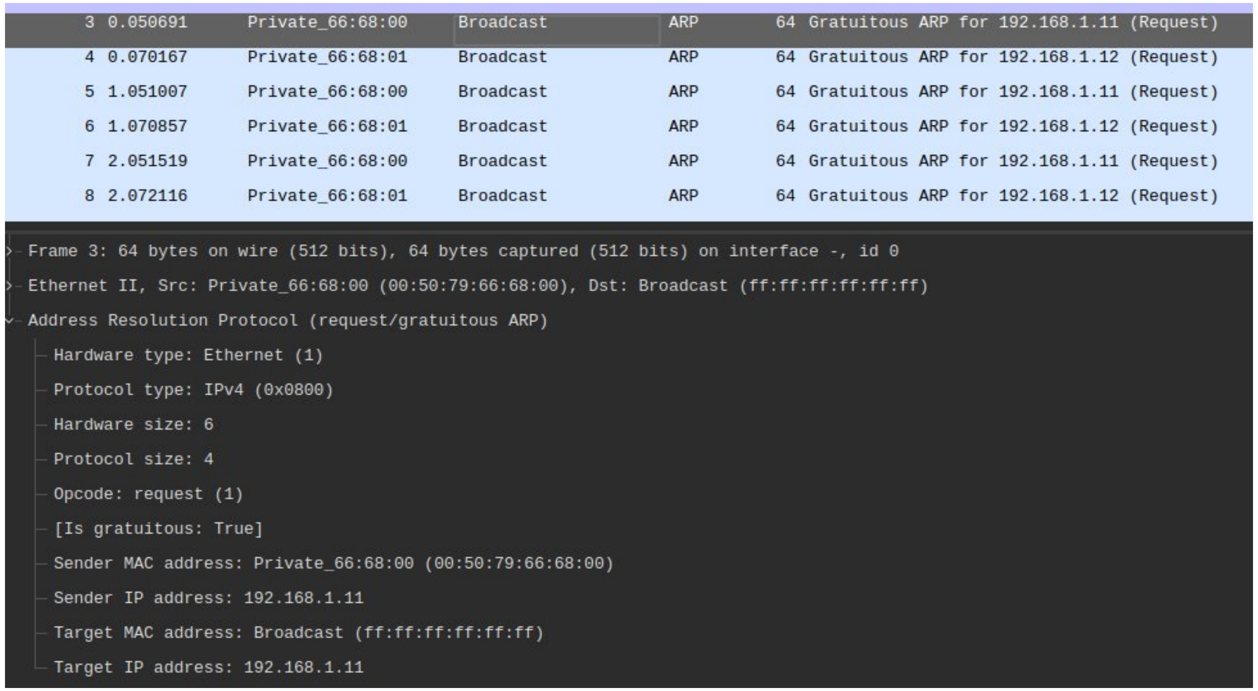
```
PC2> ip 192.168.1.12/24 192.168.1.1
Checking for duplicate address...
PC2 : 192.168.1.12 255.255.255.0 gateway 192.168.1.1

PC2> save
Saving startup configuration to startup.vpc
.  done

PC2>
```



```
PC1> ping 192.168.1.12

84 bytes from 192.168.1.12 icmp_seq=1 ttl=64 time=0.172 ms
84 bytes from 192.168.1.12 icmp_seq=2 ttl=64 time=0.249 ms
84 bytes from 192.168.1.12 icmp_seq=3 ttl=64 time=0.285 ms
```

2. Анализ трафика в GNS3 посредством Wireshark

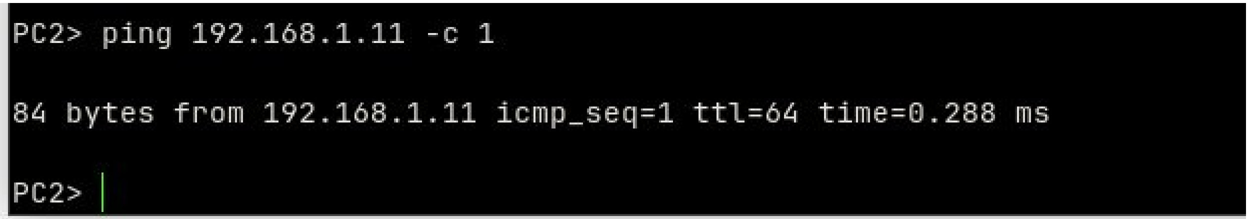
Анализ ARP-трафика



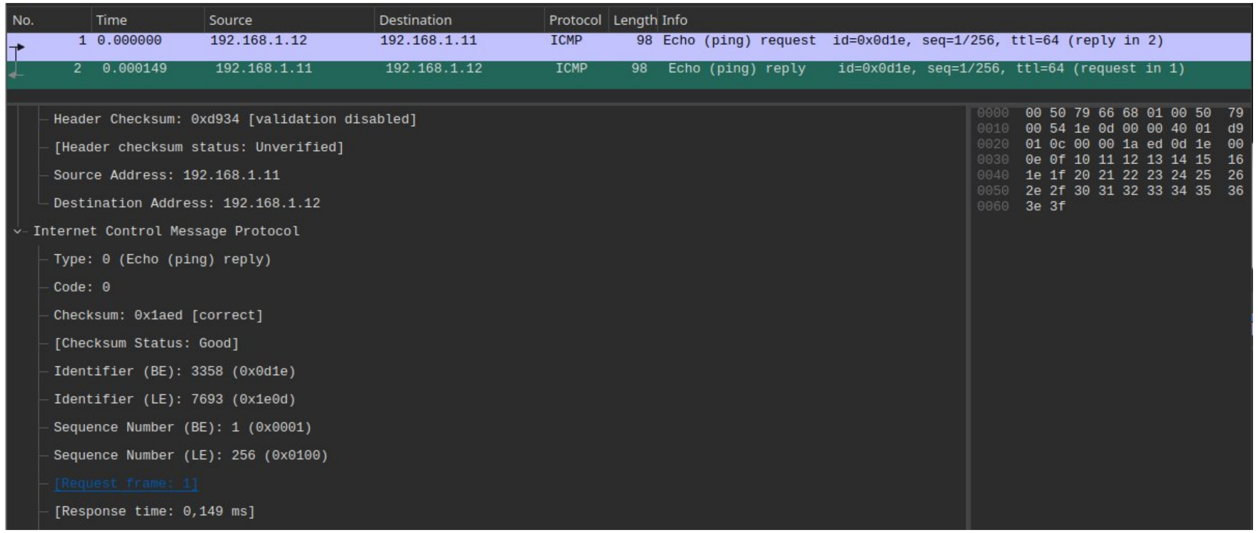
```
  3 0.050691    Private_66:68:00   Broadcast   ARP    64 Gratuitous ARP for 192.168.1.11 (Request)
  4 0.070167    Private_66:68:01   Broadcast   ARP    64 Gratuitous ARP for 192.168.1.12 (Request)
  5 1.051007    Private_66:68:00   Broadcast   ARP    64 Gratuitous ARP for 192.168.1.11 (Request)
  6 1.070857    Private_66:68:01   Broadcast   ARP    64 Gratuitous ARP for 192.168.1.12 (Request)
  7 2.051519    Private_66:68:00   Broadcast   ARP    64 Gratuitous ARP for 192.168.1.11 (Request)
  8 2.072116    Private_66:68:01   Broadcast   ARP    64 Gratuitous ARP for 192.168.1.12 (Request)

> Frame 3: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0
> Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
v Address Resolution Protocol (request/gratuitous ARP)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (1)
    [Is gratuitous: True]
    Sender MAC address: Private_66:68:00 (00:50:79:66:68:00)
    Sender IP address: 192.168.1.11
    Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff)
    Target IP address: 192.168.1.11
```

2. Анализ трафика в GNS3 посредством Wireshark

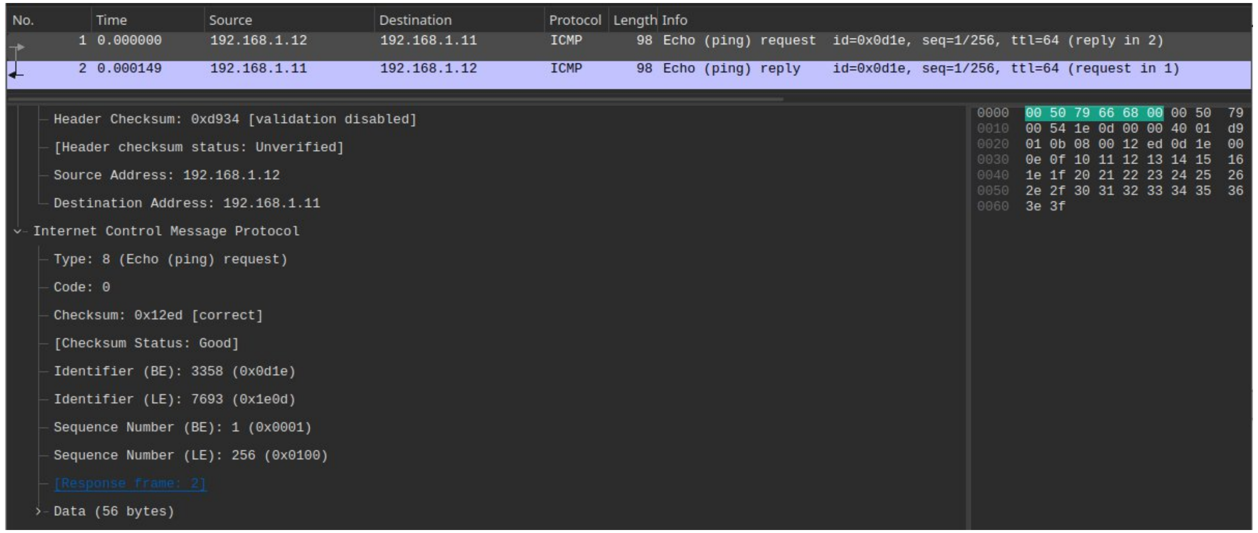
Анализ ICMP-трафика



```
PC2> ping 192.168.1.11 -c 1

84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=0.288 ms

PC2>
```



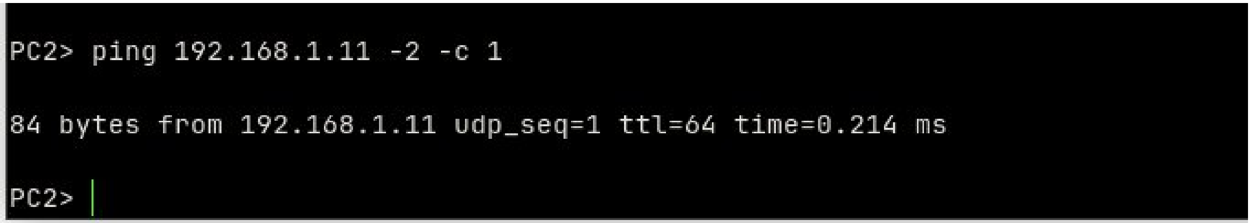
```
No.   Time      Source        Destination   Protocol Length Info
    1 0.000000  192.168.1.12  192.168.1.11  ICMP        98 Echo (ping) request  id=0x0d1e, seq=1/256, ttl=64 (reply in 2)
    2 0.000149  192.168.1.11  192.168.1.12  ICMP        98 Echo (ping) reply    id=0x0d1e, seq=1/256, ttl=64 (request in 1)

    Header Checksum: 0xd934 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.11
    Destination Address: 192.168.1.12
  Internet Control Message Protocol
    Type: 0 (Echo (ping) reply)
    Code: 0
    Checksum: 0x1aed [correct]
    [Checksum Status: Good]
    Identifier (BE): 3358 (0x0d1e)
    Identifier (LE): 7693 (0x1e0d)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Request frame: 1]
    [Response time: 0,149 ms]

0000  00 50 79 66 68 01 00 50  79
0010  00 54 1e 0d 00 00 40 01  d9
0020  01 0c 00 00 1a ed 0d 1e  00
0030  0e 0f 10 11 12 13 14 15  16
0040  1e 1f 20 21 22 23 24 25  26
0050  2e 2f 30 31 32 33 34 35  36
0060  3e 3f
```



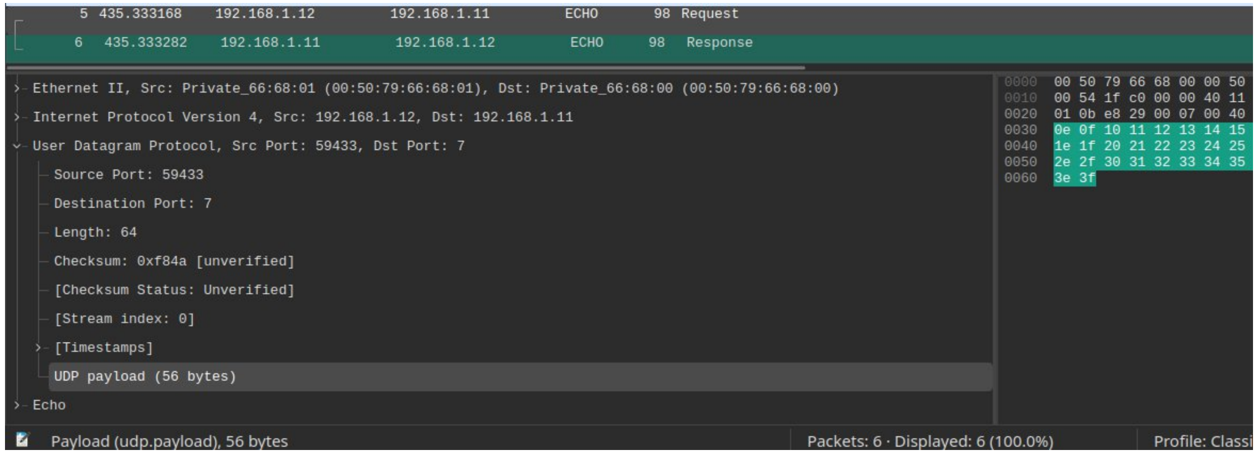
```
No.   Time      Source        Destination   Protocol Length Info
    1 0.000000  192.168.1.12  192.168.1.11  ICMP        98 Echo (ping) request  id=0x0d1e, seq=1/256, ttl=64 (reply in 2)
    2 0.000149  192.168.1.11  192.168.1.12  ICMP        98 Echo (ping) reply    id=0x0d1e, seq=1/256, ttl=64 (request in 1)

    Header Checksum: 0xd934 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 192.168.1.12
    Destination Address: 192.168.1.11
  Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x12ed [correct]
    [Checksum Status: Good]
    Identifier (BE): 3358 (0x0d1e)
    Identifier (LE): 7693 (0x1e0d)
    Sequence Number (BE): 1 (0x0001)
    Sequence Number (LE): 256 (0x0100)
    [Response frame: 2]
  > Data (56 bytes)

0000  00 50 79 66 68 00 00 50  79
0010  00 54 1e 0d 00 00 40 01  d9
0020  01 0b 08 00 12 ed 0d 1e  00
0030  0e 0f 10 11 12 13 14 15  16
0040  1e 1f 20 21 22 23 24 25  26
0050  2e 2f 30 31 32 33 34 35  36
0060  3e 3f
```

2. Анализ трафика в GNS3 посредством Wireshark

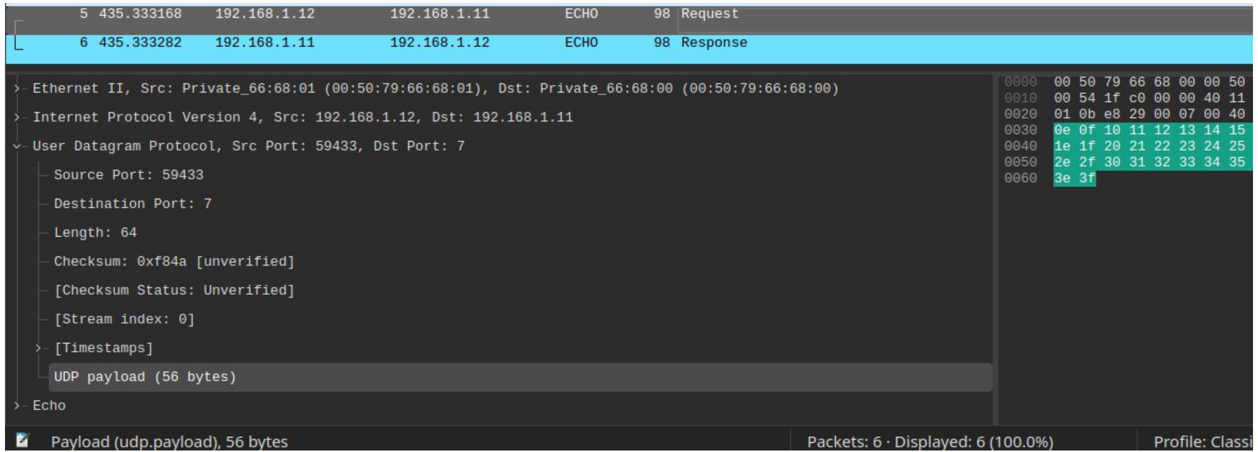
Анализ UDP-трафика



```
PC2> ping 192.168.1.11 -2 -c 1

84 bytes from 192.168.1.11 udp_seq=1 ttl=64 time=0.214 ms

PC2>
```



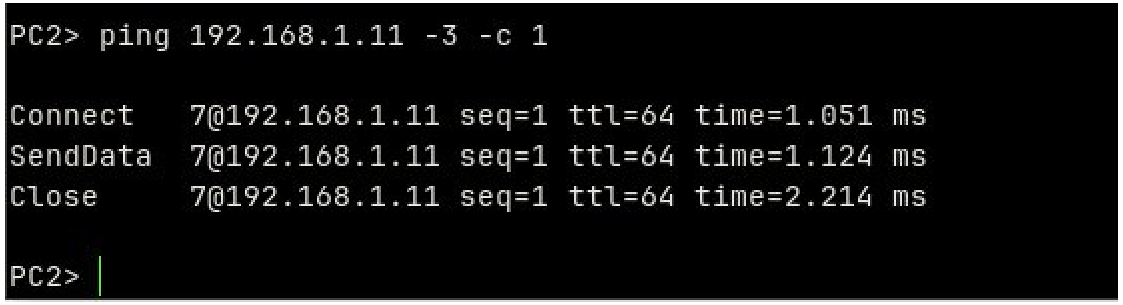
```
    5 435.333168    192.168.1.12        192.168.1.11        ECHO      98 Request
    6  435.333282    192.168.1.11        192.168.1.12        ECHO      98  Response

> Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.11
v User Datagram Protocol, Src Port: 59433, Dst Port: 7
    Source Port: 59433
    Destination Port: 7
    Length: 64
    Checksum: 0xf84a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (56 bytes)
> Echo

0000  00 50 79 66 68 00 00 50
0010  00 54 1f c0 00 00 40 11
0020  01 0b e8 29 00 07 00 40
0030  0e 0f 10 11 12 13 14 15
0040  1e 1f 20 21 22 23 24 25
0050  2e 2f 30 31 32 33 34 35
0060  3e 3f

Payload (udp.payload), 56 bytes          Packets: 6 · Displayed: 6 (100.0%)          Profile: Classi
```



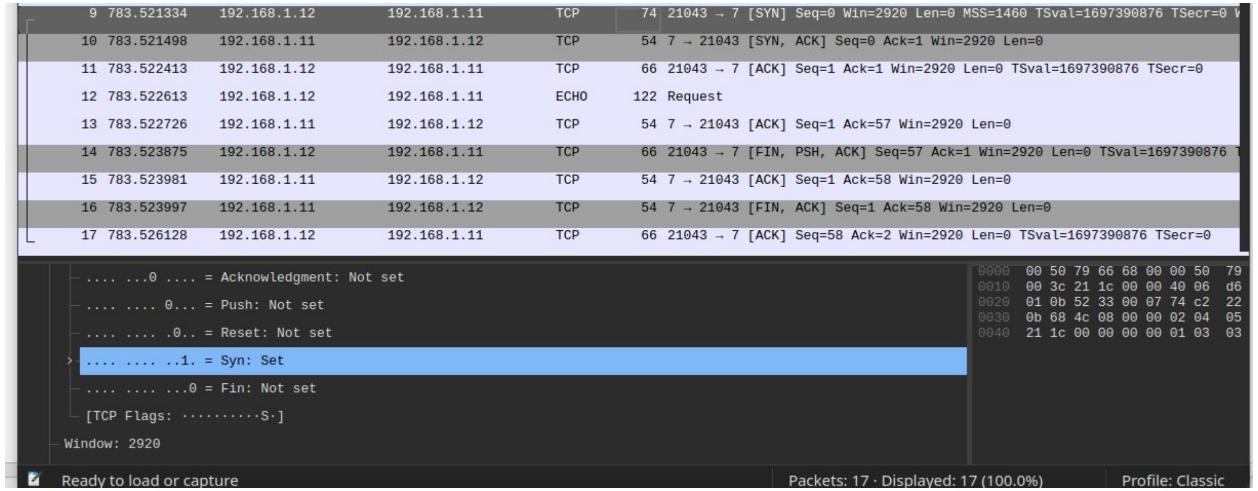
```
    5 435.333168    192.168.1.12        192.168.1.11        ECHO      98 Request
    6 435.333282    192.168.1.11        192.168.1.12        ECHO      98 Response

> Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Private_66:68:00 (00:50:79:66:68:00)
> Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.11
v User Datagram Protocol, Src Port: 59433, Dst Port: 7
    Source Port: 59433
    Destination Port: 7
    Length: 64
    Checksum: 0xf84a [unverified]
    [Checksum Status: Unverified]
    [Stream index: 0]
  > [Timestamps]
    UDP payload (56 bytes)
> Echo

0000  00 50 79 66 68 00 00 50
0010  00 54 1f c0 00 00 40 11
0020  01 0b e8 29 00 07 00 40
0030  0e 0f 10 11 12 13 14 15
0040  1e 1f 20 21 22 23 24 25
0050  2e 2f 30 31 32 33 34 35
0060  3e 3f

Payload (udp.payload), 56 bytes          Packets: 6 · Displayed: 6 (100.0%)          Profile: Classi
```

2. Анализ трафика в GNS3 посредством Wireshark

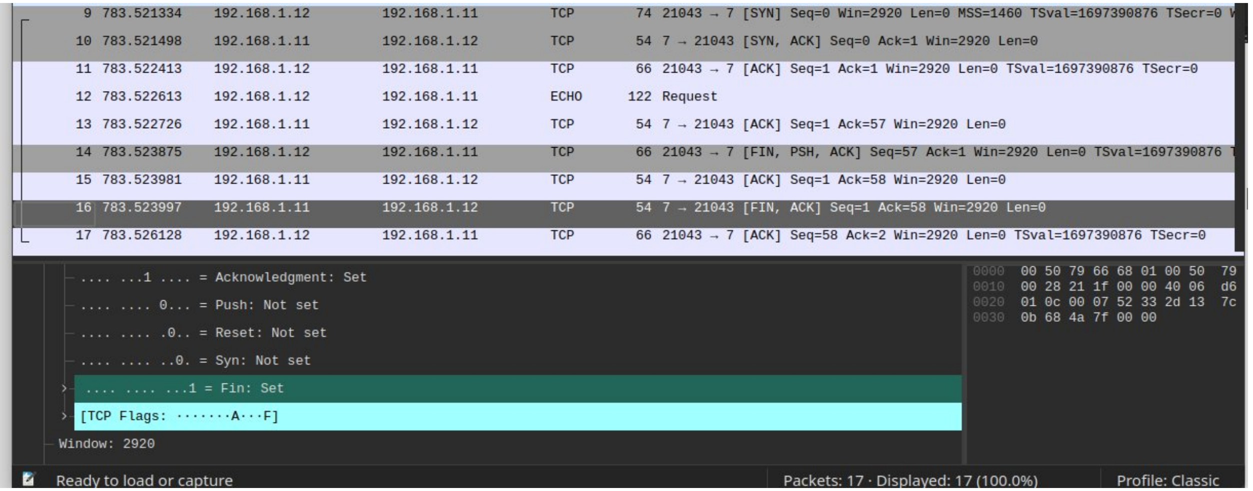
Анализ TCP-трафика



```
PC2> ping 192.168.1.11 -3 -c 1

Connect   7@192.168.1.11 seq=1 ttl=64 time=1.051 ms
SendData  7@192.168.1.11 seq=1 ttl=64 time=1.124 ms
Close     7@192.168.1.11 seq=1 ttl=64 time=2.214 ms

PC2>
```

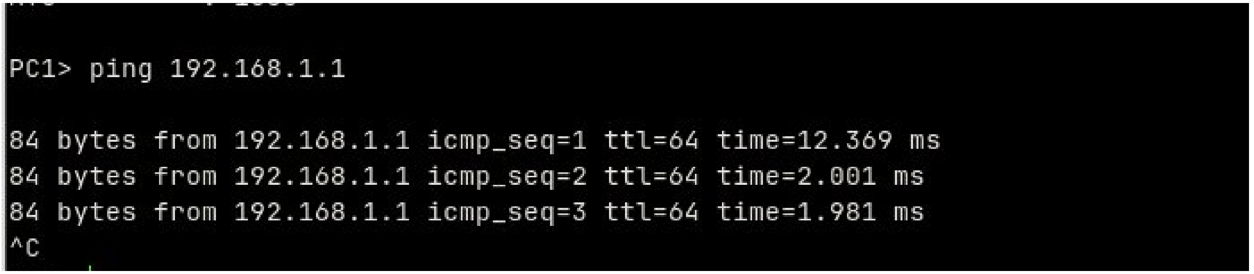


```
 9 783.521334   192.168.1.12   192.168.1.11   TCP    74 21043 → 7 [SYN] Seq=0 Win=2920 Len=0 MSS=1460 TSval=1697390876 TSecr=0 W
10 783.521498   192.168.1.11   192.168.1.12   TCP    54 7 → 21043 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0
11 783.522413   192.168.1.12   192.168.1.11   TCP    66 21043 → 7 [ACK] Seq=1 Ack=1 Win=2920 Len=0 TSval=1697390876 TSecr=0
12 783.522613   192.168.1.12   192.168.1.11   ECHO  122 Request
13 783.522726   192.168.1.11   192.168.1.12   TCP    54 7 → 21043 [ACK] Seq=1 Ack=57 Win=2920 Len=0
14 783.523875   192.168.1.12   192.168.1.11   TCP    66 21043 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1697390876 T
15 783.523981   192.168.1.11   192.168.1.12   TCP    54 7 → 21043 [ACK] Seq=1 Ack=58 Win=2920 Len=0
16 783.523997   192.168.1.11   192.168.1.12   TCP    54 7 → 21043 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
17 783.526128   192.168.1.12   192.168.1.11   TCP    66 21043 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1697390876 TSecr=0

  .... ...0 .... = Acknowledgment: Not set          0000  00 50 79 66 68 00 00 50  79
  .... .... 0... = Push: Not set                    0010  00 3c 21 1c 00 00 40 06  d6
  .... .... .0.. = Reset: Not set                   0020  01 0b 52 33 00 07 74 c2  22
> .... .... ..1. = Syn: Set                         0030  0b 68 4c 08 00 00 02 04  05
  .... .... ...0 = Fin: Not set                     0040  21 1c 00 00 00 00 01 03  03
  [TCP Flags: ··········S·]
Window: 2920

Ready to load or capture          Packets: 17 · Displayed: 17 (100.0%)          Profile: Classic
```

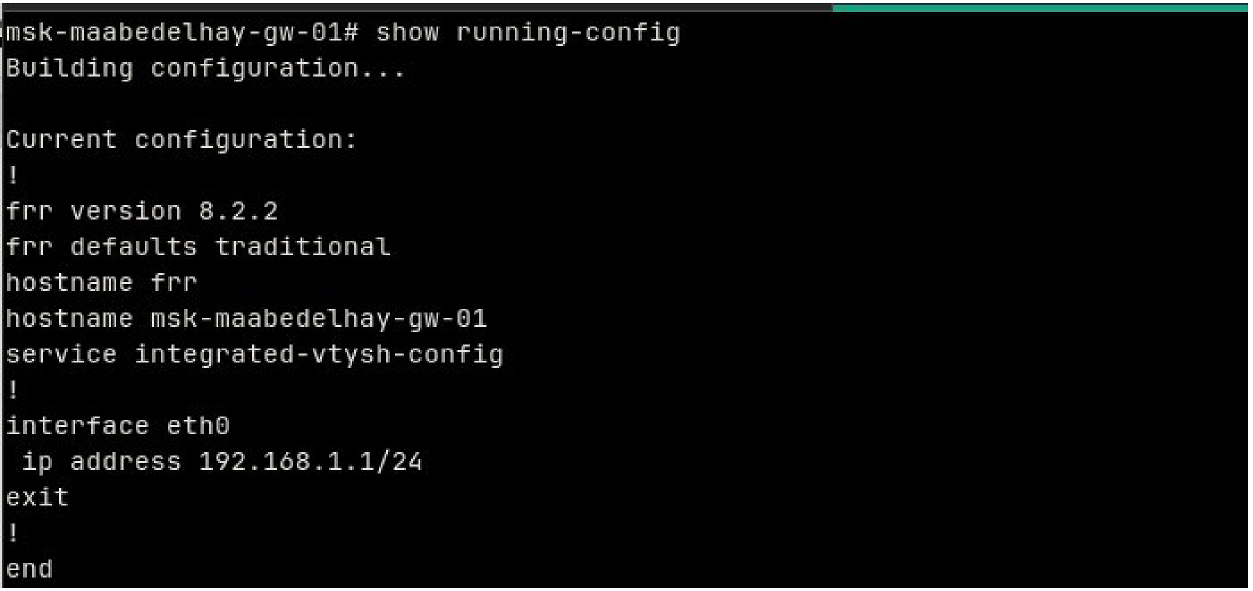


```
 9 783.521334   192.168.1.12   192.168.1.11   TCP    74 21043 → 7 [SYN] Seq=0 Win=2920 Len=0 MSS=1460 TSval=1697390876 TSecr=0 W
10 783.521498   192.168.1.11   192.168.1.12   TCP    54 7 → 21043 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0
11 783.522413   192.168.1.12   192.168.1.11   TCP    66 21043 → 7 [ACK] Seq=1 Ack=1 Win=2920 Len=0 TSval=1697390876 TSecr=0
12 783.522613   192.168.1.12   192.168.1.11   ECHO  122 Request
13 783.522726   192.168.1.11   192.168.1.12   TCP    54 7 → 21043 [ACK] Seq=1 Ack=57 Win=2920 Len=0
14 783.523875   192.168.1.12   192.168.1.11   TCP    66 21043 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1697390876 T
15 783.523981   192.168.1.11   192.168.1.12   TCP    54 7 → 21043 [ACK] Seq=1 Ack=58 Win=2920 Len=0
16 783.523997   192.168.1.11   192.168.1.12   TCP    54 7 → 21043 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
17 783.526128   192.168.1.12   192.168.1.11   TCP    66 21043 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1697390876 TSecr=0

  .... ...1 .... = Acknowledgment: Set              0000  00 50 79 66 68 01 00 50  79
  .... .... 0... = Push: Not set                    0010  00 28 21 1f 00 00 40 06  d6
  .... .... .0.. = Reset: Not set                   0020  01 0c 00 07 52 33 2d 13  7c
  .... .... ..0. = Syn: Not set                     0030  0b 68 4a 7f 00 00
> .... .... ...1 = Fin: Set
> [TCP Flags: ·······A···F]
Window: 2920

Ready to load or capture          Packets: 17 · Displayed: 17 (100.0%)          Profile: Classic
```

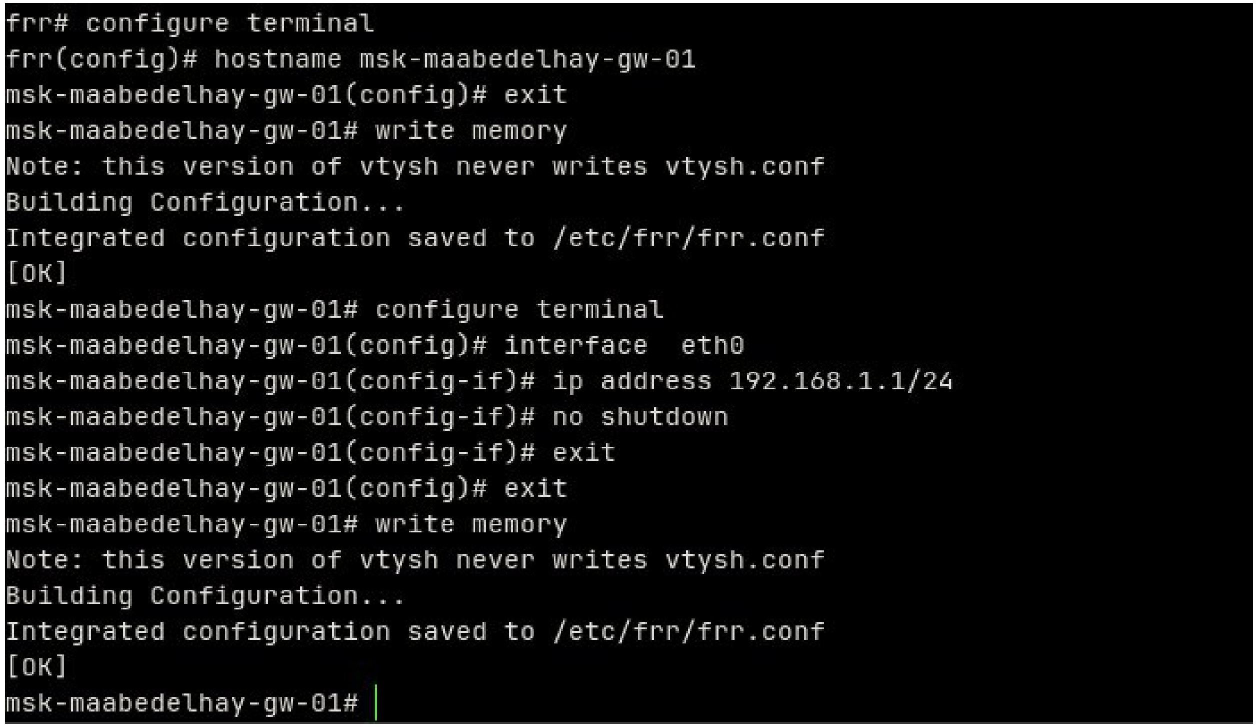
3. Сети на базе маршрутизатора FRR



```
PC1> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=12.369 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.001 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=1.981 ms
^C
```

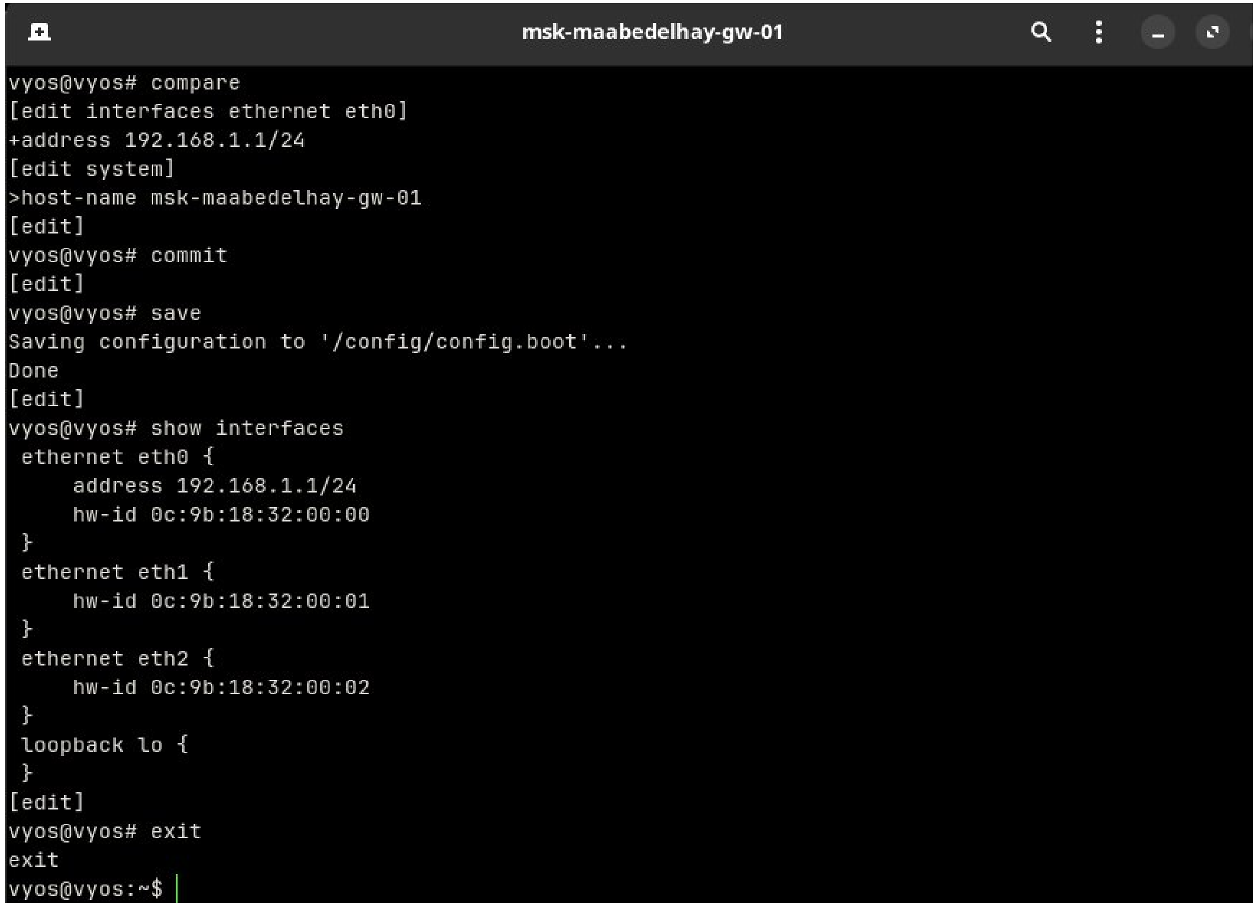


```
msk-maabedelhay-gw-01# show running-config
Building configuration...

Current configuration:
!
frr version 8.2.2
frr defaults traditional
hostname frr
hostname msk-maabedelhay-gw-01
service integrated-vtysh-config
!
interface eth0
 ip address 192.168.1.1/24
exit
!
end
```

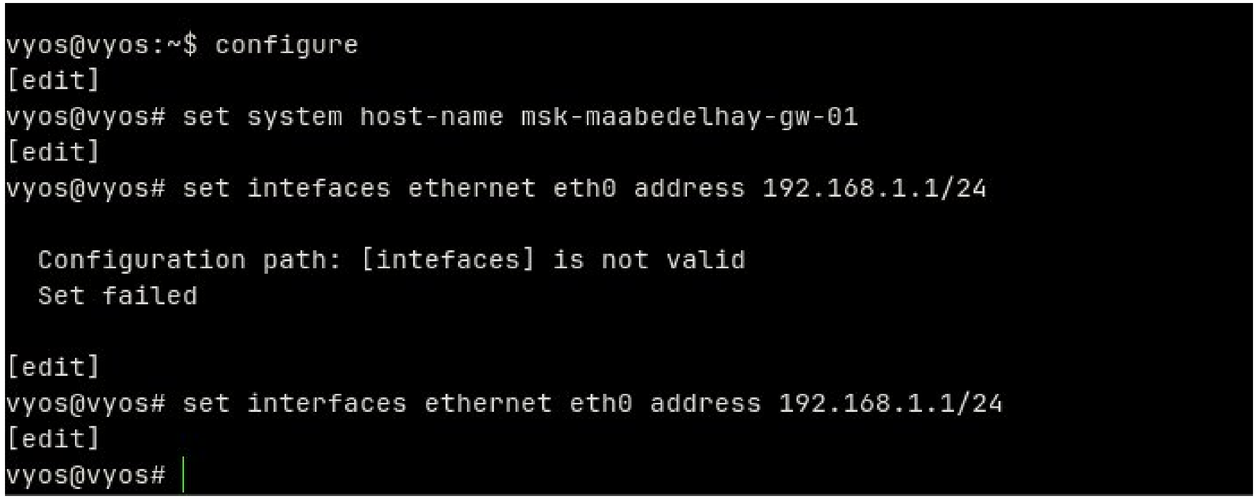


```
frr# configure terminal
frr(config)# hostname msk-maabedelhay-gw-01
msk-maabedelhay-gw-01(config)# exit
msk-maabedelhay-gw-01# write memory
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
msk-maabedelhay-gw-01# configure terminal
msk-maabedelhay-gw-01(config)# interface  eth0
msk-maabedelhay-gw-01(config-if)# ip address 192.168.1.1/24
msk-maabedelhay-gw-01(config-if)# no shutdown
msk-maabedelhay-gw-01(config-if)# exit
msk-maabedelhay-gw-01(config)# exit
msk-maabedelhay-gw-01# write memory
Note: this version of vtysh never writes vtysh.conf
Building Configuration...
Integrated configuration saved to /etc/frr/frr.conf
[OK]
msk-maabedelhay-gw-01#
```

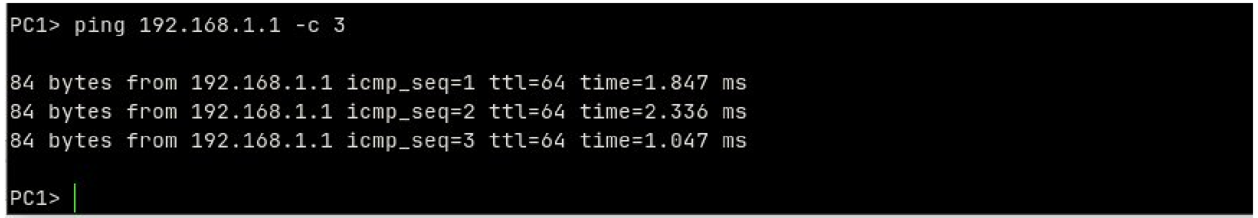
3. Сети на базе маршрутизатора Vyos



```
vyos@vyos# compare
[edit interfaces ethernet eth0]
+address 192.168.1.1/24
[edit system]
>host-name msk-maabedelhay-gw-01
[edit]
vyos@vyos# commit
[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos# show interfaces
 ethernet eth0 {
     address 192.168.1.1/24
     hw-id 0c:9b:18:32:00:00
 }
 ethernet eth1 {
     hw-id 0c:9b:18:32:00:01
 }
 ethernet eth2 {
     hw-id 0c:9b:18:32:00:02
 }
 loopback lo {
 }
[edit]
vyos@vyos# exit
exit
vyos@vyos:~$
```



```
vyos@vyos:~$ configure
[edit]
vyos@vyos# set system host-name msk-maabedelhay-gw-01
[edit]
vyos@vyos# set intefaces ethernet eth0 address 192.168.1.1/24

  Configuration path: [intefaces] is not valid
  Set failed

[edit]
vyos@vyos# set interfaces ethernet eth0 address 192.168.1.1/24
[edit]
vyos@vyos#
```



```
PC1> ping 192.168.1.1 -c 3

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=1.847 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.336 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=1.047 ms

PC1>
```

Вывод

Построил простейшие модели сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, проанализировал трафик посредством Wireshark.

Спасибо За Внимание