

Российский Университет Дружбы Народов

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

Отчёт

о выполнении лабораторной работы № 5

Простые сети в GNS3. Анализ трафика

дисциплина: Сетевые технологии

Студент: Танрибергенов Эльдар

Группа: НПИбд-02-20

Студ. билет № 1032208074

Москва, 2022 г.

Цели работы:

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

Ход работы:

1. Моделирование простейшей сети на базе коммутатора в GNS3

- Запустил GNS3 VM и GNS3 (рис. 1.1). Создал новый проект.

В рабочей области GNS3 разместил коммутатор Ethernet и два VPCS (рис. 1.2).

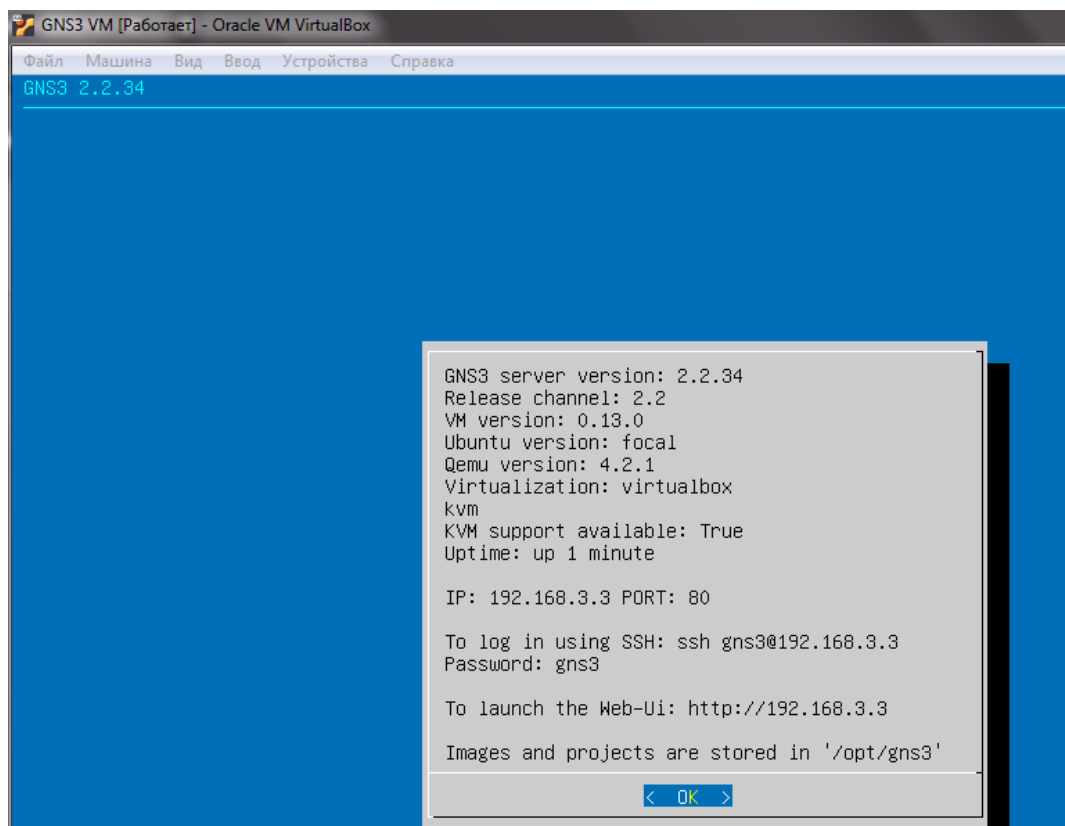


Рис. 1.1. Запуск GNS3 VM

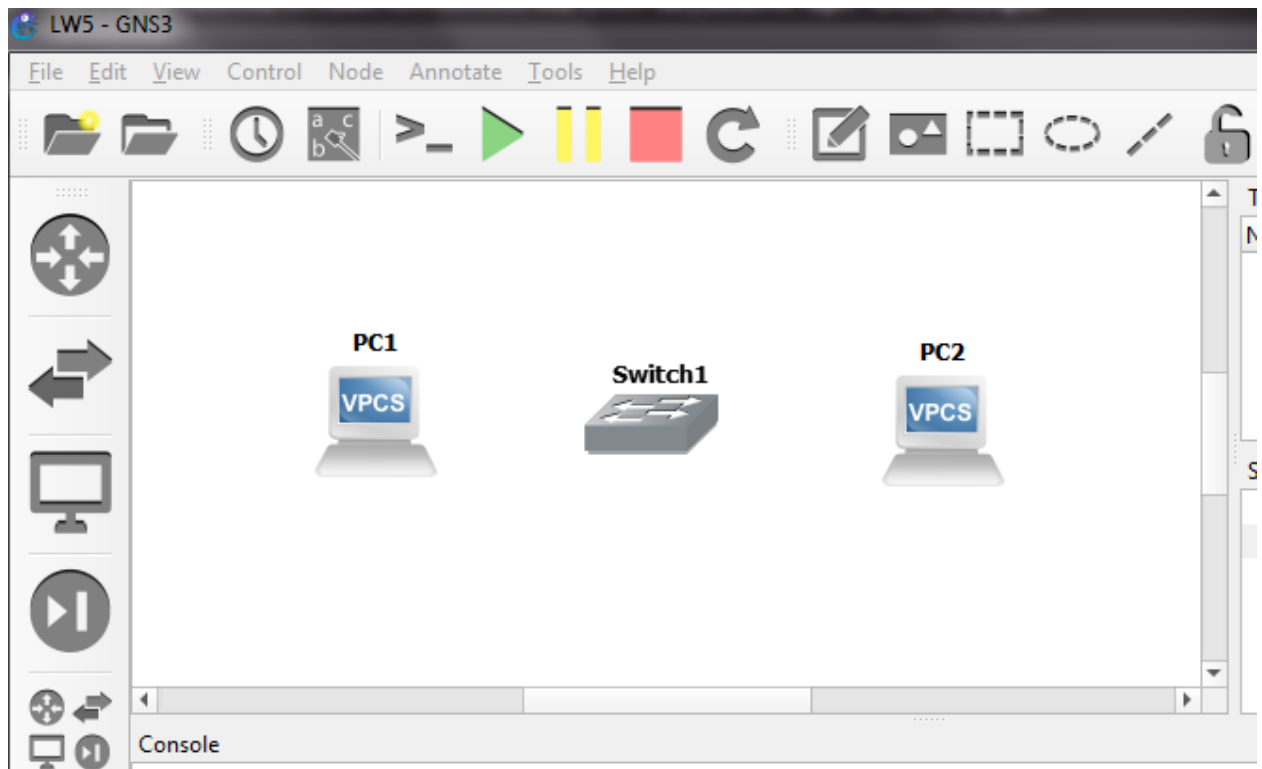


Рис. 1.2. GNS3: добавление устройств

- Щёлкнув на устройстве правой кнопкой мыши по PC-1, выбрал в меню Configure . Изменил название устройства, включив в имя устройства имя учётной записи. Коммутатору присвоил название msk-user-sw-01, где вместо user указал имя учётной записи. Соединил VPCS с коммутатором. Отобразил обозначение интерфейсов соединения. Результат – рис. 1.3.



Рис. 1.3. GNS3: Топология сети

- С помощью меню, вызываемого правой кнопкой мыши, запустил «Start» PC-1 (рис. 1.4), затем вызвал его терминал «Console» (рис. 1.5). Для просмотра синтаксиса возможных для ввода команд набрал «/?» (рис. 1.6).

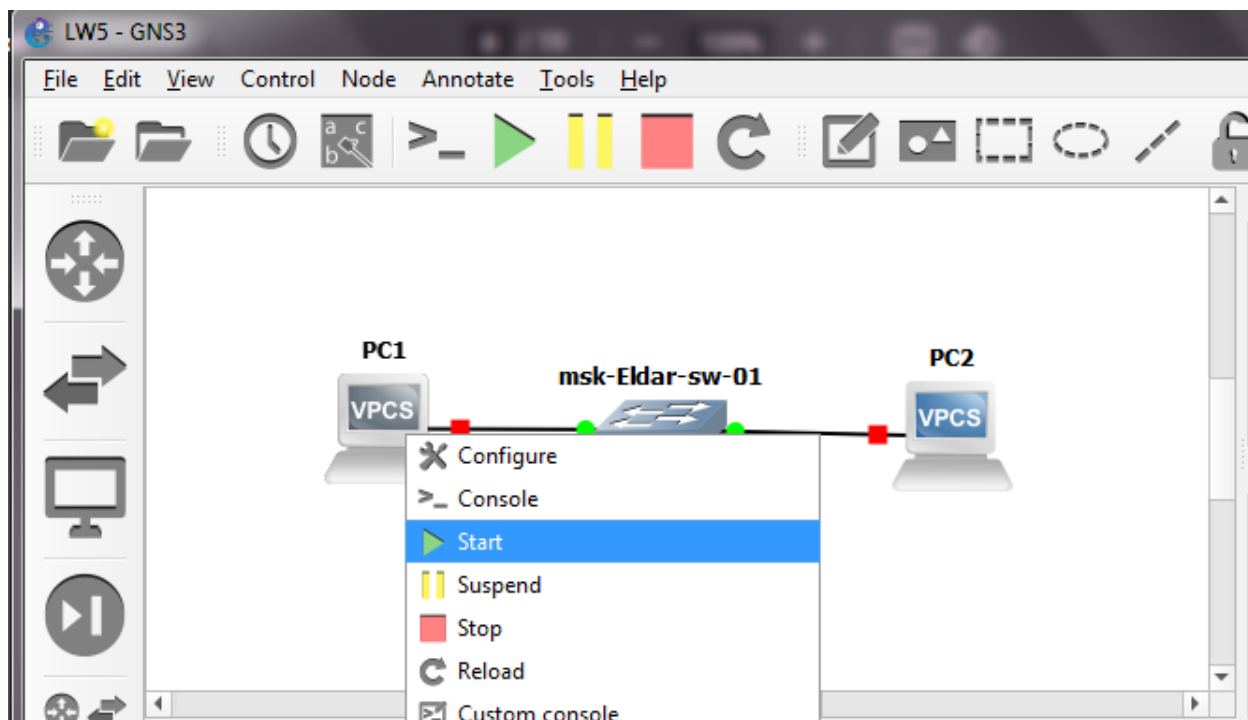


Рис. 1.4. PC1: запуск узла

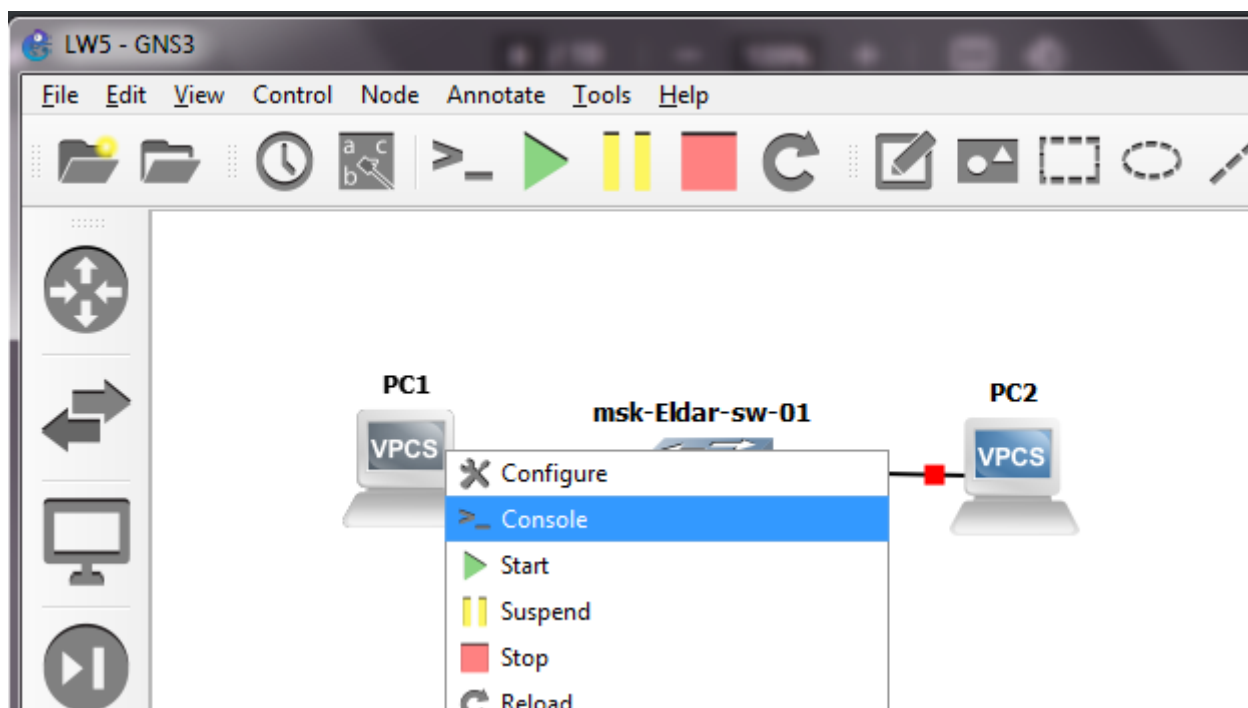
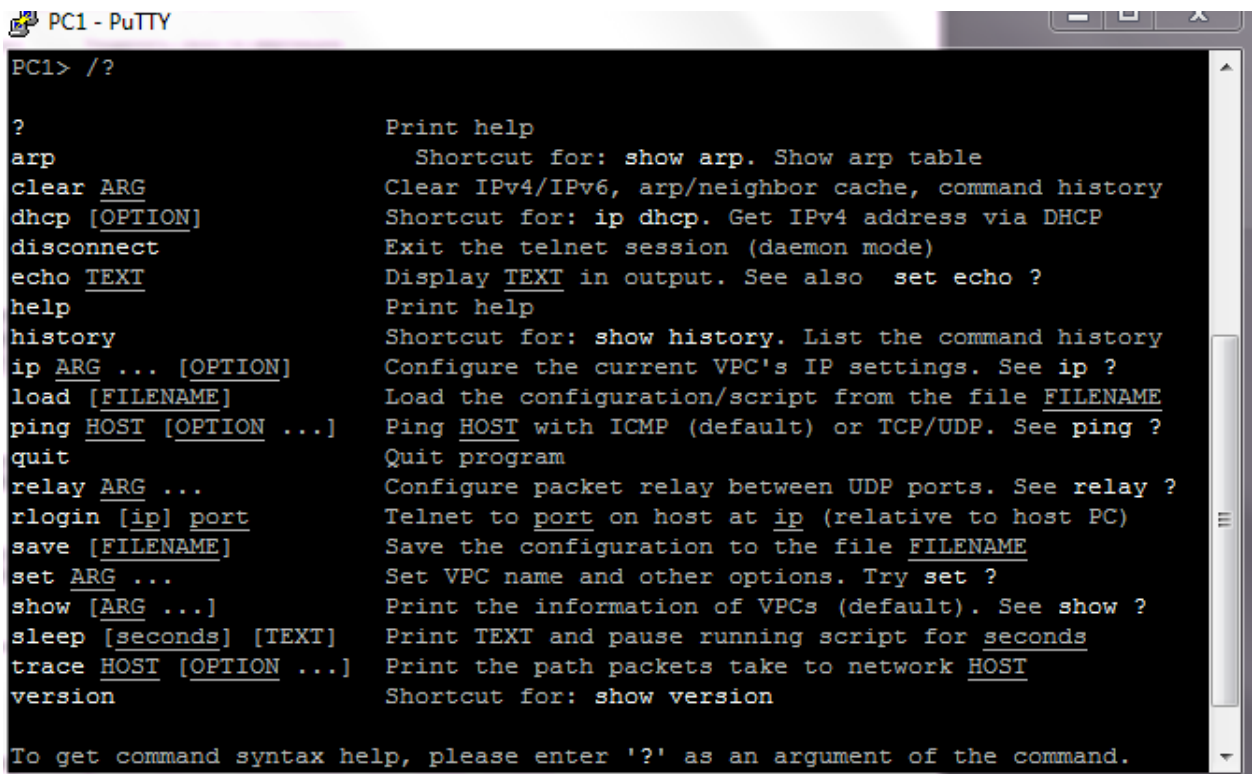


Рис. 1.5. PC1: запуск терминала



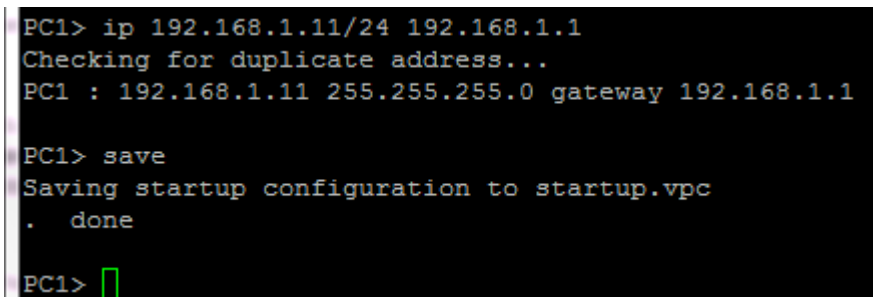
```
PC1> /?

?                Print help
arp              Shortcut for: show arp. Show arp table
clear ARG        Clear IPv4/IPv6, arp/neighbor cache, command history
dhcp [OPTION]    Shortcut for: ip dhcp. Get IPv4 address via DHCP
disconnect       Exit the telnet session (daemon mode)
echo TEXT        Display TEXT in output. See also set echo ?
help             Print help
history          Shortcut for: show history. List the command history
ip ARG ... [OPTION] Configure the current VPC's IP settings. See ip ?
load [FILENAME]  Load the configuration/script from the file FILENAME
ping HOST [OPTION ...] Ping HOST with ICMP (default) or TCP/UDP. See ping ?
quit            Quit program
relay ARG ...    Configure packet relay between UDP ports. See relay ?
rlogin [ip] port Telnet to port on host at ip (relative to host PC)
save [FILENAME]  Save the configuration to the file FILENAME
set ARG ...      Set VPC name and other options. Try set ?
show [ARG ...]   Print the information of VPCs (default). See show ?
sleep [seconds] [TEXT] Print TEXT and pause running script for seconds
trace HOST [OPTION ...] Print the path packets take to network HOST
version          Shortcut for: show version

To get command syntax help, please enter '?' as an argument of the command.
```

Рис. 1.5. Список возможных команд

- Для задания IP-адреса 192.168.1.11 в сети 192.168.1.0/24 ввёл (рис. 1.6): ip 192.168.1.11/24 192.168.1.1
Здесь 192.168.1.1 — адрес шлюза. Для сохранения конфигурации необходимо ввести команду save.



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

PC1> █
```

Рис. 1.6. PC-1: Задание IP-адреса

- Аналогичным образом задал IP-адрес 192.168.1.12 для PC-2 (рис. 1.7).

```
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> █
```

Рис. 1.7. PC-2: Задание IP-адреса

- Проверил работоспособность соединения между PC-1 и PC-2 с помощью команды ping (рис. 1.8 – 1.9).

```
PC1 - PuTTY
ping 192.168.1.12

84 bytes from 192.168.1.12 icmp_seq=1 ttl=64 time=0.169 ms
84 bytes from 192.168.1.12 icmp_seq=2 ttl=64 time=0.286 ms
84 bytes from 192.168.1.12 icmp_seq=3 ttl=64 time=0.265 ms
84 bytes from 192.168.1.12 icmp_seq=4 ttl=64 time=0.302 ms
84 bytes from 192.168.1.12 icmp_seq=5 ttl=64 time=0.485 ms

PC1> █
```

Рис. 1.8. PC-1: Пингование PC-2

```
PC2 - PuTTY
ping 192.168.1.11

84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=0.358 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=0.273 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=0.317 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=0.249 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=0.593 ms

PC2> █
```

Рис. 1.9. PC-2: Пингование PC-1

- Остановил в проекте все узлы («Control Stop all nodes») (рис. 1.10).

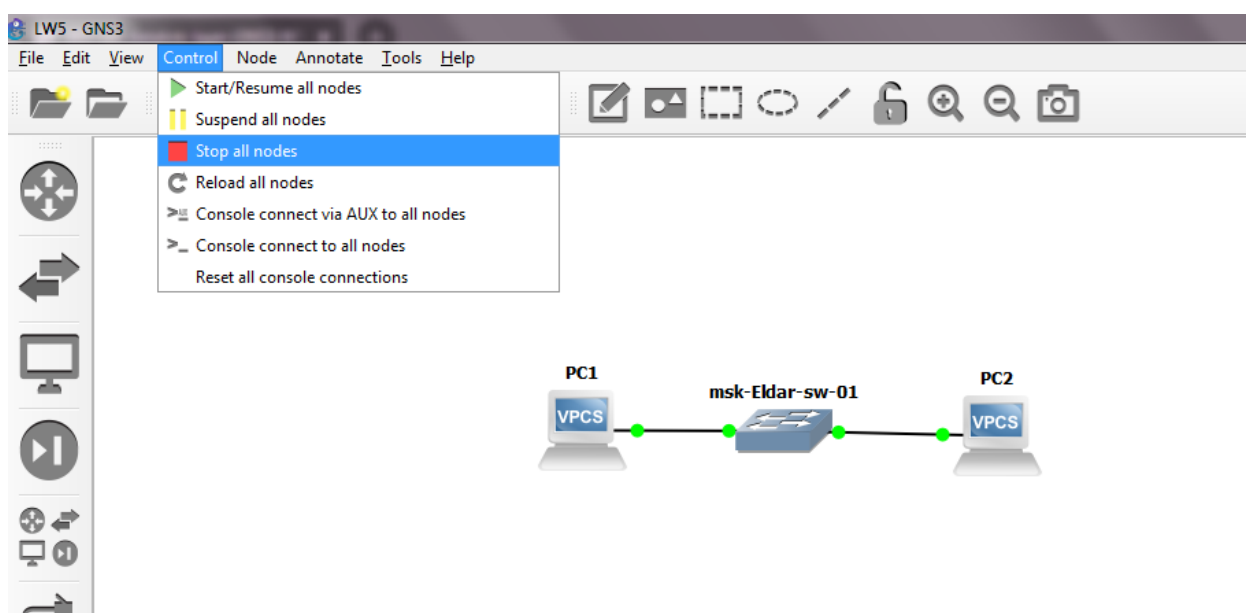


Рис. 1.10. Остановка всех узлов

2. Анализ трафика в GNS3 посредством Wireshark

1. Запустил на соединении между PC-1 и коммутатором анализатор трафика. Для этого щёлкнул правой кнопкой мыши на соединении, выбрал в меню «Start capture» (рис. 2.1). Запустился Wireshark (рис. 2.2), а в проекте GNS3 на соединении появился значок лупы.

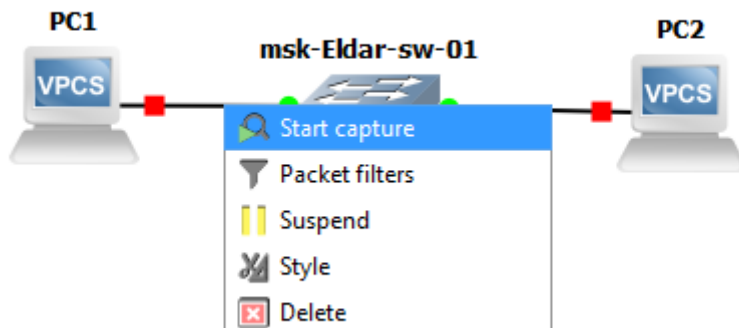
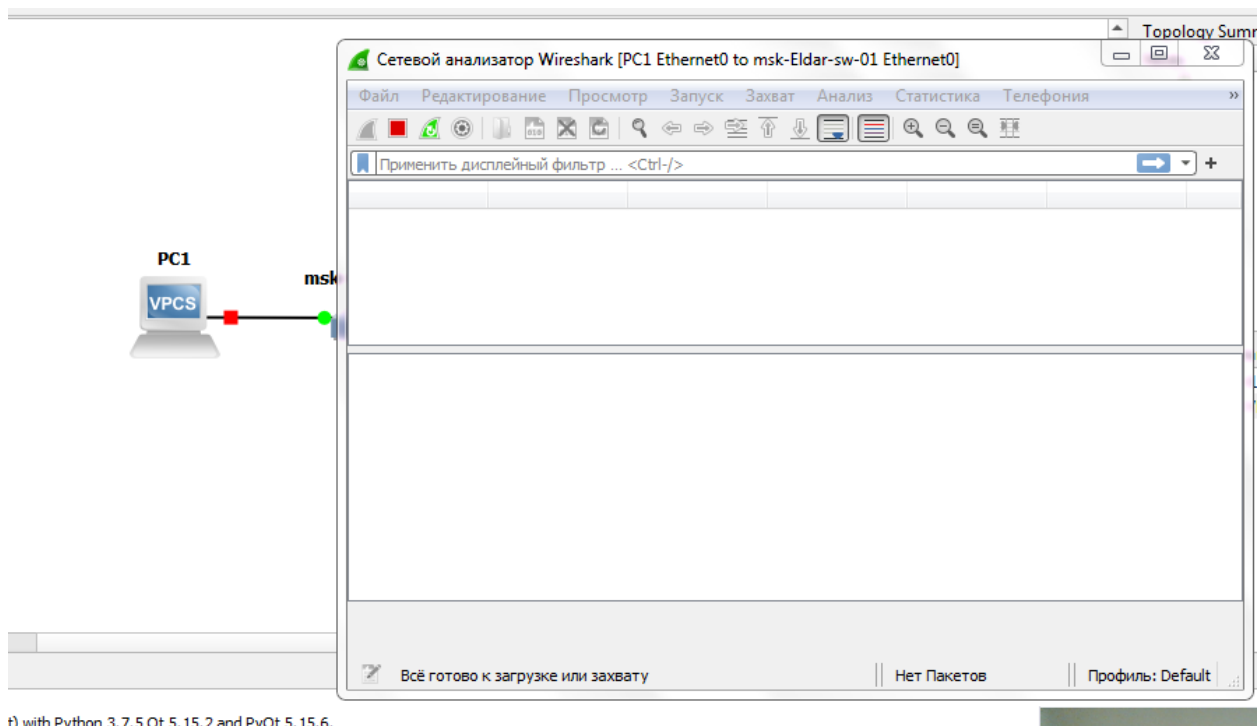


Рис. 2.1. Запуск захвата трафика



t) with Python 3.7.5 Qt 5.15.2 and PyQt 5.15.6.

Рис. 2.2. Wireshark

2. В проекте GNS3 запустил все узлы (меню GNS3 «Control Start/Resume all nodes») (рис. 2.3). В окне Wireshark (рис. 2.4) отобразилась информация по протоколу ARP. Пояснение – таблица. 2.1.

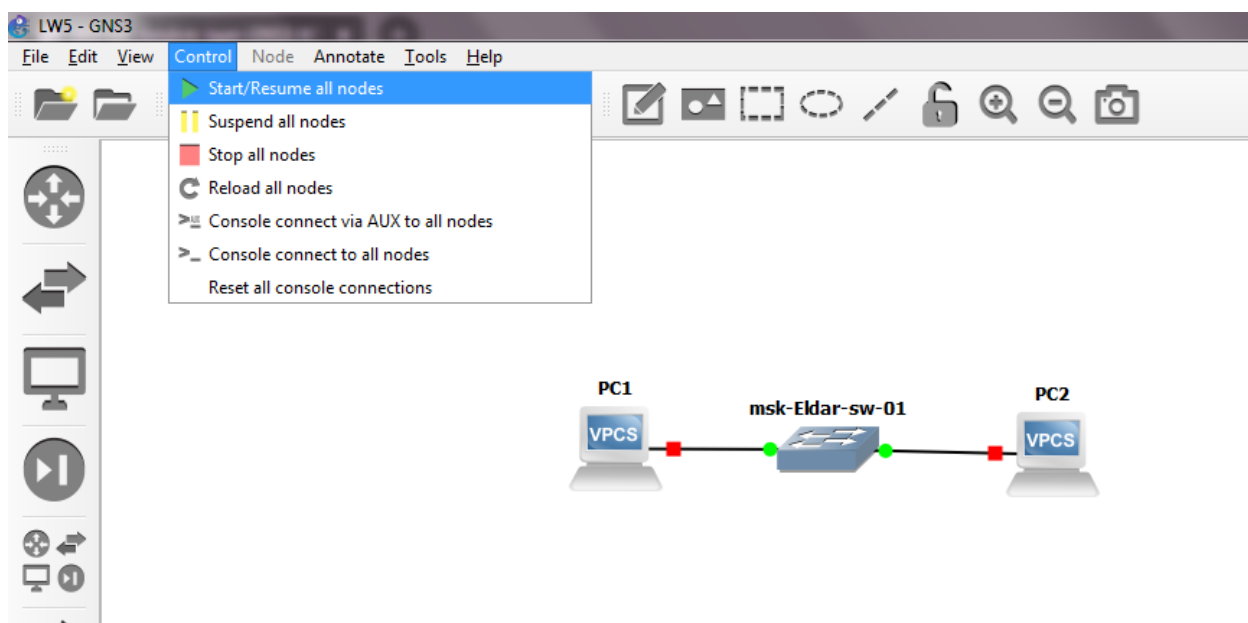


Рис. 2.3. Запуск всех узлов

Захват из - [PC1 Ethernet0 to msk-Eldar-sw-01 Ethernet0]						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь						
Применить дисплейный фильтр ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::2	ICMPv6	62	Router Solicitation
2	0.009518	::	ff02::2	ICMPv6	62	Router Solicitation
3	0.050192	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
4	0.059767	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
5	1.051155	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
6	1.060298	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
7	2.051702	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
8	2.061367	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)

▶ Frame 3: 64 bytes on wire (512 bits), 64 bytes captured (512 bits) on interface -, id 0 ▶ Ethernet II, Src: Private_66:68:01 (00:50:79:66:68:01), Dst: Broadcast (ff:ff:ff:ff:ff:ff) ▲ 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_66:68:01 (00:50:79:66:68:01) Sender IP address: 192.168.1.12 Target MAC address: Broadcast (ff:ff:ff:ff:ff:ff) Target IP address: 192.168.1.12

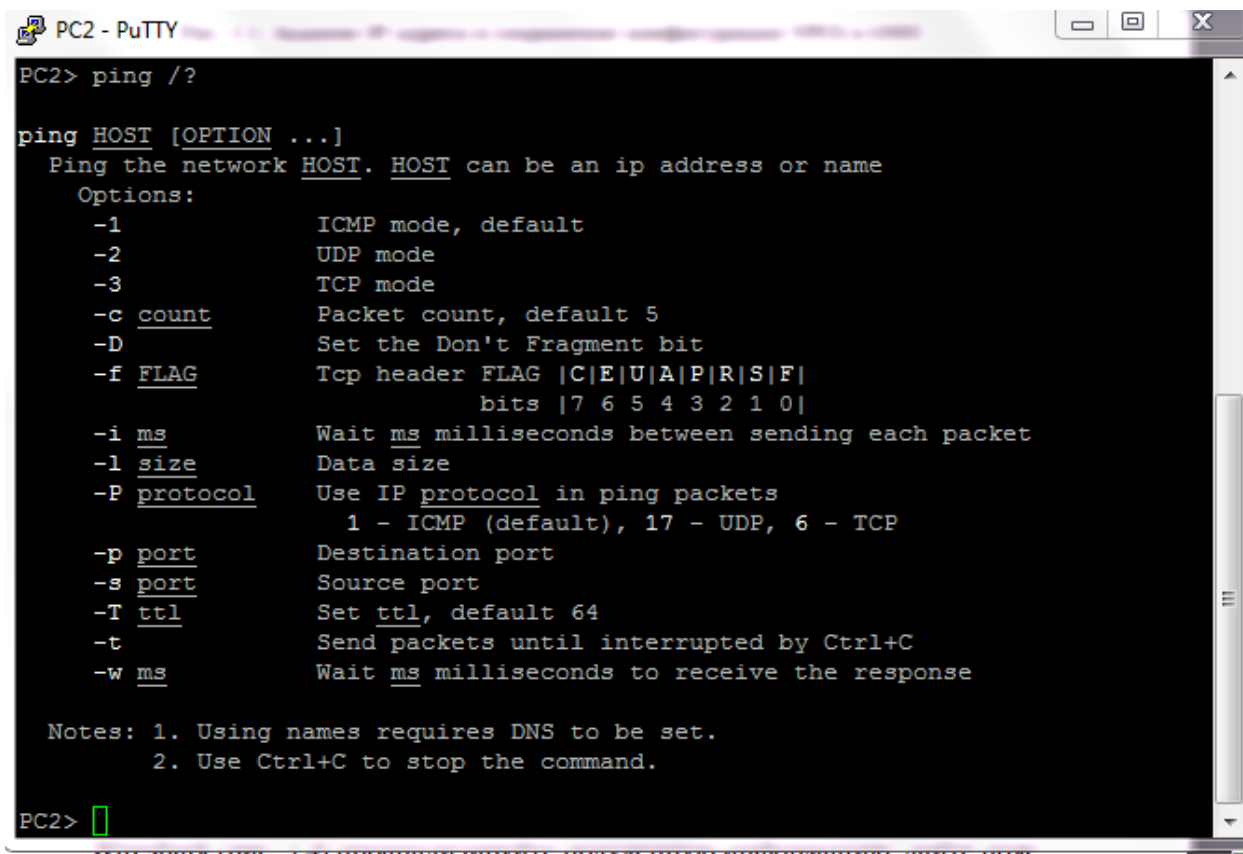
Рис. 2.4. Просмотр пакетов ARP

Таблица. 2.1

Характеристика	Значение
Длина пакета	64 байт (512 бит)
Идентификатор интерфейса	0
Тип устройства	Ethernet (1)
Тип пакета	Запрос
MAC-адрес отправителя	00:50:79:66:68:01
MAC-адрес получателя	ff:ff:ff:ff:ff:ff
IP-адрес отправителя	192.168.1.12
IP-адрес получателя	192.168.1.12

- В терминале PC-2 посмотрел информацию по опциям команды ping, введя ping «/?» (рис. 2.5). Затем сделал один эхо-запрос в ICMP-моду к узлу PC-1 (рис. 2.6). В окне

Wireshark (рис. 2.7 – 2.8) проанализировал полученную информацию: обычные эхо-запрос и ответ – указана длина пакетов, указаны идентификаторы BE и LE, указаны порядковые номера BE и LE, указаны ip-адреса отправителя и получателя, контрольная сумма правильная.



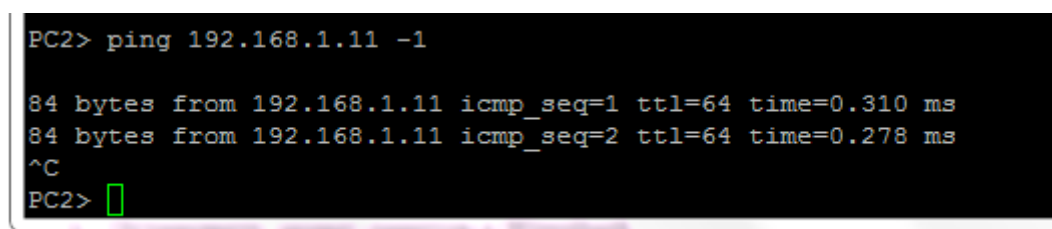
```
PC2> ping /?

ping HOST [OPTION ...]
  Ping the network HOST. HOST can be an ip address or name
  Options:
    -1             ICMP mode, default
    -2             UDP mode
    -3             TCP mode
    -c count       Packet count, default 5
    -D             Set the Don't Fragment bit
    -f FLAG        Tcp header FLAG |C|E|U|A|P|R|S|F|
                  bits |7 6 5 4 3 2 1 0|
    -i ms          Wait ms milliseconds between sending each packet
    -l size        Data size
    -P protocol    Use IP protocol in ping packets
                  1 - ICMP (default), 17 - UDP, 6 - TCP
    -p port        Destination port
    -s port        Source port
    -T ttl         Set ttl, default 64
    -t            Send packets until interrupted by Ctrl+C
    -w ms          Wait ms milliseconds to receive the response

  Notes: 1. Using names requires DNS to be set.
         2. Use Ctrl+C to stop the command.

PC2> 
```

Рис. 2.5. Информация по команде ping



```
PC2> ping 192.168.1.11 -1

84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=0.310 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=0.278 ms
^C
PC2> 
```

Рис. 2.6. Пингование узла PC-1 в ICMP-режиме

11	229.626495	192.168.1.12	192.168.1.11	ICMP	98 Echo (ping) request	id=0xb6b1, seq=1/256, ttl=64 (reply in 12)
12	229.626621	192.168.1.11	192.168.1.12	ICMP	98 Echo (ping) reply	id=0xb6b1, seq=1/256, ttl=64 (request in 11)
13	230.627700	192.168.1.12	192.168.1.11	ICMP	98 Echo (ping) request	id=0xb7b1, seq=2/512, ttl=64 (reply in 14)
14	230.627818	192.168.1.11	192.168.1.12	ICMP	98 Echo (ping) reply	id=0xb7b1, seq=2/512, ttl=64 (request in 13)

▶ Frame 11: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
 ▶ 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
 ▶ Internet Control Message Protocol
 Type: 8 (Echo (ping) request)
 Code: 0
 Checksum: 0x6959 [correct]
 [Checksum Status: Good]
 Identifier (BE): 46769 (0xb6b1)
 Identifier (LE): 45494 (0xb1b6)
 Sequence Number (BE): 1 (0x0001)
 Sequence Number (LE): 256 (0x0100)
 [Response frame: 12]
 ▶ Data (56 bytes)

Рис. 2.7. Эхо-запрос ICMP

11	229.626495	192.168.1.12	192.168.1.11	ICMP	98 Echo (ping) request	id=0xb6b1, seq=1/256, ttl=64 (reply in 12)
12	229.626621	192.168.1.11	192.168.1.12	ICMP	98 Echo (ping) reply	id=0xb6b1, seq=1/256, ttl=64 (request in 11)
13	230.627700	192.168.1.12	192.168.1.11	ICMP	98 Echo (ping) request	id=0xb7b1, seq=2/512, ttl=64 (reply in 14)
14	230.627818	192.168.1.11	192.168.1.12	ICMP	98 Echo (ping) reply	id=0xb7b1, seq=2/512, ttl=64 (request in 13)

▶ Frame 12: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
 ▶ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
 ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.12
 ▶ Internet Control Message Protocol
 Type: 0 (Echo (ping) reply)
 Code: 0
 Checksum: 0x7159 [correct]
 [Checksum Status: Good]
 Identifier (BE): 46769 (0xb6b1)
 Identifier (LE): 45494 (0xb1b6)
 Sequence Number (BE): 1 (0x0001)
 Sequence Number (LE): 256 (0x0100)
 [Request frame: 11]
 [Response time: 0.126 ms]
 ▶ Data (56 bytes)

Рис. 2.8. Эхо-ответ ICMP

4. Сделал один эхо-запрос в UDP-режиме к узлу PC-1 (рис.2.9). В окне Wireshark (рис. 2.10 – 2.11) проанализировал полученную информацию: Указаны порты отправителя и получателя, длина пакета, контрольная сумма не сверялась.

```

PC2> ping 192.168.1.11 -2

84 bytes from 192.168.1.11 udp_seq=1 ttl=64 time=0.556 ms
^C
PC2> 

```

Рис. 2.9. Пингование узла PC-1 в UDP-режиме

27	422.725636	192.168.1.12	192.168.1.11	ECHO	98 Request
28	422.725872	192.168.1.11	192.168.1.12	ECHO	98 Response

```

▶ Frame 27: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
▶ 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
▲ User Datagram Protocol, Src Port: 1273, Dst Port: 7
    Source Port: 1273
    Destination Port: 7
    Length: 64
    Checksum: 0xdb7b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    ▶ [Timestamps]
    UDP payload (56 bytes)
▶ Echo
  
```

Рис. 2.10. Эхо-запрос UDP

27	422.725636	192.168.1.12	192.168.1.11	ECHO	98 Request
28	422.725872	192.168.1.11	192.168.1.12	ECHO	98 Response

```

▶ Frame 28: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
▶ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.12
▲ User Datagram Protocol, Src Port: 7, Dst Port: 1273
    Source Port: 7
    Destination Port: 1273
    Length: 64
    Checksum: 0xdb7b [unverified]
    [Checksum Status: Unverified]
    [Stream index: 1]
    ▶ [Timestamps]
    UDP payload (56 bytes)
▶ Echo

```

Рис. 2.11. Эхо-ответ UDP

5. Сделал один эхо-запрос в TCP-моду к узлу PC-1 (рис.2.12).. В окне Wireshark (рис. 2.13 – 2.14) проанализировал полученную информацию: сначала устанавливается соединение (запрос-ответ-подтверждение), далее идёт отправка пакета, подтверждение получения пакета.

```
PC2> ping 192.168.1.11 -3

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=1.039 ms
Close      7@192.168.1.11 seq=1 ttl=64 time=2.183 ms
^CConnect  7@192.168.1.11 timeout

PC2> █
```

Рис. 2.12. Пингование узла PC-1 в TCP-режиме

Применить дисплейный фильтр ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
79	580.239936	192.168.1.12	192.168.1.11	ECHO	122	Request
80	580.240094	192.168.1.11	192.168.1.12	TCP	54	7 → 8015 [ACK] Seq=1 Ack=57 Win=2920 Len=0
81	580.241159	192.168.1.12	192.168.1.11	TCP	66	8015 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1666364181 TSecr=0
82	580.241367	192.168.1.11	192.168.1.12	TCP	54	7 → 8015 [ACK] Seq=1 Ack=58 Win=2920 Len=0
83	580.241393	192.168.1.11	192.168.1.12	TCP	54	7 → 8015 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
84	580.243540	192.168.1.12	192.168.1.11	TCP	66	8015 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1666364181 TSecr=0

▶ 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

4 ▶ Transmission Control Protocol, Src Port: 8015, Dst Port: 7, Seq: 1, Ack: 1, Len: 56

Source Port: 8015

Destination Port: 7

[Stream index: 5]

[Conversation completeness: Complete, WITH_DATA (31)]

[TCP Segment Len: 56]

Sequence Number: 1 (relative sequence number)

Sequence Number (raw): 1856209680

[Next Sequence Number: 57 (relative sequence number)]

Acknowledgment Number: 1 (relative ack number)

Acknowledgment number (raw): 1643464098

1000 = Header Length: 32 bytes (8)

▶ Flags: 0x018 (PSH, ACK)

Window: 2920

[Calculated window size: 2920]

[Window size scaling factor: -2 (no window scaling used)]

Checksum: 0xab8a [unverified]

[Checksum Status: Unverified]

Urgent Pointer: 0

▶ Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps

▶ [Timestamps]

▶ [SEQ/ACK analysis]

TCP payload (56 bytes)

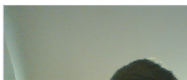


Рис. 2.13. Захваченные пакеты TCP: Request

79	580.239936	192.168.1.12	192.168.1.11	ECHO	122 Request
80	580.240094	192.168.1.11	192.168.1.12	TCP	54 7 → 8015 [ACK] Seq=1 Ack=57 Win=2920 Len=0
81	580.241159	192.168.1.12	192.168.1.11	TCP	66 8015 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1666364181 TSecr=0
82	580.241367	192.168.1.11	192.168.1.12	TCP	54 7 → 8015 [ACK] Seq=1 Ack=58 Win=2920 Len=0
83	580.241393	192.168.1.11	192.168.1.12	TCP	54 7 → 8015 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
84	580.243540	192.168.1.12	192.168.1.11	TCP	66 8015 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1666364181 TSecr=0

▶ Frame 80: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface -, id 0
 ▶ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
 ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.12
 ▶ Transmission Control Protocol, Src Port: 7, Dst Port: 8015, Seq: 1, Ack: 57, Len: 0

Source Port: 7
 Destination Port: 8015
 [Stream index: 5]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 1643464098
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 57 (relative ack number)
 Acknowledgment number (raw): 1856209736
 0101 = Header Length: 20 bytes (5)
 ▶ Flags: 0x010 (ACK)
 Window: 2920
 [Calculated window size: 2920]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0xc41d [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 ▶ [Timestamps]
 ▶ [SEQ/ACK analysis]

0000 00 50 79 66 68 01 00 50 79 66 68 00 08 00 45 00 ·Pyfh···P yfh···E·

Рис. 2.14. Захваченные пакеты TCP: FIN, PSH, ACK

79	580.239936	192.168.1.12	192.168.1.11	ECHO	122 Request
80	580.240094	192.168.1.11	192.168.1.12	TCP	54 7 → 8015 [ACK] Seq=1 Ack=57 Win=2920 Len=0
81	580.241159	192.168.1.12	192.168.1.11	TCP	66 8015 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1666364181 TSecr=0
82	580.241367	192.168.1.11	192.168.1.12	TCP	54 7 → 8015 [ACK] Seq=1 Ack=58 Win=2920 Len=0
83	580.241393	192.168.1.11	192.168.1.12	TCP	54 7 → 8015 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
84	580.243540	192.168.1.12	192.168.1.11	TCP	66 8015 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1666364181 TSecr=0

▶ Frame 80: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface -, id 0
 ▶ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
 ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.12
 ▶ Transmission Control Protocol, Src Port: 7, Dst Port: 8015, Seq: 1, Ack: 57, Len: 0

Source Port: 7
 Destination Port: 8015
 [Stream index: 5]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 1643464098
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 57 (relative ack number)
 Acknowledgment number (raw): 1856209736
 0101 = Header Length: 20 bytes (5)
 ▶ Flags: 0x010 (ACK)
 Window: 2920
 [Calculated window size: 2920]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0xc41d [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 ▶ [Timestamps]
 ▶ [SEQ/ACK analysis]

0000 00 50 79 66 68 01 00 50 79 66 68 00 08 00 45 00 ·Pyfh···P yfh···E·

Рис. 2.15. Захваченные пакеты TCP: ACK

No.	Time	Source	Destination	Protocol	Length	Info
79	580.239936	192.168.1.12	192.168.1.11	ECHO	122	Request
80	580.240094	192.168.1.11	192.168.1.12	TCP	54	7 → 8015 [ACK] Seq=1 Ack=57 Win=2920 Len=0
81	580.241159	192.168.1.12	192.168.1.11	TCP	66	8015 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1666364181 TSecr=0
82	580.241367	192.168.1.11	192.168.1.12	TCP	54	7 → 8015 [ACK] Seq=1 Ack=58 Win=2920 Len=0
83	580.241393	192.168.1.11	192.168.1.12	TCP	54	7 → 8015 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
84	580.243540	192.168.1.12	192.168.1.11	TCP	66	8015 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1666364181 TSecr=0

▶ Frame 81: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface -, id 0
 ▶ 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
 ▶ Transmission Control Protocol, Src Port: 8015, Dst Port: 7, Seq: 57, Ack: 1, Len: 0
 Source Port: 8015
 Destination Port: 7
 [Stream index: 5]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 57 (relative sequence number)
 Sequence Number (raw): 1856209736
 [Next Sequence Number: 58 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 1643464098
 1000 = Header Length: 32 bytes (8)
 ▶ Flags: 0x019 (FIN, PSH, ACK)
 Window: 2920
 [Calculated window size: 2920]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0x18a3 [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 ▶ [Timestamps]

Рис. 2.16. Захваченные пакеты TCP: FIN, ACK

No.	Time	Source	Destination	Protocol	Length	Info
79	580.239936	192.168.1.12	192.168.1.11	ECHO	122	Request
80	580.240094	192.168.1.11	192.168.1.12	TCP	54	7 → 8015 [ACK] Seq=1 Ack=57 Win=2920 Len=0
81	580.241159	192.168.1.12	192.168.1.11	TCP	66	8015 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1666364181 TSecr=0
82	580.241367	192.168.1.11	192.168.1.12	TCP	54	7 → 8015 [ACK] Seq=1 Ack=58 Win=2920 Len=0
83	580.241393	192.168.1.11	192.168.1.12	TCP	54	7 → 8015 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
84	580.243540	192.168.1.12	192.168.1.11	TCP	66	8015 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1666364181 TSecr=0

▶ Frame 82: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface -, id 0
 ▶ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
 ▶ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.12
 ▶ Transmission Control Protocol, Src Port: 7, Dst Port: 8015, Seq: 1, Ack: 58, Len: 0
 Source Port: 7
 Destination Port: 8015
 [Stream index: 5]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 1643464098
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 58 (relative ack number)
 Acknowledgment number (raw): 1856209737
 0101 = Header Length: 20 bytes (5)
 ▶ Flags: 0x010 (ACK)
 Window: 2920
 [Calculated window size: 2920]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0xc41c [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0

Рис. 2.17. Захваченные пакеты TCP: ACK

81	580.241159	192.168.1.12	192.168.1.11	TCP	66 8015 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1666364181 TSecr=0
82	580.241367	192.168.1.11	192.168.1.12	TCP	54 7 → 8015 [ACK] Seq=1 Ack=58 Win=2920 Len=0
83	580.241393	192.168.1.11	192.168.1.12	TCP	54 7 → 8015 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
84	580.243540	192.168.1.12	192.168.1.11	TCP	66 8015 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1666364181 TSecr=0

▷ Frame 83: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface -, id 0
 ▷ Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: Private_66:68:01 (00:50:79:66:68:01)
 ▷ Internet Protocol Version 4, Src: 192.168.1.11, Dst: 192.168.1.12
 ▣ Transmission Control Protocol, Src Port: 7, Dst Port: 8015, Seq: 1, Ack: 58, Len: 0
 Source Port: 7
 Destination Port: 8015
 [Stream index: 5]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 1643464098
 [Next Sequence Number: 2 (relative sequence number)]
 Acknowledgment Number: 58 (relative ack number)
 Acknowledgment number (raw): 1856209737
 0101 = Header Length: 20 bytes (5)
 ▷ Flags: 0x011 (FIN, ACK)
 Window: 2920
 [Calculated window size: 2920]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0xd525 [unverified]
 [Checksum Status: Unverified]

Рис. 2.18. Захваченные пакеты TCP: FIN, ACK

83	580.241393	192.168.1.11	192.168.1.12	TCP	54 7 → 8015 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
84	580.243540	192.168.1.12	192.168.1.11	TCP	66 8015 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1666364181 TSecr=0

▷ Frame 84: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface -, id 0
 ▷ 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
 ▣ Transmission Control Protocol, Src Port: 8015, Dst Port: 7, Seq: 58, Ack: 2, Len: 0
 Source Port: 8015
 Destination Port: 7
 [Stream index: 5]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 58 (relative sequence number)
 Sequence Number (raw): 1856209737
 [Next Sequence Number: 58 (relative sequence number)]
 Acknowledgment Number: 2 (relative ack number)
 Acknowledgment number (raw): 1643464099
 1000 = Header Length: 32 bytes (8)
 ▷ Flags: 0x010 (ACK)
 Window: 2920
 [Calculated window size: 2920]
 [Window size scaling factor: -2 (no window scaling used)]
 Checksum: 0x18aa [unverified]
 [Checksum Status: Unverified]
 Urgent Pointer: 0
 Options: (12 bytes), No-Operation (NOP), No-Operation (NOP), Timestamps
 ▷ [Timestamps]
 ▷ [SEQ/ACK analysis]

Рис. 2.19. Захваченные пакеты TCP: ACK

6. Остановил захват пакетов в Wireshark (рис. 2.20).

Захват из - [PC1 Ethernet0 to msk-Eldar-sw-01 Ethernet0]						
Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспров						
Остановить захват пакетов						
Применить дисплейный фильтр ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
79	580.239936	192.168.1.12	192.168.1.11	ECHO	122	Reque
80	580.240094	192.168.1.11	192.168.1.12	TCP	54	7 → 8
81	580.241159	192.168.1.12	192.168.1.11	TCP	66	8015
82	580.241367	192.168.1.11	192.168.1.12	TCP	54	7 → 8
83	580.241393	192.168.1.11	192.168.1.12	TCP	54	7 → 8
84	580.243540	192.168.1.12	192.168.1.11	TCP	66	8015

▷ Frame 84: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface -

Рис. 2.20. Остановка захвата пакетов Wireshark

3. Моделирование простейшей сети на базе маршрутизатора FRR в GNS

1. Запустил GNS3 VM (рис. 3.1) и GNS3. Создал новый проект (рис. 3.2).

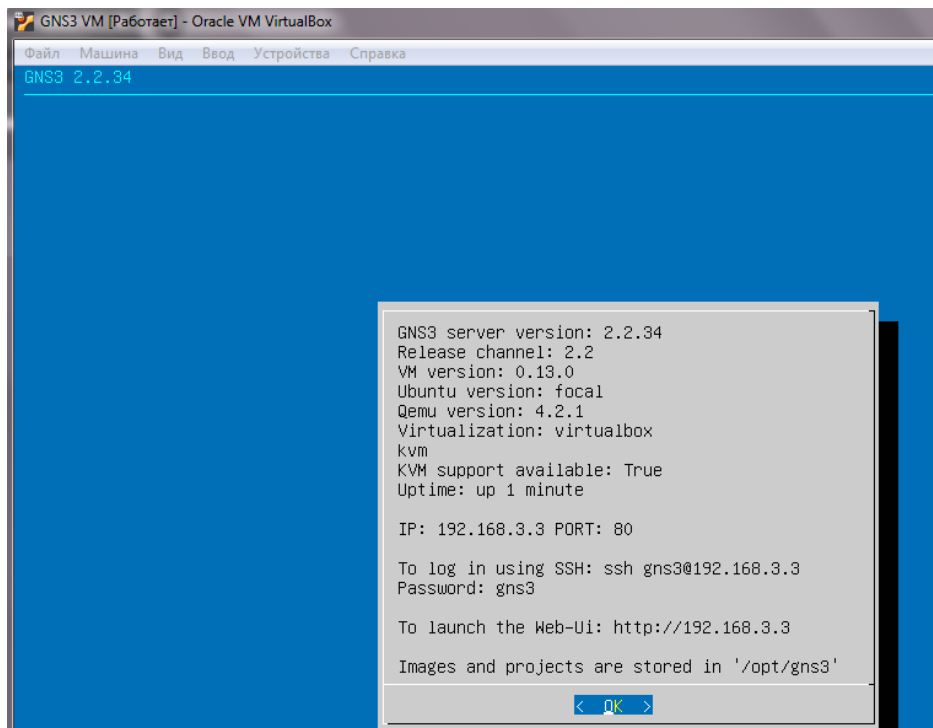


Рис. 3.1. Запуск GNS3 VM

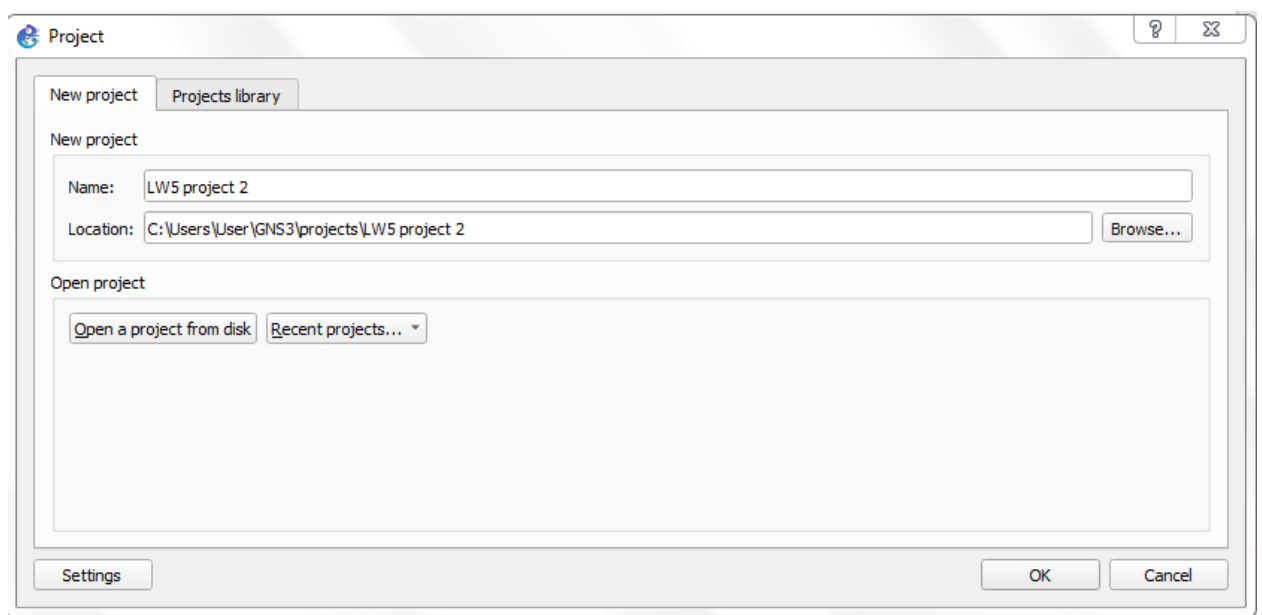


Рис. 3.2. Создание нового проекта

2. В рабочей области GNS3 разместил VPCS, коммутатор Ethernet и маршрутизатор FRR (рис. 3.3).

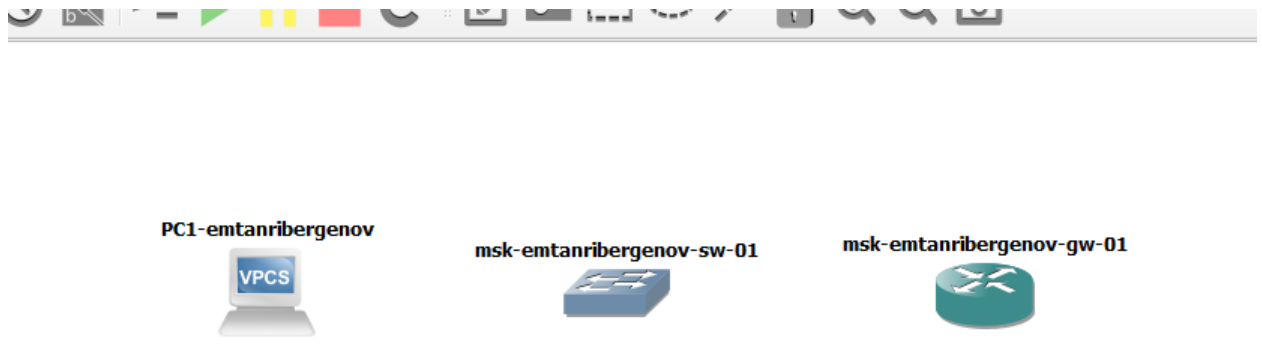


Рис. 3.3. Топология сети

3. Изменил отображаемые названия устройств (рис. 3.4).

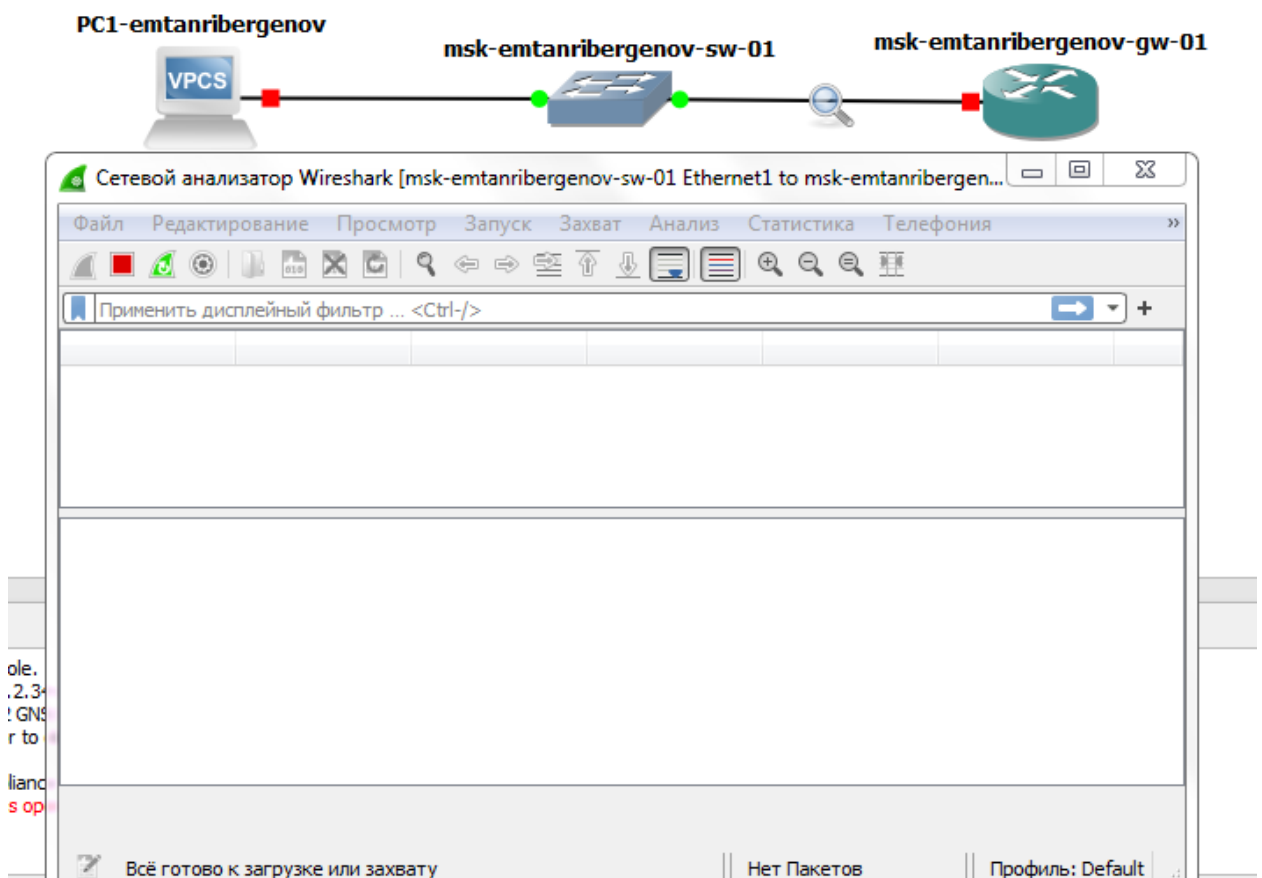


Рис. 3.4. Изменённые названия устройств и захват трафика между коммутатором и маршрутизатором

4. Включил захват трафика на соединении между коммутатором и маршрутизатором (рис. 3.4).
5. Запустил все устройства проекта. Открыл консоль всех устройств проекта (рис. 3.5).



Рис. 3.5. Запуск всех устройств и их терминалов

6. Настроил IP-адресацию для интерфейса узла PC1 (рис. 3.6).



Рис. 3.6. Настройка IP-адресации узла PC1

7. Настроил IP-адресацию для интерфейса локальной сети маршрутизатора (рис. 3.7).

```
Hello, this is FRRouting (version 8.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

frr# configure terminal
frr(config)# hostname msk-entanribergenov-gw-01
msk-entanribergenov-gw-01(config)# exit
msk-entanribergenov-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-entanribergenov-gw-01#
msk-entanribergenov-gw-01# configure terminal
msk-entanribergenov-gw-01(config)# interface eth0
msk-entanribergenov-gw-01(config-if)# ip address 192.168.1.1/24
msk-entanribergenov-gw-01(config-if)# no shutdown
msk-entanribergenov-gw-01(config-if)# exit
msk-entanribergenov-gw-01(config)#
msk-entanribergenov-gw-01(config)# exit
msk-entanribergenov-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-entanribergenov-gw-01#
```

Рис. 3.7. Настройка IP-адресации маршрутизатора

8. Проверил конфигурацию маршрутизатора и настройки IP-адресации (рис. 3.8).

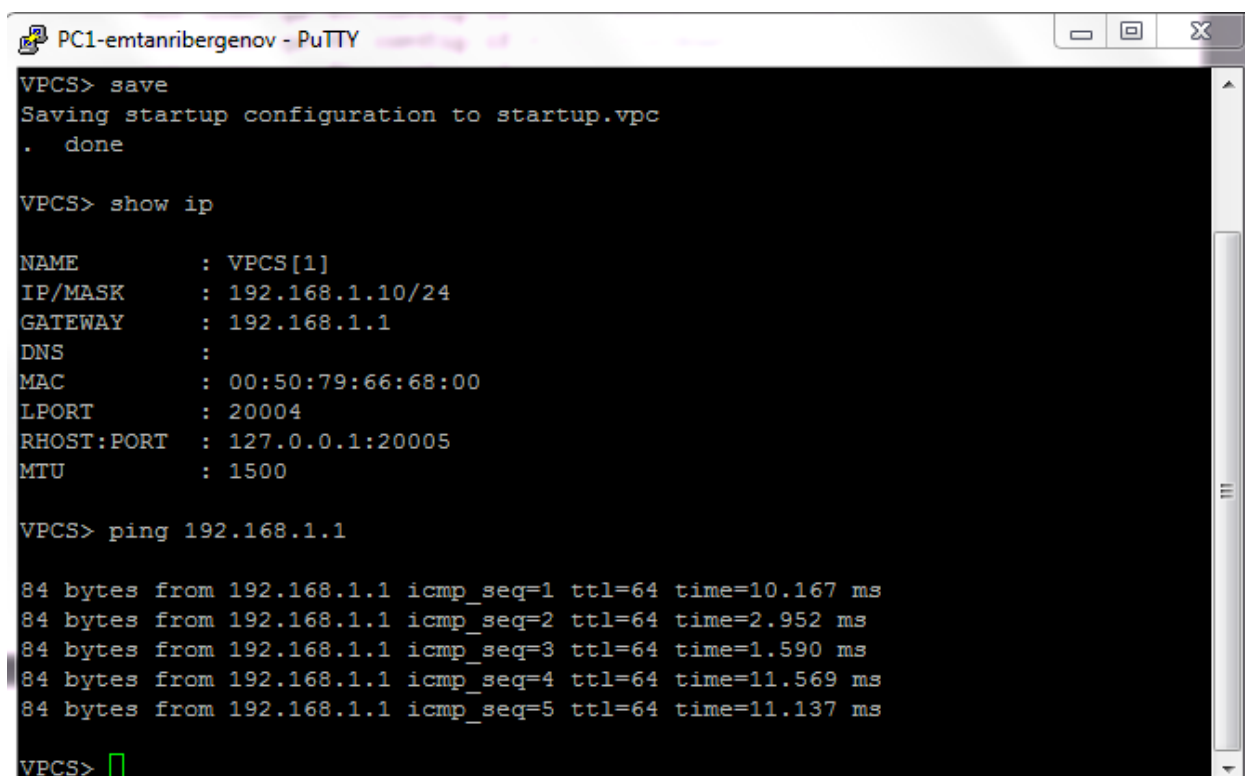
```
msk-emtanribergenov-gw-01# show running-config
Building configuration...

Current configuration:
!
frr version 8.1
frr defaults traditional
hostname frr
hostname msk-emtanribergenov-gw-01
service integrated-vtysh-config
!
interface eth0
 ip address 192.168.1.1/24
exit
!
end
msk-emtanribergenov-gw-01# show interface brief
Interface      Status   VRF      Addresses
-----
eth0           up       default  192.168.1.1/24
eth1           down     default
eth2           down     default
eth3           down     default
eth4           down     default
eth5           down     default
eth6           down     default
eth7           down     default
lo             up       default
pimreg        up       default

msk-emtanribergenov-gw-01#
```

Рис. 3.8. Просмотр конфигурации маршрутизатора

9. Проверил подключение. Узел PC1 успешно отправляет эхо-запросы на адрес маршрутизатора 192.168.1.1 (рис. 3.9).



```
VPCS> save
Saving startup configuration to startup.vpc
. done

VPCS> show ip

NAME       : VPCS[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 20004
RHOST:PORT : 127.0.0.1:20005
MTU        : 1500

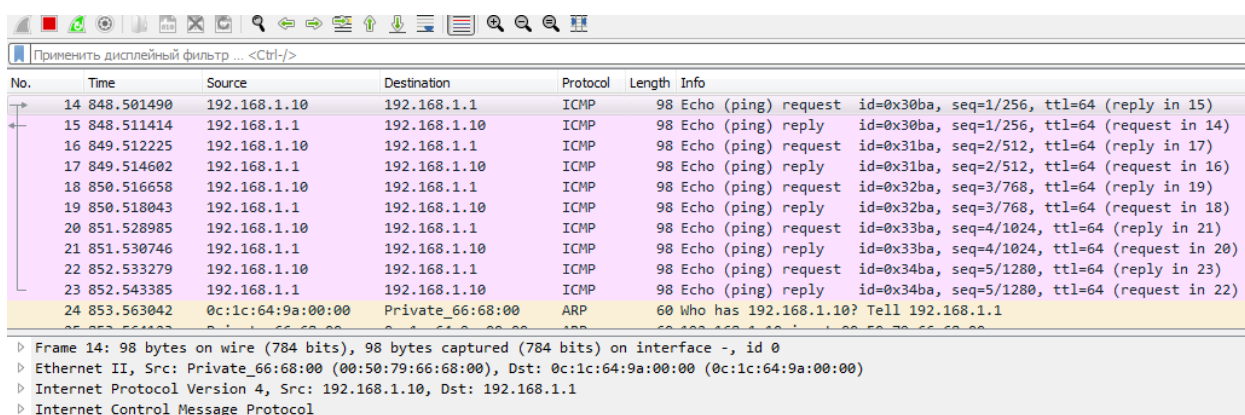
VPCS> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=10.167 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.952 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=1.590 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=11.569 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=11.137 ms

VPCS> 
```

Рис. 3.9. Пингование маршрутизатора узлом PC1

10. В окне Wireshark (рис. 3.10) проанализировал полученную информацию: эхо-запросы успешно отправились.



No.	Time	Source	Destination	Protocol	Length	Info
14	848.501490	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x30ba, seq=1/256, ttl=64 (reply in 15)
15	848.511414	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x30ba, seq=1/256, ttl=64 (request in 14)
16	849.512225	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x31ba, seq=2/512, ttl=64 (reply in 17)
17	849.514602	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x31ba, seq=2/512, ttl=64 (request in 16)
18	850.516658	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x32ba, seq=3/768, ttl=64 (reply in 19)
19	850.518043	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x32ba, seq=3/768, ttl=64 (request in 18)
20	851.528985	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x33ba, seq=4/1024, ttl=64 (reply in 21)
21	851.530746	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x33ba, seq=4/1024, ttl=64 (request in 20)
22	852.533279	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x34ba, seq=5/1280, ttl=64 (reply in 23)
23	852.543385	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x34ba, seq=5/1280, ttl=64 (request in 22)
24	853.563042	0c:1c:64:9a:00:00	Private_66:68:00	ARP	60	Who has 192.168.1.10? Tell 192.168.1.1

Frame 14: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0
Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: 0c:1c:64:9a:00:00 (0c:1c:64:9a:00:00)
Internet Protocol Version 4, Src: 192.168.1.10, Dst: 192.168.1.1
Internet Control Message Protocol

Рис. 3.10. Wireshark

11. Остановил захват пакетов в Wireshark (рис. 3.11). Остановил все устройства в проекте (рис. 3.12).

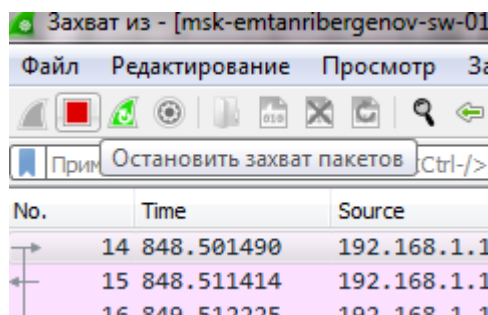


Рис. 3.11. Остановка захвата пакетов

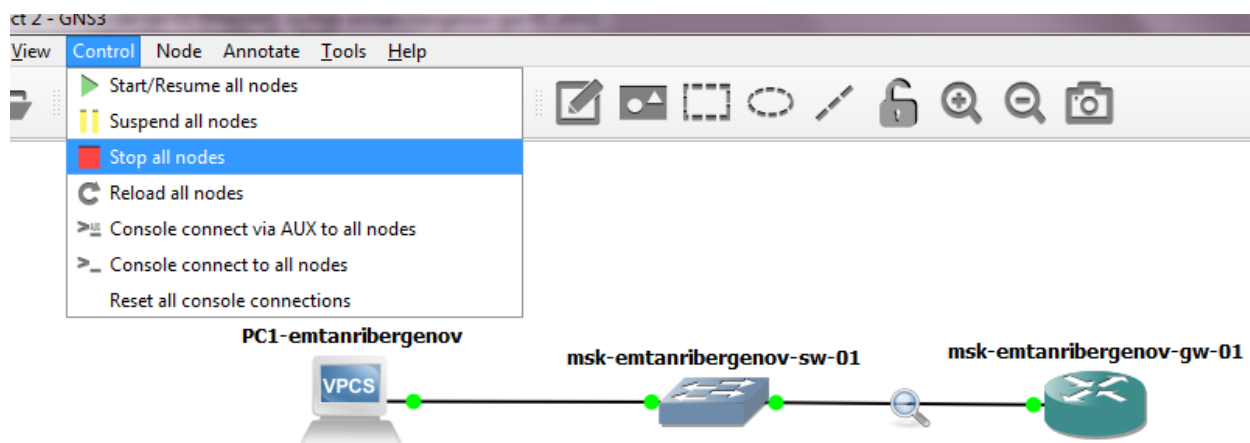


Рис. 3.12. Остановка всех узлов

4. Моделирование простейшей сети на базе маршрутизатора VyOS в GNS3

1. Запустил GNS3 VM и GNS3. Создал новый проект (рис. 4.1).

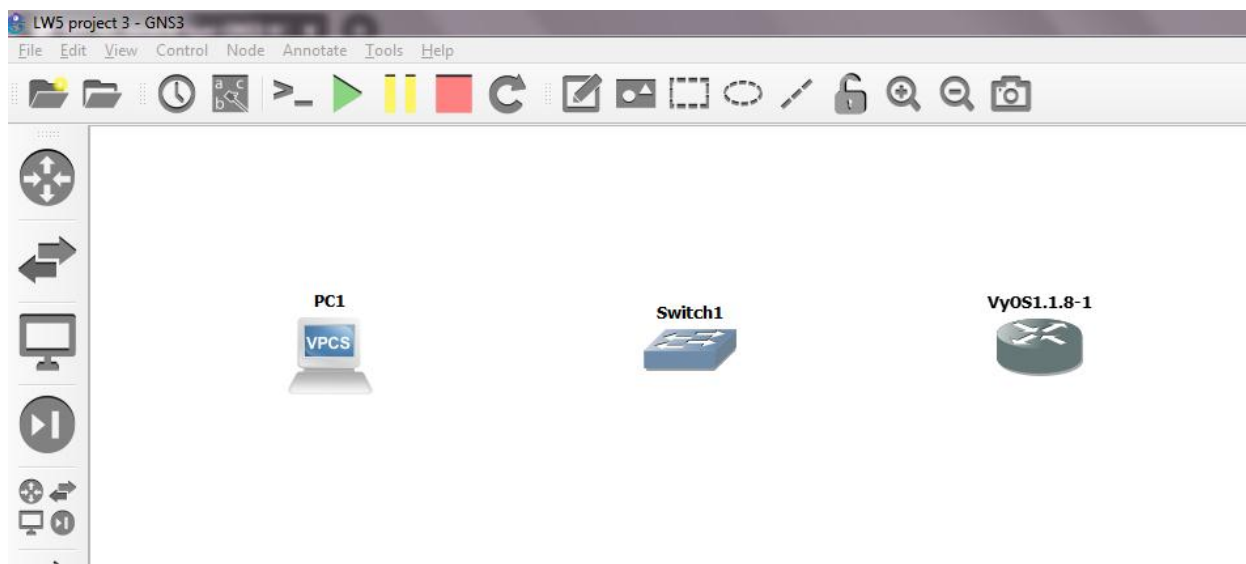


Рис. 4.1. Новый проект

- В рабочей области GNS3 разместите VPCS, коммутатор Ethernet и маршрутизатор VyOS. Изменил отображаемые названия устройств (рис. 4.2).

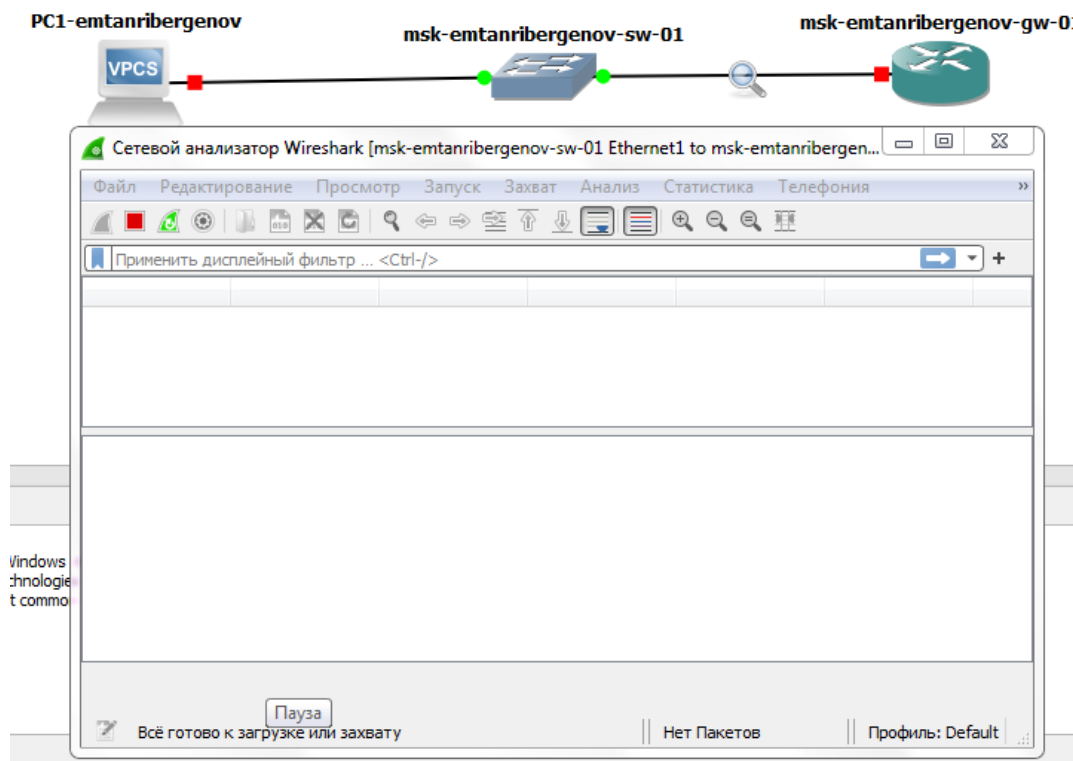


Рис. 4.2. Топология сети и захват трафика

- Запустил все устройства проекта. Открыл консоль всех устройств проекта (рис. 4.3).

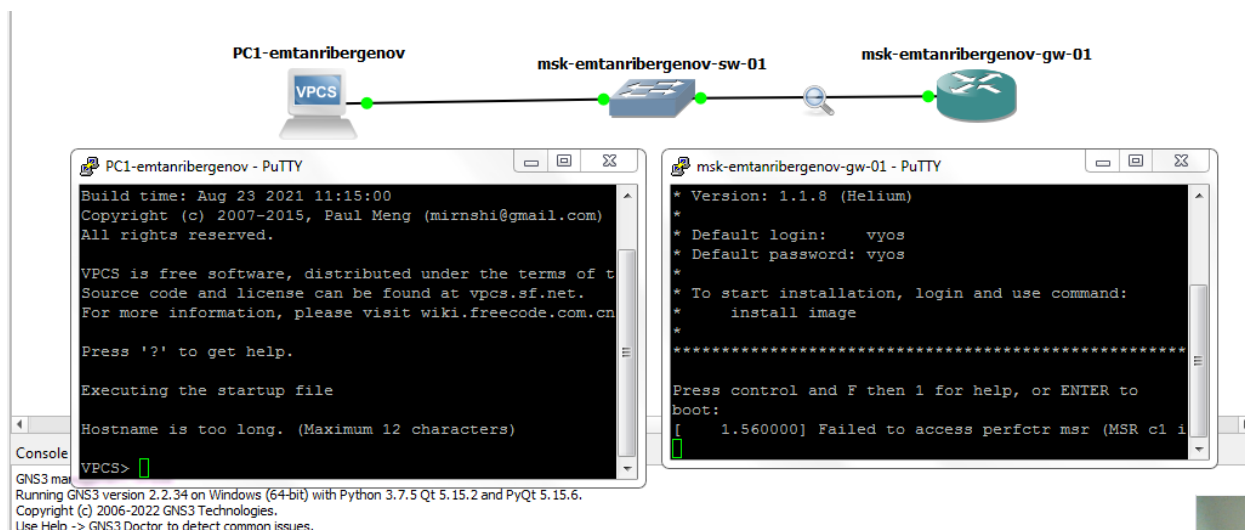
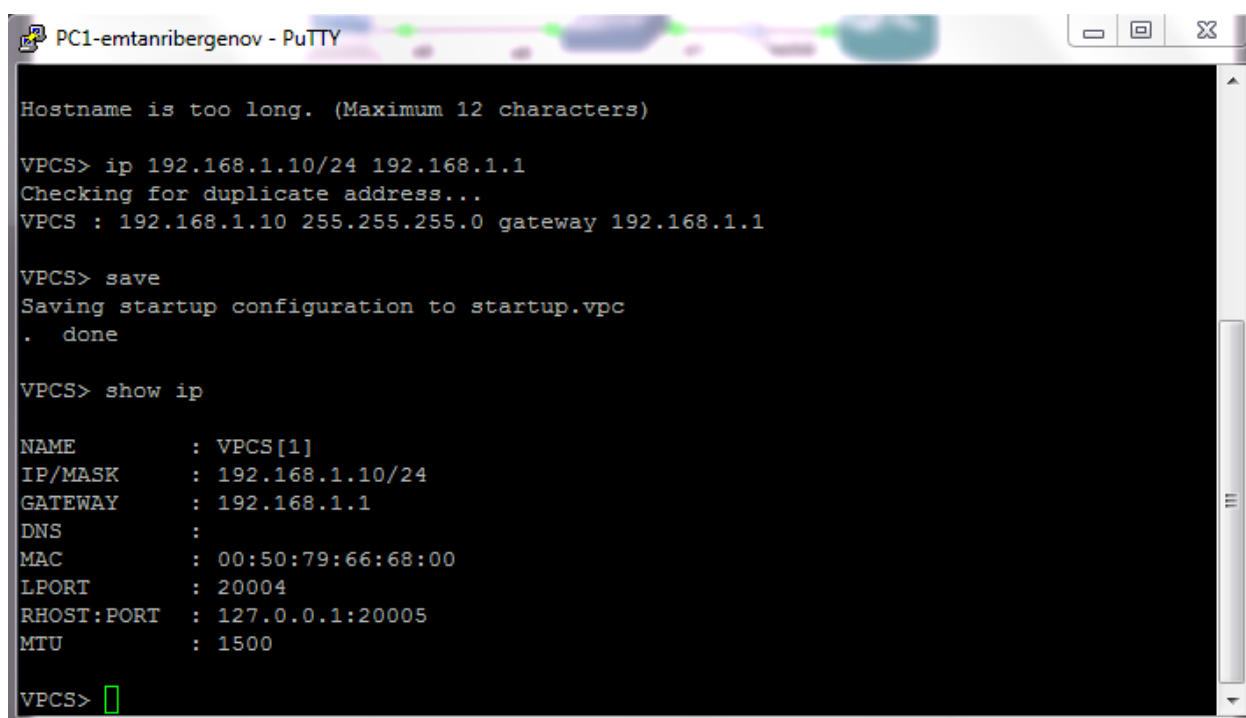


Рис. 4.3. Запуск устройств, их терминалов

4. Настроил IP-адресацию для интерфейса узла PC1 (рис. 4.4).



```
PC1-emtandribergenov - PuTTY

Hostname is too long. (Maximum 12 characters)

VPCS> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
VPCS : 192.168.1.10 255.255.255.0 gateway 192.168.1.1

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

VPCS> show ip

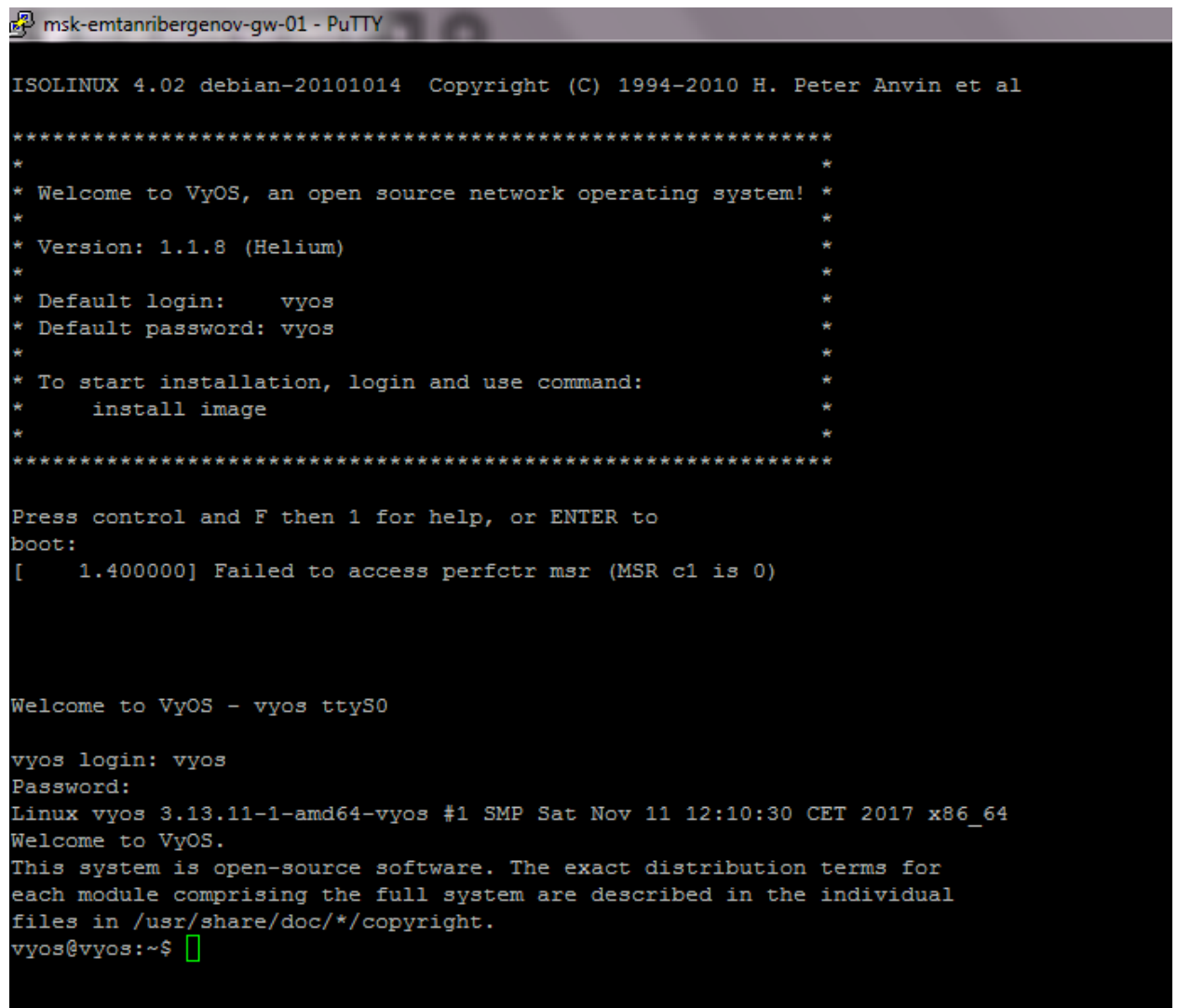
NAME       : VPCS[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 20004
RHOST:PORT : 127.0.0.1:20005
MTU        : 1500

VPCS> █
```

Рис. 4.4. Настройка IP-адресации для интерфейса узла PC1

5. Настроил маршрутизатор VyOS:

- После загрузки ввёл логин vyos и пароль vyos (рис. 4.5).



```
msk-emtandribergenov-gw-01 - PuTTY
ISOLINUX 4.02 debian-20101014 Copyright (C) 1994-2010 H. Peter Anvin et al
*****
*
* Welcome to VyOS, an open source network operating system! *
*
* Version: 1.1.8 (Helium) *
*
* Default login: vyos *
* Default password: vyos *
*
* To start installation, login and use command: *
* install image *
*
*****

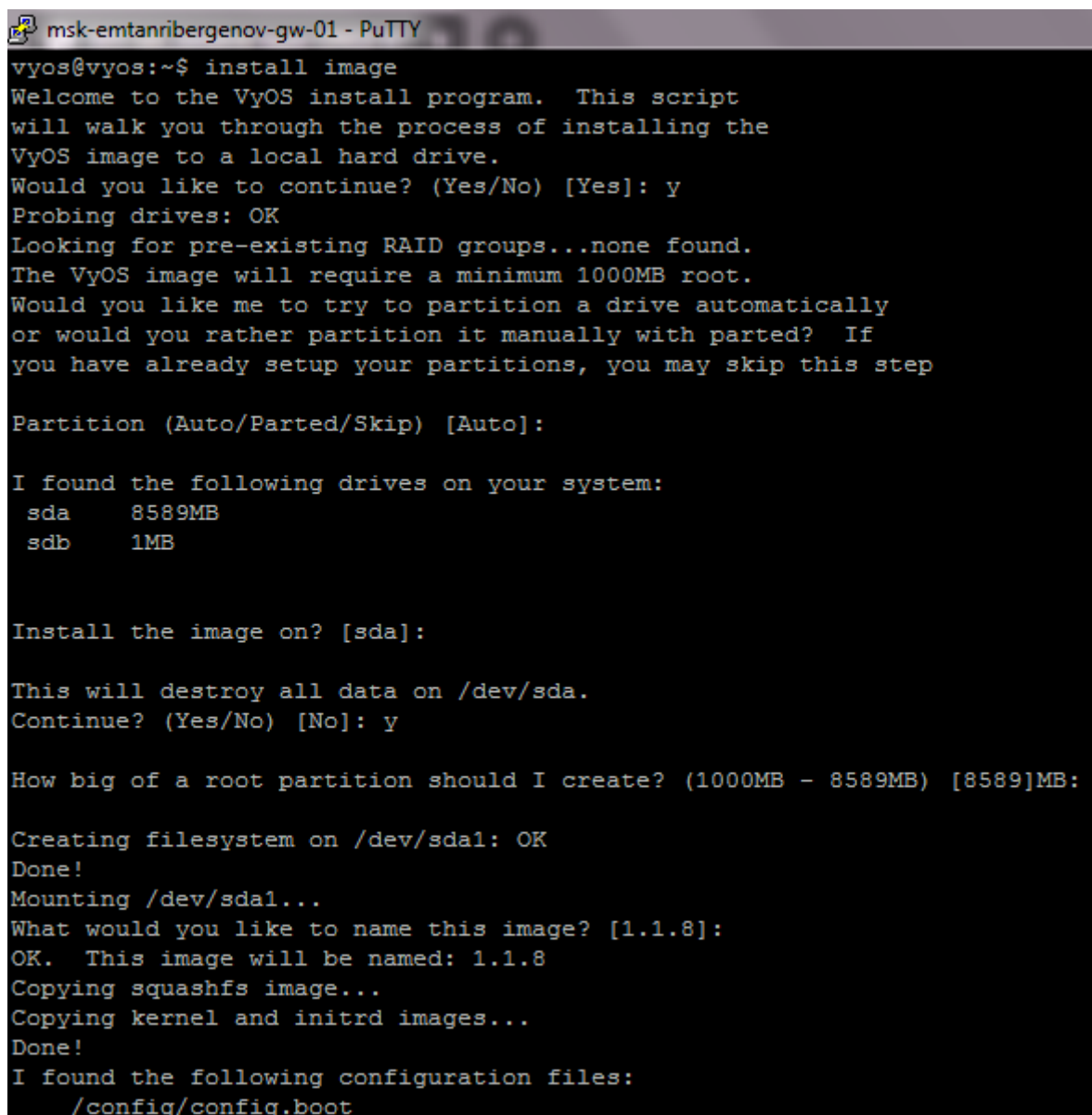
Press control and F then 1 for help, or ENTER to
boot:
[ 1.400000] Failed to access perfctr msr (MSR c1 is 0)

Welcome to VyOS - vyos ttyS0

vyos login: vyos
Password:
Linux vyos 3.13.11-1-amd64-vyos #1 SMP Sat Nov 11 12:10:30 CET 2017 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$
```

Рис. 4.5. Авторизация

- Загрузил систему (рис. 4.6 – 4.7)



```
msk-emtanribergenov-gw-01 - PuTTY
vyos@vyos:~$ install image
Welcome to the VyOS install program.  This script
will walk you through the process of installing the
VyOS image to a local hard drive.
Would you like to continue? (Yes/No) [Yes]: y
Probing drives: OK
Looking for pre-existing RAID groups...none found.
The VyOS image will require a minimum 1000MB root.
Would you like me to try to partition a drive automatically
or would you rather partition it manually with parted?  If
you have already setup your partitions, you may skip this step

Partition (Auto/Parted/Skip) [Auto]:

I found the following drives on your system:
sda      8589MB
sdb       1MB

Install the image on? [sda]:

This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]: y

How big of a root partition should I create? (1000MB - 8589MB) [8589]MB:

Creating filesystem on /dev/sda1: OK
Done!
Mounting /dev/sda1...
What would you like to name this image? [1.1.8]:
OK.  This image will be named: 1.1.8
Copying squashfs image...
Copying kernel and initrd images...
Done!
I found the following configuration files:
/config/config.boot
```

Рис. 4.6. Загрузка системы

```

Install the image on? [sda]:

This will destroy all data on /dev/sda.
Continue? (Yes/No) [No]: y

How big of a root partition should I create? (1000MB - 8589MB) [8589]MB:

Creating filesystem on /dev/sda1: OK
Done!
Mounting /dev/sda1...
What would you like to name this image? [1.1.8]:
OK. This image will be named: 1.1.8
Copying squashfs image...
Copying kernel and initrd images...
Done!
I found the following configuration files:
    /config/config.boot
    /opt/vyatta/etc/config.boot.default
Which one should I copy to sda? [/config/config.boot]:

Copying /config/config.boot to sda.
Enter password for administrator account
Enter password for user 'vyos':
Retype password for user 'vyos':
I need to install the GRUB boot loader.
I found the following drives on your system:
sda    8589MB
sdb     1MB

Which drive should GRUB modify the boot partition on? [sda]:

Setting up grub: OK
Done!
vyos@vyos:~$ reboot

```

Рис. 4.7. Загрузка системы

- Перезапустил маршрутизатор (рис. 4.8).

```

vyos@vyos:~$ reboot
Proceed with reboot? (Yes/No) [No] y

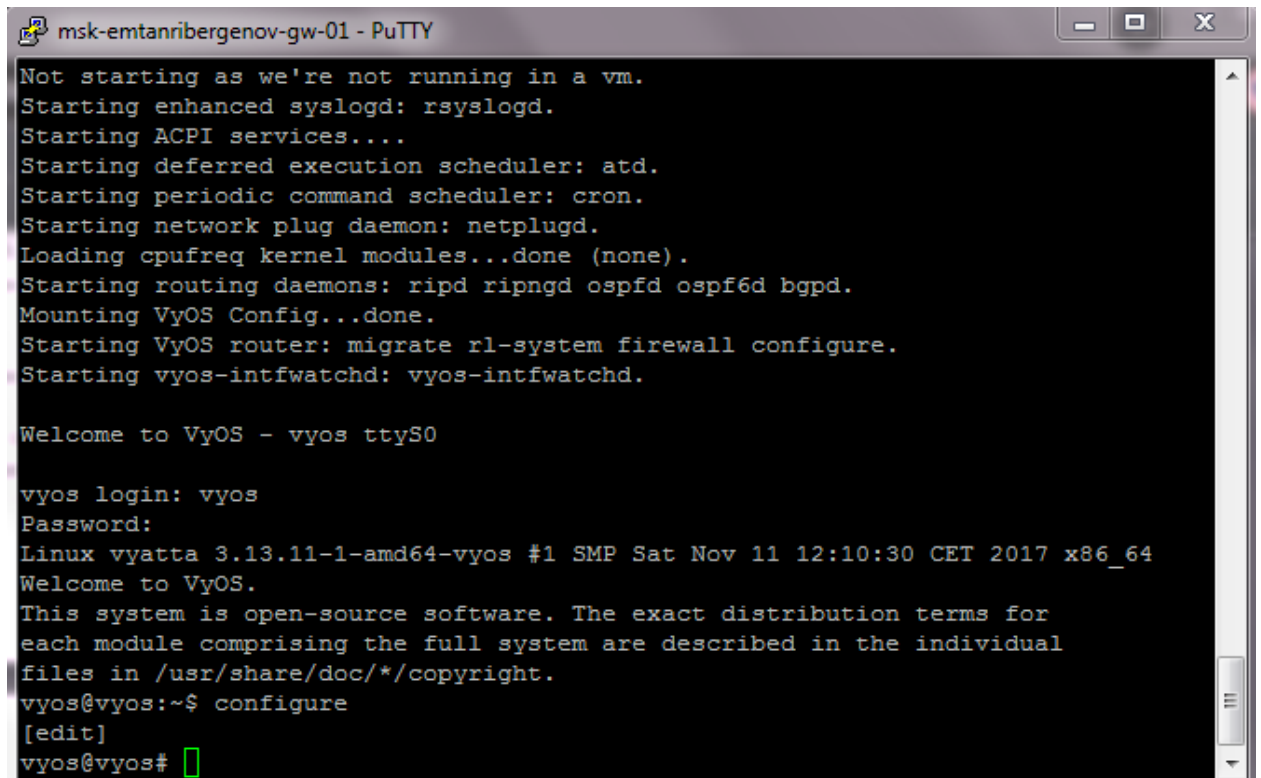
Broadcast message from root@vyos (ttyS0) (Fri Oct 21 15:59:33 2022):

The system is going down for reboot NOW!

```

Рис. 4.8.

- Перешёл в режим конфигурирования (рис. 4.9).



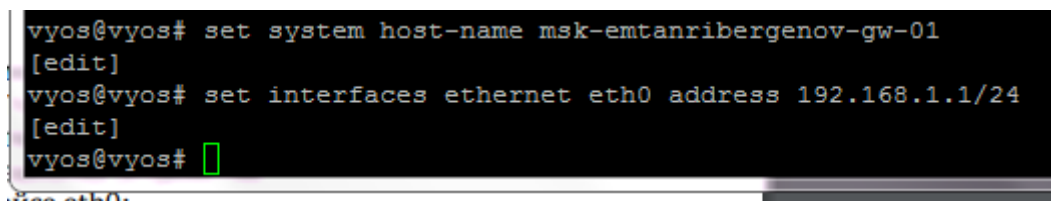
```
msk-emtanribergenov-gw-01 - PuTTY
Not starting as we're not running in a vm.
Starting enhanced syslogd: rsyslogd.
Starting ACPI services....
Starting deferred execution scheduler: atd.
Starting periodic command scheduler: cron.
Starting network plug daemon: netplugd.
Loading cpufreq kernel modules...done (none).
Starting routing daemons: ripd ripngd ospfd ospf6d bgpd.
Mounting VyOS Config...done.
Starting VyOS router: migrate rl-system firewall configure.
Starting vyos-intfwatcd: vyos-intfwatcd.

Welcome to VyOS - vyos ttyS0

vyos login: vyos
Password:
Linux vyatta 3.13.11-1-amd64-vyos #1 SMP Sat Nov 11 12:10:30 CET 2017 x86_64
Welcome to VyOS.
This system is open-source software. The exact distribution terms for
each module comprising the full system are described in the individual
files in /usr/share/doc/*/copyright.
vyos@vyos:~$ configure
[edit]
vyos@vyos#
```

Рис. 4.9. Режим конфигурирования

- Изменил имя устройства (рис. 4.10).
- Задал IP-адрес на интерфейсе eth0 (рис. 4.10).



```
vyos@vyos# set system host-name msk-emtanribergenov-gw-01
[edit]
vyos@vyos# set interfaces ethernet eth0 address 192.168.1.1/24
[edit]
vyos@vyos#
```

Рис. 4.10. Изменение имени и настройка IP-адресации

- Посмотрел внесённые в конфигурацию изменения (рис. 4.11).
- Применил изменения в конфигурации и сохранил саму конфигурацию (рис. 4.11).

```
vyos@vyos# compare
[edit interfaces ethernet eth0]
+address 192.168.1.1/24
[edit system]
>host-name msk-emtandribergenov-gw-01
[edit]
vyos@vyos# commit
[ system host-name msk-emtandribergenov-gw-01 ]
Stopping enhanced syslogd: rsyslogd.
Starting enhanced syslogd: rsyslogd.

[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos#
```

Рис. 4.11. Просмотр изменений в конфигурации и сохранение их

- Посмотрел информацию об интерфейсах маршрутизатора (рис. 4.12).
- Вышел из режима конфигурирования (рис. 4.12).

```
vyos@vyos# show interfaces
ethernet eth0 {
    address 192.168.1.1/24
    hw-id 0c:66:a7:4b:00:00
}
ethernet eth1 {
    hw-id 0c:66:a7:4b:00:01
}
ethernet eth2 {
    hw-id 0c:66:a7:4b:00:02
}
loopback lo {
}
[edit]
vyos@vyos# exit
exit
vyos@vyos:~$
```

Рис. 4.12. Информация об интерфейсах маршрутизатора и выход из режима конфигурирования

6. Проверил подключение. Узел PC1 успешно отправляет эхо-запросы на адрес маршрутизатора 192.168.1.1 (рис. 4.13).

```
VPCS> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=0.957 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.713 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=1.758 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=1.352 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=2.259 ms

VPCS> █
```

Рис. 4.13. Пингование маршрутизатора узлом PC1

7. В окне Wireshark (рис. 4.14). проанализировал полученную информацию: успешная отправка эхо-запросов, адрес маршрутизатора – широковещательный.

Применить дисплейный фильтр ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
14	242.520666	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
15	243.520693	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
16	244.520962	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
17	301.154722	::	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
18	301.234860	::	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
19	301.364649	::	ff02::1:ff4b:0	ICMPv6	78	Neighbor Solicitation for fe80::e66:a7ff:fe4b:0
20	302.374791	fe80::e66:a7ff:fe4b...	ff02::16	ICMPv6	150	Multicast Listener Report Message v2
21	302.386201	fe80::e66:a7ff:fe4b...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
22	302.855090	fe80::e66:a7ff:fe4b...	ff02::16	ICMPv6	150	Multicast Listener Report Message v2
23	303.234716	fe80::e66:a7ff:fe4b...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
24	1051.590649	::	ff02::16	ICMPv6	110	Multicast Listener Report Message v2
25	1051.609623	::	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
26	1051.679669	::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
27	1052.039813	::	ff02::1:ff4b:0	ICMPv6	78	Neighbor Solicitation for fe80::e66:a7ff:fe4b:0
28	1053.052681	fe80::e66:a7ff:fe4b...	ff02::16	ICMPv6	150	Multicast Listener Report Message v2
29	1053.069629	fe80::e66:a7ff:fe4b...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
30	1053.139942	fe80::e66:a7ff:fe4b...	ff02::16	ICMPv6	150	Multicast Listener Report Message v2
31	1053.919622	fe80::e66:a7ff:fe4b...	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
32	1462.360561	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.1? Tell 192.168.1.10
33	1462.361713	0c:66:a7:4b:00:00	Private_66:68:00	ARP	60	192.168.1.1 is at 0c:66:a7:4b:00:00
34	1462.362741	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x22c4, seq=1/256, ttl=64 (reply in 35)
35	1462.363504	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x22c4, seq=1/256, ttl=64 (request in 34)
36	1463.364137	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x23c4, seq=2/512, ttl=64 (reply in 37)
37	1463.366558	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x23c4, seq=2/512, ttl=64 (request in 36)
38	1464.367468	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x24c4, seq=3/768, ttl=64 (reply in 39)
39	1464.368968	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x24c4, seq=3/768, ttl=64 (request in 38)
40	1465.370969	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x25c4, seq=4/1024, ttl=64 (reply in 41)
41	1465.372092	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x25c4, seq=4/1024, ttl=64 (request in 40)
42	1466.373686	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0x26c4, seq=5/1280, ttl=64 (reply in 43)
43	1466.374606	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0x26c4, seq=5/1280, ttl=64 (request in 42)
44	1467.364913	0c:66:a7:4b:00:00	Private_66:68:00	ARP	60	Who has 192.168.1.10? Tell 192.168.1.1
45	1467.365340	Private_66:68:00	0c:66:a7:4b:00:00	ARP	60	192.168.1.10 is at 00:50:79:66:68:00

Рис. 4.14. Wireshark

8. Остановил захват пакетов в Wireshark (рис. 4.15). Остановил все устройства в проекте (рис. 4.16). Завершил работу с GNS3 (рис. 4.17).

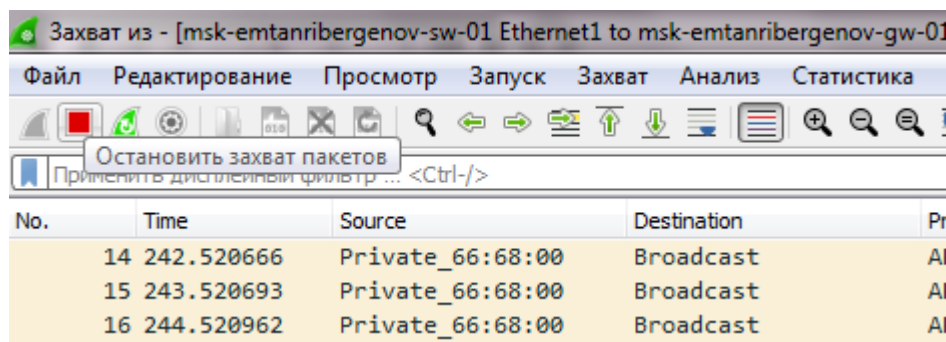


Рис. 4.15. Остановка захвата пакетов

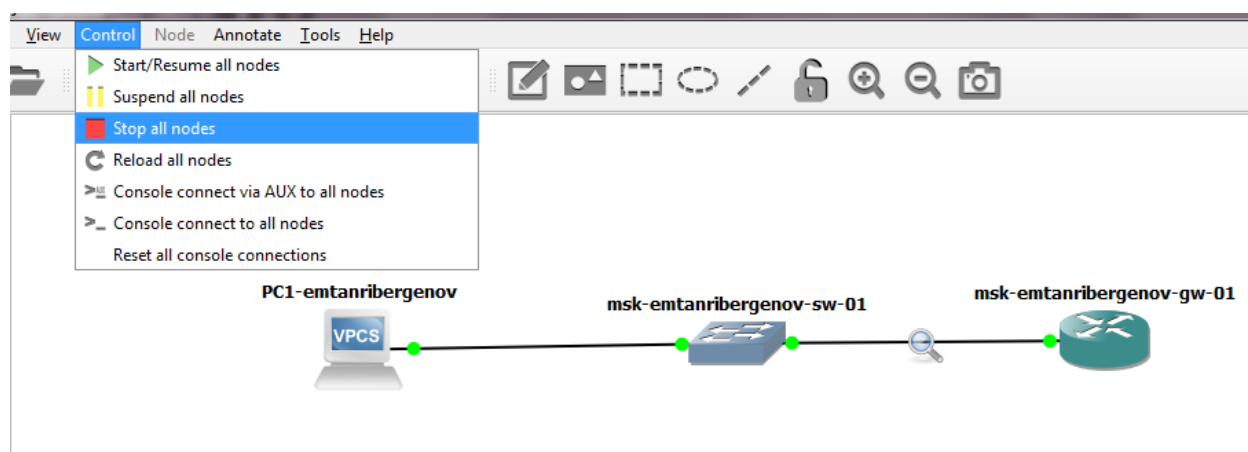


Рис. 4.16. Остановка всех устройств

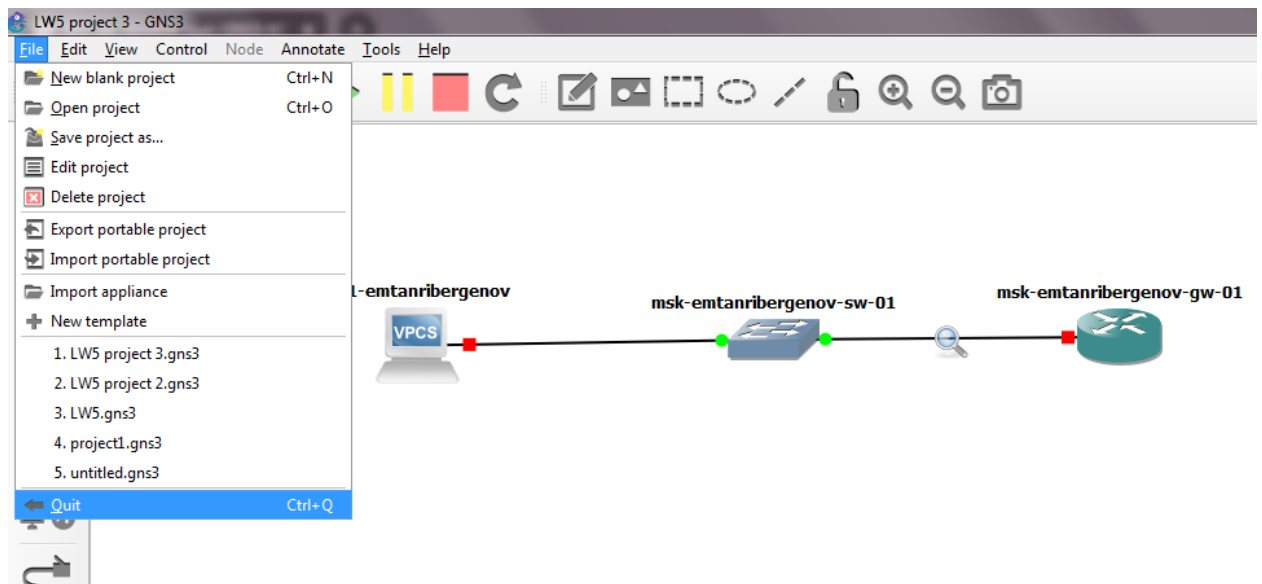


Рис. 4.17. Выход из GNS3

Вывод:

В результате лабораторной работы я освоил навык построения простейших моделей сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, а также попрактиковал анализ трафика посредством Wireshark.