

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ №5

дисциплина: Сетевые технологии

Студент: Боровикова Карина Владимировна

Группа: НПИбд-01-20

МОСКВА

2021 г.

Цель работы

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

Ход выполнения работы

1. Моделирование простейшей сети на базе коммутатора в GNS3

1. Запустим GNS3 VM и GNS3. Создадим новый проект.
2. В рабочей области GNS3 разместим коммутатор Ethernet и два VPCS. Щёлкнув на устройстве правой кнопкой мыши выберем в меню Configure. Изменим название устройства, включив в имя устройства имя учётной записи выполняющего работу студента. Коммутатору присвоим название msk-kvborovikova-sw-01. Соедините VPCS с коммутатором. Отобразите обозначение интерфейсов соединения (Рис.1).

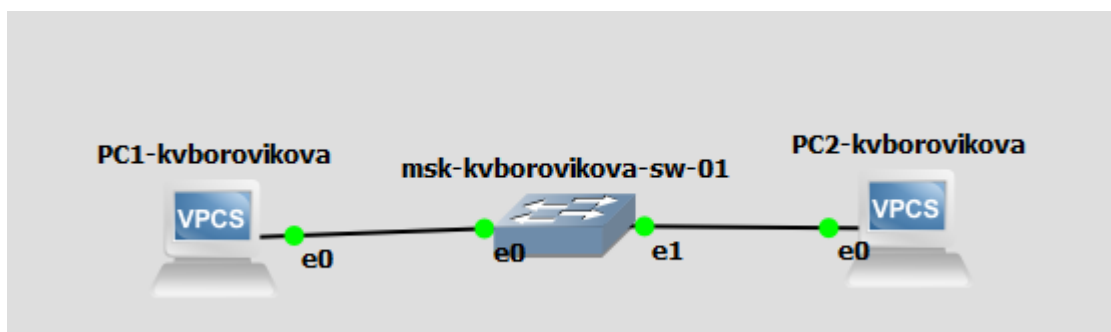


Рисунок 1. Топология простейшей сети в GNS3

3. Зададим IP-адреса VPCS. Для этого с помощью меню, вызываемого правой кнопкой мыши, запустим Start, например, PC-1, затем вызовем его терминал Console. Для просмотра синтаксиса возможных для ввода команд наберем /? (Рис. 2). Для задания IP-адреса 192.168.1.11 в сети 192.168.1.0/24 введем:

```
ip 192.168.1.11/24 192.168.1.1
```

Здесь 192.168.1.1 — адрес шлюза. Для уточнения синтаксиса перед вводом можно ввести ip /?. Для сохранения конфигурации необходимо ввести команду save. Аналогичным образом зададим IP-адрес 192.168.1.12 для PC-2 (Рис. 3)

4. Проверим работоспособность соединения между PC-1 и PC-2 с помощью команды ping (Рис. 3).
5. Остановим в проекте все узлы (меню GNS3 -> Control -> Stop all nodes).

```
PC1-kvborovikova - PuTTY
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Hostname is too long. (Maximum 12 characters)

VPCS> /?

?                                Print help
! COMMAND [ARG ...]          Invoke an OS COMMAND with optional ARG(s)
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

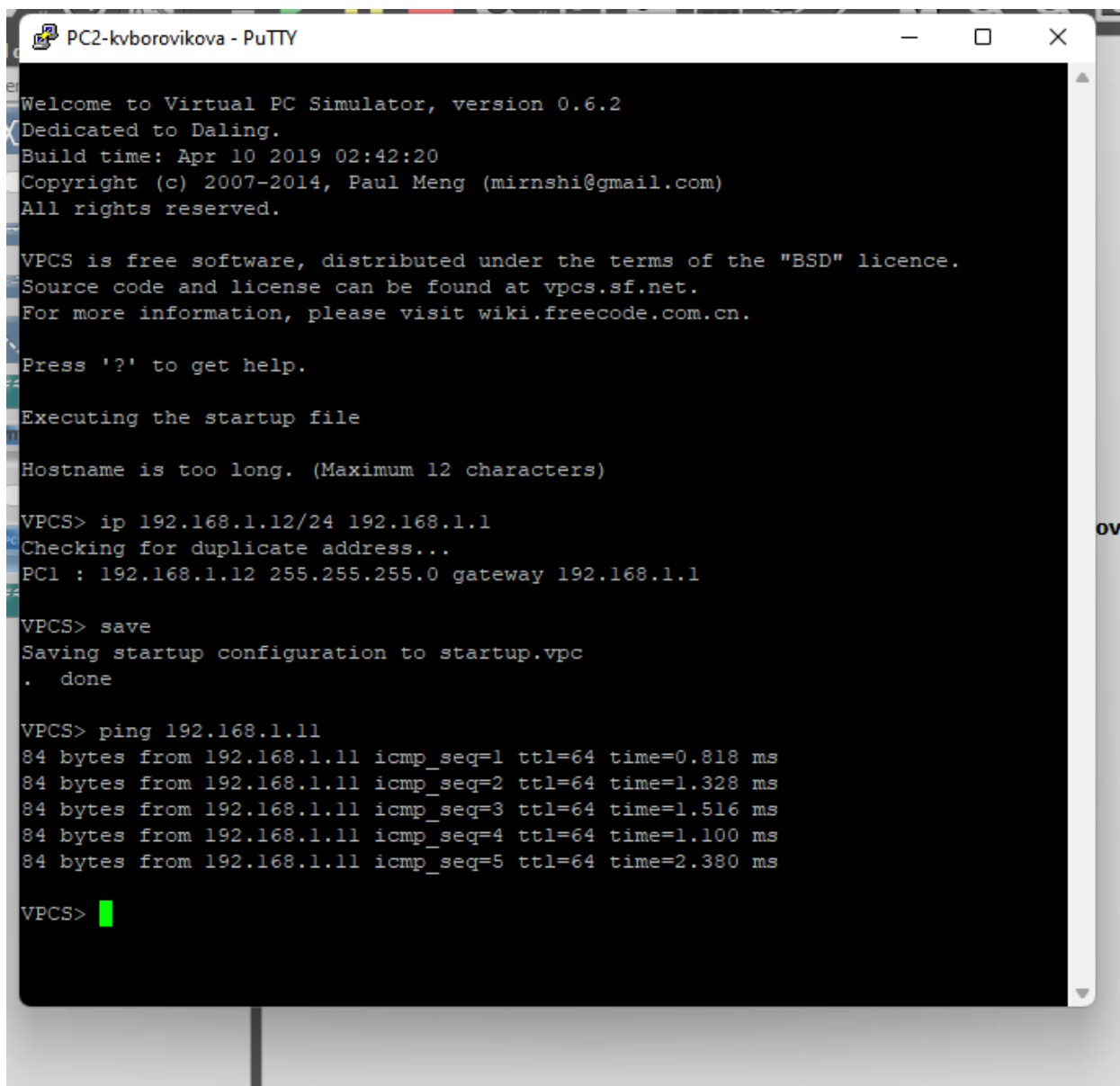
To get command syntax help, please enter '?' as an argument of the command.

VPCS> 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

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

VPCS> █
```

Рисунок 2. Задаем IP адрес для PC1, предварительно узнав справку по командам



```
PC2-kvborovikova - PuTTY

Welcome to Virtual PC Simulator, version 0.6.2
Dedicated to Daling.
Build time: Apr 10 2019 02:42:20
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence.
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Hostname is too long. (Maximum 12 characters)

VPCS> ip 192.168.1.12/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.12 255.255.255.0 gateway 192.168.1.1

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

VPCS> ping 192.168.1.11
84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=0.818 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=1.328 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=1.516 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=1.100 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=2.380 ms

VPCS> 
```

Рисунок 3. Ip-адресация для PC-2 и проверка соединения компьютеров с помощью ping

2. Анализ трафика в GNS3 посредством Wireshark

1. Запустим на соединении между PC-1 и коммутатором анализатор трафика. Для этого щёлкнем правой кнопкой мыши на соединении, выберем в меню Start capture. Запустился Wireshark, а в проекте GNS3 на соединении появится значок лупы.
2. В проекте GNS3 стартуем все узлы (меню GNS3 Control Start/Resume all nodes). В окне Wireshark (Рис. 4) отобразилась информация по протоколу ARP (Рис. 5, 6). В запросах отображена основная информация по запросам: длина кадра, тип, MAC-адрес источника и шлюза
3. В терминале PC-2 посмотрим информацию по опциям команды ping, введя ping /?. Затем сделаем один эхо-запрос в ICMP-моду к узлу PC-1 (Рис.11, 5, 7). В

запросах отображена основная информация по запросам: длина кадра, тип, MAC-адрес источника и шлюза

- 4. Сделайте один эхо-запрос в UDP-мде к узлу PC-1. В запросах отображена основная информация по запросам: длина кадра, тип, MAC-адрес источника и шлюза. (Рис. 11, 5, 8)
- 5. Сделаем один эхо-запрос в TCP-мде к узлу PC-1. В запросах отображена основная информация по запросам: длина кадра, тип, MAC-адрес источника и шлюза. (Рис. 11, 9, 10)
- 6. Остановим захват пакетов в Wireshark.



Рисунок 4. Анализ трафика в Wireshark

Захват из - [PC1-kvborovikova Ethernet0 to msk-kvborovikova-sw-01 Ethernet0]

Файл Редактирование Просмотр Запуск Захват Анализ Статистика Телефония Беспроводной Инструменты Помощь

Применить дисплейный фильтр ... <Ctrl-F>

No.	Time	Source	Destination	Protocol	Length	Info
2	0.052899	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
3	1.054459	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
4	2.054724	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.11 (Request)
5	81.900993	::	ff02::2	ICMPv6	62	Router Solicitation
6	81.952910	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
7	82.954530	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
8	83.955140	Private_66:68:01	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.12 (Request)
9	629.477671	Private_66:68:01	Broadcast	ARP	64	Who has 192.168.1.11? Tell 192.168.1.12
10	629.478650	Private_66:68:00	Private_66:68:01	ARP	64	192.168.1.11 is at 00:50:79:66:68:00
11	629.479631	192.168.1.12	192.168.1.11	ICMP	98	Echo (ping) request id=0xf6ea, seq=1/256, ttl=64 (reply in 12)
12	629.479631	192.168.1.11	192.168.1.12	ICMP	98	Echo (ping) reply id=0xf6ea, seq=1/256, ttl=64 (request in 11)
13	630.481772	192.168.1.12	192.168.1.11	ICMP	98	Echo (ping) request id=0xf7ea, seq=2/512, ttl=64 (reply in 14)
14	630.481772	192.168.1.11	192.168.1.12	ICMP	98	Echo (ping) reply id=0xf7ea, seq=2/512, ttl=64 (request in 13)
15	631.484304	192.168.1.12	192.168.1.11	ICMP	98	Echo (ping) request id=0xf8ea, seq=3/768, ttl=64 (reply in 16)
16	631.484304	192.168.1.11	192.168.1.12	ICMP	98	Echo (ping) reply id=0xf8ea, seq=3/768, ttl=64 (request in 15)
17	632.486957	192.168.1.12	192.168.1.11	ICMP	98	Echo (ping) request id=0xf9ea, seq=4/1024, ttl=64 (reply in 18)
18	632.487921	192.168.1.11	192.168.1.12	ICMP	98	Echo (ping) reply id=0xf9ea, seq=4/1024, ttl=64 (request in 17)
19	633.490510	192.168.1.12	192.168.1.11	ICMP	98	Echo (ping) request id=0xfaea, seq=5/1280, ttl=64 (reply in 20)
20	633.491490	192.168.1.11	192.168.1.12	ICMP	98	Echo (ping) reply id=0xfaea, seq=5/1280, ttl=64 (request in 19)
21	740.007529	192.168.1.12	192.168.1.11	ECHO	98	Request
22	740.008494	192.168.1.11	192.168.1.12	ECHO	98	Response
23	741.009893	192.168.1.12	192.168.1.11	ECHO	98	Request
24	741.009893	192.168.1.11	192.168.1.12	ECHO	98	Response
25	742.012840	192.168.1.12	192.168.1.11	ECHO	98	Request
26	742.012840	192.168.1.11	192.168.1.12	ECHO	98	Response
27	743.015468	192.168.1.12	192.168.1.11	ECHO	98	Request
28	743.015468	192.168.1.11	192.168.1.12	ECHO	98	Response
29	744.017866	192.168.1.12	192.168.1.11	ECHO	98	Request
30	744.017866	192.168.1.11	192.168.1.12	ECHO	98	Response

▼ Frame 21: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0

> Interface id: 0 (-)

Рисунок 5. Трафик, захваченный в Wireshark

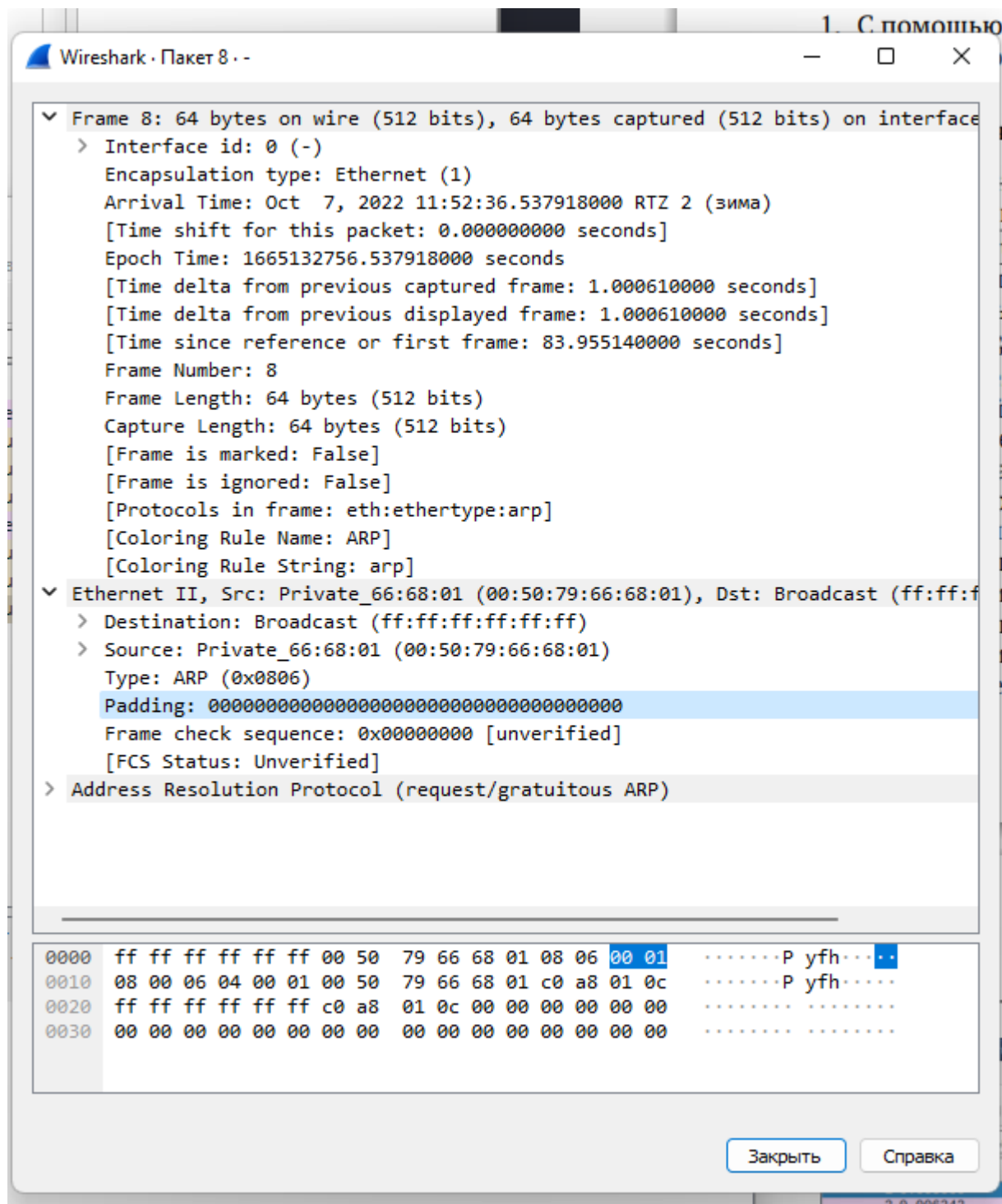


Рисунок 6. ARP пакет

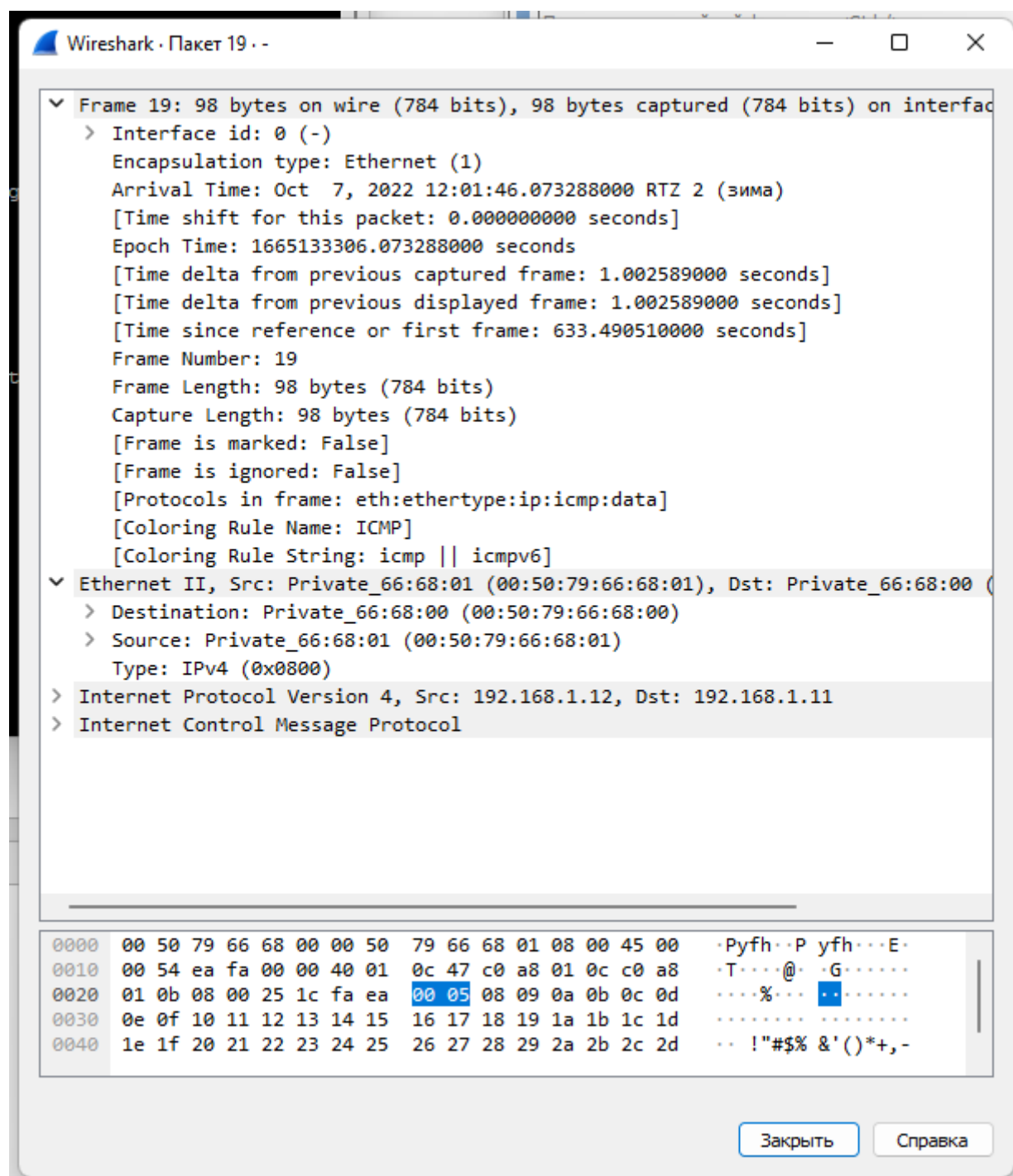


Рисунок 7. ICMP пакет

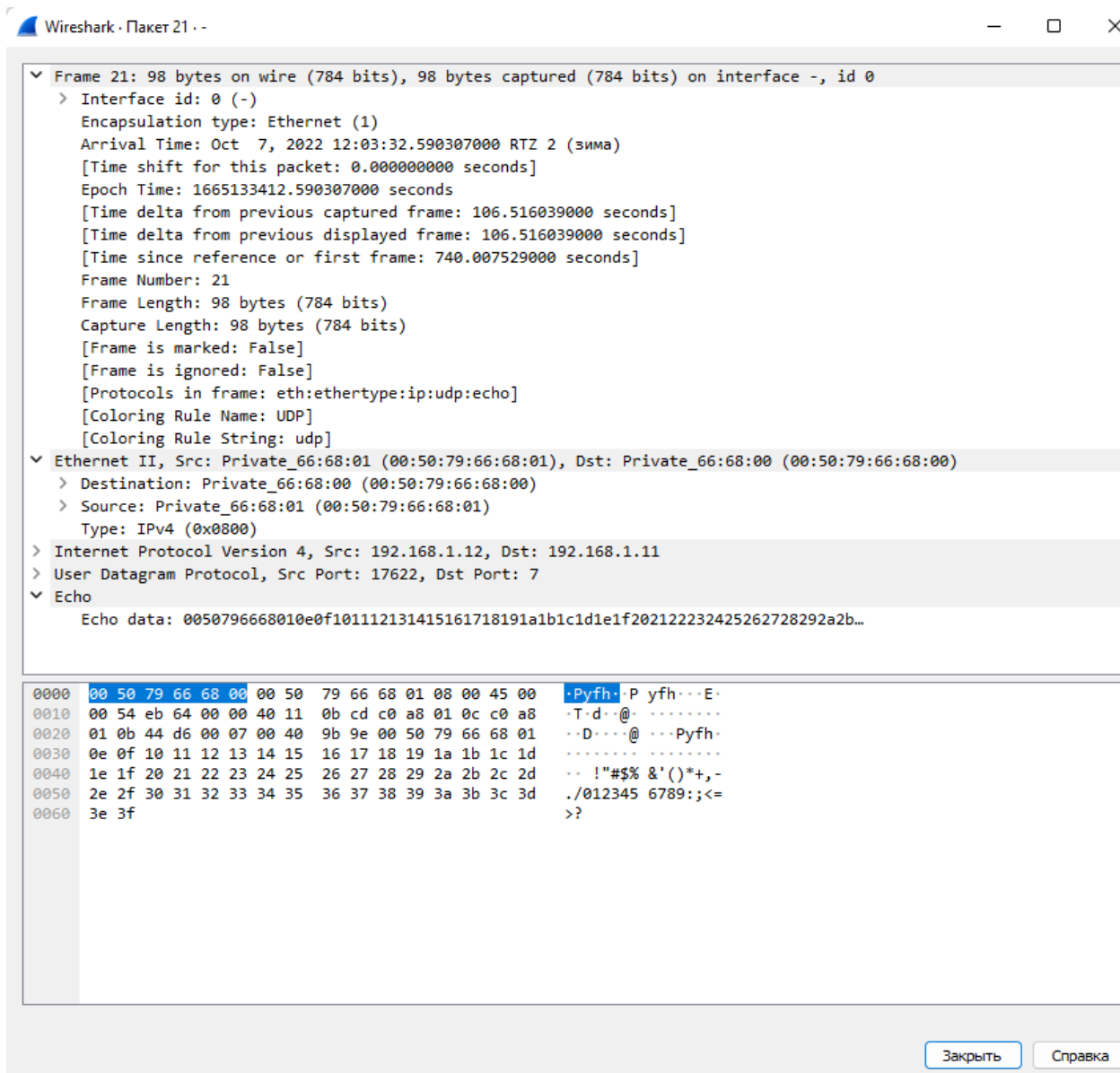


Рисунок 8. UDP пакет

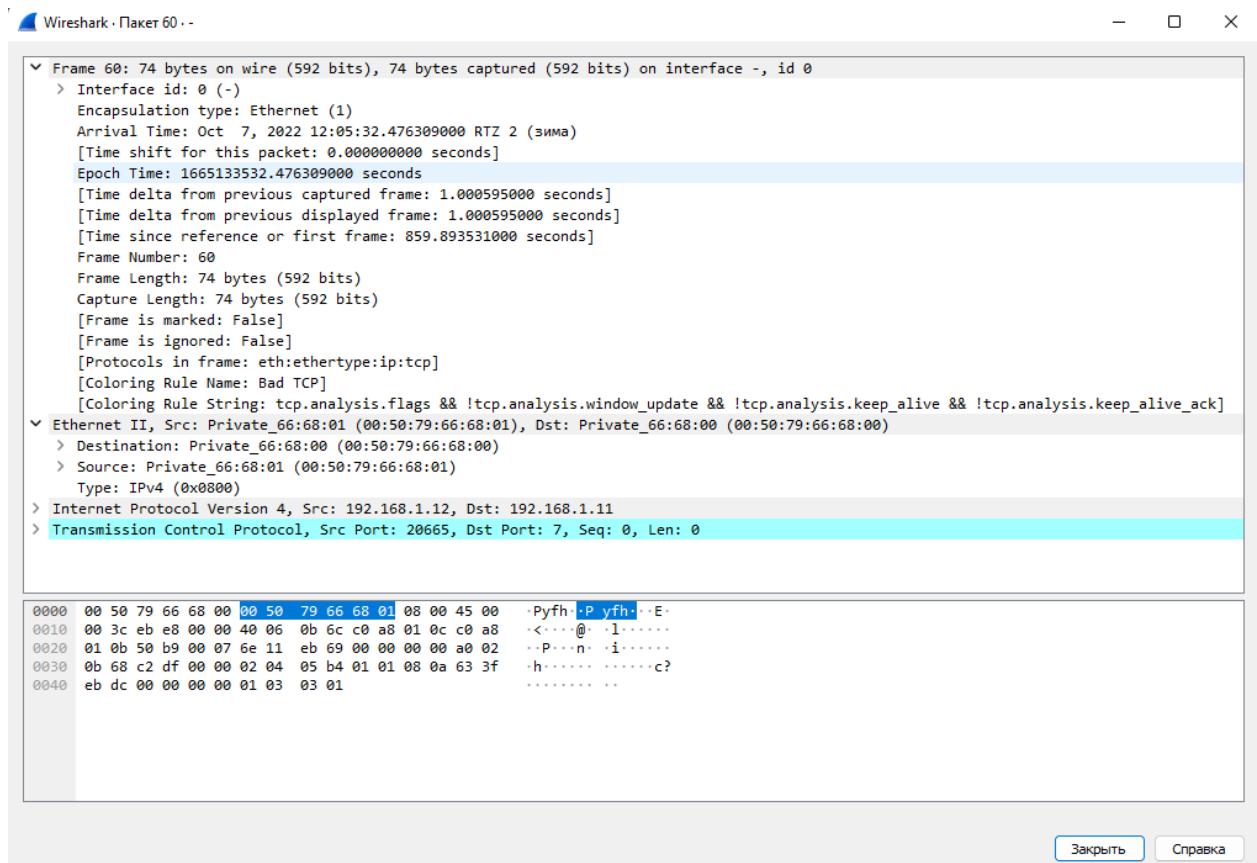


Рисунок 9. TCP пакет

Захват из - [PCI-kvborovikova Ethernet0 to msk-kvborovikova-sw-01 Ethernet0]						
Файл Редактирование Просмотр Запуск Анализ Статистика Телефония Беспроводной Инструменты Помощь						
Применить дисплейный фильтр ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
43	857.871242	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0
44	857.873199	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [ACK] Seq=1 Ack=1 Win=2920 Len=0 TSval=1665133530 TSecr=0
45	857.874179	192.168.1.12	192.168.1.11	ECHO	122	Request
46	857.875164	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [ACK] Seq=1 Ack=57 Win=2920 Len=0
47	857.878098	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1665133530 TSecr=0
48	857.878098	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [ACK] Seq=1 Ack=58 Win=2920 Len=0
49	857.878098	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
50	857.882016	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1665133530 TSecr=0
51	858.882173	192.168.1.12	192.168.1.11	TCP	74	[TCP Port numbers reused] 20665 → 7 [SYN] Seq=0 Win=2920 Len=0 MSS=1460 TSval=1665133531 TSecr=0
52	858.882173	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0
53	858.884119	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [ACK] Seq=1 Ack=1 Win=2920 Len=0 TSval=1665133531 TSecr=0
54	858.886078	192.168.1.12	192.168.1.11	ECHO	122	Request
55	858.886078	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [ACK] Seq=1 Ack=57 Win=2920 Len=0
56	858.889030	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1665133531 TSecr=0
57	858.889030	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [ACK] Seq=1 Ack=58 Win=2920 Len=0
58	858.889030	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
59	858.892936	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1665133531 TSecr=0
60	859.893531	192.168.1.12	192.168.1.11	TCP	74	[TCP Port numbers reused] 20665 → 7 [SYN] Seq=0 Win=2920 Len=0 MSS=1460 TSval=1665133532 TSecr=0
61	859.893531	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0
62	859.895474	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [ACK] Seq=1 Ack=1 Win=2920 Len=0 TSval=1665133532 TSecr=0
63	859.897446	192.168.1.12	192.168.1.11	ECHO	122	Request
64	859.897446	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [ACK] Seq=1 Ack=57 Win=2920 Len=0
65	859.901350	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1665133532 TSecr=0
66	859.901350	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [ACK] Seq=1 Ack=58 Win=2920 Len=0
67	859.901350	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
68	859.905284	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1665133532 TSecr=0
69	860.905913	192.168.1.12	192.168.1.11	TCP	74	[TCP Port numbers reused] 20665 → 7 [SYN] Seq=0 Win=2920 Len=0 MSS=1460 TSval=1665133533 TSecr=0
70	860.905913	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [SYN, ACK] Seq=0 Ack=1 Win=2920 Len=0
71	860.907882	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [ACK] Seq=1 Ack=1 Win=2920 Len=0 TSval=1665133533 TSecr=0
72	860.909833	192.168.1.12	192.168.1.11	ECHO	122	Request
73	860.909833	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [ACK] Seq=1 Ack=57 Win=2920 Len=0
74	860.913760	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [FIN, PSH, ACK] Seq=57 Ack=1 Win=2920 Len=0 TSval=1665133533 TSecr=0
75	860.913760	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [ACK] Seq=1 Ack=58 Win=2920 Len=0
76	860.913760	192.168.1.11	192.168.1.12	TCP	54	7 → 20665 [FIN, ACK] Seq=1 Ack=58 Win=2920 Len=0
77	860.917677	192.168.1.12	192.168.1.11	TCP	66	20665 → 7 [ACK] Seq=58 Ack=2 Win=2920 Len=0 TSval=1665133533 TSecr=0
▼ Frame 21: 98 bytes on wire (784 bits), 98 bytes captured (784 bits) on interface -, id 0						
Interface id: 0 (-)						
Encapsulation type: Ethernet (1)						
Arrival Time: Oct 7, 2022 12:03:32.590307000 RTZ 2 (зима)						
[Time shift for this packet: 0.000000000 seconds]						
Epoch Time: 1665133412.590307000 seconds						
[Time delta from previous captured frame: 106.516039000 seconds]						
[Time delta from previous displayed frame: 106.516039000 seconds]						
[Time since reference or first frame: 740.007529000 seconds]						
Frame Number: 21						
0000	00 50 79 66 68 00 00 50	79 66 68 01 08 00 45 00	Pyfh..P yfh...E			
0010	00 54 eb 64 00 00 40 11	0b cd c0 a8 01 0c c0 a8	T.d..@:			
0020	01 0b 44 d6 00 07 00 40	9b 9e 00 50 79 66 68 01	.D...@...Pyfh.			
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		>?			

Рисунок 10. Трафик в Wireshark

```
PC2-kvborovikova - PuTTY

VPCS> 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.

VPCS> ping 192.168.1.11 -1
84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=1.089 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=0.931 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=1.474 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=1.698 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=1.581 ms

VPCS> ping 192.168.1.11 -2
84 bytes from 192.168.1.11 udp_seq=1 ttl=64 time=0.838 ms
84 bytes from 192.168.1.11 udp_seq=2 ttl=64 time=1.370 ms
84 bytes from 192.168.1.11 udp_seq=3 ttl=64 time=1.245 ms
84 bytes from 192.168.1.11 udp_seq=4 ttl=64 time=1.114 ms
84 bytes from 192.168.1.11 udp_seq=5 ttl=64 time=1.354 ms

VPCS> ping 192.168.1.11 -1 -c 1
84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=1.475 ms

VPCS> ping 192.168.1.11 -2 -c 1
84 bytes from 192.168.1.11 udp_seq=1 ttl=64 time=1.026 ms

VPCS> ping 192.168.1.11 -3 -c 1
Connect    7@192.168.1.11 seq=1 ttl=64 time=14.682 ms
SendData   7@192.168.1.11 seq=1 ttl=64 time=15.397 ms
Close      7@192.168.1.11 seq=1 ttl=64 time=30.794 ms

VPCS> 
```

Рисунок 11. Команды в терминале PC2

3. Моделирование простейшей сети на базе маршрутизатора FRR в GNS3

1. Запустим GNS3 VM и GNS3. Создадим новый проект.
2. В рабочей области GNS3 разместим VPCS, коммутатор Ethernet и маршрутизатор

FRR (Рис.12).

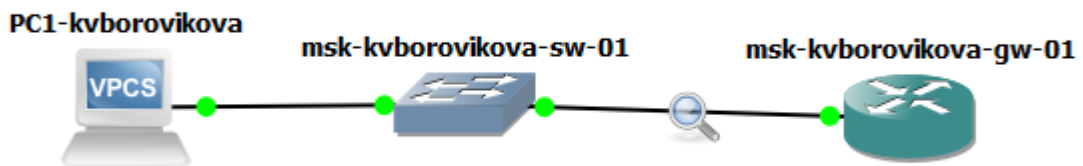


Рисунок 12. Топология простейшей сети с маршрутизатором в GNS3

3. Изменим отображаемые названия устройств. Коммутатору присвоим название по принципу msk-user-sw-0x, маршрутизатору — по принципу mskuser-gw-0x, VPCS — по принципу PCx-user, где вместо user укажем имя учётной записи, вместо x — порядковый номер устройства.
4. Включим захват трафика на соединении между коммутатором и маршрутизатором.
5. Запустим все устройства проекта. Откроем консоль всех устройств проекта.
6. Настроим IP-адресацию для интерфейса узла PC1(Рис.14):

```
ip 192.168.1.10/24 192.168.1.1
save
show ip
```

7. Настроим IP-адресацию для интерфейса локальной сети маршрутизатора (Рис.13): Router# configure terminal

```
Router(config)# hostname msk-user-gw-01
msk-user-gw-01(config)# exit
msk-user-gw-01# write memory
msk-user-gw-01# configure terminal
msk-user-gw-01(config)# interface eth0
msk-user-gw-01(config-if)# ip address 192.168.1.1/24
msk-user-gw-01(config-if)# no shutdown
msk-user-gw-01(config-if)# exit
msk-user-gw-01(config)# exit
```

```
msk-user-gw-01# write memory
```

8. Проверим конфигурацию маршрутизатора и настройки IP-адресации (Рис.13):

```
msk-user-gw-01# show running-config
```

```
msk-user-gw-01# show interface brief
```

9. Проверим подключение. Узел РС успешно отправляет эхо-запросы на адрес маршрутизатора 192.168.1.1 (Рис.14).

10. В окне Wireshark проанализируем полученную информацию (Рис.15).

11. Остановим захват пакетов в Wireshark. Остановим все устройства в проекте.

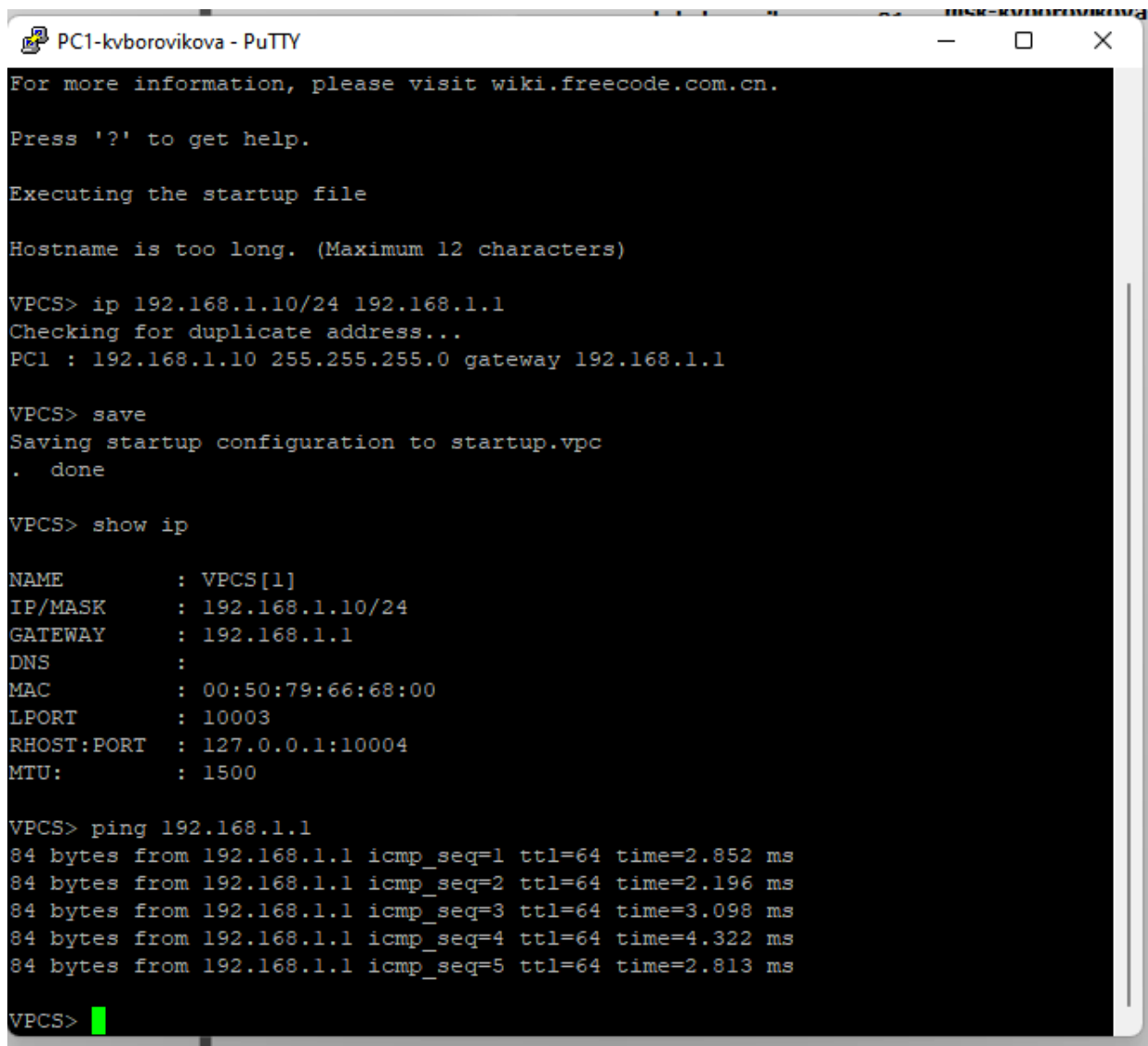
```
msk-kvborovikova-gw-01 - PuTTY
You may change this message by editing /etc/motd.

Hello, this is FRRouting (version 7.5.1).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

frr# configure terminal
frr(config)# hostname msk-kvborovikova-gw-01
msk-kvborovikova-gw-01(config)# exit
msk-kvborovikova-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-kvborovikova-gw-01# configure terminal
msk-kvborovikova-gw-01(config)# interface eth0
msk-kvborovikova-gw-01(config-if)# ip address 192.168.1.1/24
msk-kvborovikova-gw-01(config-if)# no shutdown
msk-kvborovikova-gw-01(config-if)# exit
msk-kvborovikova-gw-01(config)# exit
msk-kvborovikova-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-kvborovikova-gw-01# show running-config
Building configuration...

Current configuration:
!
frr version 7.5.1
frr defaults traditional
hostname frr
hostname msk-kvborovikova-gw-01
service integrated-vtysh-config
!
interface eth0
 ip address 192.168.1.1/24
!
line vty
!
end
msk-kvborovikova-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
msk-kvborovikova-gw-01#
```

Рисунок 13. Консоль маршрутизатора FRR



```
PC1-kvborovikova - PuTTY
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Hostname is too long. (Maximum 12 characters)

VPCS> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
PC1 : 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      : 10003
RHOST:PORT : 127.0.0.1:10004
MTU        : 1500

VPCS> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=2.852 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.196 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=3.098 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=4.322 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=2.813 ms

VPCS> 
```

Рисунок 14. Консоль PC1

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	::	ff02::2	ICMPv6	62	Router Solicitation
2	49.275261	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
3	50.284503	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
4	51.294990	Private_66:68:00	Broadcast	ARP	64	Gratuitous ARP for 192.168.1.10 (Request)
5	182.950986	::	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
6	183.051674	::	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
7	183.301284	::	ff02::1:ff02::0	ICMPv6	86	Neighbor Solicitation for fe80::e37:36ff:fed2::0
8	184.315553	fe80::e37:36ff:fed2::	ff02::16	ICMPv6	150	Multicast Listener Report Message v2
9	184.341551	fe80::e37:36ff:fed2::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
10	184.731074	fe80::e37:36ff:fed2::	ff02::16	ICMPv6	90	Multicast Listener Report Message v2
11	185.350930	fe80::e37:36ff:fed2::	ff02::16	ICMPv6	150	Multicast Listener Report Message v2
12	330.738922	Private_66:68:00	Broadcast	ARP	64	Who has 192.168.1.1? Tell 192.168.1.10
13	330.739937	0c:37:36:d2:00:00	Private_66:68:00	ARP	60	192.168.1.1 is at 0c:37:36:d2:00:00
14	330.752938	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xa97f, seq=1/256, ttl=64 (reply in 15)
15	330.754942	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xaa7f, seq=1/256, ttl=64 (request in 14)
16	331.783387	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xaa7f, seq=2/512, ttl=64 (reply in 17)
17	331.784388	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xab7f, seq=2/512, ttl=64 (request in 16)
18	332.801018	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xab7f, seq=3/768, ttl=64 (reply in 19)
19	332.803021	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xab7f, seq=3/768, ttl=64 (request in 18)
20	333.831135	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xac7f, seq=4/1024, ttl=64 (reply in 21)
21	333.834134	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xac7f, seq=4/1024, ttl=64 (request in 20)
22	334.847060	192.168.1.10	192.168.1.1	ICMP	98	Echo (ping) request id=0xad7f, seq=5/1280, ttl=64 (reply in 23)
23	334.849070	192.168.1.1	192.168.1.10	ICMP	98	Echo (ping) reply id=0xad7f, seq=5/1280, ttl=64 (request in 22)
24	335.831221	0c:37:36:d2:00:00	Private_66:68:00	ARP	60	Who has 192.168.1.10? Tell 192.168.1.1
25	335.831221	Private_66:68:00	0c:37:36:d2:00:00	ARP	60	192.168.1.10 is at 00:50:79:66:68:00

> Frame 1: 62 bytes on wire (496 bits), 62 bytes captured (496 bits) on interface -, id 0
 > Ethernet II, Src: Private_66:68:00 (00:50:79:66:68:00), Dst: IPv6mcast_02 (33:33:00:00:00:02)
 > Internet Protocol Version 6, Src: ::, Dst: ff02::2
 > Internet Control Message Protocol v6

0000 33 33 00 00 00 02 00 50 79 66 68 00 86 dd 60 00 33P yfh...
 wireshark_3G1SU1.pcapng

Пакеты: 25 · Показаны: 25 (100.0%)

Профиль: Default

Рисунок 15. Захваченный трафик в Wireshark

4. Моделирование простейшей сети на базе маршрутизатора VyOS в GNS3

1. Запустим GNS3 VM и GNS3. Создадим новый проект.
2. В рабочей области GNS3 разместим VPCS, коммутатор Ethernet и маршрутизатор VyOS (Рис. 16)

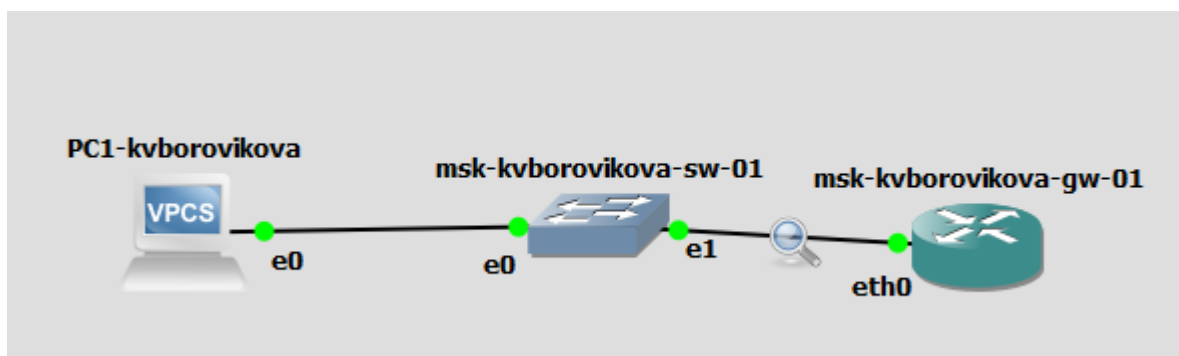


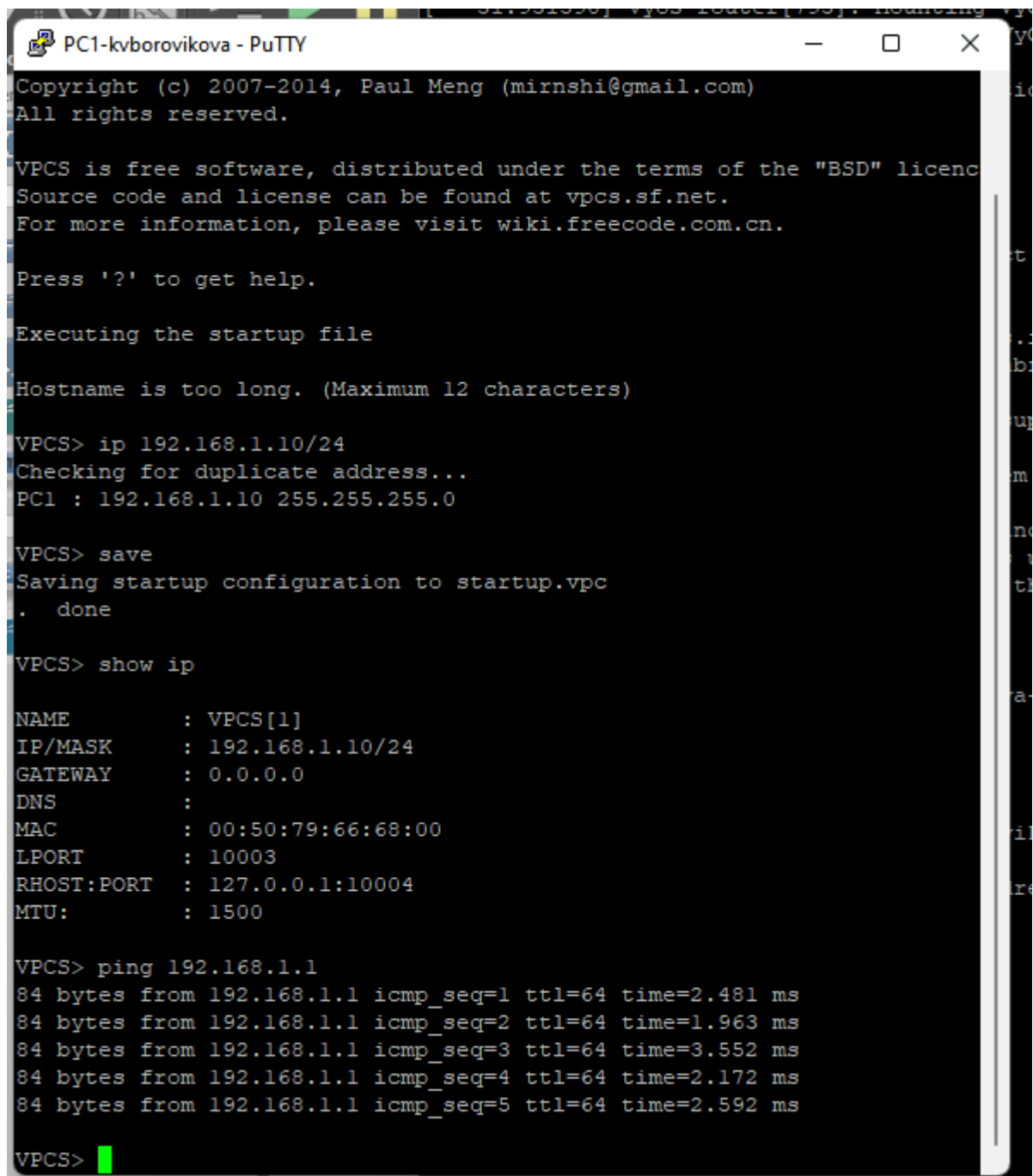
Рисунок 16. Топология сети

3. Изменим отображаемые названия устройств. Коммутатору присвоим название по принципу msk-user-sw-0x, маршрутизатору — по принципу mskuser-gw-0x, VPCS —

по принципу PCx-user, где вместо user укажем имя учётной записи, вместо x — порядковый номер устройства.

4. Включим захват трафика на соединении между коммутатором и маршрутизатором.
5. Запустим все устройства проекта. Откроем консоль всех устройств проекта.
6. Настроим IP-адресацию для интерфейса узла PC1 (Рис. 17):

```
ip 192.168.1.10/24 192.168.1.1
save
show ip
```



```
PC1-kvborovikova - PuTTY
Copyright (c) 2007-2014, Paul Meng (mirnshi@gmail.com)
All rights reserved.

VPCS is free software, distributed under the terms of the "BSD" licence
Source code and license can be found at vpcs.sf.net.
For more information, please visit wiki.freecode.com.cn.

Press '?' to get help.

Executing the startup file

Hostname is too long. (Maximum 12 characters)

VPCS> ip 192.168.1.10/24
Checking for duplicate address...
PC1 : 192.168.1.10 255.255.255.0

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

VPCS> show ip

NAME       : VPCS[1]
IP/MASK    : 192.168.1.10/24
GATEWAY    : 0.0.0.0
DNS        :
MAC        : 00:50:79:66:68:00
LPORT      : 10003
RHOST:PORT : 127.0.0.1:10004
MTU        : 1500

VPCS> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=2.481 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=1.963 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=3.552 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=2.172 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=2.592 ms

VPCS>
```

Рисунок 17. Консоль PC1

7. Настройте маршрутизатор VyOS (Рис.18):

- После загрузки введем логин vyos и пароль vyos:

```
vyos login: vyos
```

```
Password:
```

В рабочем режиме в командной строке отображается символ \$.

- Установим систему на диск:

```
vyos@vyos:~$ install image
```

Далее ответим на вопросы диалога установки, в котором в большинстве пунктов можно соглашаться с предлагаемыми по умолчанию значениями, нажимая Enter . По завершении диалога перезапустим маршрутизатор, введя команду reboot.

- Перейдем в режим конфигурирования:

```
vyos@vyos$ configure
```

```
vyos@vyos#
```

- Изменим имя устройства (вместо user укажем свою учётную запись):

```
vyos@vyos#set system host-name msk-user-gw-01
```

Изменения в имени устройства вступят в силу после применения и сохранения конфигурации и перезапуска устройства.

- Зададим IP-адрес на интерфейсе eth0:

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

- Посмотрим внесённые в конфигурацию изменения:

```
vyos@vyos# compare
```

- Применим изменения в конфигурации и сохраним саму конфигурацию:

```
vyos@vyos# commit
```

```
vyos@vyos# save
```

- Посмотрим информацию об интерфейсах маршрутизатора:

```
vyos@vyos# show interfaces
```

- Выйдете из режима конфигурирования:

```
vyos@vyos# exit
```

```
vyos@vyos$
```

```
msk-kvborovikova-gw-01 - PuTTY
[ 30.943635] vyos-router[793]: Started watchfrr.
[ 31.931590] vyos-router[793]: Mounting VyOS Config...done.
[ 38.463007] vyos-router[793]: Starting VyOS router: migrate rl-system firewall
1 configure.
[ 39.344423] vyos-config[823]: Configuration success

Welcome to VyOS - vyos ttyS0

vyos login: vyos
Password:
Linux vyos 5.4.156-amd64-vyos #1 SMP Thu Oct 28 18:19:14 UTC 2021 x86_64
Welcome to VyOS!

Check out project news at https://blog.vyos.io
and feel free to report bugs at https://phabricator.vyos.net

Visit https://support.vyos.io to create a support ticket.

You can change this banner using "set system login banner post-login" command.

VyOS is a free software distribution that includes multiple components,
you can check individual component licenses under /usr/share/doc/*/copyright
Use of this pre-built image is governed by the EULA you can find at
/usr/share/vyos/EULA
vyos@vyos:~$ configure
[edit]
vyos@vyos# system host-name msk-kvborovikova-gw-01

Invalid command: [system]

[edit]
vyos@vyos# set system host-name msk-kvborovikova-gw-01
[edit]
vyos@vyos# set interfaces ethernet eth0 address 192.168.1.1/24
[edit]
vyos@vyos# compare
[edit interfaces ethernet eth0]
+address 192.168.1.1/24
[edit system]
>host-name msk-kvborovikova-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:b4:d3:09:00:00
  }
  ethernet eth1 {
    hw-id 0c:b4:d3:09:00:01
  }
  ethernet eth2 {
    hw-id 0c:b4:d3:09:00:02
  }
  loopback lo {
  }
[edit]
vyos@vyos# exit
exit
vyos@vyos:~$
```

Рисунок 18. Консоль маршрутизатора VyOS

8. Проверим подключение. Узел успешно отправляет эхо-запросы на адрес маршрутизатора 192.168.1.1 (Рис.17).

9. В окне Wireshark проанализируем полученную информацию (Рис.19). Видим запросы ARP и ICMP. ICMP запросы – эхо, которые мы отправляли с PC1 на PC2 и обратно, ARP запросы – запросы MAC адресов, то есть поиск устройств в сети.

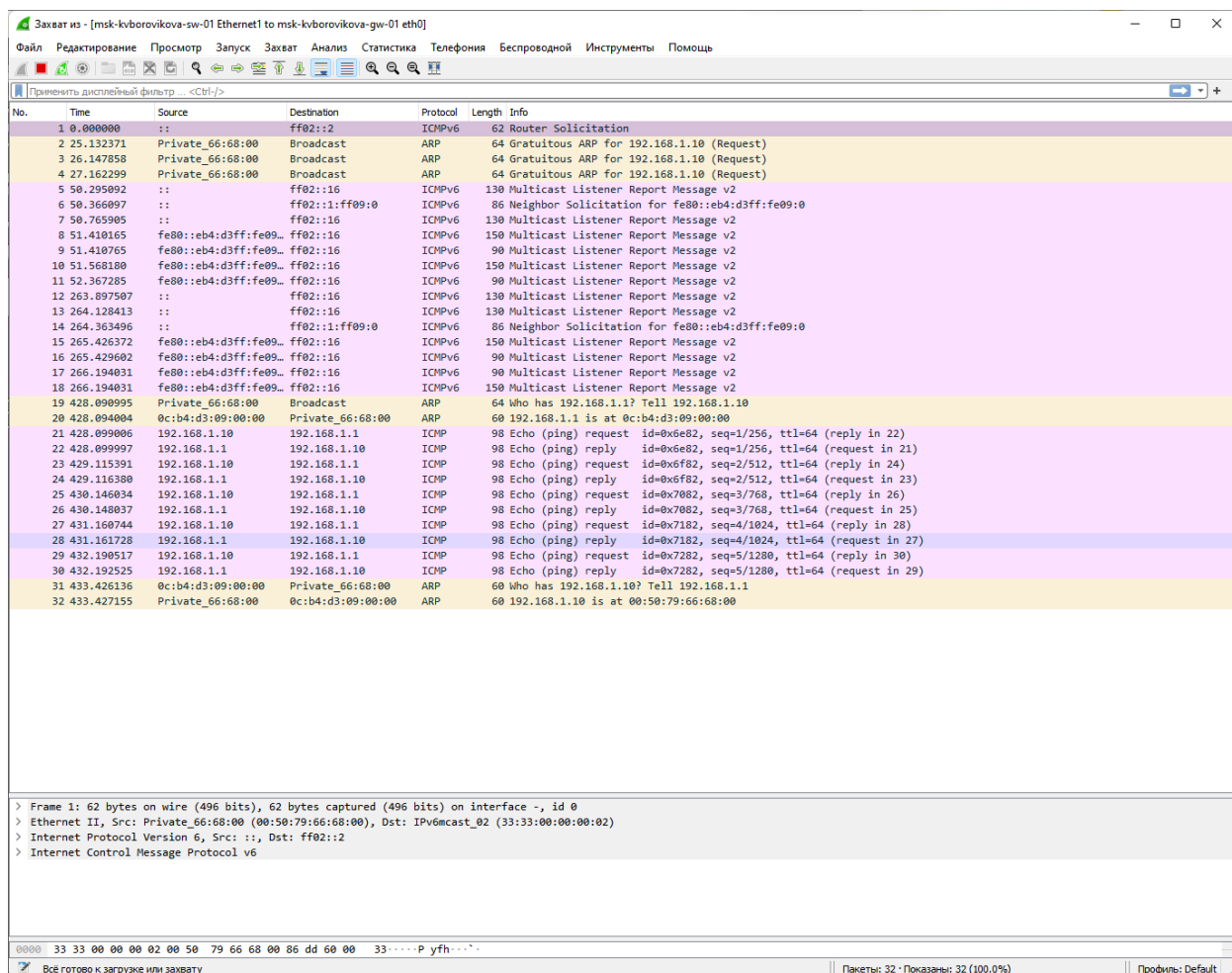


Рисунок 19. Захваченный трафик в Wireshark

10. Остановим захват пакетов в Wireshark. Остановим все устройства в проекте. Завершим работу с GNS3.

Вывод

В ходе выполнения лабораторной работы я построила простейшую модель сети на базе коммутатора и маршрутизаторов FRR и VyOS, а также проанализировала трафик посредством VyOS