

Содержание

0.1	Title	3
0.2	Generic options	3
0.3	Pdf output format	3
1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
3.1	Моделирование простейшей сети на базе коммутатора в GNS3	6
3.2	Анализ трафика в GNS3 посредством Wireshark	8
3.3	Моделирование простейшей сети на базе маршрутизатора FRR в GNS3	13

Список иллюстраций

3.1	Топология простейшей сети в GNS3	6
3.2	Просмотр синтаксиса возможных для ввода команд VPCS в GNS3	6
3.3	Задание IP-адреса и сохранение конфигурации VPCS в GNS3	7
3.4	Задание IP-адреса и сохранение конфигурации VPCS в GNS3	7
3.5	Эхо-запросы	8
3.6	Запуск анализатора трафика на соединении	8
3.7	Анализ трафика в Wireshark	9
3.8	Информация по опциям команды ping	9
3.9	Эхо-запрос в ICMP-mode к узлу PC-1	10
3.10	Анализ трафика в Wireshark	10
3.11	Эхо-запрос в UDP-mode к узлу PC-1	11
3.12	Анализ трафика в Wireshark	11
3.13	Эхо-запрос в TCP-mode к узлу PC-1	12
3.14	Анализ трафика в Wireshark	12
3.15	Топология простейшей сети с маршрутизатором в GNS3	13
3.16	Настройка IP-адресации	13
3.17	Ошибка1 Невозможно использование KVM	14
3.18	Ошибка2 Невозможно использование KVM	14

Список таблиц

0.1 Title

title: «Отчёт по лабораторной работе №5» subtitle: «Сетевые технологии» license: «CC BY»

0.2 Generic options

lang: ru-RU toc-title: «Содержание»

0.3 Pdf output format

toc: true # Table of contents toc-depth: 2 lof: true # List of figures lot: true # List of tables
fontsize: 12pt linespread: 1.5 papersize: a4 documentclass: scrreprt ## I18n polyglossia
polyglossia-lang: name: russian polyglossia-otherlangs: name: english ## I18n babel babel-
lang: russian babel-otherlangs: english —

1 Цель работы

Цель данной работы – построение простейших моделей сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, анализ трафика посредством Wireshark.

2 Задание

1. Построить в GNS3 топологию сети, состоящей из коммутатора Ethernet и двух оконечных устройств (персональных компьютеров).
2. Задать оконечным устройствам IP-адреса в сети 192.168.1.0/24. Проверить связь.
3. С помощью Wireshark захватить и проанализировать ARP-сообщения.
4. С помощью Wireshark захватить и проанализировать ICMP-сообщения.
5. Построить в GNS3 топологию сети, состоящей из маршрутизатора FRR, коммутатора Ethernet и оконечного устройства.
6. Задать оконечному устройству IP-адрес в сети 192.168.1.0/24.
7. Присвоить интерфейсу маршрутизатора адрес 192.168.1.1/24
8. Проверить связь.
9. Построить в GNS3 топологию сети, состоящей из маршрутизатора VyOS, коммутатора Ethernet и оконечного устройства.
10. Задать оконечному устройству IP-адрес в сети 192.168.1.0/24.
11. Присвоить интерфейсу маршрутизатора адрес 192.168.1.1/24
12. Проверить связь.

3 Выполнение лабораторной работы

3.1 Моделирование простейшей сети на базе коммутатора в GNS3

Запускаю GNS3 VM и GNS3 и создаю новый проект. В рабочей области GNS3 размещаю коммутатор Ethernet и два VPCS. Переименовываю их согласно заданию (рис. 3.1).



Рисунок 3.1: Топология простейшей сети в GNS3

Захожу к консоли Putty и просматриваю синтаксис возможных для ввода команд VPCS в GNS3 (рис. 3.2).

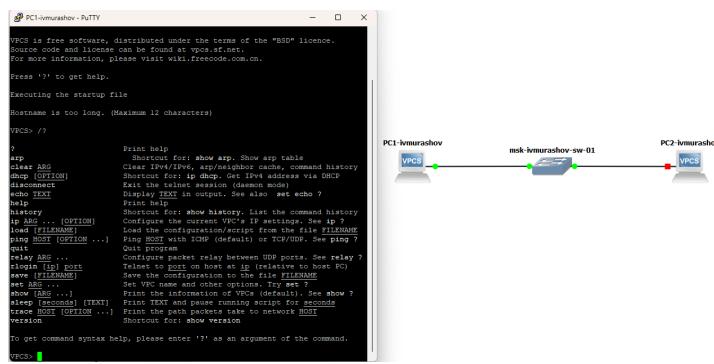
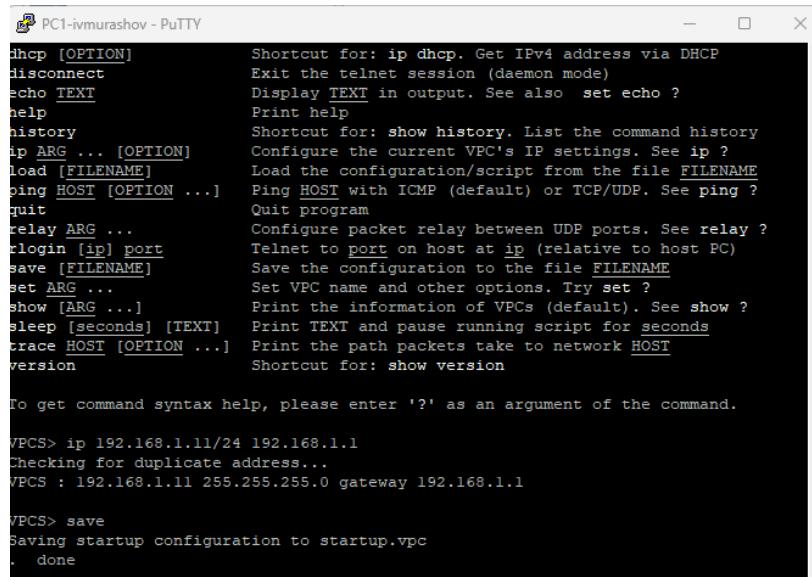


Рисунок 3.2: Просмотр синтаксиса возможных для ввода команд VPCS в GNS3

Задаю IP-адрес 192.168.1.11 в сети 192.168.1.0/24 для PC-1 (рис. 3.3).



```
PC1-ivmurashov - PuTTY

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 ...
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

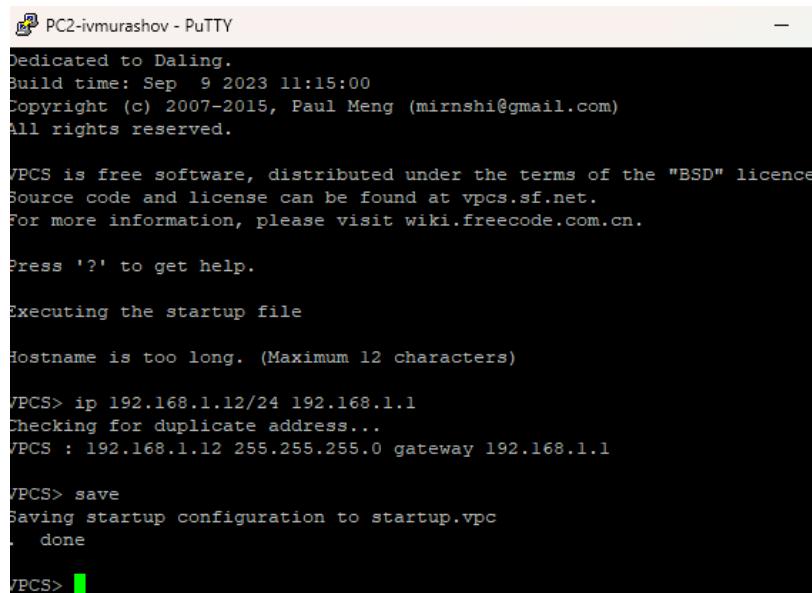
To get command syntax help, please enter '?' as an argument of the command.

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

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

Рисунок 3.3: Задание IP-адреса и сохранение конфигурации VPCS в GNS3

Аналогичным образом задаю IP-адрес 192.168.1.12 для PC-2 (рис. 3.4).



```
PC2-ivmurashov - PuTTY

Dedicated to Daling.
Build time: Sep 9 2023 11:15:00
Copyright (c) 2007-2015, 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...
VPCS : 192.168.1.12 255.255.255.0 gateway 192.168.1.1

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

VPCS> █
```

Рисунок 3.4: Задание IP-адреса и сохранение конфигурации VPCS в GNS3

Проверяю работоспособность соединения между PC-1 и PC-2 с помощью команды ping (рис. 3.5).

```

PC1-ivmurashev - PuTTY
show [And ...] Print the information of VPCs (default). See show ?
[seconds] [TEXT] Print the output of running scripts for seconds
trace [FILE] [OPTION ...] Print the path packets take to network [PORT]
version Shortcut for: show version

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

VPCS> ip 192.168.1.1/24 192.168.1.1
Checking for duplicate address...
VPCS : 192.168.1.1.255.255.0 gateway 192.168.1.1

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

VPCS> ping 192.168.1.12
64 bytes from 192.168.1.12 icmp_seq=1 ttl=64 time=0.007 ms
64 bytes from 192.168.1.12 icmp_seq=2 ttl=64 time=0.461 ms
64 bytes from 192.168.1.12 icmp_seq=3 ttl=64 time=0.390 ms
64 bytes from 192.168.1.12 icmp_seq=4 ttl=64 time=0.449 ms
64 bytes from 192.168.1.12 icmp_seq=5 ttl=64 time=0.529 ms
64 bytes from 192.168.1.12 icmp_seq=6 ttl=64 time=0.524 ms
VPCS> []

PC2-ivmurashev - PuTTY
Press '?' to get help.
Executing the startup file
Hostname is too long. (Maximum 12 characters)
VPCS> ip 192.168.1.1/24 192.168.1.1
Checking for duplicate address...
VPCS : 192.168.1.1.255.255.0 gateway 192.168.1.1

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

VPCS> ping 192.168.1.11
64 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=0.430 ms
64 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=0.515 ms
64 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=0.393 ms
64 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=0.406 ms
64 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=0.524 ms
VPCS> []

```

Рисунок 3.5: Эхо-запросы

3.2 Анализ трафика в GNS3 посредством Wireshark

Запускаю на соединении между PC-1 и коммутатором анализатор трафика (рис. 3.6).



Рисунок 3.6: Запуск анализатора трафика на соединении

В проекте GNS3 стартаю все узлы, в окне Wireshark отображается информация по протоколу ARP. В поле физического уровня отображается длина кадра (64 бита). В поле канального уровня можем посмотреть mac-адреса источника и получателя. По нулевому и первому битам можем определить тип mac-адресов (получатель – локально администрируемый и широковещательный; источник - глобально администрируемый и одиночный) (рис. 3.7).

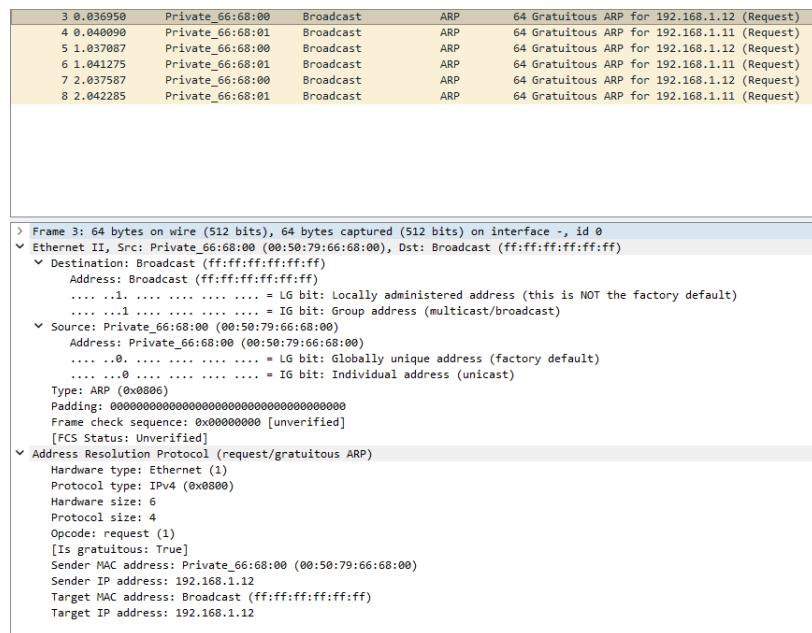


Рисунок 3.7: Анализ трафика в Wireshark

В терминале PC-2 просматриваю информацию по опциям команды ping, введя ping ? (рис. 3.8).

```
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.
```

Рисунок 3.8: Информация по опциям команды ping

Затем делаю эхо-запрос в ICMP-моде к узлу PC-1 (рис. 3.9).

```

PC2-ivmurashev - PuTTY

VPCS> ping -l 192.168.1.11
Cannot resolve -l

VPCS> ping 192.168.1.11 -l

84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=0.950 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=0.748 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=2.182 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=0.582 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=0.331 ms

```

Рисунок 3.9: Эхо-запрос в ICMP-моде к узлу PC-1

В окне Wireshark видим, что в поле сетевого уровня отображается протокол ICMP и IP-адреса отправителя и получателя (рис. 3.10).

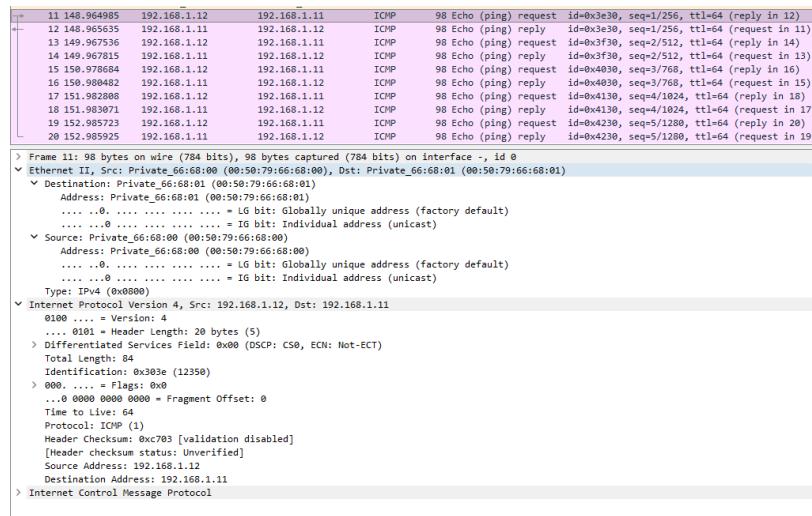


Рисунок 3.10: Анализ трафика в Wireshark

Затем делаю эхо-запрос в UDP-моде к узлу PC-1 (рис. 3.11).

```

PC2-ivmurashov - PuTTY
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=2.182 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=0.582 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=0.331 ms

VPCS> ping 192.168.1.11 -2

84 bytes from 192.168.1.11 udp_seq=1 ttl=64 time=1.458 ms
84 bytes from 192.168.1.11 udp_seq=2 ttl=64 time=0.653 ms
84 bytes from 192.168.1.11 udp_seq=3 ttl=64 time=0.695 ms
84 bytes from 192.168.1.11 udp_seq=4 ttl=64 time=0.772 ms
84 bytes from 192.168.1.11 udp_seq=5 ttl=64 time=0.552 ms

```

Рисунок 3.11: Эхо-запрос в UDP-моде к узлу PC-1

В окне Wireshark видим, что в поле сетевого уровня отображается протокол UDP и IP-адреса отправителя и получателя. В поле канального уровня по нулевому и первому битам можем определить тип mac-адресов: получатель и источник - глобально администрируемые и одиночные, так как биты равны 0 (рис. 3.12).

Frame	Source IP	Destination IP	Type	Description
21	247.257558	192.168.1.12	ECHO	98 Request
22	247.258568	192.168.1.11	ECHO	98 Response
23	248.260121	192.168.1.12	ECHO	98 Request
24	248.260550	192.168.1.11	ECHO	98 Response
25	249.263788	192.168.1.12	ECHO	98 Request
26	249.264151	192.168.1.11	ECHO	98 Response
27	250.267635	192.168.1.12	ECHO	98 Request
28	250.268124	192.168.1.11	ECHO	98 Response
29	251.270077	192.168.1.12	ECHO	98 Request
30	251.270343	192.168.1.11	ECHO	98 Response

> Frame 21: 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)
 Address: Private_66:68:01 (00:50:79:66:68:01)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 ▼ Source: Private_66:68:00 (00:50:79:66:68:00)
 Address: Private_66:68:00 (00:50:79:66:68:00)
 0. = LG bit: Globally unique address (factory default)
 0. = IG bit: Individual address (unicast)
 Type: IPv4 (0x0800)
 ▼ Internet Protocol Version 4, Src: 192.168.1.12, Dst: 192.168.1.11
 0100 = Version: 4
 0101 = Header Length: 20 bytes (5)
 > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 Total Length: 84
 Identification: 0x30a1 (12449)
 > 000. = Flags: 0x0
 0 0000 0000 0000 = Fragment Offset: 0
 Time to Live: 64
 Protocol: UDP (17)
 Header Checksum: 0xc690 [validation disabled]
 [Header checksum status: Unverified]
 Source Address: 192.168.1.12
 Destination Address: 192.168.1.11
 > User Datagram Protocol, Src Port: 3267, Dst Port: 7
 > Echo

Рисунок 3.12: Анализ трафика в Wireshark

Затем делаю эхо-запрос в TCP-моде к узлу PC-1 (рис. 3.13).

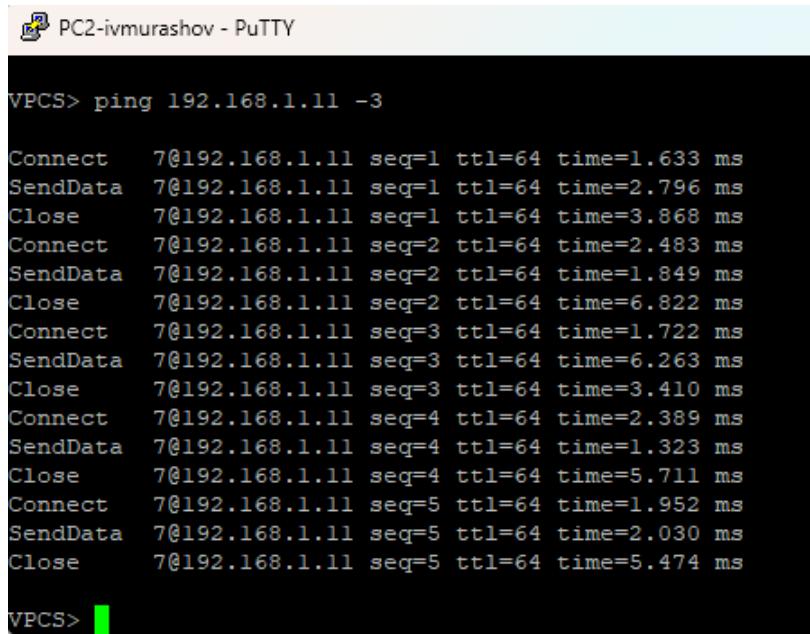


Рисунок 3.13: Эхо-запрос в TCP-моде к узлу PC-1

В окне Wireshark видим, что в поле сетевого уровня отображается протокол TCP и IP-адреса отправителя и получателя. В поле канального уровня по нулевому и первому битам можем определить тип мас-адресов: получатель и источник - глобально администрируемые и одиночные, так как биты равны 0 (рис. 3.14).

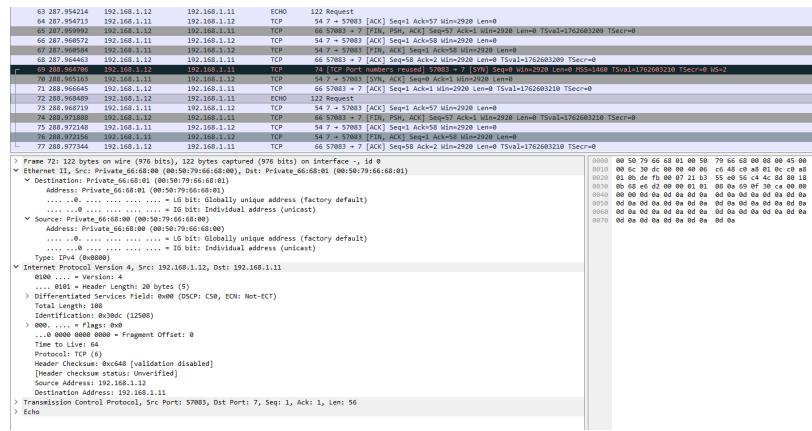


Рисунок 3.14: Анализ трафика в Wireshark

3.3 Моделирование простейшей сети на базе маршрутизатора FRR в GNS3

В рабочей области GNS3 размещаю VPCS, коммутатор Ethernet и маршрутизатор FRR и изменю отображаемые названия устройств (рис. 3.15).

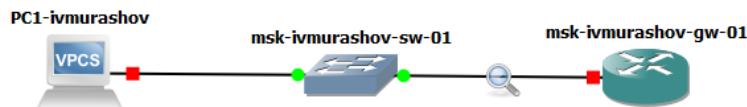


Рисунок 3.15: Топология простейшей сети с маршрутизатором в GNS3

В консоли PC-1 настраиваю IP-адресацию (рис. 3.16).

```
PC1-ivmurashov - 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>
```

Рисунок 3.16: Настройка IP-адресации

Но при попытке запуска получаю сообщение об ошибке и недоступности KVM виртуализации (рис. 3.17, рис. 3.18)

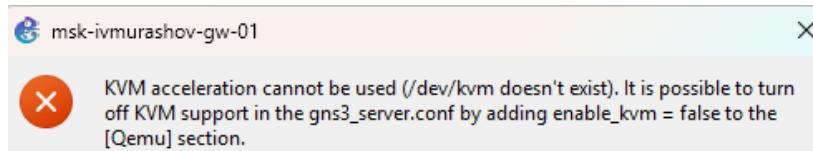


Рисунок 3.17: Ошибка1 | Невозможно использование KVM

```
GNS3 management console.  
Running GNS3 version 2.2.52 on Windows (64-bit) with Python 3.10.11 Qt 5.15.2 and PyQt 5.15.11.  
Copyright (c) 2006-2025 GNS3 Technologies.  
Use Help -> GNS3 Doctor to detect common issues.  
>>> Timeout after 5 seconds for request http://admin@192.168.56.1:3080/v2/version. Please check the connection is not blocked by a firewall or an anti-virus.  
>>> Timeout after 5 seconds for request http://admin@192.168.56.1:3080/v2/version. Please check the connection is not blocked by a firewall or an anti-virus.  
>>> Timeout after 5 seconds for request http://admin@192.168.56.1:3080/v2/version. Please check the connection is not blocked by a firewall or an anti-virus.  
KVM acceleration cannot be used (/dev/kvm doesn't exist). It is possible to turn off KVM support in the gns3_server.conf by adding enable_kvm = false to the [Qemu] section.  
error while starting msk-ivmurashov-gw-01: KVM acceleration cannot be used (/dev/kvm doesn't exist). It is possible to turn off KVM support in the gns3_server.conf by adding enable_kvm = false to the [Qemu] section.  
KVM acceleration cannot be used (/dev/kvm doesn't exist). It is possible to turn off KVM support in the gns3_server.conf by adding enable_kvm = false to the [Qemu] section.
```

Рисунок 3.18: Ошибка2 | Невозможно использование KVM

Как бы я не пытался исправить эту ошибку, ничего не вышло (даже переустановливал GNS3). В связи с чем, к сожалению, не имею возможности довести до конца выполнение данной лабораторной работы.