

Лабораторная работа №5

Простые сети в GNS3. Анализ трафика

Спелов Андрей Николаевич

Содержание

1	Цель работы	6
2	Выполнение лабораторной работы	7
3	Выводы	23
	Список литературы	24

Список иллюстраций

2.1	Создание нового проекта в GNS3.	7
2.2	Размещение коммутатора Ethernet и двух VPCS. Изменение названия устройства. Присвоение коммутатору названия. Соединение VPCS с коммутатором. Отображение обозначения интерфейсов соединения.	7
2.3	Просмотр синтаксиса возможных для ввода команд.	8
2.4	Задание IP-адреса и сохранение конфигурации VPCS в GNS3 для PC-1-anspelov.	8
2.5	Задание IP-адреса и сохранение конфигурации VPCS в GNS3 для PC-2-anspelov.	9
2.6	Проверка работоспособности соединения между PC-1 и PC-2. . . .	9
2.7	Остановка в проекте всех узлов.	9
2.8	Запуск на соединении между PC-1-anspelov и коммутатором анализатор трафика.	10
2.9	Отображение информация по протоколу ARP в окне Wireshark. . .	10
2.10	Просмотр информации по опциям команды ping. Отправка одного эхо-запроса в ICMP-моду к узлу PC-1-anspelov.	11
2.11	Просмотр полученной информации в окне Wireshark.	11
2.12	Отправка одного эхо-запроса в UDP-моду к узлу PC-1-anspelov. . .	11
2.13	Просмотр полученной информации в окне Wireshark.	12
2.14	Отправка одного эхо-запроса в TCP-моду к узлу PC-1-anspelov. . .	12
2.15	Просмотр полученной информации в окне Wireshark.	12
2.16	Остановка захвата пакетов в Wireshark.	12
2.17	Создание нового проекта в GNS3.	13
2.18	Размещение VPCS, коммутатора Ethernet и маршрутизатора FRR. Изменение отображаемых названий устройств.	13
2.19	Включение захвата трафика на соединении между коммутатором и маршрутизатором.	14
2.20	Открытие консоли всех устройств проекта.	14
2.21	Настройка IP-адресации для интерфейса узла PC-1-anspelov. . . .	15
2.22	Настроим IP-адресацию для интерфейса локальной сети маршрутизатора и проверим конфигурацию маршрутизатора и настройки IP-адресации	16
2.23	Проверка подключения.	17
2.24	Получение информации в окне Wireshark.	17
2.25	Остановка захвата пакетов в Wireshark.	17
2.26	Создание нового проекта в GNS3.	18

2.27	Размещение VPCS, коммутатора Ethernet и маршрутизатора VyOS. Изменение отображаемых названий устройств.	18
2.28	Включение захвата трафика на соединении между коммутатором и маршрутизатором.	18
2.29	Открытие консолей всех устройств проекта.	19
2.30	Настройка IP-адресации для интерфейса узла PC-1-anspelov. . . .	19
2.31	Ввод логина и пароля. Отображение рабочего режима.	20
2.32	Установка системы на диск. Она уже установлена.	20
2.33	Переход в режим конфигурирования. Изменение имени устрой- ства. Настройка IP-адреса на интерфейсе eth0. Просмотр внесённых в конфигурацию изменений. Применение изменений в конфигурации и сохранение самой конфигурации.	21
2.34	Просмотр информации об интерфейсах маршрутизатора. Выход из режима конфигурирования.	21
2.35	Проверка подключения.	22
2.36	Получение информации в окне Wireshark.	22
2.37	Завершение работы с GNS3.	22

Список таблиц

1 Цель работы

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

2 Выполнение лабораторной работы

Запустим GNS3 VM и GNS3 и создадим новый проект(рис. 2.1).

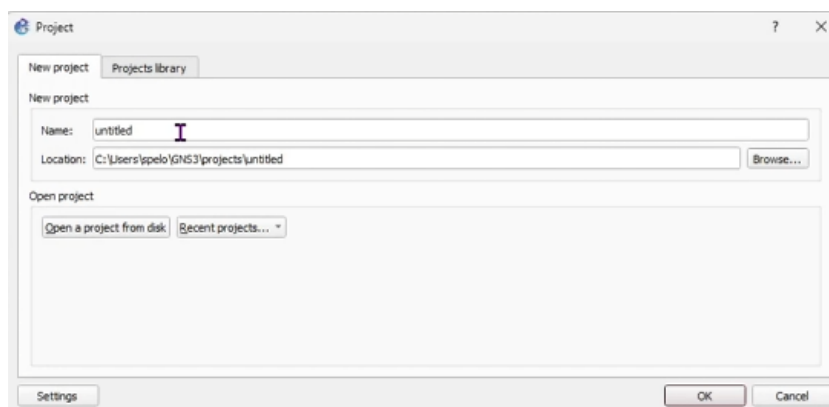


Рис. 2.1: Создание нового проекта в GNS3.

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 нашей учётной записи. Коммутатору присвоим название msk-anspelov-sw-01. Соединим VPCS с коммутатором. Отобразим обозначение интерфейсов соединения (рис. 2.2).



Рис. 2.2: Размещение коммутатора Ethernet и двух VPCS. Изменение названия устройства. Присвоение коммутатору названия. Соединение VPCS с коммутатором. Отображение обозначения интерфейсов соединения.

Зададим IP-адреса VPCS. Для этого с помощью меню, вызываемого правой кнопкой мыши, запустим Start, PC-1-anspelov, затем вызовем его терминал Console. Для просмотра синтаксиса возможных для ввода команд наберем /? (рис. 2.3).

```
PC1-anspelov> /?

?                               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.
```

Рис. 2.3: Просмотр синтаксиса возможных для ввода команд.

Для задания IP-адреса 192.168.1.11 в сети 192.168.1.0/24 введём: ip 192.168.1.11/24 192.168.1.1. Здесь 192.168.1.1 — адрес шлюза. Для сохранения конфигурации введём команду save(рис. 2.4).

```
PC1-anspelov> 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-anspelov> save
Saving startup configuration to startup.vpc
. done

PC1-anspelov> █
```

Рис. 2.4: Задание IP-адреса и сохранение конфигурации VPCS в GNS3 для PC-1-anspelov.

Аналогичным образом зададим IP-адрес 192.168.1.12 для PC-2 (рис. 2.5).


```

PC2-anspelov> 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

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

PC2-anspelov>

```

Рис. 2.5: Задание IP-адреса и сохранение конфигурации VPCS в GNS3 для PC-2-anspelov.

Проверим работоспособность соединения между PC-1 и PC-2 с помощью команды ping (рис. 2.6).

```

PC2-anspelov> ping 192.168.1.11
84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=0.914 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=0.968 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=0.925 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=1.447 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=1.327 ms

PC2-anspelov> ping 192.168.1.12
192.168.1.12 icmp_seq=1 ttl=64 time=0.001 ms
192.168.1.12 icmp_seq=2 ttl=64 time=0.001 ms
192.168.1.12 icmp_seq=3 ttl=64 time=0.001 ms
192.168.1.12 icmp_seq=4 ttl=64 time=0.001 ms
192.168.1.12 icmp_seq=5 ttl=64 time=0.001 ms

PC2-anspelov>

```

Рис. 2.6: Проверка работоспособности соединения между PC-1 и PC-2.

Остановим в проекте все узлы (меню GNS3, Control, Stop all nodes) (рис. 2.7).

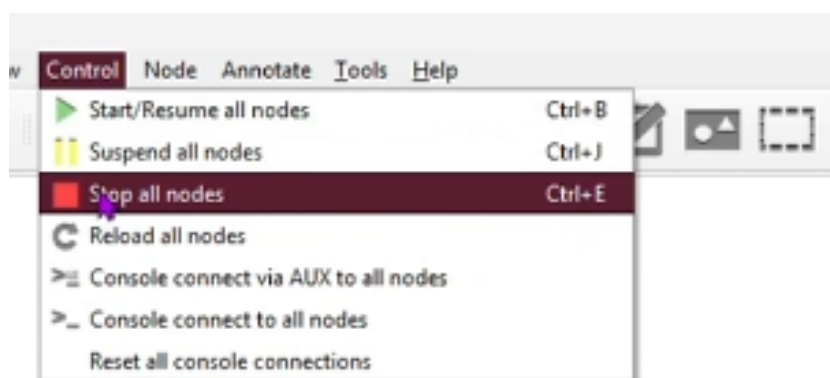


Рис. 2.7: Остановка в проекте всех узлов.

Запустим на соединении между PC-1-anspelov 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 появился значок лупы(рис. 2.8).



Рис. 2.8: Запуск на соединении между PC-1-anspelov и коммутатором анализатор трафика.

В проекте GNS3 стартуем все узлы (меню GNS3, Control, Start/Resume all nodes). В окне Wireshark отобразилась информация по протоколу ARP (рис. 2.9).

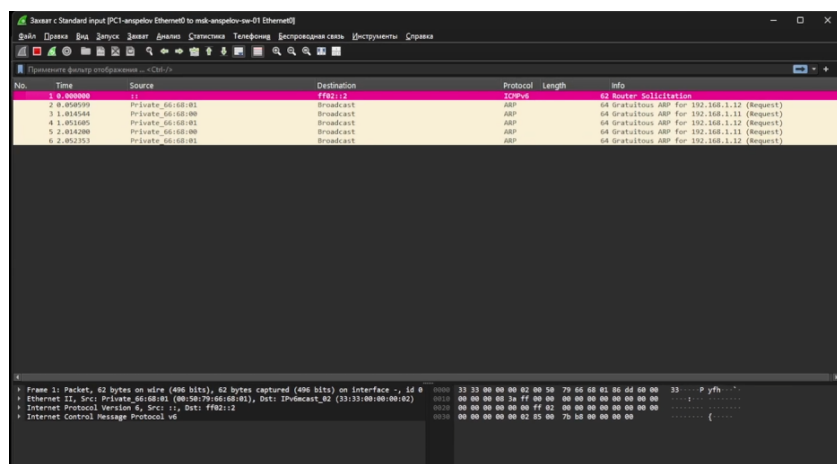


Рис. 2.9: Отображение информация по протоколу ARP в окне Wireshark.

В терминале PC-2-anspelov посмотрим информацию по опциям команды ping, введя ping /?. Затем сделаем один эхо-запрос в ICMP-моду к узлу PC-1-anspelov.

(рис. 2.10).

```
PC2-anspelov> ping /?

ping HOST [OPTION ...]
  Ping the network HOST. HOST can be an ip address or name
  Options:
    -l          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-anspelov> ping 192.168.1.11 -l -c 1
64 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=1.161 ms

PC2-anspelov>
```

Рис. 2.10: Просмотр информации по опциям команды ping. Отправка одного эхо-запроса в ICMP-моду к узлу PC-1-anspelov.

В окне Wireshark можем посмотреть полученную информацию(рис. 2.11).

8 182.875339	Private_66:66:00	Private_66:66:01	ARP	64 192.168.1.11 is at 00:50:79:66:66:00
9 182.875843	192.168.1.12	192.168.1.11	ICMP	96 Echo (ping) request id=0x017, seq=1/256, ttl=64 (req-)
10 182.876352	192.168.1.11	192.168.1.12	ICMP	96 Echo (ping) reply id=0x017, seq=1/256, ttl=64 (rep-)

Рис. 2.11: Просмотр полученной информации в окне Wireshark.

Теперь сделаем один эхо-запрос в UDP-моду к узлу PC-1-anspelov(рис. 2.12).

```
PC2-anspelov> ping 192.168.1.11 -2 -c 1
64 bytes from 192.168.1.11 udp_seq=1 ttl=64 time=0.996 ms

PC2-anspelov>
```

Рис. 2.12: Отправка одного эхо-запроса в UDP-моду к узлу PC-1-anspelov.

В окне Wireshark получили новую информацию (рис. 2.13).

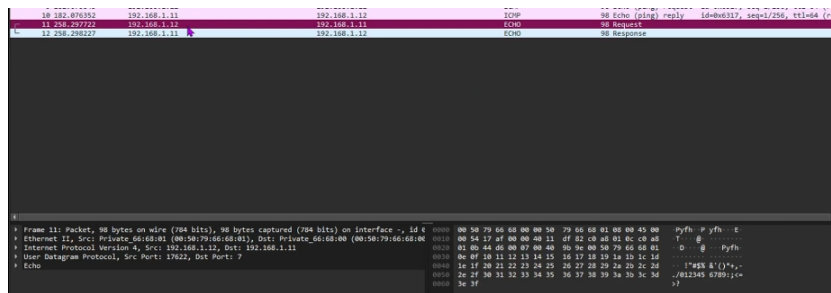


Рис. 2.13: Просмотр полученной информации в окне Wireshark.

Сделаем один эхо-запрос в TCP-море к узлу PC-1-anspелov(рис. 2.14).

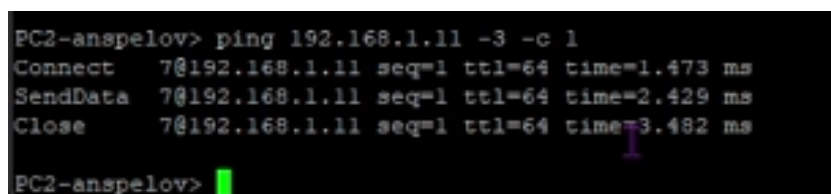


Рис. 2.14: Отправка одного эхо-запроса в TCP-море к узлу PC-1-anspелov.

В окне Wireshark получили новую информацию(рис. 2.15).

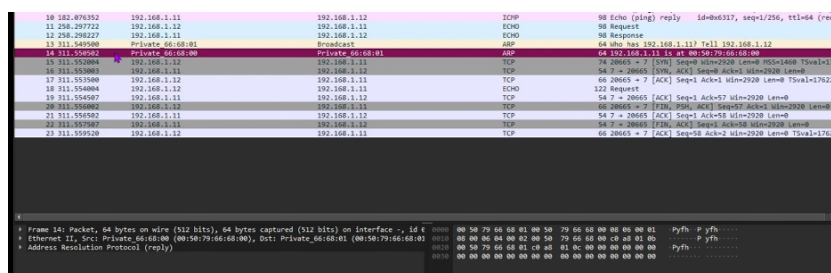


Рис. 2.15: Просмотр полученной информации в окне Wireshark.

Остановим захват пакетов в Wireshark(рис. 2.16).

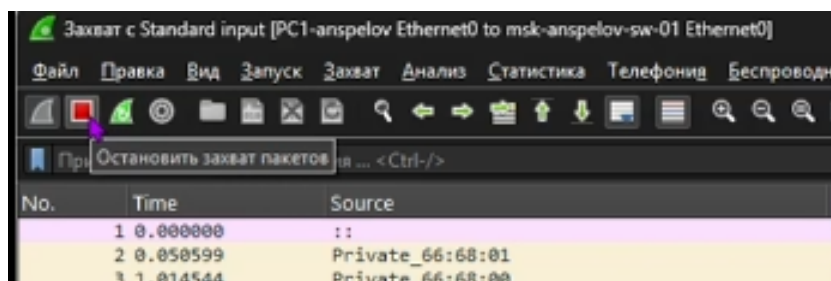


Рис. 2.16: Остановка захвата пакетов в Wireshark.

Создадим новый проект в GNS3(рис. 2.17).

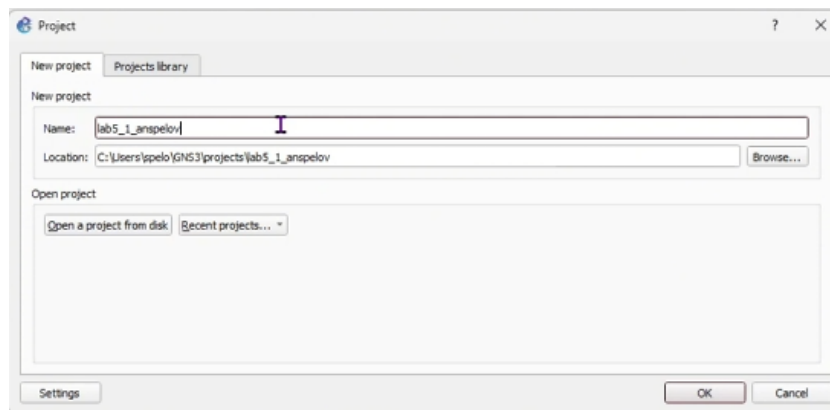


Рис. 2.17: Создание нового проекта в GNS3.

В рабочей области GNS3 разместим VPCS, коммутатор Ethernet и маршрутизатор FRR. Изменим отображаемые названия устройств. Коммутатору присвоим название `msk-anspelov-sw-01`, маршрутизатору — `msk-anspelov-gw-01`, VPCS — `PC1-anspelov` (рис. 2.18).

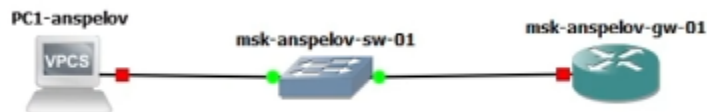


Рис. 2.18: Размещение VPCS, коммутатора Ethernet и маршрутизатора FRR. Изменение отображаемых названий устройств.

Включим захват трафика на соединении между коммутатором и маршрутизатором(рис. 2.19).

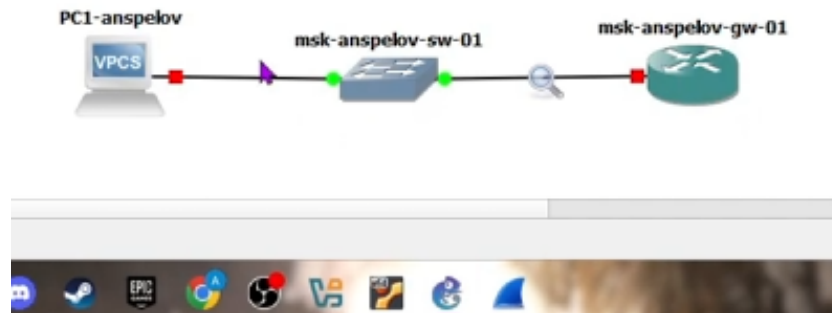


Рис. 2.19: Включение захвата трафика на соединении между коммутатором и маршрутизатором.

Запустим все устройства проекта и откроем консоль всех устройств проекта(рис. 2.20).

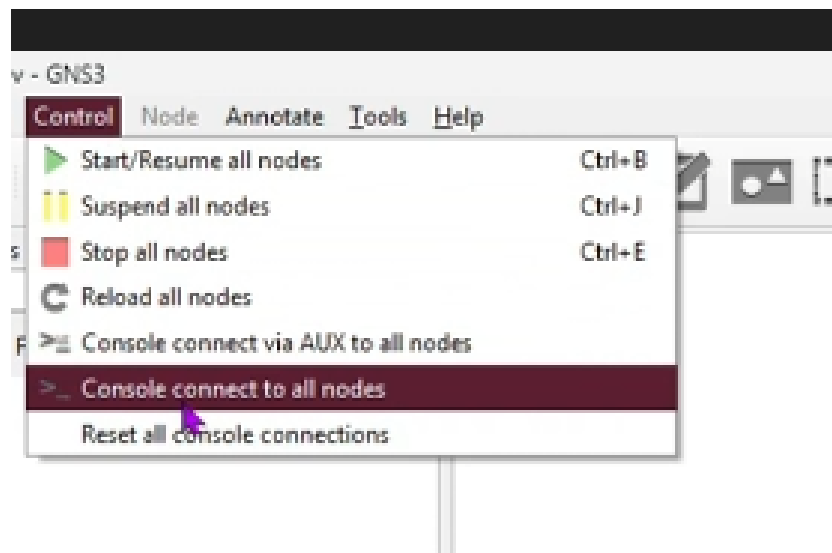


Рис. 2.20: Открытие консоли всех устройств проекта.

Настроим IP-адресацию для интерфейса узла PC-1-anspelov(рис. 2.21).

```

PC1-anspelov> 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

PC1-anspelov> save
Saving startup configuration to startup.vpc
. done

PC1-anspelov> show ip

NAME       : PC1-anspelov[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

PC1-anspelov>

```

Рис. 2.21: Настройка IP-адресации для интерфейса узла PC-1-anspelov.

Настроим IP-адресацию для интерфейса локальной сети маршрутизатора и проверим конфигурацию маршрутизатора и настройки IP-адресации(рис. 2.22).

```

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

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

```

Рис. 2.22: Настроим IP-адресацию для интерфейса локальной сети маршрутизатора и проверим конфигурацию маршрутизатора и настройки IP-адресации

Теперь проверим подключение. Узел PC-1-anspelov успешно отправляет эхо-запросы на адрес маршрутизатора 192.168.1.1(рис. 2.23).

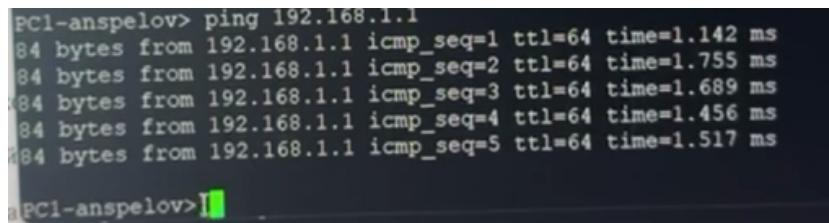


Рис. 2.23: Проверка подключения.

В окне Wireshark получили информацию(рис. 2.24).

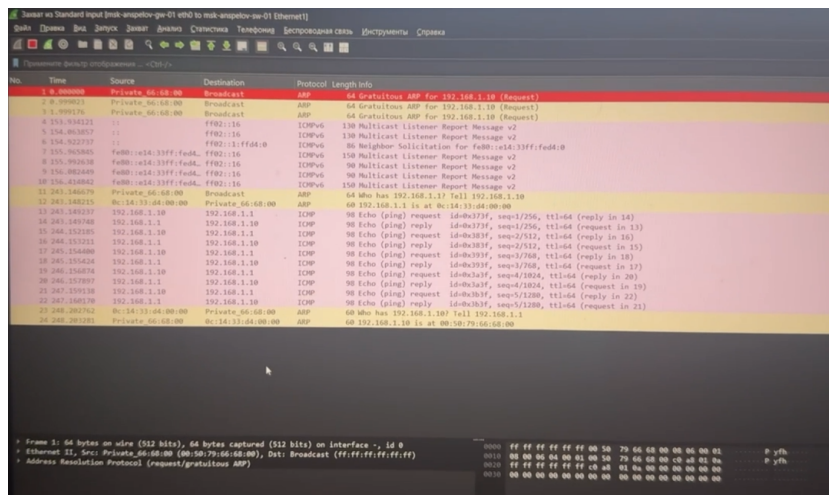


Рис. 2.24: Получение информации в окне Wireshark.

Остановим захват пакетов в Wireshark и всех устройства в проекте(рис. 2.25).

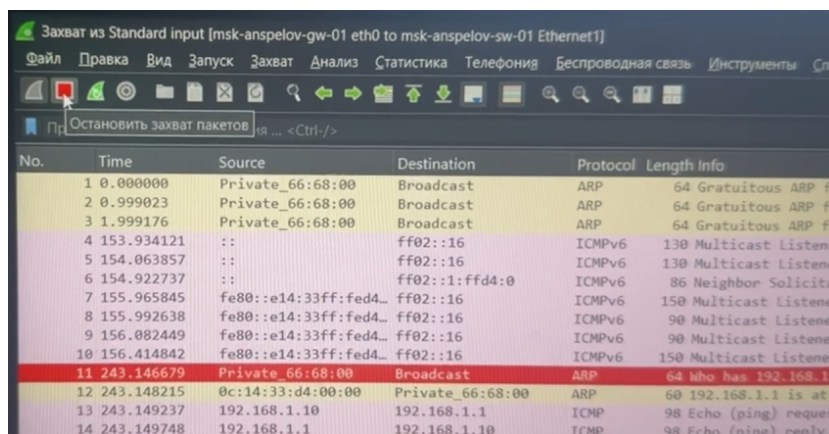


Рис. 2.25: Остановка захвата пакетов в Wireshark.

Создадим новый проект в GNS3(рис. 2.26).

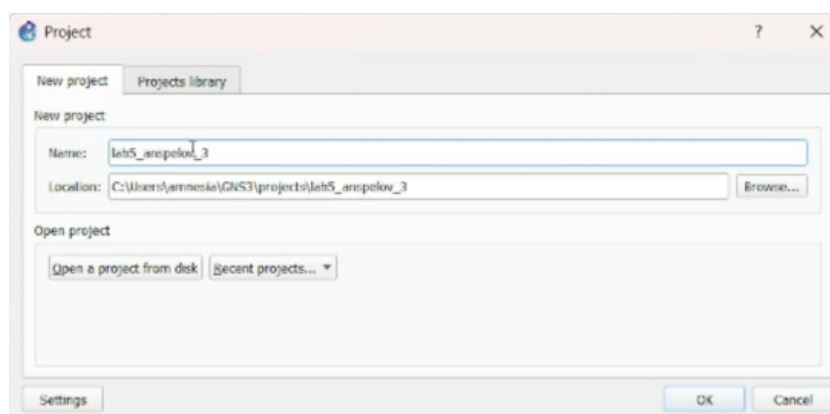


Рис. 2.26: Создание нового проекта в GNS3.

В рабочей области GNS3 разместим VPCS, коммутатор Ethernet и маршрутизатор VyOS. Изменим отображаемые названия устройств. Коммутатору присвоим название по msk-anspelov-sw-01, маршрутизатору — msk-anspelov-gw-01, VPCS — PC-1-anspelov(рис. 2.27).



Рис. 2.27: Размещение VPCS, коммутатора Ethernet и маршрутизатора VyOS. Изменение отображаемых названий устройств.

Включим захват трафика на соединении между коммутатором и маршрутизатором(рис. 2.28).



Рис. 2.28: Включение захвата трафика на соединении между коммутатором и маршрутизатором.

Запустим все устройства проекта. Откроем консоль всех устройств проек-

та(рис. 2.29).

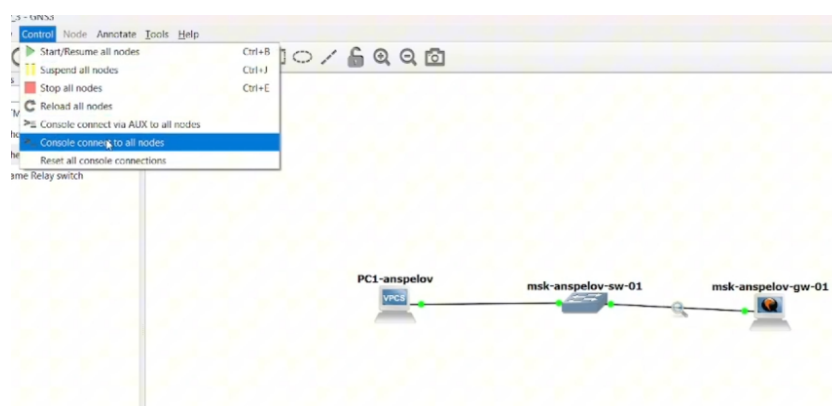


Рис. 2.29: Открытие консолей всех устройств проекта.

Настроим IP-адресацию для интерфейса узла PC-1-anspelov(рис. 2.30).

```
PC1-anspelov> 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

PC1-anspelov> save
Saving startup configuration to startup.vpc
. done

PC1-anspelov> show ip

NAME       : PC1-anspelov[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

PC1-anspelov>
```

Рис. 2.30: Настройка IP-адресации для интерфейса узла PC-1-anspelov.

Настроим маршрутизатор VyOS: После загрузки введём логин vyos и пароль vyos. В рабочем режиме в командной строке отобразился символ \$(рис. 2.31).

```
vyos login: vyos
Password:
Welcome to VyOS!

┌───┐
│ . vyOS 2025.11.08-0018-rolling  
│ └───┐ current
```

* Documentation: <https://docs.vyos.io/en/latest>
* Project news: <https://blog.vyos.io>
* Bug reports: <https://vyos.dev>

You can change this banner using "set system login banner"

VyOS is a free software distribution that includes multiple components.
You can check individual component licenses under /usr/share/licenses/

WARNING: This VyOS system is not a stable long-term support system.
It is not intended for production use.

vyos@vyos:~\$

Рис. 2.31: Ввод логина и пароля. Отображение рабочего режима.

Установим систему на диск. Она уже установлена, так как установка VyOS производится через виртуальную машину с помощью установки vyos.vdi (рис. 2.32).

```
vyos@vyos:~$ install image
The system is already installed. Please use "add system image" instead.
vyos@vyos:~$
```

Рис. 2.32: Установка системы на диск. Она уже установлена.

Перейдём в режим конфигурирования. Изменим имя устройства. Зададим IP-адрес на интерфейсе eth1. Посмотрим внесённые в конфигурацию изменения. Применим изменения в конфигурации и сохраним саму конфигурацию. (рис. 2.33).

```

vyos@msk-anspelov-gw-01# set interfaces ethernet eth1 address 192.168.1.1/24
[edit]
vyos@msk-anspelov-gw-01# compare
[interfaces ethernet eth1]
+ address "192.168.1.1/24"
[system]
- host-name "msk-anspelov-gw-01"
+ host-name "mak-anspelov-gw-01"

[edit]
vyos@msk-anspelov-gw-01# set system host-name msk-anspelov-gw-01
[edit]
vyos@msk-anspelov-gw-01# compare
[interfaces ethernet eth1]
+ address "192.168.1.1/24"

[edit]
vyos@msk-anspelov-gw-01# commit
[edit]
vyos@msk-anspelov-gw-01# save

```

Рис. 2.33: Переход в режим конфигурирования. Изменение имени устройства. Настройка IP-адреса на интерфейсе eth0. Просмотр внесённых в конфигурацию изменений. Применение изменений в конфигурации и сохранение самой конфигурации.

Посмотрим информацию об интерфейсах маршрутизатора. Выйдем из режима конфигурирования.(рис. 2.34).

```

vyos@msk-anspelov-gw-01# show interfaces
  ethernet eth1 {
    address 192.168.1.1/24
    hw-id 0c:57:8d:50:00:00
  }
  loopback lo {
  }
[edit]
vyos@msk-anspelov-gw-01# exit
exit
vyos@vyos:~$

```

Рис. 2.34: Просмотр информации об интерфейсах маршрутизатора. Выход из режима конфигурирования.

Проверим подключение. Узел PC-1-anspelov успешно отправляет эхо-запросы на адрес маршрутизатора 192.168.1.1(рис. 2.35).

```
PC1-anspelov> ping 192.168.1.1
84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=1.027 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=13.484 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=1.703 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=2.806 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=1.401 ms
PC1-anspelov>
```

Рис. 2.35: Проверка подключения.

В окне Wireshark получили информацию(рис. 2.36).

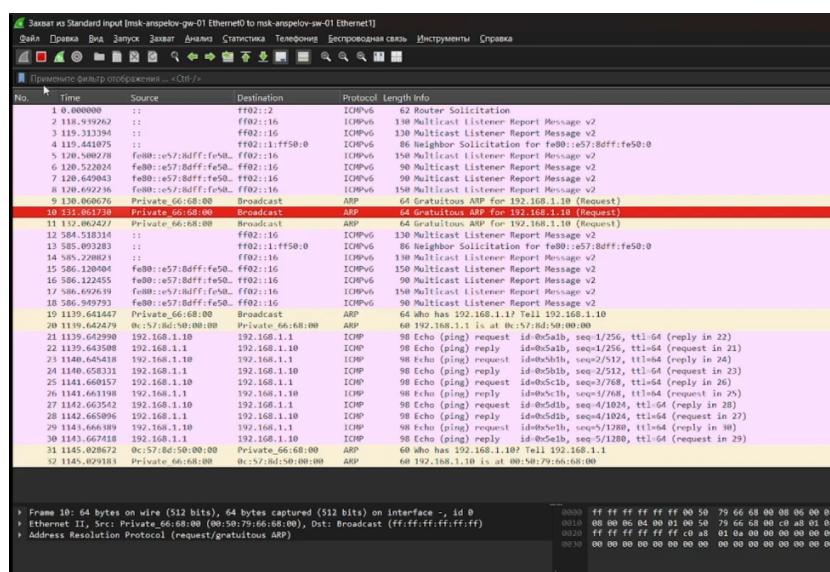


Рис. 2.36: Получение информации в окне Wireshark.

Остановим захват пакетов в Wireshark и всех устройств в проекте. Завершим работу с GNS3(рис. 2.37).

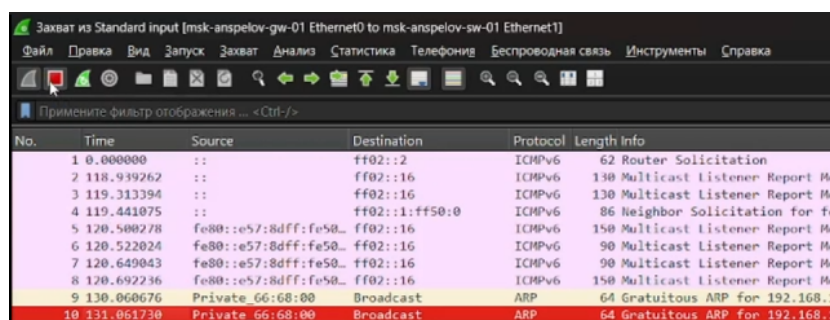


Рис. 2.37: Завершение работы с GNS3.

3 Выводы

В ходе выполнения лабораторной работы мы научились выполнять построение простейших моделей сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3 и научились анализировать трафик посредством Wireshark.

Список литературы