

Лабораторная работа №5

Простые сети в GNS3. Анализ трафика

Андреева Софья Владимировна

Содержание

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	9
3.3 Моделирование простейшей сети на базе маршрутизатора FRR в GNS3	13
3.4 Моделирование простейшей сети на базе маршрутизатора VyOS в GNS3	17
4 Выводы	21

Список иллюстраций

3.1 Добавление устройств и изменение их имен Соединение VPCS с коммутатором	6
3.2 Параметры импорта	7
3.3 Задание IP-адреса PC1-svandreeva	8
3.4 Задание IP-адреса PC2-svandreeva	8
3.5 Проверка соединения между PC-1 и PC-2	9
3.6 Запуск анализатора трафика	9
3.7 ARP пакеты	10
3.8 ARP пакеты	10
3.9 Эхо-запрос в ICMP-моде	11
3.10 ICMP пакеты	11
3.11 Эхо-запрос в UDP-моде	12
3.12 UDP пакеты	12
3.13 Эхо-запрос в TCP-моде	13
3.14 TCP пакеты	13
3.15 Рабочая область	14
3.16 Захват трафика	14
3.17 Настройка IP-адресации для интерфейса узла PC-1	15
3.18 Настройка IP-адресации для интерфейса локальной сети маршрутизатора	15
3.19 Проверка конфигурации маршрутизатора и настройки IP-адресации	16
3.20 Проверка подключения	16
3.21 Анализ информации в Wireshark	17
3.22 Захват трафика на соединении между коммутатором и маршрутизатором	18
3.23 Настройка IP-адресации для интерфейса узла PC-1	18
3.24 Режим конфигурации маршрутизатора VyOS	19
3.25 Режим конфигурации маршрутизатора VyOS	19
3.26 Проверка соединения	20
3.27 Анализ трафика Wireshark	20

1 Цель работы

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

2 Задание

1. Смоделировать простейшую сеть на базе коммутатора в GNS3
2. Проанализировать трафик в GNS3 посредством Wireshark
3. Смоделировать простейшую сеть на базе маршрутизатора FRR в GNS3
4. Смоделировать простейшую сеть на базе маршрутизатора VyOS в GNS3

3 Выполнение лабораторной работы

3.1 Моделирование простейшей сети на базе коммутатора в GNS3

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.

Запустим GNS3 VM и GNS3 и создадим новый проект. В рабочей области GNS3 разместим коммутатор Ethernet и два VPCS. Щёлкнув на устройстве правой кнопкой мыши в меню Configure изменим название устройства, включив в имя устройства имя своей учётной записи. Коммутатору присвоим название msk-svandreeva-sw-01. Затем соединим VPCS с коммутатором и отобразим обозначение интерфейсов соединения(рис. fig. 3.1).

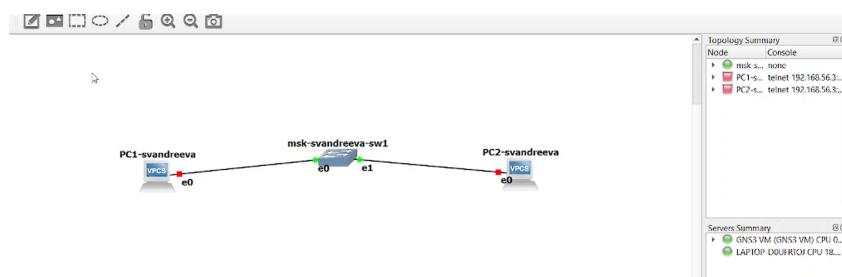
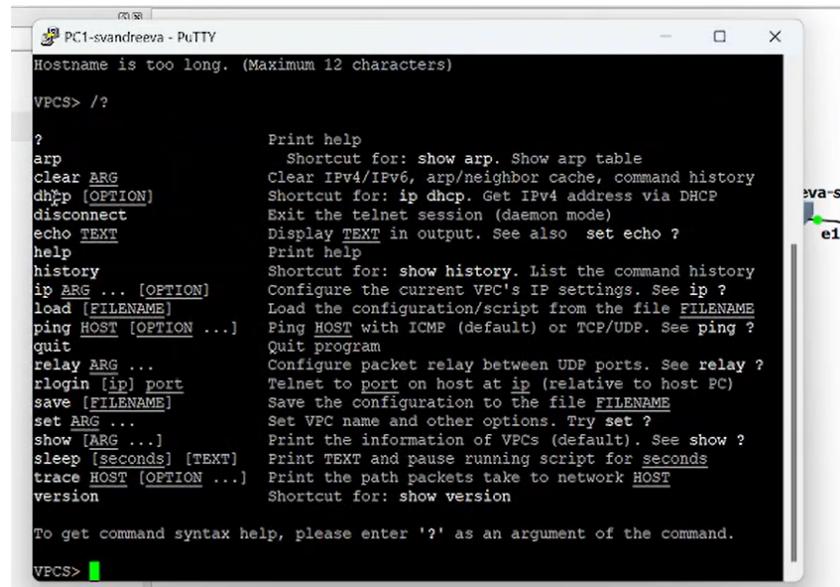


Рис. 3.1: Добавление устройств и изменение их имен Соединение VPCS с коммутатором

Зададим IP-адреса VPCS. Для этого с помощью меню, вызываемого правой

кнопкой мыши, запустим Start, PC-1, затем вызовим его терминал Console. Для просмотра синтаксиса возможных для ввода команд наберем /?(рис. fig. 3.2).



```
PC1-svandreeva - Putty
Hostname is too long. (Maximum 12 characters)

VPCS> /?

?
arp Print help
clear ARG Shortcut for: show arp. Show arp table
dhcp [OPTION] Clear IPv4/IPv6, arp/neighbor cache, command history
disconnect Shortcut for: ip dhcp. Get IPv4 address via DHCP
echo TEXT Exit the telnet session (daemon mode)
help Display TEXT in output. See also set echo ?
history Print help
ip ARG ... [OPTION] Shortcut for: show history. List the command history
load [FILENAME] Configure the current VPC's IP settings. See ip ?
ping HOST [OPTION ...] Load the configuration/script from the file FILENAME
quit Ping HOST with ICMP (default) or TCP/UDP. See ping ?
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>
```

Рис. 3.2: Параметры импорта

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
```

А для сохранения конфигураций введём команду save(рис. fig. 3.3).

```

? 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.

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

```

Рис. 3.3: Задание IP-адреса PC1-svandreeva

Те же действия проделаем для второго VPCS(рис. fig. 3.4):

```

? 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.

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>

```

Рис. 3.4: Задание IP-адреса PC2-svandreeva

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

The screenshot shows two PuTTY sessions. The left window, titled 'PC1-svandreeva - PuTTY', displays VPCS command-line help and configuration. The right window, titled 'PC2-svandreeva - PuTTY', shows the output of a 'ping' command from PC2 to PC1, with several ICMP echo requests and replies visible.

```

PC1-svandreeva - PuTTY
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 192.168.1.12/24 192.168.1.1
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> ping 192.168.1.11
84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=0.874 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=0.537 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=0.433 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=0.667 ms
84 bytes from 192.168.1.12 icmp_seq=5 ttl=64 time=0.423 ms
84 bytes from 192.168.1.12 icmp_seq=6 ttl=64 time=0.352 ms
84 bytes from 192.168.1.12 icmp_seq=7 ttl=64 time=0.345 ms
84 bytes from 192.168.1.12 icmp_seq=8 ttl=64 time=0.552 ms

PC2-svandreeva - PuTTY
n ping packets
17 - UDP, 6 - TCP
64
l interrupted by Ctrl+C
nds to receive the response
to be set.
mmand.

qtile
2.54 on Windows (64-bit) with Python 3.10.11 Qt 5.15.2 and PyQt 5.15.11.
VPCS>

```

Рис. 3.5: Проверка соединения между PC-1 и PC-2

В конце остановим в проекте все узлы(меню GNS3 Control Stop all nodes).

3.2 Анализ трафика в GNS3 посредством Wireshark

1. С помощью Wireshark захватить и проанализировать ARP-сообщения.
2. С помощью Wireshark захватить и проанализировать ICMP-сообщения.

Запустим на соединении между PC-1 и коммутатором анализатор трафика. Для этого щёлкнём правой кнопкой мыши на соединении, выберем в меню Start capture(рис. fig. 3.6).

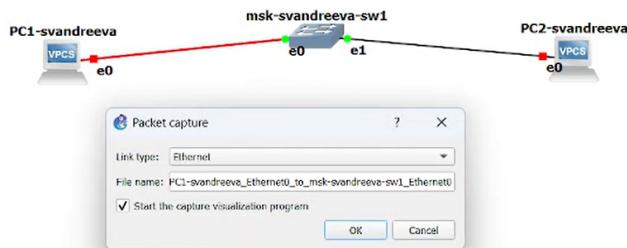


Рис. 3.6: Запуск анализатора трафика

Запустился Wireshark, а в проекте GNS3 на соединении появился значок (рис. fig. 3.7).

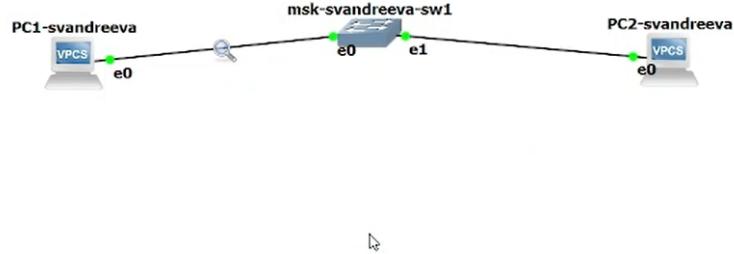


Рис. 3.7: ARP пакеты

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

Изучим запрос и ответ ARP в программе Wireshark(рис. fig. 3.8). В обоих случаях длина кадра равняется 64 байт. В начале сформировались запросы безвоздмездных пакетов ARP для PC-1(в этом случае источник – Private_66:68:00, а пункт назначения - Broadcast) и для PC-2(в этом случае источник – Private_66:68:01, а пункт назначения - Broadcast). Затем был сформирован запрос от PC-2 на передачу MAC-адреса PC-1 и получен ответ – MAC-адрес.

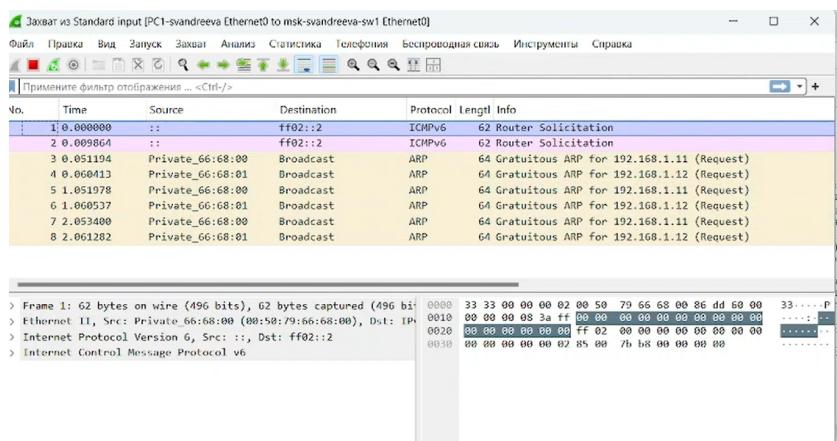


Рис. 3.8: ARP пакеты

В терминале PC-2 посмотрим информацию по опциям команды ping, введя ping/? . Затем сделаем один эхо-запрос в ICMP-моде к узлу PC-1(рис. fig. 3.9). Изучим эхо-запрос и эхо-ответ ICMP в программе Wireshark(рис. fig. 3.10). В обоих случаях длина кадра равняется 98 байт. В случае эхо-запроса точка назначения – PC-1, а источник – PC-2, в случае же эхо-ответа – наоборот.

```
PC2-svandreeva - PuTTY
-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=0.532 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=1.029 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=0.635 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=0.600 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=0.649 ms

VPCS>
```

Рис. 3.9: Эхо-запрос в ICMP-моде

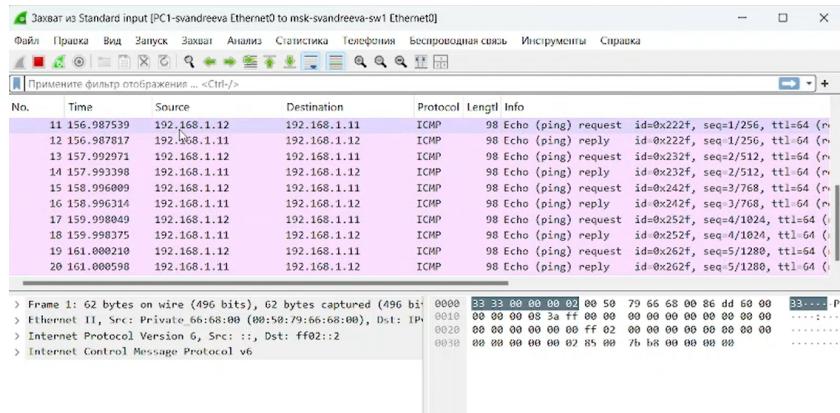


Рис. 3.10: ICMP пакеты

Сделаем один эхо-запрос в UDP-моде к узлу PC-1(рис. fig. 3.11). В окне Wireshark проанализируем полученную информацию(рис. fig. 3.12). В обоих случаях длина кадра равняется 98 байт. В случае эхо-запроса точка назначения – PC-1, а источник – PC-2, в случае же эхо-ответа – наоборот.

```

PC2-svandreeva - PUTTY
-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=0.532 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=1.029 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=0.635 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=0.600 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=0.649 ms

VPCS> ping 192.168.1.11 -2

84 bytes from 192.168.1.11 udp_seq=1 ttl=64 time=0.556 ms
84 bytes from 192.168.1.11 udp_seq=2 ttl=64 time=0.249 ms
84 bytes from 192.168.1.11 udp_seq=3 ttl=64 time=0.617 ms
84 bytes from 192.168.1.11 udp_seq=4 ttl=64 time=0.287 ms
84 bytes from 192.168.1.11 udp_seq=5 ttl=64 time=0.345 ms

VPCS>

```

Рис. 3.11: Эхо-запрос в UDP-моде

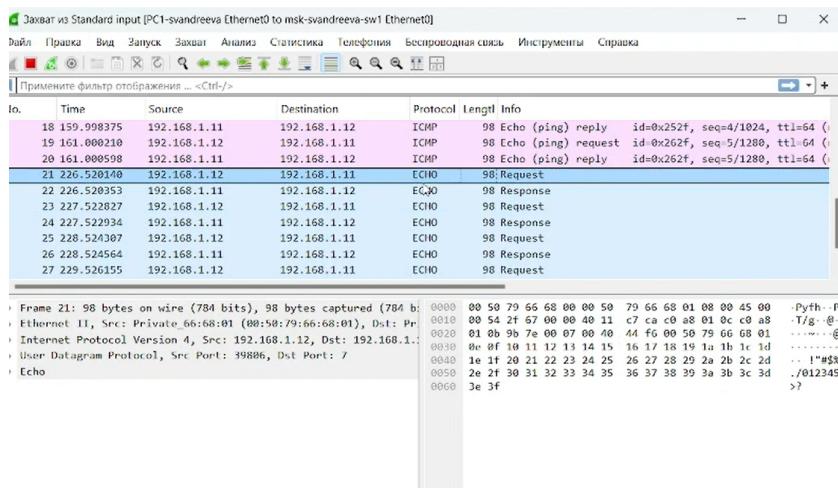


Рис. 3.12: UDP пакеты

Сделаем один эхо-запрос в TCP-моде к узлу PC-1(fig. 3.13). В окне Wireshark проанализируем полученную информацию(fig. 3.14). Порт источника задан случайно равен 35487, порт назначения равен 7. В случае ответа порты заданы наоборот. Также можно увидеть handshake протокола TCP. В первом пакете установлен бит SYN(Syn: set). Во втором пакете установлены биты SYN и ACK(Syn: set, Acknowldgment: set). А в следующем пакете установлен бит ACK(Acknowledgment: set). Также есть пакеты с битом FIN, завершающим handshake.

```

PC2-svandreeva - PuTTY
VPCS> ping 192.168.1.11 -2

84 bytes from 192.168.1.11 udp_seq=1 ttl=64 time=0.556 ms
84 bytes from 192.168.1.11 udp_seq=2 ttl=64 time=0.249 ms
84 bytes from 192.168.1.11 udp_seq=3 ttl=64 time=0.617 ms
84 bytes from 192.168.1.11 udp_seq=4 ttl=64 time=0.287 ms
84 bytes from 192.168.1.11 udp_seq=5 ttl=64 time=0.345 ms

VPCS> ping 192.168.1.11 -3

Connect 7@192.168.1.11 seq=1 ttl=64 time=2.569 ms
SendData 7@192.168.1.11 seq=1 ttl=64 time=1.106 ms
Close 7@192.168.1.11 seq=1 ttl=64 time=3.902 ms
Connect 7@192.168.1.11 seq=2 ttl=64 time=1.256 ms
SendData 7@192.168.1.11 seq=2 ttl=64 time=2.904 ms
Close 7@192.168.1.11 seq=2 ttl=64 time=4.951 ms
Connect 7@192.168.1.11 seq=3 ttl=64 time=1.821 ms
SendData 7@192.168.1.11 seq=3 ttl=64 time=1.965 ms
Close 7@192.168.1.11 seq=3 ttl=64 time=3.090 ms
Connect 7@192.168.1.11 seq=4 ttl=64 time=1.158 ms
SendData 7@192.168.1.11 seq=4 ttl=64 time=1.249 ms
Close 7@192.168.1.11 seq=4 ttl=64 time=4.700 ms
Connect 7@192.168.1.11 seq=5 ttl=64 time=1.081 ms

```

Рис. 3.13: Эхо-запрос в TCP-моде

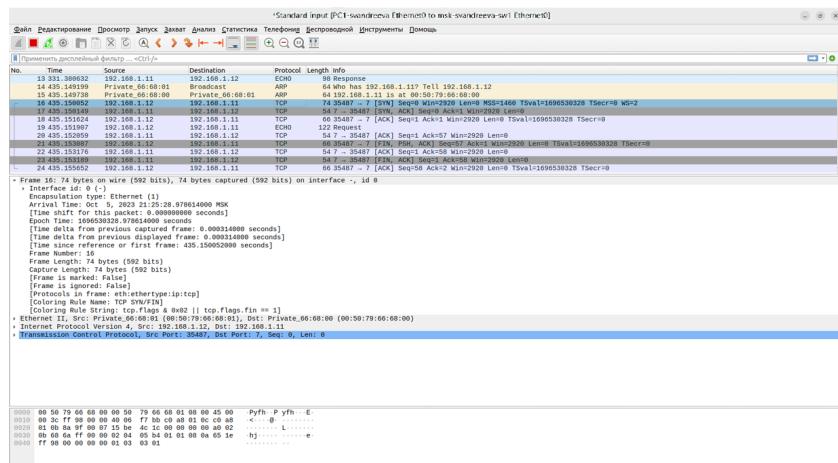


Рис. 3.14: TCP пакеты

Остановим захват пакетов в Wireshark.

3.3 Моделирование простейшей сети на базе маршрутизатора FRR в GNS3

- Построить в GNS3 топологию сети, состоящей из маршрутизатора FRR, ком- мутатора Ethernet и оконечного устройства.

2. Задать оконечному устройству IP-адрес в сети 192.168.1.0/24.
3. Присвоить интерфейсу маршрутизатора адрес 192.168.1.1/24
4. Проверить связь.

Запустим GNS3 VM и GNS3. Создадим новый проект. В рабочей области GNS3 разместим VPCS, коммутатор Ethernet и маршрутизатор FRR. Изменим отображаемые названия устройств. Включим захват трафика на соединении между коммутатором и маршрутизатором. Затем запустим все устройства проекта. Откроем консоль всех устройств проекта.

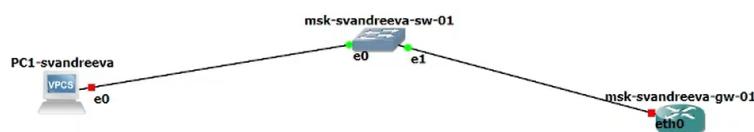


Рис. 3.15: Рабочая область

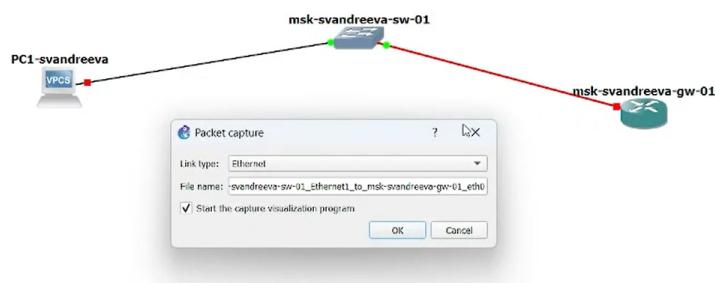


Рис. 3.16: Захват трафика

Настроим IP-адресацию для интерфейса узла PC1(fig. 3.17):

```

PC1-svandreeva - PuTTY
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...
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. 3.17: Настройка IP-адресации для интерфейса узла РС-1

Настроим IP-адресацию для интерфейса локальной сети маршрутизатора(fig. 3.18):

```

msk svandreeva-gw-01 - PuTTY
frr# configure terminal
frr(config)# hostname msk-svandreeva-gw-01
msk-svandreeva-gw-01(config)# exit
msk-svandreeva-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-svandreeva-gw-01# configure terminal
% Unknown command: configure terminal
msk-svandreeva-gw-01# configure terminal
msk-svandreeva-gw-01(config)# interface eth0
msk-svandreeva-gw-01(config-if)# ip address 192.168.1.1/24
% Unknown command: ip address 192.168.1.1/24
msk-svandreeva-gw-01(config-if)# ip address 192.168.1.1/24
msk-svandreeva-gw-01(config-if)# no shutdown
msk-svandreeva-gw-01(config-if)# exit
msk-svandreeva-gw-01(config)# exit
msk-svandreeva-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-svandreeva-gw-01# show running

```

Рис. 3.18: Настройка IP-адресации для интерфейса локальной сети маршрутизатора

Проверим конфигурацию маршрутизатора и настройки IP-адресации(fig. 3.19):

```

msk svandreeva gw-01 - PuTTY
hostname frr
hostname msk-svandreeva-gw-01
service integrated-vtysh-config
!
interface eth0
ip address 192.168.1.1/24
exit
!
end
msk-svandreeva-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-svandreeva-gw-01#

```

Рис. 3.19: Проверка конфигурации маршрутизатора и настройки IP-адресации

Проверим подключение. Узел PC1 успешно отправлять эхо-запросы ICMP на адрес маршрутизатора 192.168.1.1(fig. 3.20).

```

PC1-svandreeva - PuTTY
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=24.128 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=1.287 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=1.748 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=1.525 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=2.576 ms

VPCS>

```

Рис. 3.20: Проверка подключения

В окне Wireshark проанализируем полученную информацию(fig. 3.21). Было отправлено 10 пакетов формата ICMP. В эхо-запросе источником является IP-адрес PC-1, а пунктом назначения – IP-адрес шлюза маршрутизатора. В эхо-ответе – наоборот. Также были сформированы ARP пакеты запрашивающий MAC-адрес шлюза маршрутизатора перед пингованием его и сообщающий этот

MAC-адрес PC-1, а затем запрашивающие MAC-адрес PC-1 и сообщающие его шлюзу.

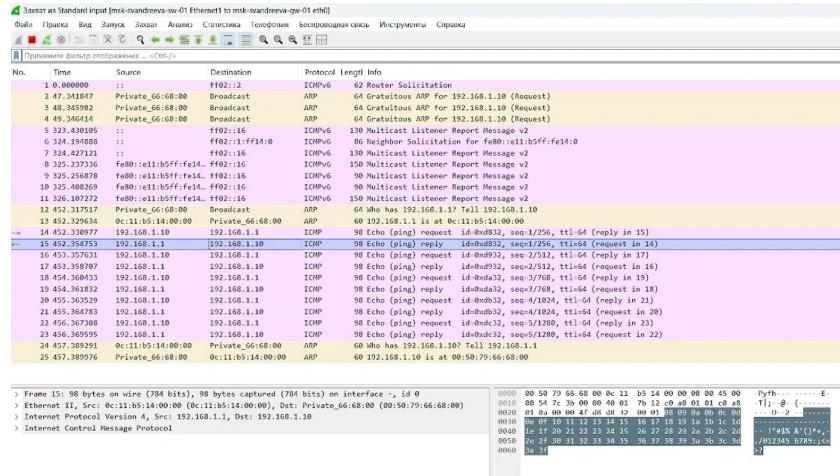


Рис. 3.21: Анализ информации в Wireshark

В конце остановим захват пакетов в Wireshark и остановим все устройства в проекте.

3.4 Моделирование простейшей сети на базе маршрутизатора VyOS в GNS3

- Построить в GNS3 топологию сети, состоящей из маршрутизатора VyOS, коммутатора Ethernet и оконечного устройства.
- Задать оконечному устройству IP-адрес в сети 192.168.1.0/24.
- Присвоить интерфейсу маршрутизатора адрес 192.168.1.1/24
- Проверить связь.

Запустим GNS3 VM и GNS3. Создадим новый проект.

В рабочей области GNS3 разместим VPCS, коммутатор Ethernet и маршрутизатор VyOS.

Изменим отображаемые названия устройств. Включим захват трафика на соединении между коммутатором и маршрутизатором. Запустим все устройства

проекта. Откройте консоль всех устройств проекта (fig. 3.22).

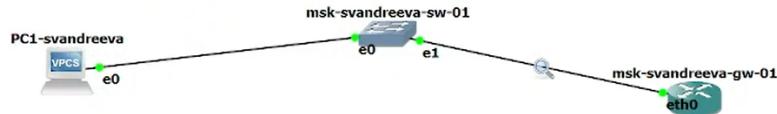


Рис. 3.22: Захват трафика на соединении между коммутатором и маршрутизатором

Настроим IP-адресацию для интерфейса узла PC1 (fig. 3.23).

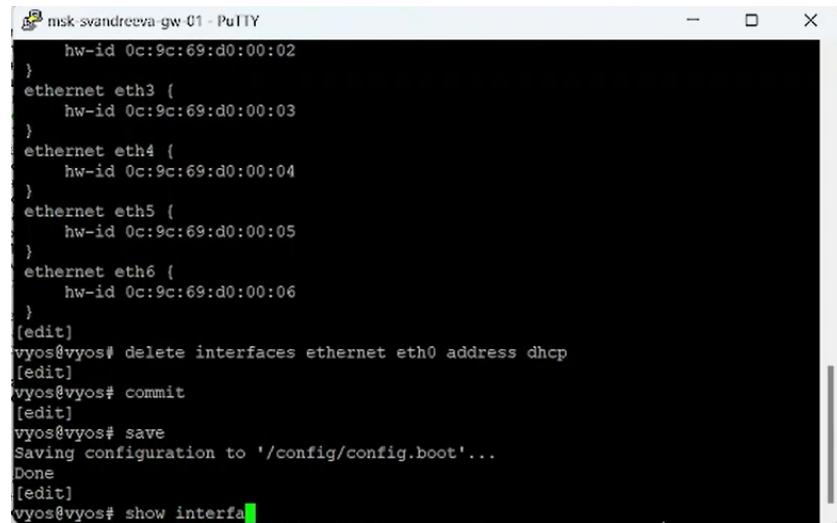
```
Executing the startup file
Hostname is too long. (Maximum 12 characters)
VPCS> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
VPCS : 192.168.1.10 255.255.255.0 gateway 192.168.1.1
VPCS> save
Saving startup configuration to startup.vpc
done
VPCS> show ip
NAME      : VPCS[1]
IP/MASK   : 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. 3.23: Настройка IP-адресации для интерфейса узла РС-1

Настроим маршрутизатор VyOS. После загрузки введем логин `vyos` и пароль `vyos`: В рабочем режиме в командной строке отображается символ `$`. Перейдем в режим конфигурирования с помощью команды `configure`. Изменим имя устройства с помощью команды `set system host-name msk-svandreeva-gw-01`. Изменения в имени устройства вступят в силу после применения и сохранения конфигурации и перезапуска устройства.

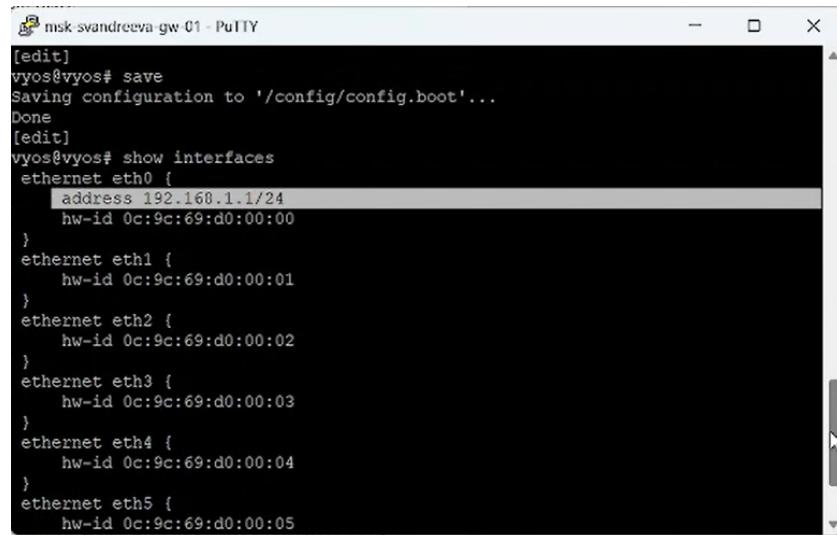
Затем зададим IP-адрес на интерфейсе `eth0`. Но так как на моем устройстве

уже был установлен dhcp адрес, то сначала я удалила его, а затем установила адрес IPv4. Также просмотрим внесённые в конфигурацию изменения, применим эти изменения и сохраним. В конце выйдем из режима конфигурирования(fig. 3.24).



```
msk svandreeva-gw-01 - PuTTY
hw-id 0c:9c:69:d0:00:02
}
ethernet eth3 {
    hw-id 0c:9c:69:d0:00:03
}
ethernet eth4 {
    hw-id 0c:9c:69:d0:00:04
}
ethernet eth5 {
    hw-id 0c:9c:69:d0:00:05
}
ethernet eth6 {
    hw-id 0c:9c:69:d0:00:06
}
[edit]
vyos@vyos# delete interfaces ethernet eth0 address dhcp
[edit]
vyos@vyos# commit
[edit]
vyos@vyos# save
Saving configuration to '/config/config.boot'...
Done
[edit]
vyos@vyos# show interfa
```

Рис. 3.24: Режим конфигурации маршрутизатора VyOS



```
[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:9c:69:d0:00:00
}
ethernet eth1 {
    hw-id 0c:9c:69:d0:00:01
}
ethernet eth2 {
    hw-id 0c:9c:69:d0:00:02
}
ethernet eth3 {
    hw-id 0c:9c:69:d0:00:03
}
ethernet eth4 {
    hw-id 0c:9c:69:d0:00:04
}
ethernet eth5 {
    hw-id 0c:9c:69:d0:00:05
```

Рис. 3.25: Режим конфигурации маршрутизатора VyOS

Проверим подключение. Узел PC1 дуспешно отправлять эхо-запросы на адрес маршрутизатора 192.168.1.1(fig. 3.26).

```

PC1-svandreeva - PuTTY
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=1.729 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=2.294 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=2.903 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=2.179 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=4.427 ms

VPCS>

```

Рис. 3.26: Проверка соединения

В окне Wireshark проанализируйте полученную информацию. Было отправлены пакеты ICMP. В эхо-запросе источником является IP-адрес PC-1, а пунктом назначения – IP-адрес шлюза маршрутизатора. В эхо-ответе – наоборот. Также были сформированы ARP пакеты запрашивающий MAC-адрес шлюза маршрутизатора перед пингованием его и сообщающий этот MAC-адрес PC-1, а затем запрашивающие MAC-адрес PC-1 и сообщающие его шлюзу.

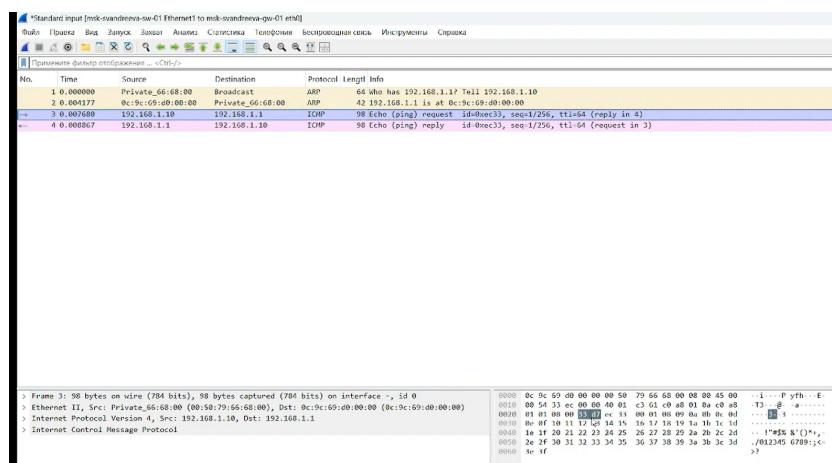


Рис. 3.27: Анализ трафика Wireshark

4 Выводы

В результате выполнения лабораторной работы были построены простейшие модели сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, а также проанализирован трафик посредством Wireshark.