РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ
ПО ЛАБОРАТОРНОЙ РАБОТЕ № 5

дисциплина:Сетевые технологии

Простые сети в GNS3.
Анализ трафика

Студент:Сатлихана Петрити
Стелина Петрити

Группа: НПИбд-02-21

МОСКВА
2023 г.

Цели работы

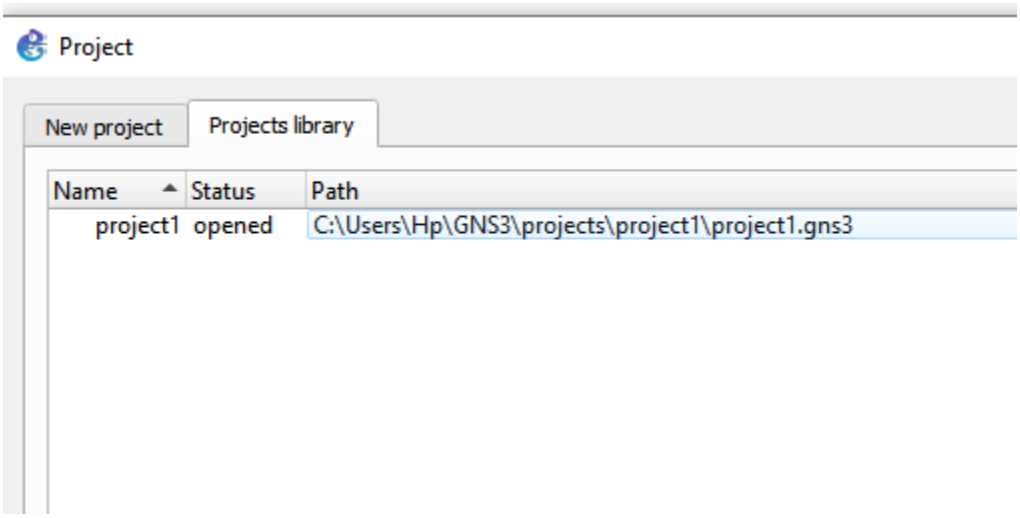
Построение простейших моделей сети на базе коммутатора и маршрутизаторов FRR и VyOS в GNS3, анализ трафика посредством Wireshark

5.3. Задания для выполнения

5.3.1. Моделирование простейшей сети на базе коммутатора в GNS3

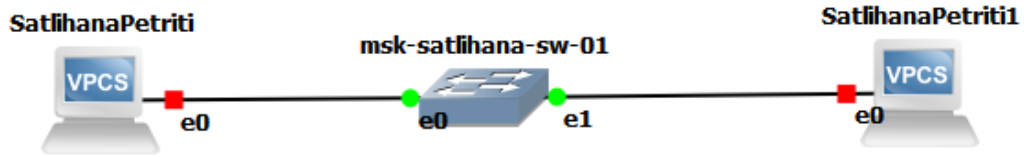
5.3.1.2. Порядок выполнения работы

1. Запустите GNS3 VM и GNS3. Создайте новый проект.



1.1. Создание нового проекта

2. В рабочей области GNS3 разместите коммутатор Ethernet и два VPCS.Щёлкнув на устройстве правой кнопкой мыши выберете в меню Configure . Измените название устройства, включив в имя устройства имя учётной записи выполняющего работу студента. Коммутатору присвойте название msk-user-sw-01, где вместо user укажите имя вашей учётной записи. Соедините VPCS с коммутатором. Отобразите обозначение интерфейсов соединения.



2.1. Топология простейшей сети в GNS3

3. Задайте IP-адреса VPCS. Для этого с помощью меню, вызываемого правой кнопкой мыши, запустите Start , например, PC-1, затем вызовите его терминал Console . Для просмотра синтаксиса возможных для ввода команд наберите /?

Для задания IP-адреса 192.168.1.11 в сети 192.168.1.0/24 введите
ip 192.168.1.11/24 192.168.1.1

```
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>
```

3.1. IP-адреса VPCS

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

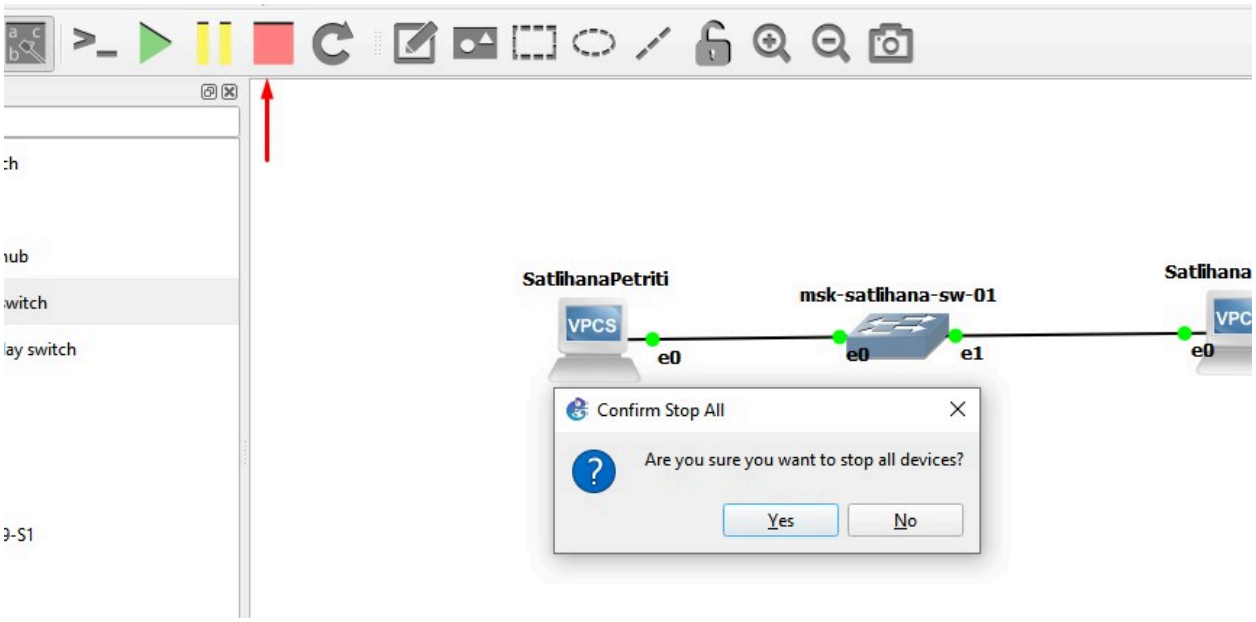
4. Проверьте работоспособность соединения между PC-1 и PC-2 с помощью команды ping.

SatlihanaPetriti1 - PuTTY

```
Executing the startup file


Checking for duplicate address...
VPCS : 192.168.1.12 255.255.255.0 gateway 192.168.1.1

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 192.168.1.12

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
```

4.1. Соединение между PC-1 и PC-2 с помощью команды ping

5. Остановите в проекте все узлы (меню GNS3 Control Stop all nodes).

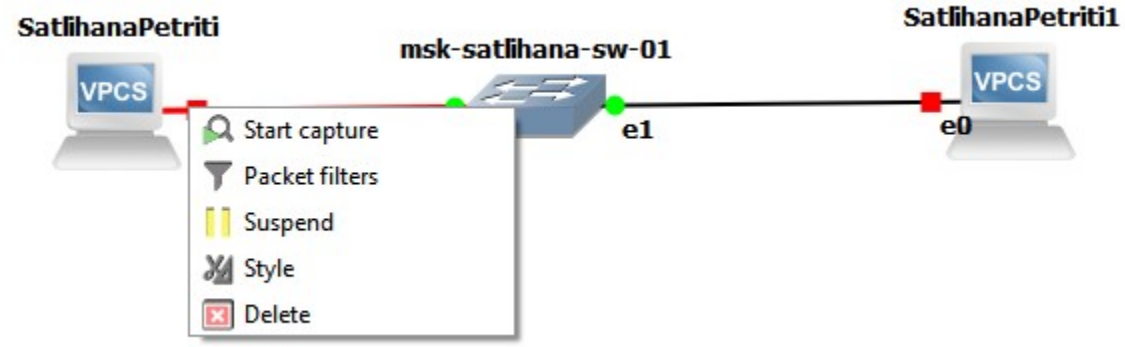


5.1. Остановка все узлы

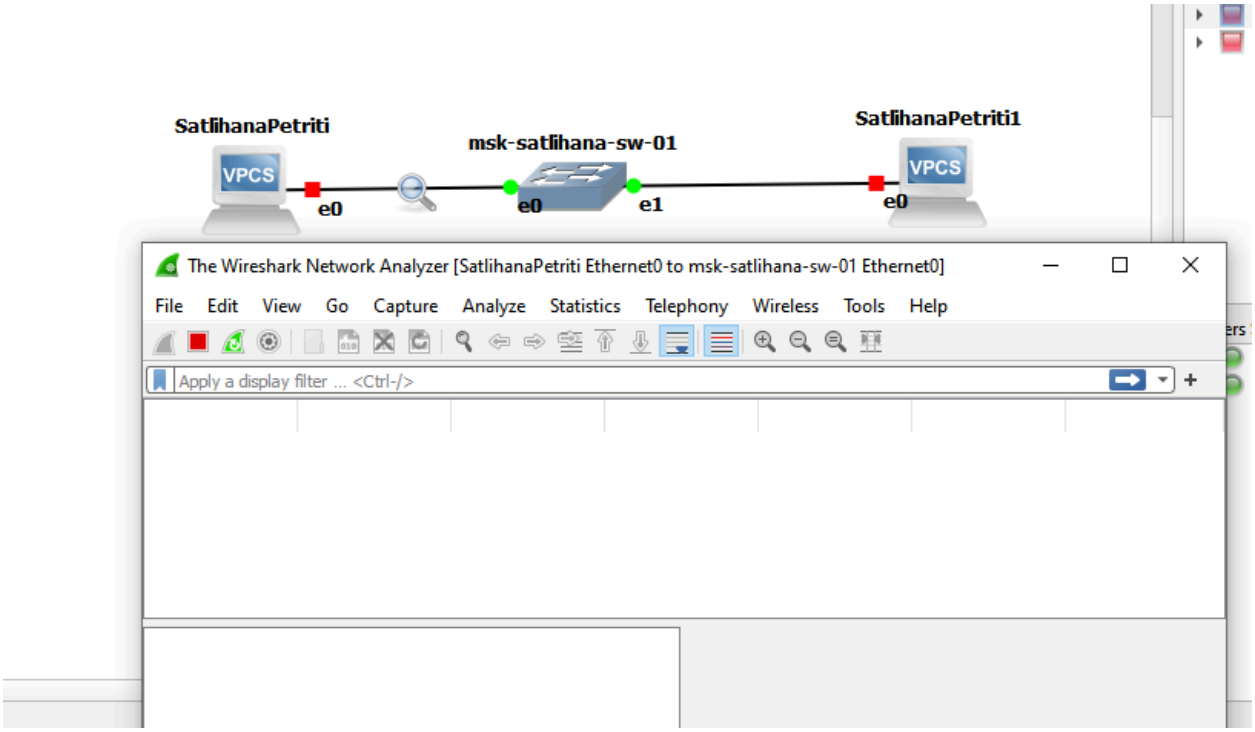
5.3.2. Анализ трафика в GNS3 посредством Wireshark

5.3.2.2. Порядок выполнения работы

1. Запустите на соединении между PC-1 и коммутатором анализатор трафика. Для этого щёлкните правой кнопкой мыши на соединении, выберете
в меню Start capture , при необходимости можете скорректировать название DUMP-файла.Запустится Wireshark, а в проекте GNS3 на соединении появится значок лупы.

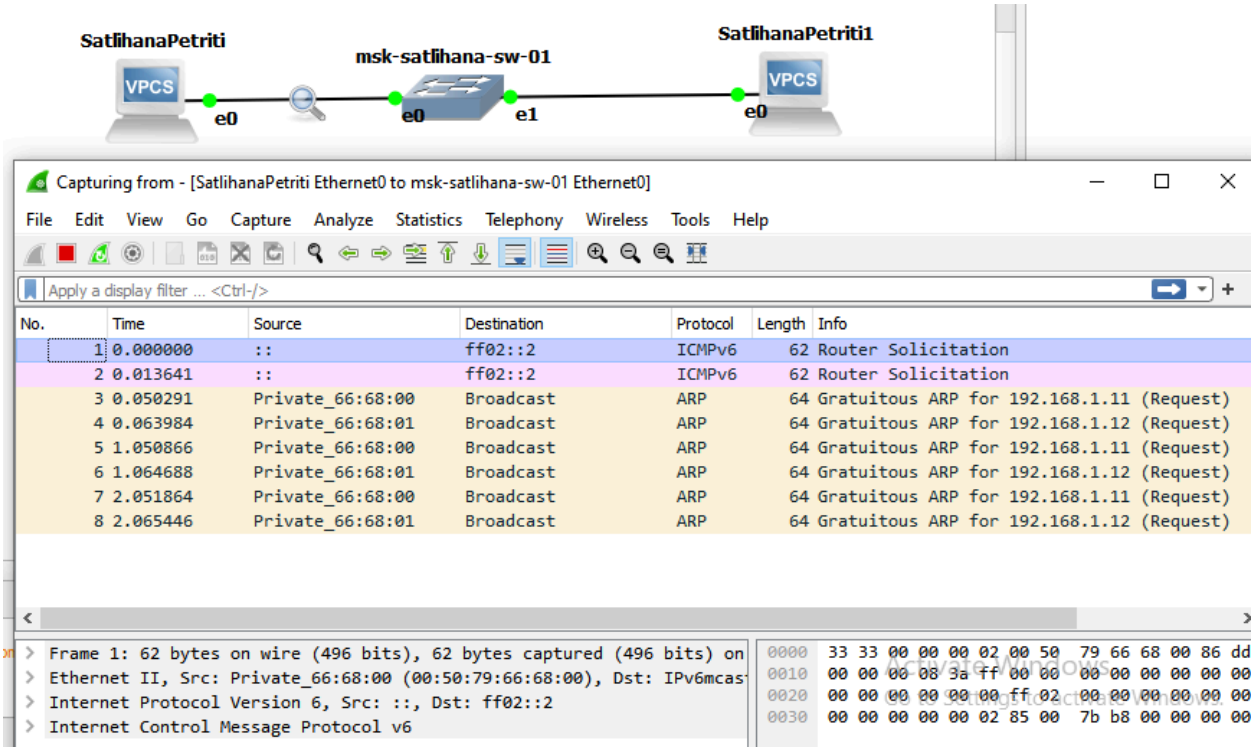


1.1. Запуск анализатора трафика на соединении между PC-1 и коммутатором



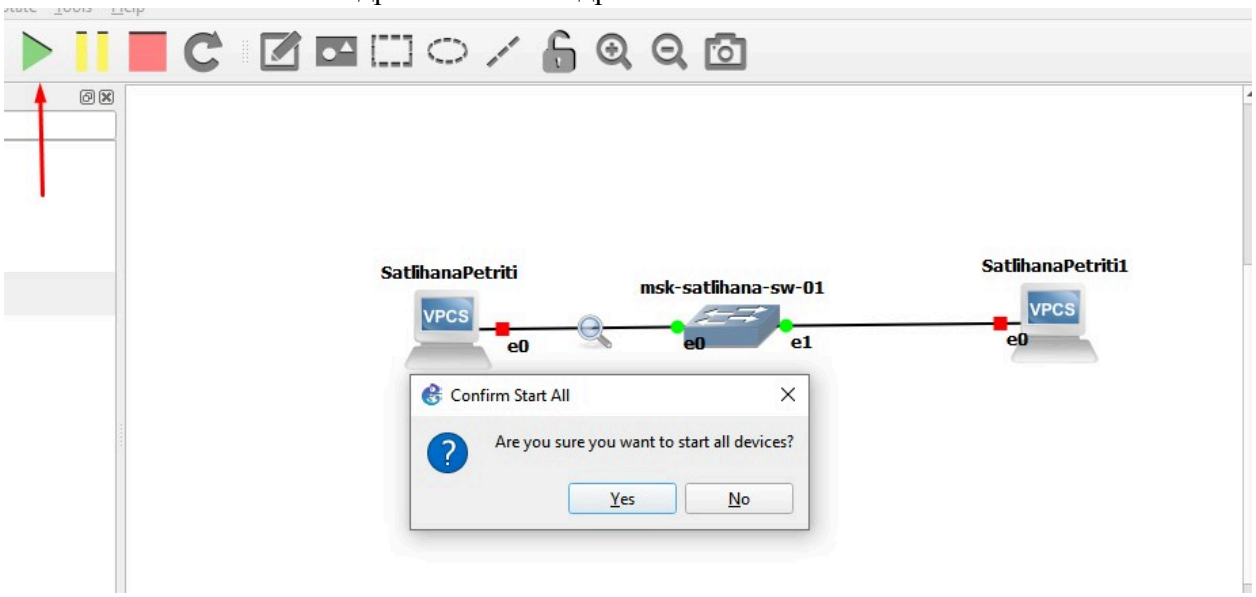
1.2 .Wireshark запустился

2. В проекте GNS3 стартуйте все узлы (меню GNS3 Control Start/Resume all nodes). В окне Wireshark (рис. 5.4) отобразится информация по протоколу ARP. Проанализируйте полученную информацию, дайте пояснения в отчёте.



2.1. Полученная в Wireshark информация по ARP- и ICMP-сообщениям

- Запросы ARP отправляются устройством для определения MAC-адреса (Media Access Control), соответствующего IP-адресу.
- В процессе захвата вы можете увидеть ARP-запросы с исходным IP-адресом и MAC-адресом и IP-адресом назначения со всеми нулями или целевым IP-адресом, для которого устройство пытается разрешить MAC-адрес.
- Запросы ARP помогают устройствам создавать свои таблицы ARP для сопоставления IP-адресов с MAC-адресами.

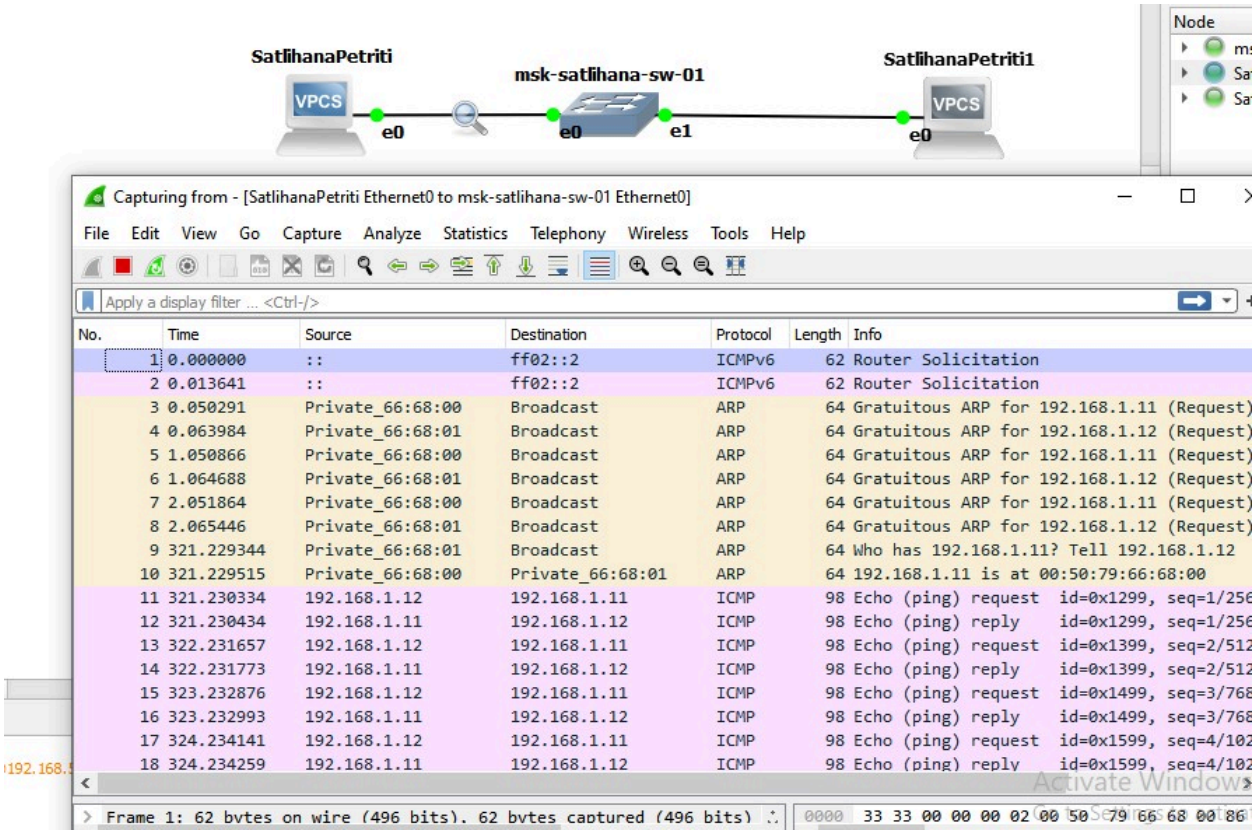


2.2. В проекте GNS3 все узлы запущены

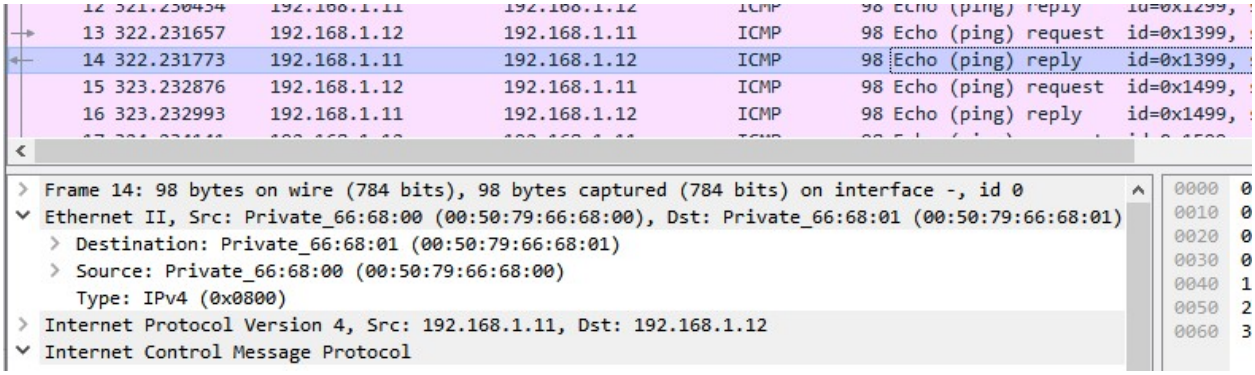
3. В терминале PC-2 посмотрите информацию по опциям команды ping, введя ping /?. Затем сделайте один эхо-запрос в ICMP-моде к узлу PC-1. В окне Wireshark (рис. 5.4) проанализируйте полученную информацию, дайте пояснения в отчёте.

```
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

84 bytes from 192.168.1.11 icmp_seq=1 ttl=64 time=0.207 ms
84 bytes from 192.168.1.11 icmp_seq=2 ttl=64 time=0.289 ms
84 bytes from 192.168.1.11 icmp_seq=3 ttl=64 time=0.280 ms
84 bytes from 192.168.1.11 icmp_seq=4 ttl=64 time=0.303 ms
84 bytes from 192.168.1.11 icmp_seq=5 ttl=64 time=0.282 ms

VPCS>
```

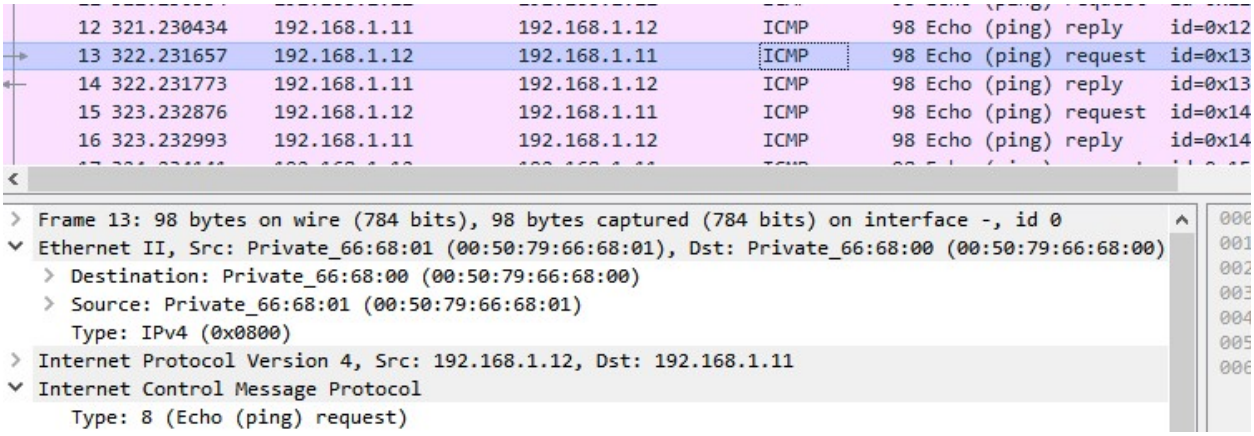
3.1. информацию о команде ping можно получить, набрав ping /?



3.2. *Полученная в Wireshark информация по ARP- и ICMP*



3.3. *информация по ICMP(reply)*



3.4. информация по ICMP(request).

Пакеты эхо-запроса ICMP и эхо-ответа: Здесь мы видим пакет эхо-запроса ICMP, отправленный PS2, и соответствующий пакет эхо-ответа ICMP, отправленный PC-1 в ответ, показывает, что он прошел успешно.
Временные метки: Временные метки помогают понять время передачи сообщения

4. Сделайте один эхо-запрос в UDP-моде к узлу PC-1. В окне Wireshark (рис. 5.4) проанализируйте полученную информацию, дайте пояснения в отчёте.

5. Сделайте один эхо-запрос в TCP-моде к узлу PC-1. В окне Wireshark (рис. 5.4) проанализируйте полученную информацию, дайте пояснения в отчёте.

6. Остановите захват пакетов в Wireshark.

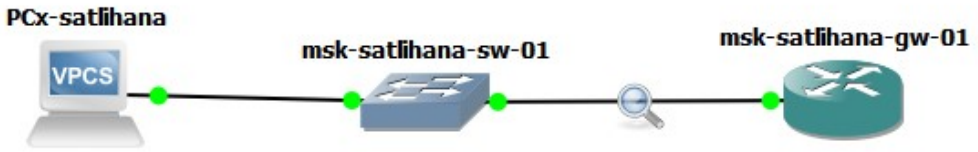
5.3.3. Моделирование простейшей сети на базе маршрутизатора FRR в GNS3

5.3.3.1. Постановка задачи

1. Построить в GNS3 топологию сети, состоящей из маршрутизатора FRR, коммутатора 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.

5.3.3.2. Порядок выполнения работы

1. Запустите GNS3 VM и GNS3. Создайте новый проект.
2. В рабочей области GNS3 разместите VPCS, коммутатор Ethernet и маршрутизатор FRR (рис. 5.5).
3. Измените отображаемые названия устройств. Коммутатору присвойте название по принципу msk-user-sw-0x, маршрутизатору — по принципу mskuser-gw-0x, VPCS — по принципу PCx-user, где вместо user укажите имя вашей учётной записи, вместо x — порядковый номер устройства.



3.1. Измените отображаемые названия устройств

4. Включите захват трафика на соединении между коммутатором и маршрутизатором.
5. Запустите все устройства проекта. Откройте консоль всех устройств проекта.
6. Настройте IP-адресацию для интерфейса узла PC1:

ip 192.168.1.10/24 192.168.1.1
save
show ip

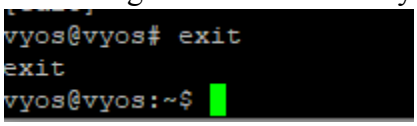
```
VPCS> ip 192.168.1.10/24 192.168.1.1
Checking for duplicate address...
VPCS : 192.168.1.10 255.255.255.0 gateway 192.168.1.1

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>
```

6.1. Запустите все устройства проекта

7. Настройте IP-адресацию для интерфейса локальной сети маршрутизатора:

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



7.1 exit

8. Проверьте конфигурацию маршрутизатора и настройки IP-адресации:
msk-user-gw-01# show running-config
msk-user-gw-01# show interface brief
9. Проверьте подключение. Узел PC1 должен успешно отправлять эхо-запросы на адрес маршрутизатора 192.168.1.1.
10. В окне Wireshark проанализируйте полученную информацию, дайте пояснения в отчёте.
11. Остановите захват пакетов в Wireshark. Остановите все устройства в проекте.

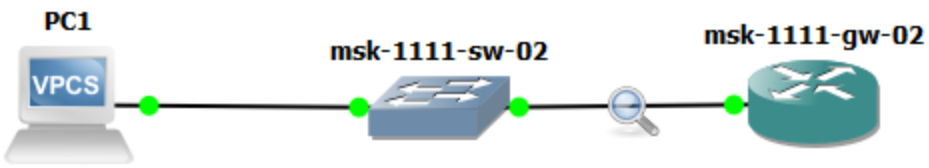
5.3.4. Моделирование простейшей сети на базе маршрутизатора VyOS в GNS3

5.3.4.1. Постановка задачи

1. Построить в GNS3 топологию сети, состоящей из маршрутизатора VyOS, коммутатора 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.

5.3.4.2. Порядок выполнения работы

1. Запустите GNS3 VM и GNS3. Создайте новый проект.
2. В рабочей области GNS3 разместите VPCS, коммутатор Ethernet и маршрут затор VyOS (рис. 5.6).
3. Измените отображаемые названия устройств. Коммутатору присвойте название по принципу msk-user-sw-0x, маршрутизатору — по принципу mskuser-gw-0x, VPCS — по принципу PCx-user, где вместо user укажите имя вашей учётной записи, вместо x — порядковый номер устройства.
4. Включите захват трафика на соединении между коммутатором и маршрутизатором.



1.2.3.4. Выполните указанные выше 4 пункта

5. Запустите все устройства проекта. Откройте консоль всех устройств проекта.
6. Настройте IP-адресацию для интерфейса узла PC1:

ip 192.168.1.10/24 192.168.1.1
save
show ip

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

PC1> show ip

NAME        : PC1[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

PC1>
```

5.6. Запуск всех устройств проекта и настройка IP-адресации

7. Настройте маршрутизатор VyOS: После загрузки введите логин vyos и пароль vyos: vyos login: vyos Password: В рабочем режиме в командной строке отображается символ $. – Установите систему на диск: vyos@vyos:~$ install image

```
vyos login: vyos
Password:
Linux vyos 4.19.195-amd64-vyos #1 SMP Thu Feb 17 12:52:59 UTC 2022 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

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

vyos@vyos:~$ install image
Welcome to the VyOS install program.  This script
will walk you through the process of installing the
VyOS image to a local hard drive.
Would you like to continue? (Yes/No) [Yes]: yes
Probing drives: OK
Looking for pre-existing RAID groups...none found.
The VyOS image will require a minimum 2000MB root.
```

7.1. введ логин vyos и пароль vyos

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

– Перейдите в режим конфигурирования:

vyos@vyos$ configure

vyos@vyos#

– Измените имя устройства (вместо user укажите 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.

– Задайте IP-адрес на интерфейсе eth0:

vyos@vyos# set interfaces ethernet eth0 address

↪ 192.168.1.1/24

– Посмотрите внесённые в конфигурацию изменения: vyos@vyos# compare

– Примените изменения в конфигурации и сохраните саму конфигурацию: vyos@vyos# commit vyos@vyos# save

– Посмотрите информацию об интерфейсах маршрутизатора: vyos@vyos# show interfaces

– Выйдете из режима конфигурирования: vyos@vyos# exit, vyos@vyos$

```
vyos@vyos:~$ configure
WARNING: You are currently configuring a live-ISO environment, changes will not persist until installed
[edit]
vyos@vyos# set system host-name msk-llll-gw-02
[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-llll-gw-02
[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:04:08:aa:00:00
 }
 ethernet eth1 {
     hw-id 0c:04:08:aa:00:01
 }
 ethernet eth2 {
     hw-id 0c:04:08:aa:00:02
 }
 loopback lo {
 }
[edit]
vyos@vyos#
```

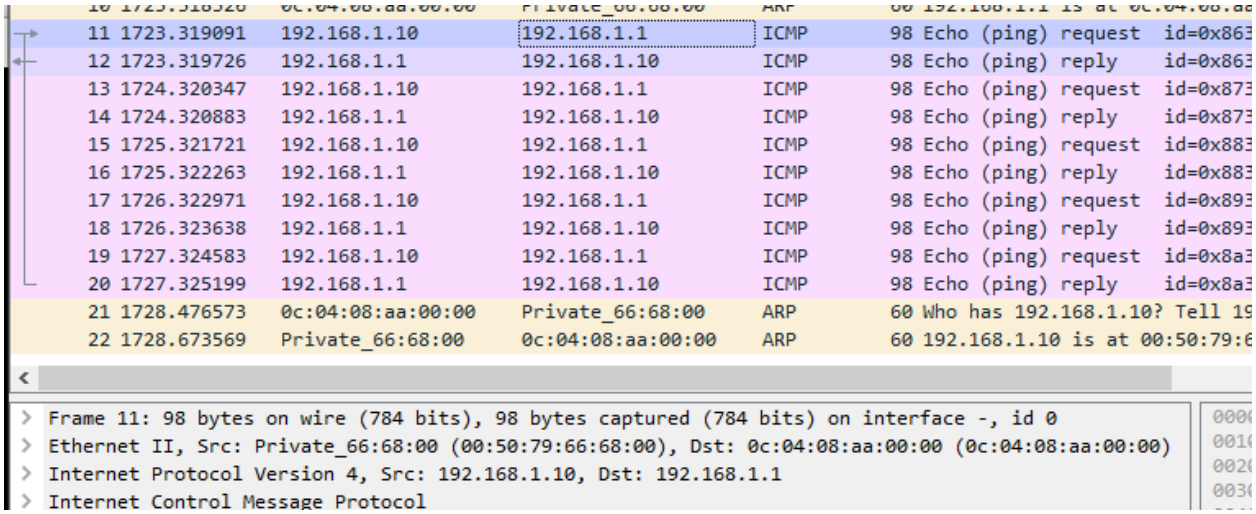
7.2. использование configure, interfaces Ethernet, compare etc.

8. Проверьте подключение. Узел PC1 должен успешно отправлять эхо-запросы на адрес маршрутизатора 192.168.1.1.

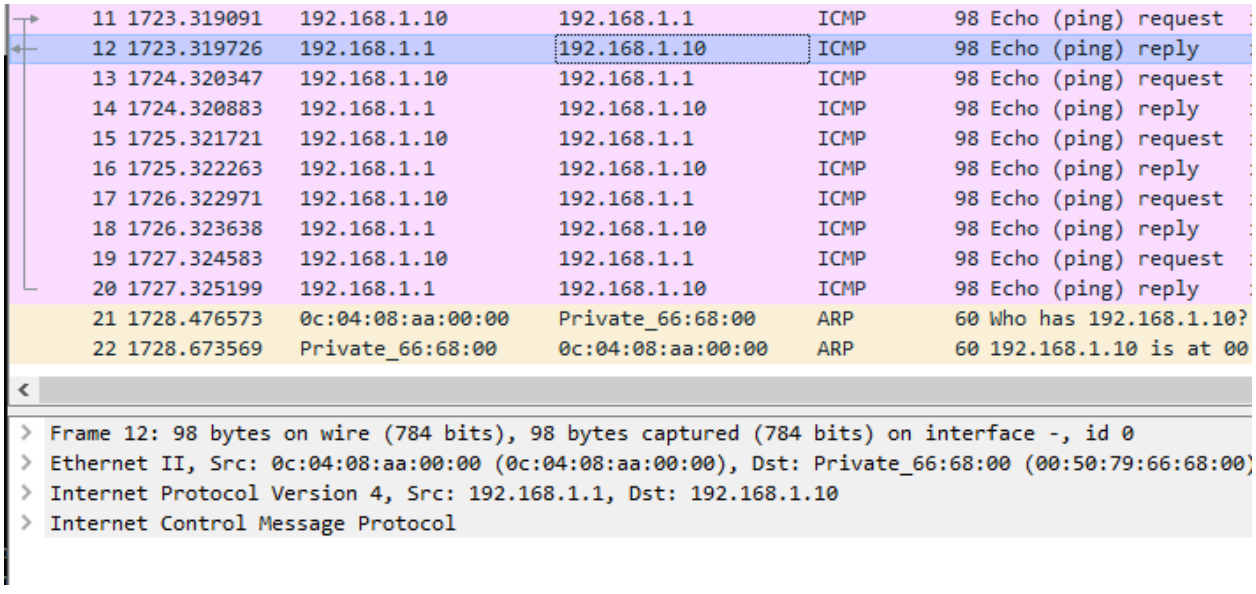
```
PC1> ping 192.168.1.1

84 bytes from 192.168.1.1 icmp_seq=1 ttl=64 time=0.766 ms
84 bytes from 192.168.1.1 icmp_seq=2 ttl=64 time=0.690 ms
84 bytes from 192.168.1.1 icmp_seq=3 ttl=64 time=0.704 ms
84 bytes from 192.168.1.1 icmp_seq=4 ttl=64 time=0.818 ms
84 bytes from 192.168.1.1 icmp_seq=5 ttl=64 time=0.779 ms

PC1>
```

8.1. Проверка подключения

9. В окне Wireshark проанализируйте полученную информацию, дайте пояснения в отчёте.



9.1.ICMP-request



9.2.*ICMP-reply*

В части запроса мы вводим IP-адрес назначения и IP-адрес источника. А в ответе - противоположность запросу. Мы также видим время общения.

Выводы

В этой лабораторной работе мы учимся строить простейшие сетевые модели на основе бесплатных коммутаторов и маршрутизаторов Ios в GNS3, анализ трафика с помощью Wireshark