Лабораторная работа № 5. Простые сети в GNS3. Анализ трафика

5.1. Цель работы

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

5.2. Предварительные сведения

5.2.1. Основные команды настройки маршрутизатора FRR

FRR — программный маршрутизатор с открытым исходным кодом.

Документация по настройке программного маршрутизатора FRR доступна на сайте `https://docs.frrouting.org/`.

Система команд в FRR похожа на систему команд, применяемую Cisco, поддерживает аббревиатуры для длинных команд и авто-заполнение/авто-подстановку с помощью клавиши Tab.

Для взаимодействия пользователя с демоном маршрутизации в FRR используется интерфейс командной строки (CLI) виртуального терминала (Virtual TeletYpe interface, VTY).

Три основных режима VTY:

- режим просмотра VTY (VTY View Mode) — предназначен для доступа к CLI только для чтения;
- режим включения VTY (VTY Enable Mode) — предназначен для чтения и записи в интерфейсе командной строки;
- другие режимы VTY (VTY Other Modes) — предназначен для описания других режимов.

Команды могут быть ограничены определенными режимами VTY.

Команды перемещения CLI:

- Ctrl + f/LEFT — переместиться вперед на один символ;
- Ctrl + b/RIGHT — перейти назад на один символ;
- Alt + f — переместиться вперед на одно слово;
- Alt + b — перейти назад на одно слово;
- Ctrl + a — Перейти к началу строки;
- Ctrl + e — переход к концу строки.

Расширенные команды CLI:

- Ctrl + c — прервать текущий ввод и перейти к следующей строке;
- Ctrl + z — завершите текущий сеанс настройки и перейдите к верхнему уровню иерархии;
- Ctrl + n/DOWN — перейти к следующей строке в буфере истории;

- Ctrl + p/UP — перейти к предыдущей строке в буфере истории;
- Tab — используется для завершения команды;
- ? — справка по командам, покажет возможные варианты завершения команды.

Основные команды настройки маршрутизатора, доступные в интерактивном режиме:

- `add` — добавить регистрацию;
- `clear` — сброс функций;
- `configure` — настроить конфигурацию из интерфейса vty;
- `copy` — копировать из одного файла в другой;
- `debug` — функции отладки;
- `disable` — отключить привилегированный режим;
- `enable` — включить привилегированный режим;
- `end` — завершить текущий режим и перейти в активный режим;
- `exit` — выйти из текущего режима и вернуться в предыдущий режим;
- `find` — найти команду CLI, соответствующую регулярному выражению;
- `graceful-restart` — команды Graceful Restart;
- `list` — распечатать список команд;
- `mtrace` — многоадресный маршрут трассировки к источнику многоадресной рассылки;
- `no` — отменить команду или установить ее значения по умолчанию;
- `output` — прямой вывод vtysh в файл;
- `ping` — отправить эхо-сообщение;
- `quit` — выход из текущего режима и переход в предыдущий режим;
- `rpki` — управление специфическими настройками rpki;
- `show` — показать информацию о работающей системе;
- `terminal` — установить параметры терминального соединения;
- `traceroute` — трассировка маршрута до пункта назначения;
- `watchfrr` — Watchfrr специальная подкоманда;
- `write` — запись текущей конфигурации в память, сеть или терминал.

Некоторые команды настройки маршрутизатора FRR, доступные в режиме конфигурации (после введения команды `configure`):

- `hostname имя_узла` — задать имя маршрутизатору;
- `domainname имя_домена` — задать название домена;
- `password пароль` — установить пароль для интерфейса vty;
- `enable password пароль` — установить пароль для режима включения vty;
- `service password-encryption` — зашифровать пароль;
- `line vty` — войти в режим конфигурации vty;
- `interface` — указать интерфейс для последующей настройки.

Пример присвоения интерфейсу eth0 IPv4-адреса, записи конфигурации в память маршрутизатора, просмотра текущей конфигурации и состояния интерфейсов:

```
frr# configure terminal
frr(config)# interface eth0
frr(config-if)# ip address 192.168.1.1/24
frr(config-if)# no shutdown
```

```
frr(config-if)# exit

frr(config)# exit
frr# write memory
frr# show running-config
frr# show interface brief
```

Пример присвоения интерфейсу eth0 IPv6-адреса, записи конфигурации в память маршрутизатора, просмотра текущей конфигурации и состояния интерфейсов:

```
frr# configure terminal
frr# interface eth0
frr(config-if)# ipv6 address 2001:db8:c0de:12::1/64
frr(config-if)# no ipv6 nd suppress-ra
frr(config-if)# ipv6 nd prefix 2001:db8:c0de:12::/64
frr(config-if)# no shutdown
frr(config-if)# exit
frr(config)# ipv6 forwarding
frr(config)# exit
frr# write memory
frr# show running-config
frr# show interface brief
```

5.2.2. Основные команды настройки маршрутизатора VyOS

VyOS — програмный маршрутизатор с открытым исходным кодом с одноимённой операционной системой на базе Debian. Документация по работе с VyOS доступна на сайте `https://docs.vyos.io/`.

Система команд в VyOS похожа на Juniper, поддерживает аббревиатуры для длинных команд и авто-заполнение/авто-подстановку с помощью клавиши Tab.

При первой загрузке маршрутизатора требуется установить образ системы:

- Ввести логин `vyos` и пароль `vyos`:
  ```
  vyos login: vyos
  Password:
  ```
- Установить систему на диск:
  ```
  vyos@vyos:~$ install image
  ```
  Далее приведён пример диалога установки, в котором в большинстве пунктов можно соглашаться с предлагаемыми по-умолчанию значениями, нажимая Enter:
  ```
  ...
  Would you like to continue? (Yes/No) [Yes]:
  ...
  Partition (Auto/Parted/Skip) [Auto]:
  ...
  Install the image on? [sda]:
  ...
  ```

```
Continue? (Yes/No) [No]: Yes
...
How big of a root partition should I create? (2000MB -
 ↪  8589MB) [8589]MB:
...
What would you like to name this image? [1.3.0-epa3]:
...
Which one should I copy to sda?
 ↪  [/opt/vyatta/etc/config/config.boot]:
...
Enter password for user 'vyos':
Retype password for user 'vyos':
...
Which drive should GRUB modify the boot partition on?
 ↪  [sda]:
...
Setting up grub: OK
Done!
```

– После завершения диалога систему следует перезагрузить командой `reboot`.

После описанной выше процедуры программные маршрутизатор готов к настройке и дальнейшему использованию.

Командный интерфейс (CLI) предоставляет встроенную справочную систему. В CLI клавиша ? может использоваться для отображения доступных команд. Прокручивать страницу с перечнем команд можно используя клавиши Shift+PageUp и Shift+PageDown.

При просмотре в страничном режиме доступны следующие команды:

– q может использоваться для отмены вывода;
– space прокрутит вниз одну страницу;
– b прокрутит назад на одну страницу;
– return прокрутит вниз на одну строку;
– up-arrow и down-arrow прокручивают вверх или вниз по одной строке за раз соответственно;
– left-arrow и right-arrow может использоваться для прокрутки влево или вправо, если на выходе есть строки, превышающие размер терминала.

Клавиша Tab может использоваться для автозавершения команд, а также для отображения справочной системы в случае конфликта или неизвестного значения команды.

VyOS имеет два режима:

– operational mode (рабочий режим) — в командной строке отображается символ $;
– configuration mode (режим настройки) — в командной строке отображается символ #.

Рабочий режим позволяет с помощью определённых команд просматривать состояние операционной системы и служб, выполнять некоторые задачи системы.

Команды, доступные в рабочем режиме (operational mode):

- `add` — добавить объект в сервис;
- `clear` — очистить системную информацию;
- `clone` — клонировать объект;
- `configure` — войти в режим настройки;
- `connect` — установить соединение;
- `copy` — копировать объект;
- `delete` — удалить объект;
- `disconnect` — разорвать соединение;
- `force` — форсировать операцию;
- `format` — форматирование устройства;
- `generate` — генерировать объект;
- `install` — установить новую систему;
- `monitor` — просмотр информации о системе;
- `ping` — отправить эхо-запрос протокола управляющих сообщений Интернета (ICMP);
- `poweroff` — выключить систему;
- `reboot` — перезагрузить систему;
- `release` — освободить указанную переменную;
- `rename` — переименовать объект;
- `renew` — обновить указанную переменную;
- `reset` — сбросить службу;
- `restart` — перезапустить отдельную службу;
- `set` — установить параметры;
- `show` — показать системную информацию;
- `telnet` — использовать Telnet-соединение для доступа к некоторому узлу;
- `traceroute` — отслеживание сетевого пути к узлу;
- `update` — обновить данные для службы;
- `wake-on-LAN` — Отправка пакета Wake-On-LAN (WOL).

Команды, доступные в режиме настройки (configuration mode):

- `confirm` — подтвердить предыдущую фиксацию-подтверждение;
- `comment` — добавить комментарий к элементу конфигурации;
- `commit` — зафиксировать текущий набор изменений;
- `commit-confirm` — зафиксировать текущий набор изменений с обязательным «подтверждением»;
- `compare` — сравнить версии конфигурации;
- `copy` — копировать элемент конфигурации;
- `delete` — удалить элемент конфигурации;
- `discard` — отменить незафиксированные изменения;
- `edit` — редактировать подэлемент;
- `exit` — выход из этого уровня конфигурации;
- `load` — загрузить конфигурацию из файла и заменить текущую конфигурацию;
- `loadkey` — загрузить пользовательский SSH-ключ из файла;

- `merge` — Загрузить конфигурацию из файла и объединить с текущей конфигурацией;
- `rename` — переименовать элемент конфигурации;
- `rollback` — откатить к предыдущей версии конфигурации (требуется перезагрузка);
- `run` — запустить команду в рабочем режиме (operational-mode);
- `save` — сохранить конфигурацию в файл;
- `set` — установить значение параметра или создать новый элемент;
- `show` — показать конфигурацию (значения по умолчанию могут быть скрыты).

VyOS использует единый файл конфигурации `/config/config.boot`, содержащий все настройки системы. Это позволяет создавать шаблоны, делать резервные копии и копировать конфигурацию системы.

Система VyOS имеет три типа конфигураций:

- *Активная конфигурация (active/running configuration)* — это конфигурация системы, которая загружена и активна в данный момент (используется VyOS). Любое изменение в конфигурации должно быть зафиксировано, чтобы принадлежать к активной/работающей конфигурации.
- *Рабочая конфигурация (working configuration)* — это та конфигурация, которая в данный момент модифицируется в режиме конфигурации. Изменения, внесенные в рабочую конфигурацию, не вступают в силу до тех пор, пока изменения не будут зафиксированы с помощью команды `commit`. В это время рабочая конфигурация станет активной или рабочей конфигурацией.
- *Сохранённая конфигурация (saved configuration)* — это конфигурация, сохраненная в файл с помощью команды `save`. Может быть несколько файлов конфигурации. Конфигурация по умолчанию (или «загрузочная») сохраняется и загружается из файла `/config/config.boot`.

Просмотреть текущую активную конфигурацию можно с помощью команды:

```
vyos@vyos:~$ show configuration
```

Просмотреть перечень команд системы, которые привели к работающей конфигурации, можно с помощью следующей команды:

```
vyos@vyos:~$ show configuration commands
```

При входе в режим конфигурации вы перемещаетесь внутри древовидной структуры, все выполняемые в этом режиме команды относятся к введённому вами уровню конфигурации. Можно выполнять команды с верхнего уровня, но команды будут довольно длинными при их ручном вводе. Текущий уровень иерархии может быть изменен командой `edit`, а все команды, выполняемые с этого момента, относятся к этому подуровню.

Примеры идентичных по смыслу команд установки ip-адреса для интерфейса eth0:

```
vyos@vyos# set interfaces ethernet eth0 address
  ↪  192.168.10.10/24
```

или

```
vyos@vyos# edit interfaces ethernet eth0

[edit interfaces ethernet eth0] address 192.168.10.10/24
```

Для перемещения по уровням иерархии можно использовать команды `up`, `top`, `exit`.

Конфигурацию можно редактировать с помощью команд `set` и `delete` в режиме конфигурации.

Пример установки ip-адреса для интерфейса eth0:

```
vyos@vyos# set interfaces ethernet eth0 address
  ↪ 192.168.10.11/24
```

Пример отмены (удаления) установки ip-адреса для интерфейса eth0:

```
vyos@vyos# delete interfaces ethernet eth0 address
  ↪ 192.168.10.11/24
```

или

```
vyos@vyos# edit interfaces ethernet eth0

[edit interfaces ethernet eth0] delete address
  ↪ 192.168.10.11/24
```

Любые изменения, которые вы делаете в конфигурации, не вступят в силу, пока не будут зафиксированы с помощью команды `commit` в режиме конфигурации. Чтобы сохранить изменения конфигурации после перезагрузки, требуется использовать команду `save`. Чтобы выйти из режима конфигурации без применения изменений, необходимо использовать команду `exit discard`. При этом все изменения в рабочем конфиге будут потеряны.

5.3. Задания для выполнения

5.3.1. Моделирование простейшей сети на базе коммутатора в GNS3

5.3.1.1. Постановка задачи

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.

5.3.1.2. Порядок выполнения работы

1. Запустите GNS3 VM и GNS3. Создайте новый проект.
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 (рис. 5.1).

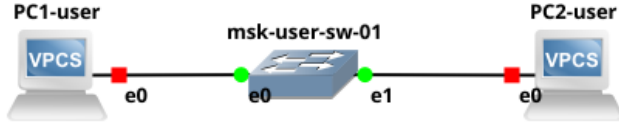

Рис. 5.1. Топология простейшей сети в GNS3

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 /? (рис. 5.2).

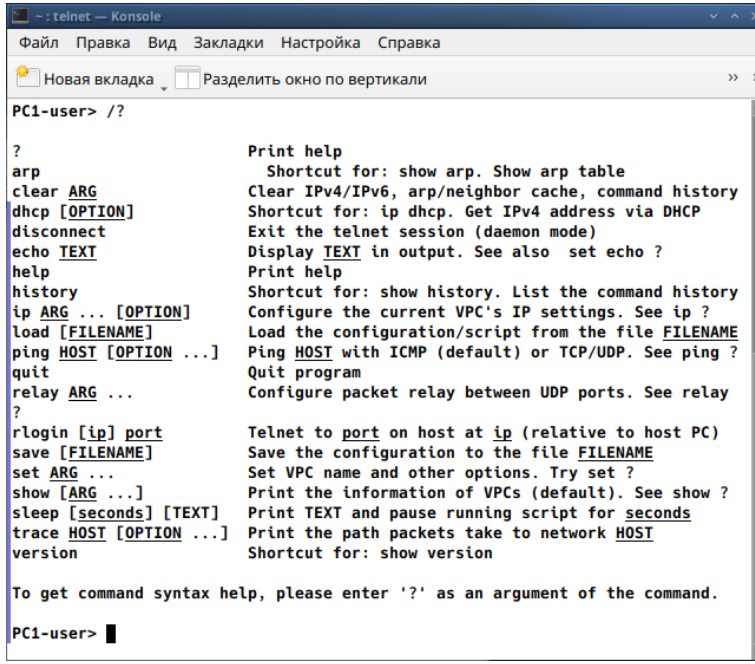

Рис. 5.2. Просмотр синтаксиса возможных для ввода команд VPCS в GNS3

Для задания IP-адреса 192.168.1.11 в сети 192.168.1.0/24 введите (рис. 5.3):

```
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`.

```
PC1-user>  ip 192.168.1.11/24 192.168.1.1
Checking for duplicate address...
PC1-user : 192.168.1.11 255.255.255.0 gateway 192.168.1.1

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

PC1-user>
```

Рис. 5.3. Задание IP-адреса и сохранение конфигурации VPCS в GNS3

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

5.3.2. Анализ трафика в GNS3 посредством Wireshark

5.3.2.1. Постановка задачи

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

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.
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.
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.
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.

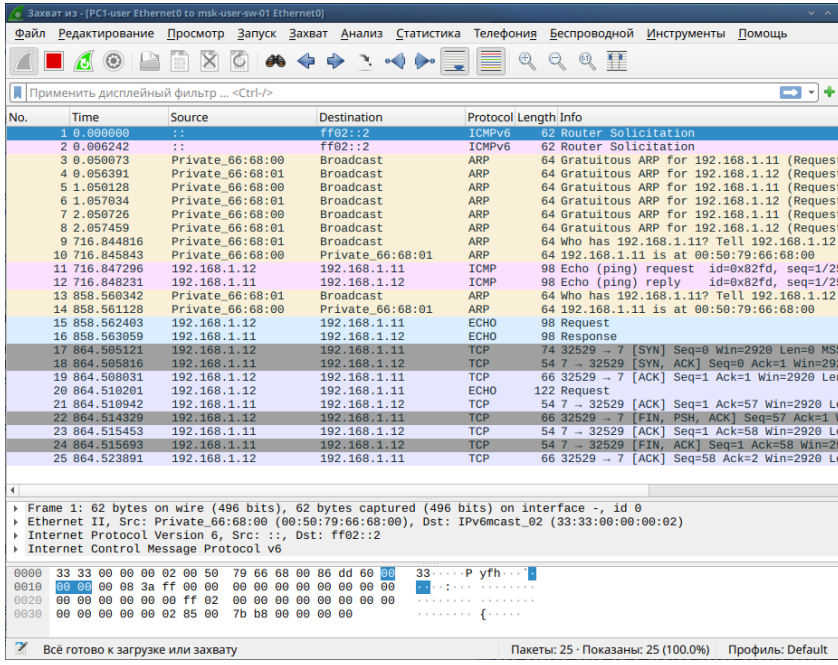

Рис. 5.4. Полученная в Wireshark информация по ARP- и ICMP-сообщениям

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).

Рис. 5.5. Топология простейшей сети с маршрутизатором в GNS3

3. Измените отображаемые названия устройств. Коммутатору присвойте название по принципу `msk-user-sw-0x`, маршрутизатору — по принципу `msk-user-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.
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
```
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
```
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 маршрутизатор VyOS (рис. 5.6).

Рис. 5.6. Топология простейшей сети с маршрутизатором в GNS3

3. Измените отображаемые названия устройств. Коммутатору присвойте название по принципу `msk-user-sw-0x`, маршрутизатору — по принципу `msk-user-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.
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
```
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
```
     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$
```

8. Проверьте подключение. Узел PC1 должен успешно отправлять эхо-запросы на адрес маршрутизатора 192.168.1.1.
9. В окне Wireshark проанализируйте полученную информацию, дайте пояснения в отчёте.
10. Остановите захват пакетов в Wireshark. Остановите все устройства в проекте. Завершите работу с GNS3.

5.4. Содержание отчёта

1. Титульный лист с указанием номера лабораторной работы и ФИО студента.
2. Формулировка задания работы.
3. Описание результатов выполнения задания:
   - скриншоты (снимки экрана), фиксирующие выполнение лабораторной работы;
   - пояснения по отображаемой информации согласно заданию
4. Выводы, согласованные с заданием работы.