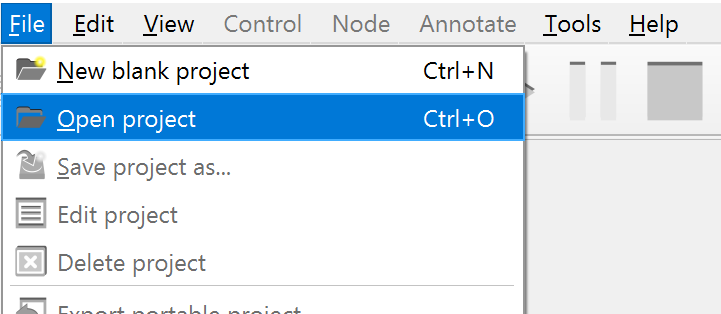
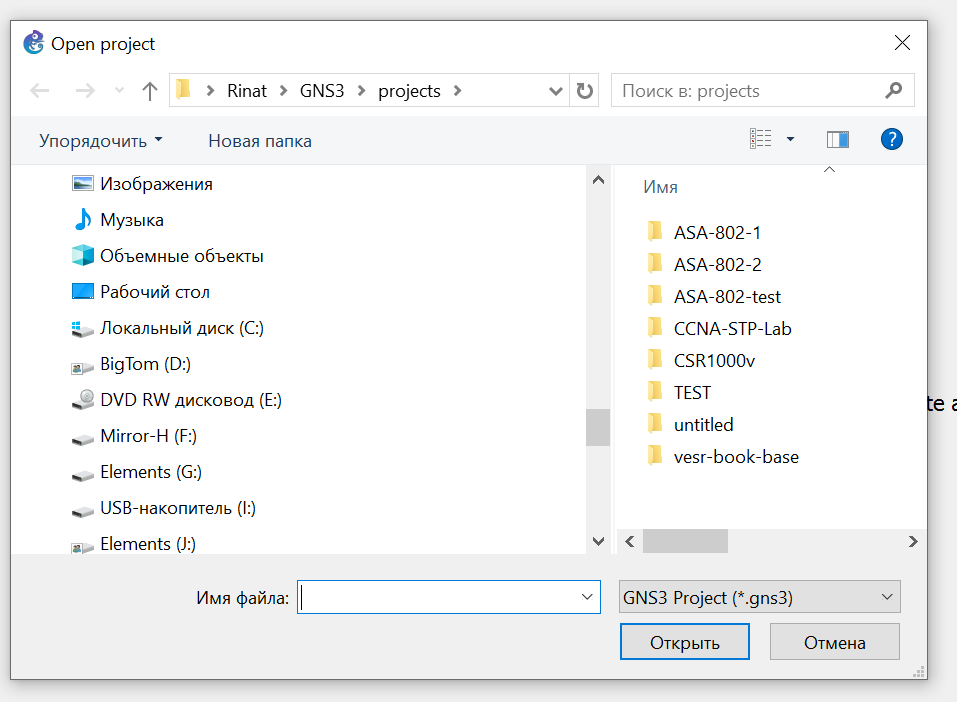
Глава 4. Базовая настройка vESR.

Продолжаем изучать возможности виртуального маршрутизатора vESR.

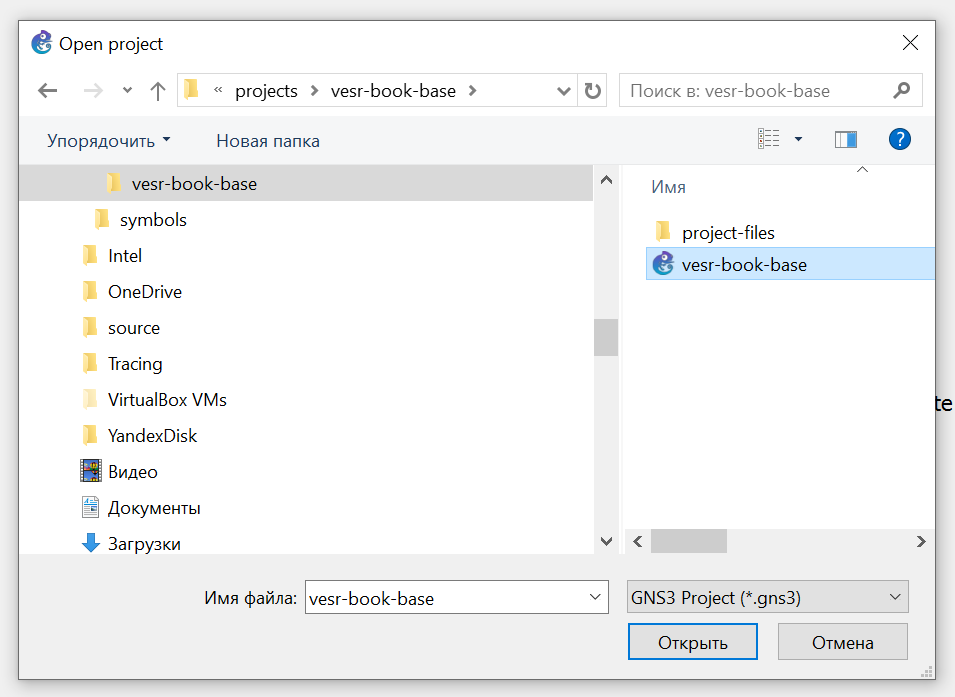
В программе GNS3 после запуска и спустя некоторое время , предназначенное для запуска виртуальной машины ( признаком успешного старта будет появление на некоторое время в верхнем левом углу панели программы зеленого информационного табло) открываем папку с проектом vesr-book-base следую последовательности нажатий клавиш на пунктах меню “File”-“Open Project”



Откроется папка на диске настроенная по умолчанию на диске на который вы поместили программу GNS3 при установке , например такая:

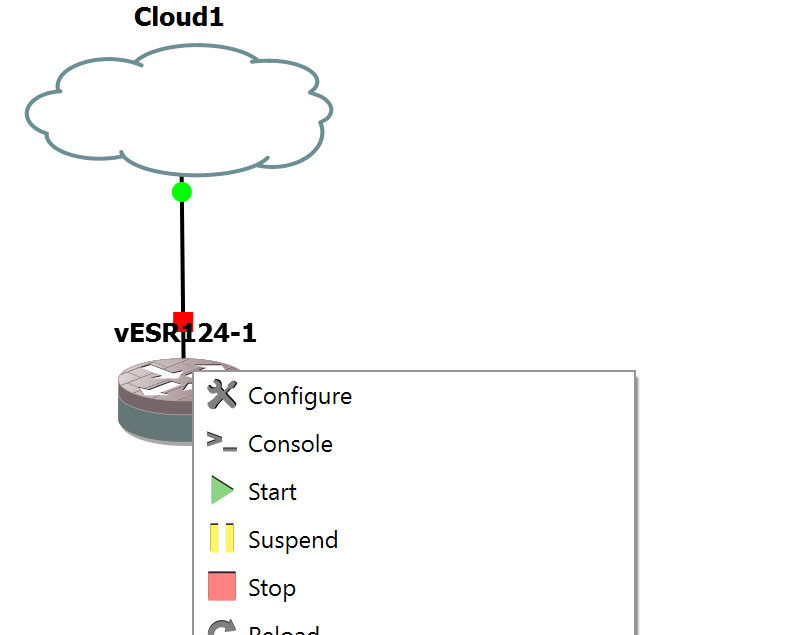


Для открытия проекта выбираете мышью vesr-book-base и нажимаете на «Открыть».



Такой же эффект можно получить просто нажав курсором мыши на иконку открытой папки на навигационной панели GNS3.

Наводим курсор мыши на иконку маршрутизатора, нажимаем правую кнопку мыши и затем еще раз нажимаем на зеленый треугольник для старта нашего устройства.

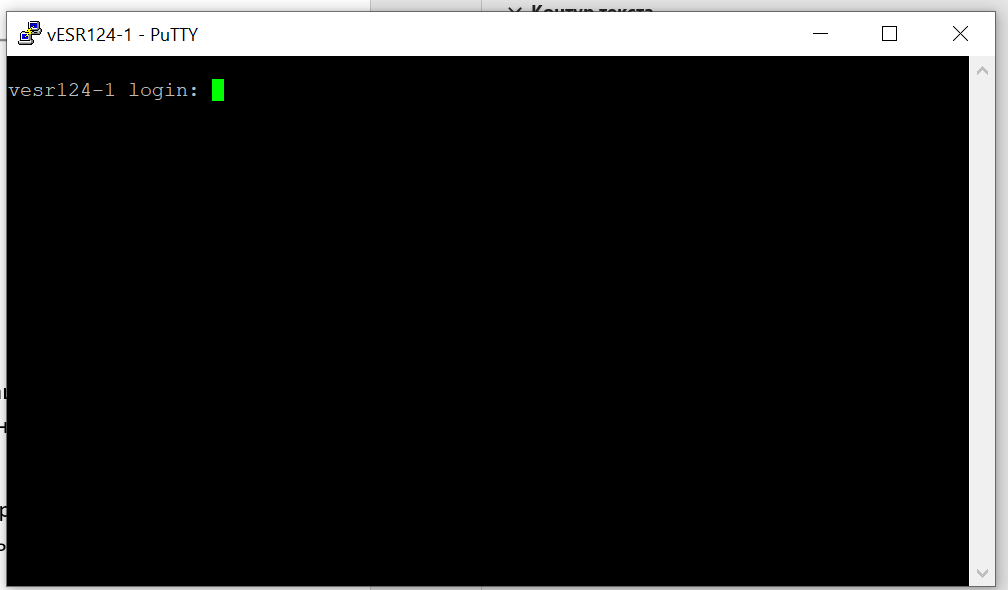


Запускается консоль Putty ( вы же при начальной конфигурации маршрутизатора в первой главе не забыли поставить галочку , указывающую на автоматический старт консоли?).

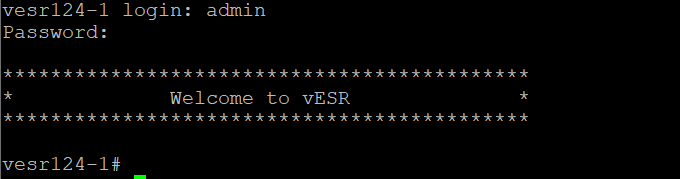
Ждем некоторое время – на моем домашнем ПК с 32 Гб и процессором 12th Gen Intel(R) Core(TM) i5-12500 3.00 GHz оно равно более минуты.

Если через более продолжительное время вы не получили приглашение в консоли на ввод логины, то вам следует вернуться к первоначальной установке маршрутизатора ( измените тип консоли на VNC, чтобы увидеть процесс первоначальной загрузки, возможно там будут диагностические сообщения с подсказками).

И так вы в консоли- что дальше? Вводите логин-admin и пароль- eve ( его мы установили на этапе первоначальной настройки).



Vesr124-1 login: admin



Процедура базовой настройки маршрутизатора состоит из следующих этапов:

* Создание новых пользователей
* Назначение имени устройства
* Установка параметров подключения к публичной сети (WAN) и локальной сети (LAN)
* Настройка проверки связности через ICMP

**Создание новых пользователей**

Для создания нового пользователя системы или настройки любого из параметров: имени пользователя, пароля, уровня привилегий, – используются команды:

username <name>

password <password>

privilege <privilege>

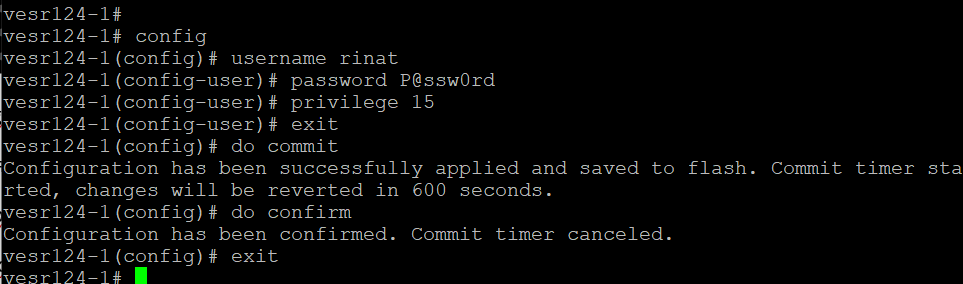
exit

**где:**

* **<name>** - имя нового пользователя;
* **<password>** - пароль для нового пользователя
* **<privilege>** - № от 1 до 15
  + Уровни привилегий 1-9 разрешают доступ к устройству и просмотр его оперативного состояния, но запрещают настройку. Уровни привилегий 10-14 разрешают как доступ, так и настройку большей части функций устройства. Уровень привилегий 15 разрешает как доступ, так и настройку всех функций устройства.

Пример:

* создание пользователя "Rinat" с паролем "P@ssw0rd" и максимальными привилегиями (15)

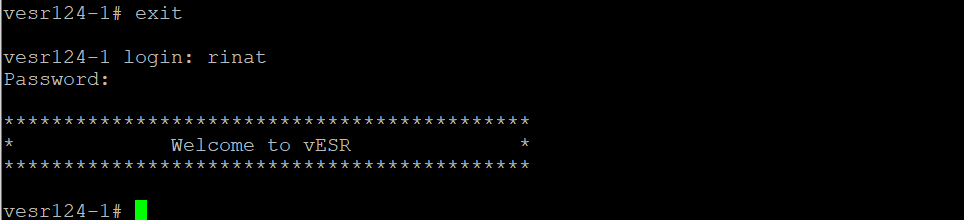


Для применения настроек:

do commit

do confirm

Проверка входа из под пользователя "rinat":



**Назначение имени устройства**

Для назначения имени устройства используются следующие команды:

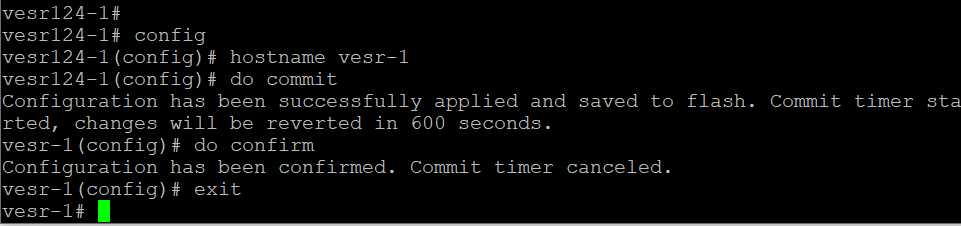
configure

hostname <new-name>

**где:**

* **<net-name>** - имя устройства

Например: изменим имя устройства на vesr-1



Готово!

**Установка параметров подключения к публичной сети (WAN) и локальной сети (LAN)**

Для настройки сетевого интерфейса маршрутизатора в публичной сети (WAN) необходимо назначить устройству параметры, определённые провайдером сети – IP-адрес, маска подсети и адрес шлюза по умолчанию.

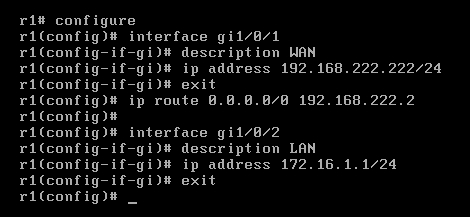
Например:

Параметры интерфейса - gi1/0/1 (WAN):

* IP-адрес: 192.168.222.222/24
* Gateway: 192.168.222.2

Параметры интерфейса - gi1/0/2 (LAN):

* IP-адрес: 172.16.1.1/24



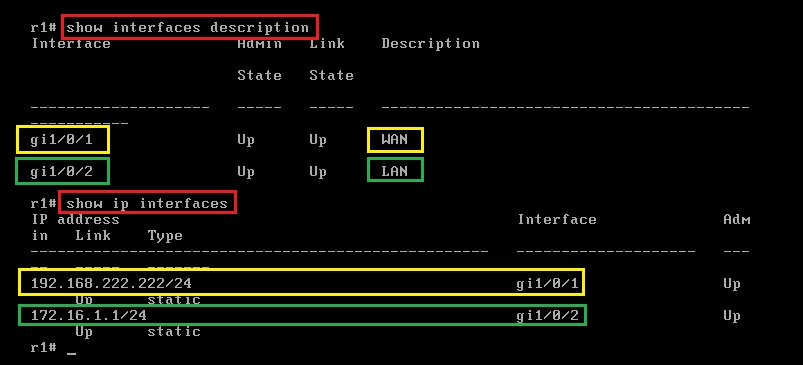
img

Проверка назначения сетевых параметров:

Copy

show interfaces description

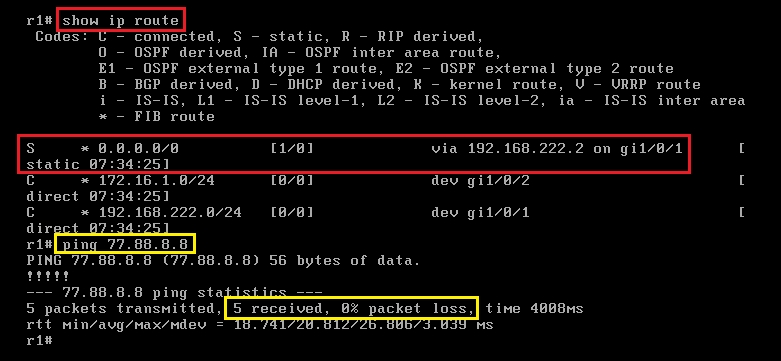
show ip interfaces



img

Copy

show ip route



img

**Настройка проверки связности через ICMP**

Firewall – комплекс аппаратных или программных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов в соответствии с заданными правилами.

Из коробки firewall - включён, но не содержит никаких правил, а значит ничего и не разрешает

Порядок обработки трафика терминируемого (направленного непосредственно на сам маршрутизатор, но не через его интерфейсы) на маршрутизаторе:

* Трафик проверяется правилами zone-pair any self. Если трафик не попал ни под одно из правил текущей zone-pair, переходим к следующему шагу
* Трафик проверяется правилами zone-pair src-zone-name self. Если трафик не попал ни под одно из правил текущей zone-pair, он отбрасывается.

Каждая команда «match» может содержать ключ «not». При использовании данного ключа под правило будут подпадать пакеты, не удовлетворяющие заданному критерию.

На маршрутизаторе всегда существует зона безопасности с именем «self». Если в качестве получателя трафика выступает сам маршрутизатор, то есть трафик не является транзитным, то в качестве параметра указывается зона «self»

Для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «LAN»:

Создание зоны безопасности:

Copy

security zone <NAME\_ZONE>

exit

Добавление интерфейса в зону безопасности:

Copy

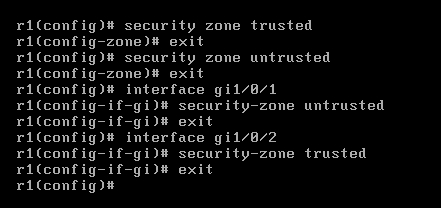
interface <№\_INT>

security-zone <NAME\_ZONE>

exit

Например:

* Создадим две зоны "trusted" для интерфейса смотрязего в LAN, и зону "untrusted" для интерфейса смотрящего в WAN
  + поместим соответствующие интерфейсы в зоны:



img

Для применения настроек:

Copy

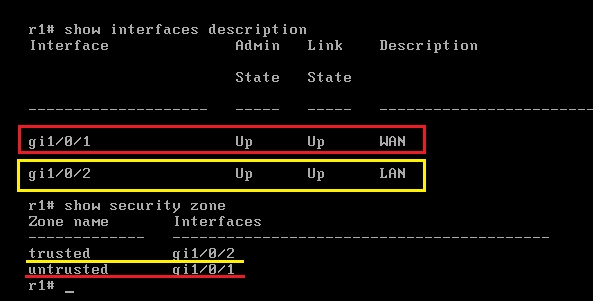
do commit

do confirm

Проверка:

Copy

show security zone



img

Для настройки правил зон безопасности потребуется создать профиль адресов сети «LAN», включающий адреса, которым разрешен доступ к маршрутизатору:

Создание профиля адесов сети:

Copy

object-group network <NAME\_PROFILE>

ip address-range <IP\_RANGE | IP\_ADDRESS>

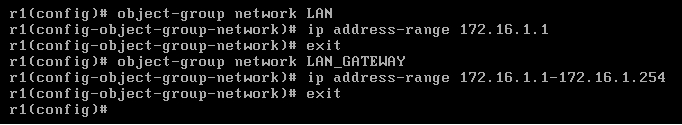
exit

**где:**

* **<NAME\_PROFILE>** - имя профиля адресов сети
* **<IP\_RANGE | IP\_ADDRESS>** - диапазон IP-адресов записаный через "-" (дефис) или IP-адрес

Например:

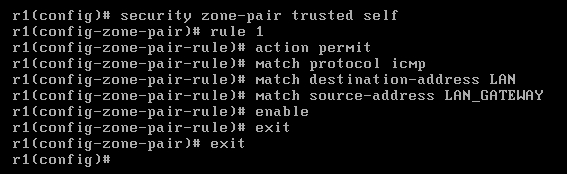
* создадим профиль "LAN" в котором укажем IP-адрес маршрутизатора интерфейса, который смотрит в LAN;
* создадим профиль "LAN\_GATEWAY" в котором укажем диапазон IP-адресов из сети LAN



img

Добавим правило, разрешающее проходить ICMP-трафику между маршрутизатором и клиентами, для того чтобы маршрутизатор начал отвечать на ICMP-запросы из зоны «trusted» - т.е. из локальной сети (LAN)

* Создадим пару зон для трафика, идущего из зоны «trusted» в зону «self»
* Действие правил разрешается командой **enable**



img

**где:**

* **<destination-address>** - ссылается на профиль адресов сети "LAN", в котором указан IP-адрес маршрутизатора;
* **<source-address>** - ссылается на профиль адресов сети "LAN\_GATEWAY", в котором указан диапазон IP-адресов сети LAN;

Для применения настроек:

Copy

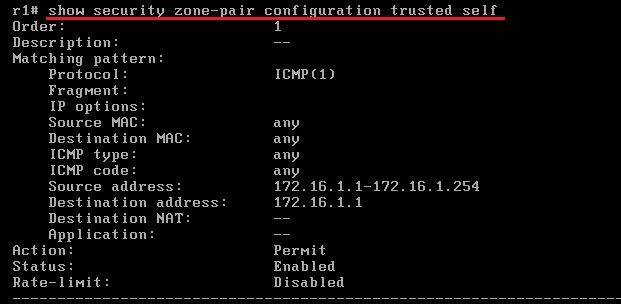
do commit

do confirm

Проверка:

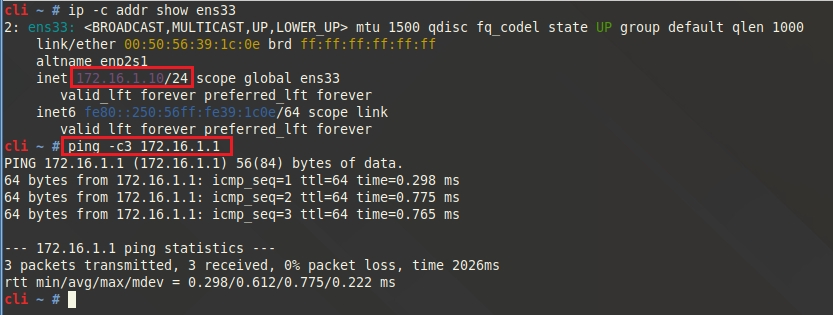
Copy

show security zone-pair configuration trusted self



img

Проверка связности с клиента из сети LAN с маршрутизатором:



img