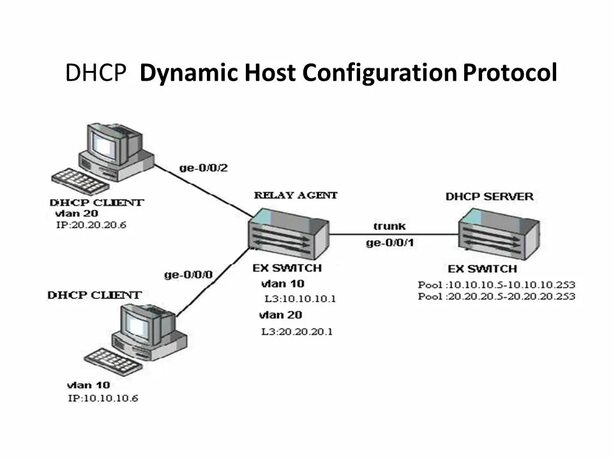
1. Настройка сервера DHCP в маршрутизаторе vESR.

**Что такое DHCP? DHCP (Dynamic Host Configuration Protocol) — это сетевой протокол, который автоматически назначает IP-адреса и другие сетевые параметры устройствам в сети.**

**Основная задача DHCP — упростить управление сетью, избавив администраторов от необходимости вручную настраивать IP-адреса для каждого устройства.**

****

**Принцип работы DHCP**

**Работа DHCP основана на взаимодействии между DHCP-клиентом (устройство, подключающееся к сети) и DHCP-сервером (устройство или сервис, управляющий распределением IP-адресов).**

**Процесс состоит из четырёх основных этапов:**

1. **DHCP Discover (Обнаружение). Устройство отправляет широковещательный запрос, пытаясь найти DHCP-сервер.**
2. **DHCP Offer (Предложение). Сервер отвечает пакетом DHCP Offer, предлагая свободный IP-адрес из своего пула адресов вместе с другими сетевыми параметрами.**
3. **DHCP Request (Запрос). Клиент получает предложение и отвечает серверу сообщением DHCP Request, подтверждая готовность принять предложенные параметры.**
4. **DHCP Acknowledgment (Подтверждение). Сервер подтверждает назначение IP-адреса и отправляет клиенту окончательные параметры. После этого устройство может полноценно работать в сети.**

**Преимущества и недостатки**

**Преимущества DHCP:**

* **автоматизация настройки сетевых параметров;**[**ServerGate.ru**](https://servergate.ru/articles/dhcp-prosto-o-slozhnom-chto-eto-takoe-i-kak-on-rabotaet-v-vashey-seti/)[**mksegment.ru**](https://mksegment.ru/b/vazhnost-dhcp-v-kompyuternyh-setyah-i-ego-osnovnye-funkcii)
* **предотвращение конфликтов IP-адресов;**[**help.sweb.ru**](https://help.sweb.ru/protokol-dhcp_1380.html)[**mksegment.ru**](https://mksegment.ru/b/vazhnost-dhcp-v-kompyuternyh-setyah-i-ego-osnovnye-funkcii)
* **снижение нагрузки на сеть за счёт использования временных IP-адресов.**

**Недостатки DHCP:**

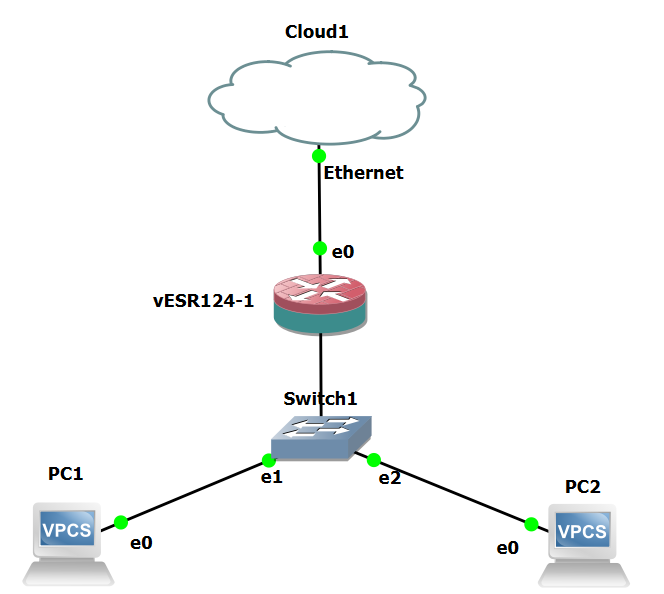
* **если DHCP-сервер выходит из строя, новые устройства не смогут получить IP-адреса и подключиться к сети;**
* **DHCP-сообщения передаются в незашифрованном виде, что делает их уязвимыми для атак;**
* **злоумышленник может настроить несанкционированный DHCP-сервер, который будет выдавать ложные IP-адреса.**

**Где используется**

**DHCP применяется в различных типах сетей — в домашних и корпоративных. Некоторые устройства, которые используют DHCP:**

* **компьютеры и ноутбуки;**
* **смартфоны и планшеты;**
* **умные устройства (камеры наблюдения, термостаты, холодильники);**
* **сетевое оборудование (маршрутизаторы, коммутаторы).**

**Добавим в нашу схему еще один виртуальный персональный компьютер, используя методы , описанные в предыдущей главе.**



Нам нужно настроить работу DHCP-сервера на базе виртуального маршрутизатора vesr-1. Задать пул IP-адресов из подсети 172.16.1.0/24 для раздачи клиентам. Для PC1 зарезервировать выдачу следующего IP-адреса 172.16.1.100, а для **PC2** зарезервировать выдачу следующего IP-адреса 172.16.1.200, а и задать время аренды адресов 3 дня. Настроить передачу клиентам маршрута по умолчанию, доменного имени и адресов DNS-серверов с помощью DHCP-опций.

1. Назначаем IP-адреса на интерфейсы:

Выполняемые команды в консоли виртуального маршрутизатора vesr-1:

configure

* на интерфейс смотрящий в сторону глобальной сети получаем сетевые параметры по DHCP

interface gi1/0/1

description connection\_WAN

ip address dhcp

exit

* на интерфейс смотрящий в сторону rtr1 и rtr2 назначаем статический адрес из подсети 172.16.1.1/24

interface gi1/0/2

description connection\_LAN

ip address 172.16.1.1/24

exit

1. Создадим зону безопасности **«trusted»** и установим принадлежность интерфейса **gi1/0/2** (смотрящего в подсеть rtr1 и rtr2) такими командами:

security zone trusted

exit

interface gi1/0/2

security-zone trusted

exit

do commit

do confirm

Вывод текущего конфига из консоли vesr-1:

vesr-1# sh running-config

hostname vesr-1

object-group network LAN

ip address-range 172.16.1.1

exit

object-group network LAN\_GATEWAY

ip address-range 172.16.1.1-172.16.1.254

exit

syslog max-files 3

syslog file-size 512

syslog file tmpsys:syslog/default

severity info

exit

syslog console

virtual-serial

exit

username admin

password encrypted $6$kx1jB3DT6zH05CQ7$WqbKGSvl/35jvx.NKDc6R5NpD5uy2623zfbWAOTPhNOQgnR.zXxQzlgYwESdboxOWSyhPPNojy0Q0.pMvR6Ld/

exit

username rinat

password encrypted $6$1wbeF/CqjcFAJrob$thjkqaTLACQVWN1bRbqzFUbO5VL24jbWHbLD2ZOXbphb.CoI7n8k3rj3j1x79RDqOLDfj2IAnECPPYIR4tmci1

privilege 15

exit

domain lookup enable

**security zone trusted**

**exit**

**security zone untrusted**

**exit**

**interface gigabitethernet 1/0/1**

**description "WAN"**

**security-zone untrusted**

**ip address dhcp**

**exit**

**interface gigabitethernet 1/0/2**

**description "LAN"**

**security-zone trusted**

**ip address 172.16.1.1/24**

**exit**

**security zone-pair trusted self**

**rule 1**

**action permit**

**match protocol icmp**

**match destination-address object-group LAN\_GATEWAY**

**enable**

**exit**

exit

security passwords default-expired

ip ssh server

ntp enable

ntp broadcast-client enable

licence-manager

host address elm.eltex-co.ru

exit

vesr-1#

Прмечание: эти шаги мы уже сделали в предыдущей главе- смотри Рис. Введенные команды в тексте выведенного конфига выделены цветом и обведены рамкой.

1. Создадим пул адресов с именем «COMPANY» и добавим в данный пул адресов диапазон IP-адресов для выдачи в аренду клиентам сервера. Укажем параметры подсети, к которой принадлежит данный пул, и время аренды для выдаваемых адресов выполнив команды:

config

ip dhcp-server pool COMPANY

network 172.16.1.0/24

default-lease-time 3:00:00

address-range 172.16.1.1-172.16.1.254

excluded-address-range 172.16.1.1 # исключаем первый адрес из выдачи

excluded-address-range 172.16.1254 # исключаем последний адрес из выдачи

address 172.16.1.100 mac-address 00:50:79:66:68:00 # MAC-адрес PC1

address 172.16.1.200 mac-address 00:50:79:66:68:01 # MAC-адрес PC2

default-router 172.16.1.1 # в качестве шлюза будет выдан IP-адрес интерфейса gi1/0/2

default-server 77.88.8.8 # в качестве DNS-сервера будет выдан IP-адрес 77.88.8.8

exit

do commit

do confirm

esr-1# config

vesr-1(config)# ip dhcp-server pool COMPANY

vesr-1(config-dhcp-server)# network 172.16.1.0/24

vesr-1(config-dhcp-server)# default-lease-time 3:00:00

vesr-1(config-dhcp-server)# address-range 172.16.1.1-172.16.1.254

vesr-1(config-dhcp-server)# excluded-address-range 172.16.1.1

vesr-1(config-dhcp-server)# excluded-address-range 172.16.1.254

vesr-1(config-dhcp-server)# address 172.16.1.100 mac-address 00:50:79:66:68:00

vesr-1(config-dhcp-server)# address 172.16.1.200 mac-address 00:50:79:66:68:01

vesr-1(config-dhcp-server)# default-router 172.16.1.1

vesr-1(config-dhcp-server)# dns-server 77.88.8.8

vesr-1(config-dhcp-server)# exit

vesr-1(config)# do commit

Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.

2025-05-29T18:28:39+00:00 %CLI-I-CRIT: user admin from console input: do commit

vesr-1(config)# do confirm

Configuration has been confirmed. Commit timer canceled.

2025-05-29T18:28:44+00:00 %CLI-I-CRIT: user admin from console input: do confirm

vesr-1(config)# exit

vesr-1#

МАС адреса виртуальных ПУ нужно взять дав команды sh ip и скопировав значения МАС адресов консолях этих ПКБ благо это делается простым вырезанием курсором мыши и нажатием сочетаний клавиш Ctrl+Insert, вставка в окно терминала соотвественно Shift+Insert :

**PC1**> sh ip

NAME : PC1[1]

IP/MASK : 0.0.0.0/0

GATEWAY : 0.0.0.0

DNS :

**MAC : 00:50:79:66:68:00**

LPORT : 13006

RHOST:PORT : 127.0.0.1:13007

MTU: : 1500

**PC2**> sh ip

NAME : PC2[1]

IP/MASK : 0.0.0.0/0

GATEWAY : 0.0.0.0

DNS :

**MAC : 00:50:79:66:68:01**

LPORT : 13008

RHOST:PORT : 127.0.0.1:13009

MTU: : 1500

1. Для разрешения прохождения сообщений протокола DHCP к серверу необходимо создать соответствующие профили портов, включающие порт источника 68 и порт назначения 67, используемые протоколом DHCP, и создать разрешающее правило в политике безопасности для прохождения пакетов протокола UDP используем набор команд :

config

object-group service dhcp\_server

port-range 67

exit

object-group service dhcp\_client

port-range 68

exit

do commit

do confirm

do show running-config

Протокол работы в консоли в режиме конфигурации:

vesr-1(config)# object-group service dhcp\_service

vesr-1(config-object-group-service)# port-range 67

vesr-1(config-object-group-service)# exit

vesr-1(config)# object-group service dhcp\_client

vesr-1(config-object-group-service)# port-range 68

vesr-1(config-object-group-service)# exit

vesr-1(config)# do commit

Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.

2025-05-29T18:47:10+00:00 %CLI-I-CRIT: user admin from console input: do commit

vesr-1(config)# do confirm

Configuration has been confirmed. Commit timer canceled.

2025-05-29T18:47:15+00:00 %CLI-I-CRIT: user admin from console input: do confirm

vesr-1(config)# do show running-config

hostname vesr-1

object-group service dhcp\_service

port-range 67

exit

object-group service dhcp\_client

port-range 68

exit

У нас уже ранее в предыдущей главе было содано одно правило для пропуска пингов файрволом.

security zone-pair trusted self

rule 1

action permit

match protocol icmp

match destination-address object-group LAN\_GATEWAY

enable

Теперь нужно добавить еще одно для пропуска пакектов протокола DHCP:

config

security zone-pair trusted self

rule 2

match protocol udp

match source-port dhcp\_client

match destination-port dhcp\_server

action permit

enable

exit

exit

vesr-1# config

vesr-1(config)# security zone-pair trusted self

vesr-1(config-security-zone-pair)# rule 2

vesr-1(config-security-zone-pair-rule)# match protocol udp

vesr-1(config-security-zone-pair-rule)# match source-port object-group dhcp\_client

vesr-1(config-security-zone-pair-rule)# match destination-port object-group dhcp\_service

vesr-1(config-security-zone-pair-rule)# action permit

vesr-1(config-security-zone-pair-rule)# enable

vesr-1(config-security-zone-pair-rule)# exit

vesr-1(config-security-zone-pair)# exit

vesr-1(config)# exit

Warning: you have uncommitted configuration changes.

vesr-1# commit

Configuration has been successfully applied and saved to flash. Commit timer started, changes will be reverted in 600 seconds.

2025-05-29T19:00:58+00:00 %CLI-I-CRIT: user admin from console input: commit

vesr-1# confirm

Configuration has been confirmed. Commit timer canceled.

2025-05-29T19:01:01+00:00 %CLI-I-CRIT: user admin from console input: confirm

vesr-1#

1. Разрешим работу сервера:

Copy

ip dhcp-server

Copy

do commit

do confirm

vesr-1# config

vesr-1(config)# ip dhcp-server

vesr-1(config)# do commit

Configuration has been successfully applied and saved to flash. Commit timer strted, changes will be reverted in 600 seconds.

2025-05-29T19:04:10+00:00 %CLI-I-CRIT: user admin from console input: do commi

vesr-1(config)# do confirm

Configuration has been confirmed. Commit timer canceled.

2025-05-29T19:04:22+00:00 %CLI-I-CRIT: user admin from console input: do confim

vesr-1(config)# exit

vesr-1#

**Включаем на РС1 и ЗС2 автоматическое получение сетевых настроек по DHCP:**

**PC1> ip dhcp**

**DORA IP 172.16.1.100/24 GW 172.16.1.1**

**PC1> save PC1**

**Saving startup configuration to PC1.vpc**

**. done**

**PC2> ip dhcp**

**DORA IP 172.16.1.200/24 GW 172.16.1.1**

**PC2> save PC2**

**Saving startup configuration to PC2.vpc**

**. done**

**Проверяем параметры DHCP-сервера:**

show ip dhcp server pool COMPANY

vesr-1# show ip dhcp server pool COMPANY

Name: COMPANY

Network: 172.16.1.0/24

Address-ranges: 172.16.1.1-172.16.1.254

Excluded-address-ranges: 172.16.1.1

172.16.1.254

Addresses: 172.16.1.100 00:50:79:66:68:00

172.16.1.200 00:50:79:66:68:01

Default-router: 172.16.1.1

Dns-server: 77.88.8.8

Max lease time (d:h:m): 001:00:00

Default lease time (d:h:m): 003:00:00

Адреса выдаются. И интерфейс маршрутизатора доступен:

PC2> ping 172.16.1.1

84 bytes from 172.16.1.1 icmp\_seq=1 ttl=64 time=4.332 ms

84 bytes from 172.16.1.1 icmp\_seq=2 ttl=64 time=1.772 ms

84 bytes from 172.16.1.1 icmp\_seq=3 ttl=64 time=3.388 ms

84 bytes from 172.16.1.1 icmp\_seq=4 ttl=64 time=3.552 ms

84 bytes from 172.16.1.1 icmp\_seq=5 ttl=64 time=2.479 ms