

# Лабораторная работа №3

Настройка DHCP-сервера

Мантуров Татархан Бесланович

## Содержание

### Цель работы

Приобрести практические навыки по установке и конфигурированию DHCP-сервера.

### Задание

1. Установить на виртуальной машине server DHCP-сервер.
2. Настроить виртуальную машину server в качестве DHCP-сервера для виртуальной внутренней сети.
3. Проверить корректность работы DHCP-сервера в виртуальной внутренней сети путём запуска виртуальной машины client и применения соответствующих утилит диагностики.
4. Настроить обновление DNS-зоны при появлении в виртуальной внутренней сети новых узлов.
5. Проверить корректность работы DHCP-сервера и обновления DNS-зоны в виртуальной внутренней сети путём запуска виртуальной машины client и применения соответствующих утилит диагностики.
6. Написать скрипт для Vagrant, фиксирующий действия по установке и настройке DHCPсервера во внутреннем окружении виртуальной машины server.  
Соответствующим образом внести изменения в Vagrantfile.

## Выполнение лабораторной работы

### Установка DHCP-сервера

После загрузки своей операционной системы перейдем в рабочий каталог с проектом:  
cd C:\Users\dasha\work\study\tbmanturov\vagrant

Запустим виртуальную машину server командой make server-up.

На виртуальной машине server войдем под своим пользователем и откроем терминал.  
Перейдем в режим суперпользователя: sudo -i

Установим dhcp: dnf -y install dhcp-server (рис. @fig:001).

```
[root@server.tbmanturov.net ~]# dnf -y install kea
Extra Packages for Enterprise Linux 10 - x86_64 38 kB/s | 30 kB    00:00
Extra Packages for E 48% [=====] 865 kB/s | 2.7 MB    00:03 ETA
```

## Установка dhcp

### Конфигурирование DHCP-сервера

Скопирем файл примера конфигурации DHCP `dhcpd.conf.example` из каталога `/usr/share/doc/dhcp*` в каталог `/etc/dhcp` и переименуйте его в файл с названием `dhcpd.conf` (рис. @fig:002):

```
GNU nano 8.1                                     /etc/kea/kea-dhcp4.conf
// don't need to remember the code names. However, some people like
// to use numerical values. For example, option "domain-name" uses
// option code 15, so you can reference to it either by
// "name": "domain-name" or "code": 15.
{
    "code": 15,
    "data": "example.org"
},
// Domain search is also a popular option. It tells the client to
// attempt to resolve names within those specified domains. For
// example, name "foo" would be attempted to be resolved as
// foo.mydomain.example.com and if it fails, then as foo.example.com
{
    "name": "domain-search",
    "data": "mydomain.example.com,example.com"
},
// String options that have a comma in their values need to have
// it escaped (i.e. each comma is preceded by two backslashes).
// That's because commas are required for separating fields in
// compound options. At the same time, we need to be conformant
// with JSON spec, that does not allow '\\". Therefore the
// slightly uncommon double backslashes notation is needed.
// Legal JSON escapes are \ followed by \\\\'nrt character
// or \u followed by 4 hexadecimal numbers (currently Kea
// supports only \u0000 to \u00ff code points).
// CSV processing translates '\\\' into '\ and '\\\' into ','
// only so for instance '\v' is translated into '\v'. But
// as it works on a JSON string value each of these '\\\''
// characters must be doubled on JSON input.
{
    "name": "boot-file-name",
    "data": "EST5EDT4\\,M3.2.0/02:00\\,M11.1.0/02:00"
}.
1.
```

### Копирование и переименование файла `dhcpd.conf.example`

Откроем файл `/etc/dhcp/dhcpd.conf` на редактирование. В этом файле:

- заменим строку `option domain-name "example.org";` на строку `option domain-name "user.net";`
- заменим строку `option domain-name-servers ns1.example.org ns2.example.org;` на строку `option domain-name-servers ns.user.net;`
- раскомментируем строку `authoritative;`
- на базе одного из приведённых в файле примеров конфигурирования подсети зададим собственную конфигурацию dhcp-сети, задав адрес подсети, диапазон адресов для распределения клиентам, адрес маршрутизатора и broadcast-адрес:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.30 192.168.1.199;
    option routers 192.168.1.1;
    option broadcast-address 192.168.1.255;
}
```

Остальные примеры задания конфигураций подсетей удалим.

Получим файл следующего содержания (рис. @fig:003):

```
GNU nano 8.1                                     /etc/kea/kea-dhcp4.conf
// don't need to remember the code names. However, some people like
// to use numerical values. For example, option "domain-name" uses
// option code 15, so you can reference to it either by
// "name": "domain-name" or "code": 15.
{
    "code": 15,
    "data": "example.org"
},
// Domain search is also a popular option. It tells the client to
// attempt to resolve names within those specified domains. For
// example, name "foo" would be attempted to be resolved as
// foo.mydomain.example.com and if it fails, then as foo.example.com
{
    "name": "domain-search",
    "data": "mydomain.example.com,example.com"
},
// String options that have a comma in their values need to have
// it escaped (i.e. each comma is preceded by two backslashes).
// That's because commas are required for separating fields in
// compound options. At the same time, we need to be conformant
// with JSON spec, that does not allow '\\". Therefore the
// slightly uncommon double backslashes notation is needed.
// Legal JSON escapes are \ followed by \\\\'nrt character
// or \u followed by 4 hexadecimal numbers (currently Kea
// supports only \u0000 to \u00ff code points).
// CSV processing translates '\\\' into '\ and '\\\' into ','
// only so for instance '\v' is translated into '\v'. But
// as it works on a JSON string value each of these '\\\''
// characters must be doubled on JSON input.
{
    "name": "boot-file-name",
    "data": "EST5EDT4\\,M3.2.0/02:00\\,M11.1.0/02:00"
}.
1.
```

## Редактирование файла

Настроим привязку dhcpcd к интерфейсу eth1 виртуальной машины server. Для этого скопируем файл dhcpcd.service из каталога /lib/systemd/system в каталог /etc/systemd/system: cp /lib/systemd/system/dhcpcd.service /etc/systemd/system/

Откроем файл /etc/systemd/system/dhcpcd.service на редактирование и заменим в нём строку ExecStart=/usr/sbin/dhcpcd -f -cf /etc/dhcp/dhcpcd.conf -user dhcpcd -group dhcpcd --no-pid на строку ExecStart=/usr/sbin/dhcpcd -f -cf /etc/dhcp/dhcpcd.conf -user dhcpcd -group dhcpcd --no-pid eth1

Получим файл следующего содержания (рис. @fig:004):

```
GNU nano 8.1                               /var/named/master/rz/192.168.1

$TTL 1D
@   IN SOA    @ server.tbmanturov.net. (
          2024072700 ; serial
              1D      ; refresh
              1H      ; retry
              1W      ; expire
              3H )    ; minimum
NS   @
A    192.168.1.1
PTR   server.tbmanturov.net.
$ORIGIN 1.168.192.in-addr.arpa.
1     PTR   server.tbmanturov.net.
1     PTR   ns.tbmanturov.net.

1 PTR dhcp.user.net
```

## Редактирование файла

Перезагрузим конфигурацию dhcpcd и разрешим загрузку DHCP-сервера при запуске виртуальной машины server (рис. @fig:005):

```
[root@server.tbmanturov.net ~]# systemctl restart named
```

## Окно терминала

Добавим запись для DHCP-сервера в конце файла прямой DNS-зоны /var/named/master/fz/user.net (рис. @fig:006): dhcp A 192.168.1.1 и в конце файла обратной зоны /var/named/master/rz/192.168.1 (рис. @fig:007): 1 PTR dhcp.user.net.

В обоих файлах изменим серийный номер файла зоны, указав текущую дату в нотации ГГГГММДДВВ.

```
GNU nano 8.1                               /var/named/master/fz/tbmanturov.net

$TTL 1D
@   IN SOA    @ server.tbmanturov.net. (
          2024072700 ; serial
              1D      ; refresh
              1H      ; retry
              1W      ; expire
              3H )    ; minimum
NS   @
A    192.168.1.1
$ORIGIN tbmanturov.net.
server    A    192.168.1.1
ns       A    192.168.1.1
```

## Изменение файла прямой DNS-зоны

```
GNU nano 8.1                               /var/named/master/rz/192.168.1

$TTL 1D
@   IN SOA    @ server.tbmanturov.net. (
          2024072700 ; serial
              1D      ; refresh
              1H      ; retry
              1W      ; expire
              3H )    ; minimum
NS   @
A    192.168.1.1
PTR   server.tbmanturov.net.
$ORIGIN 1.168.192.in-addr.arpa.
1     PTR   server.tbmanturov.net.
1     PTR   ns.tbmanturov.net.
```

## Изменение файла обратной DNS-зоны

Перезапустим named и проверим, что можно обратиться к DHCP-серверу по имени с помощью команды ping (рис. @fig:008).

```
[root@server.tbmanturov.net ~]# systemctl restart named
```

## Перезапуск системы и пингование DHCP-сервера

Пингование сервера успешно, пакеты отправлены и получены назад.

Далее внесем изменения в настройки межсетевого экрана узла server, разрешив работу с DHCP (рис. @fig:009):

## Команды firewall

Восстановим контекст безопасности в SELinux (рис. @fig:010):

```
[root@server.tbmanturov.net ~]# restorecon -vR /etc  
[root@server.tbmanturov.net ~]# restorecon -vR /var/named  
[root@server.tbmanturov.net ~]# restorecon -vR /var/lib/ke
```

В дополнительном терминале запустим мониторинг происходящих в системе событий.

## Мониторинг происходящих в системе процессов

А в основном рабочем терминале запустим DHCP-сервер: `systemctl start dhcpc`

Запуск DHCP-сервера прошёл успешно, поэтому не выключая виртуальной машины server и не прерывая на ней мониторинга происходящих в системе процессов, приступим к анализу работы DHCP-сервера на клиенте.

## Анализ работы DHCP-сервера

Перед запуском виртуальной машины client в каталоге с проектом в вашей операционной системе в подкаталоге vagrant/provision/client создадим файл 01-routing.sh (рис. @fig:012):



### Создание файла

Пропишем в нём следующий скрипт (рис. @fig:013):

```
#!/bin/bash
# Provisioning script $0"
nmcli connection modify "System eth1" ipv4.gateway "192.168.1.1"
nmcli connection up "System eth1"
nmcli connection modify eth0 ipv4.never-default true
nmcli connection modify eth0 ipv6.never-default true
nmcli connection down eth0
nmcli connection up eth0
```

### Редактирование файла

Этот скрипт изменяет настройки NetworkManager так, чтобы весь трафик на виртуальной машине client шёл по умолчанию через интерфейс eth1.

В Vagrantfile подключим этот скрипт в разделе конфигурации для клиента (рис. @fig:014):

```
server.vm.provision "shell",
  type: "script",
  path: "provision/server/01-dummy.sh"
```

```
## Client configuration
config.vm.define "client", autostart: false do |client|
  client.vm.box = "rockylinux10"
  client.vm.hostname = "client"
  client.vm.boot_timeout = 1440
  client.ssh.insert_key = false
  client.ssh.username = 'vagrant'
  client.ssh.password = 'vagrant'

  client.vm.network :private_network,
    type: "dhcp",
    virtualbox_intnet: true
end
```

```
client.vm.provider :virtualbox do |virtualbox|
```

### Редактирование Vagrantfile

Зафиксируем внесённые изменения для внутренних настроек виртуальной машины client и запустим её, введя в терминале (рис. @fig:015):

```
C:\work\tbmanturov\vagrant>vagrant up client --provision
```

Команда make client-provision

После загрузки виртуальной машины client можно увидеть на виртуальной машине server на терминале с мониторингом происходящих в системе процессов записи о подключении к виртуальной внутренней сети узла client и выдачи ему IP-адреса из соответствующего диапазона адресов. Также информацию о работе DHCP-сервера можно наблюдать в файле /var/lib/dhcpd/dhcpd.leases:

```

# The format of this file is documented in the dhcpcd.leases(5) manual page.
# This lease file was written by isc-dhcp-4.4.2b1

# authoring-byte-order entry is generated, DO NOT DELETE
authoring-byte-order little-endian;

lease 192.168.1.30 {           //указан выданный ip-адрес
    starts 1 2023/11/13 21:22:54; //указана дата и время начала аренды
    ends 1 2023/11/13 21:32:54; //указана дата и время начала аренды
    tstp 1 2023/11/13 21:32:54; //инструкция tstamp присутствует, если используется протокол обработки отказа
    cltt 1 2023/11/13 21:22:54; //время последней транзакции клиента
    binding state free;        //объявляет состояние привязки аренды
    hardware ethernet 08:00:27:ab:7b:01; //mac-адрес сетевого интерфейса,
    на котором будет использоваться аренда
    uid "\001\010\000\253{\001"; //идентификатор клиента
    set ddns-fwd-name = "client.tbmanturov.net.";
    set ddns-txt = "3197659e2c40e26a0e15932b7c018329f7";
    set ddns-rev-name = "30.1.168.192.in-addr.arpa.";
}
server-duid "\000\001\000\001,\347\334\307\010\000^iA";

```

Войдем в систему виртуальной машины client под своим пользователем и откроем терминал. В терминале введем ifconfig (рис. @fig:016).

```

tbmanturov@client:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 10.0.2.15  netmask 255.255.255.0 broadcast 10.0.2.255
        inet6 fd17:625c:037:2:a00:27ff:fe40:fb8b  prefixlen 64  scopeid 0x0<
global>
        inet6 fe80::a00:27ff:fe40:fb8b  prefixlen 64  scopeid 0x20<link>
ether 08:00:27:40:fb:bb  txqueuelen 1000  (Ethernet)
RX packets 736  bytes 88259 (86.1 Kib)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 654  bytes 114857 (111.6 Kib)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    ether 08:00:27:53:e3:55  txqueuelen 1000  (Ethernet)
RX packets 9  bytes 540 (540.0 B)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 28  bytes 4239 (4.1 KiB)
TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536

```

Команда ifconfig

### Настройка обновления DNS-зоны

На виртуальной машине server под пользователем с правами суперпользователя отредактируем файл /etc/named/tbmanturov.net, разрешив обновление зоны с локального адреса, т.е. заменив в этом файле в строке allow-update слово none на 127.0.0.1 (рис. @fig:017):

```

;DO NOT EDIT THIS FILE - IT IS AUTO-GENERATED BY THE DHCP SERVER
// /etc/named/tbmanturov.net
Modified: 2023-11-13T11:22:54+03:00
// Provided by Red Hat caching-nameserver package
//
// BIND named zone configuration for zone recommended by
// IFC 1927 section 4.1 - localhost TLDs and address zones
// (see https://www.iana.org/assignments/rfc6303
// (c)2007 R W Franks
// See /usr/share/doc/bind*/sample/ for example named configuration files.
// Note: empty zones enable 'rec' option is default.
// If private ranges should be forwarded add
// disable-empty-zone "; into options.
//
zone "tbmanturov.net" IN {
    type master;
    file "/etc/named/tbmanturov.net";
    update-policy {
        grant DHCP_UPDATER wildcard *.user.net A DHCID;
    };
};
zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "/etc/named/1.168.192.in-addr.arpa";
    update-policy {
        grant DHCP_UPDATER wildcard *.1.168.192.in-addr.arpa PTR DHCID;
    };
};

```

Редактирование файла

Перезапустим DHCP-сервер: `systemctl restart dhcpcd`

Внесем изменения в конфигурационный файл /etc/dhcp/dhcpd.conf, добавив в него разрешение на динамическое обновление DNS-записей с локального узла прямой и обратной зон (рис. @fig:018):

```

ONU man 0.1
listen-on port 53 { 127.0.0.1; any; }
listen-on v6 port 53 { ::1; };
direct;
dump-file    "/var/named/data/cache_dump.db";
statistics-file "/var/named/data/named_stats.txt";
memstatistics-file "/var/named/data/named_mem_stats.txt";
secroots-file "/var/named/data/named_secroots";
recurring-file "/var/named/data/named/recurring";
allow-query  { localhost; 192.168.0.16; };
allow-transfer { 192.168.0.8; 192.168.0.9; };
allow-recursion { 192.168.0.8; 192.168.0.9; };
forward first;
dnssec-validation no;
/
- If you are building an AUTHORITATIVE DNS server, do NOT enable recursion.
- If you are building a RECURSIVE (caching) DNS server, you need to enable
  recursion.
- If your recursive DNS server has a public IP address, you MUST enable access
  control to limit queries to your legitimate users. Failing to do so will
  cause your server to become part of large scale DNS amplification
  attacks. Implementing BCP38 within your network would greatly
  reduce such attack surface
recursion yes;

managed-keys-directory "/var/named/dynamic";
geopip-directory "/usr/share/GeoIP";

pid-file "/run/named/named.pid";
session-keyfile "/run/named/session.key";

/* https://redesigned-project.org/wiki/Changes/CryptoPolicy */
#include "/etc/cryptopp-policies/back-end/kind.config";

```

## Редактирование файла

Перезапуск DHCP-сервера прошёл успешно, и в каталоге прямой DNS-зоны /var/named/master/fz появился файл `tbmanturov.net.jnl`, в котором в бинарном файле автоматически вносятся изменения записей зоны (рис. @fig:019@fig:020).

```
[root@server tmanutovo.net ~]# cat /etc/named/keys/dhcp_updater.key
key "DHCP_UPDATER" {
    algorithm hmac-sha512;
    secret "2nZtW0C0YtfPq9hIwEMYPltD5PxQ4UuIhILRRlN7jT0SeSBCY09uYtEPcFvFTY+xQRgT8VpZTc+HFe46A=";
};
```

## Окно терминала

```
[root@server tbanantuov.net ~]# cat /etc/named/keys/dhcp_updater.key
key "DHCP_UPDATER" {
    algorithm hmac-sha512;
    secret "ZTn2Q0C9YtqfQ9hGwEMYPltD5PxNq4Uuu2hLIRRN7jTT05eSBcV9yJtYePCFVF7YxRq78VpZrTc+HFE46A=="
```

## Бинарный файл

## **Внесение изменений в настройки внутреннего окружения виртуальной машины**

Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера (рис. @fig-024):

```
 1 01-routing.sh
 2
 3 Vagrantfile > □
 4
 5 server.ssh.insert_key = false
 6 server.ssh.username = "vagrant",
 7 server.ssh.password = "vagrant"
 8
 9 server.vm.network :private_network,
10   ip: "192.168.1.1",
11   virtualbox__intnet: true
12
13 server.vm.provider :virtualbox do |virtualbox|
14   virtualbox.customize ["modifyifm", :id, "--vrdpport", "3391"]
15   virtualbox.customize ["modifyfvm", :id, "--vrdeport", "3391"]
16 end
17
18 server.vm.provision "server dummy",
19   type: "shell",
20   preserve_order: true,
21   path: "provision/server/01-dummy.sh" I
22
23 server.vm.provision "server dhcp",
24   type: "shell",
25   preserve_order: true,
26   path: "provision/server/dhcp.sh"
```

## Редактирование файла

## Выводы

В процессе выполнения этой лабораторной работы я приобрела практические навыки по установке и конфигурированию DHCP-сервера.

