

Лабораторная работа № 3

Настройка DHCP-сервера

Абд эль хай мохамад

Содержание

| | |
|--|-----------|
| Цель работы | 2 |
| Выполнение лабораторной работы..... | 2 |
| Установка DHCP-сервера..... | 2 |
| Конфигурирование DHCP-сервера..... | 2 |
| Анализ работы DHCP-сервера..... | 6 |
| Настройка обновления DNS-зоны | 9 |
| Анализ работы DHCP-сервера после настройки обновления DNS-зоны..... | 10 |
| Внесение изменений в настройки внутреннего окружения виртуальной машины | 11 |
| Вывод:..... | 12 |
| Ответы на контрольные вопросы: | 12 |
| Вывод..... | 17 |

Цель работы

Приобретение практических навыков по установке и конфигурированию DHCP сервера

Выполнение лабораторной работы

Установка DHCP-сервера

1. Загружаю операционную систему и перехожу в рабочий каталог с проектом
2. Запускаю виртуальную машину
3. На виртуальной машине server вхожу под своим пользователем и перехожу в режим суперпользователя
4. Устанавливаю dhcp

Конфигурирование DHCP-сервера

1. Копирую файл примера конфигурации DHCP `dhcpd.conf.example` из каталога `/usr/share/doc/dhcp*` в каталог `/etc/dhcp` и переименовываю его в файл с названием `dhcpd.conf`:

```
[root@server.maabeldelhay.net dhcp]# cp /usr/share/doc/dhcp*/dhcpd.conf.example /etc/dhcp
[root@server.maabeldelhay.net dhcp]# ls
dhclient.d  dhcpd6.conf  dhcpd.conf.example
[root@server.maabeldelhay.net dhcp]# mv dhcpd.conf.example dhcpd.conf
[root@server.maabeldelhay.net dhcp]# ls
dhclient.d  dhcpd6.conf  dhcpd.conf
[root@server.maabeldelhay.net dhcp]#
```

2. Открываю файл `/etc/dhcp/dhcpd.conf` на редактирование.
В этом файле:
 - заменяю строку `option domain-name "example.org;"` на строку `option domain-name "maabeldelhay.net;"`
 - заменяю строку `option domain-name-servers ns1.example.org ns2.example.org;` на строку `option domain-name-servers ns.maabeldelhay.net;`
 - раскомментирую строку `authoritative;`
 - на базе одного из приведённых в файле примеров конфигурирования подсети задаю 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 удаляю.

```
# option definitions common to all supported networks...
option domain-name "maabedelhay.net";
option domain-name-servers ns.maabedelhay.net;

default-lease-time 600;
max-lease-time 7200;

# Use this to enable / disable dynamic dns updates globally.
#ddns-update-style none;
```

The screenshot shows a terminal window titled "server [Running] - Oracle VM VirtualBox". The terminal is running the GNU nano 5.6.1 editor, editing the file /etc/dhcp/dhcpd.conf. The current configuration shows a comment about BOOTP clients and a subnet declaration for 192.168.1.0/24. The terminal window has a menu bar with "File", "Machine", "View", "Input", "Devices", and "Help". The terminal output shows the following configuration:

```
GNU nano 5.6.1 dhcpd.conf Modified

# This declaration allows BOOTP clients to get dynamic addresses,
# which we don't really recommend.

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

3. Настраиваю привязку dhcpd к интерфейсу eth1 виртуальной машины server.
Для этого копирую файл dhcpd.service из каталога /lib/systemd/system в каталог /etc/systemd/system

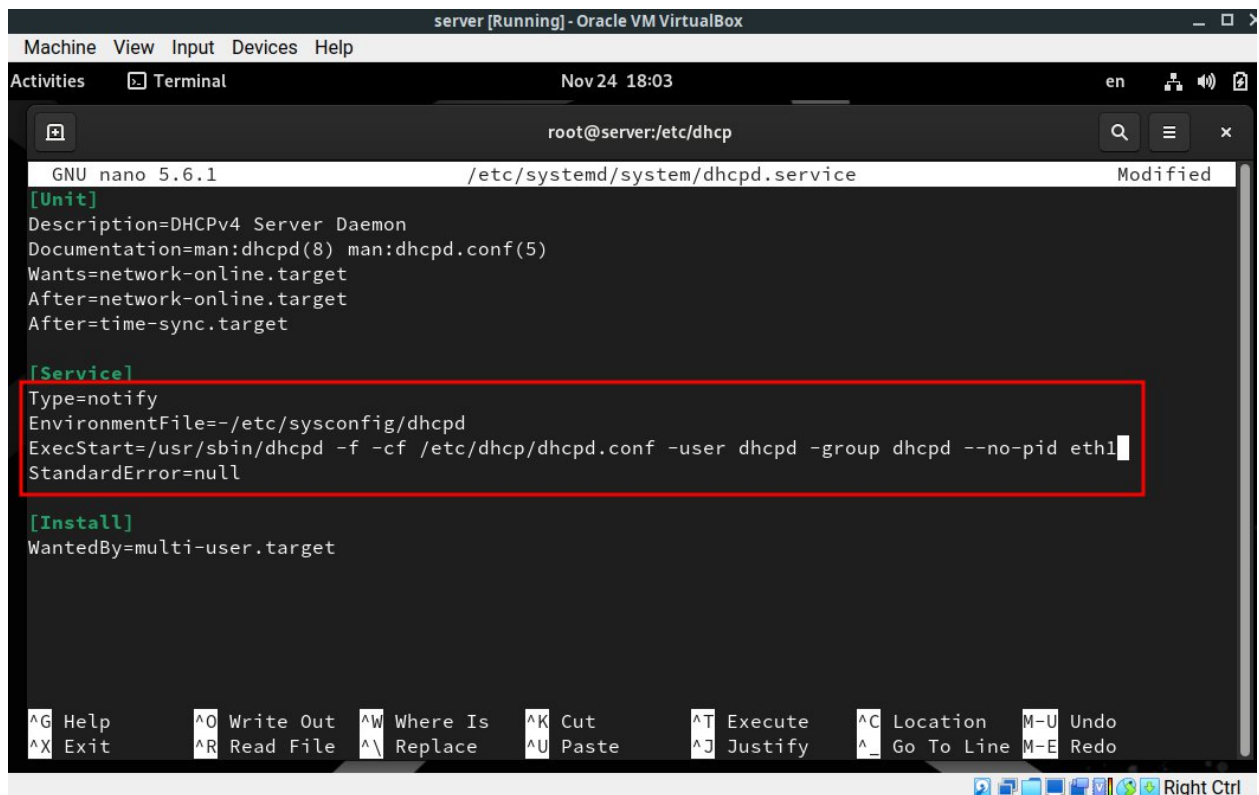
Открываю файл /etc/systemd/system/dhcpd.service на редактирование и

заменяю в нём строку

ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid

на строку

ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid eth1



```
server [Running] - Oracle VM VirtualBox
Machine View Input Devices Help
Activities Terminal Nov 24 18:03 en
root@server:/etc/dhcp
GNU nano 5.6.1 /etc/systemd/system/dhcpd.service Modified
[Unit]
Description=DHCPv4 Server Daemon
Documentation=man:dhcpd(8) man:dhcpd.conf(5)
Wants=network-online.target
After=network-online.target
After=time-sync.target

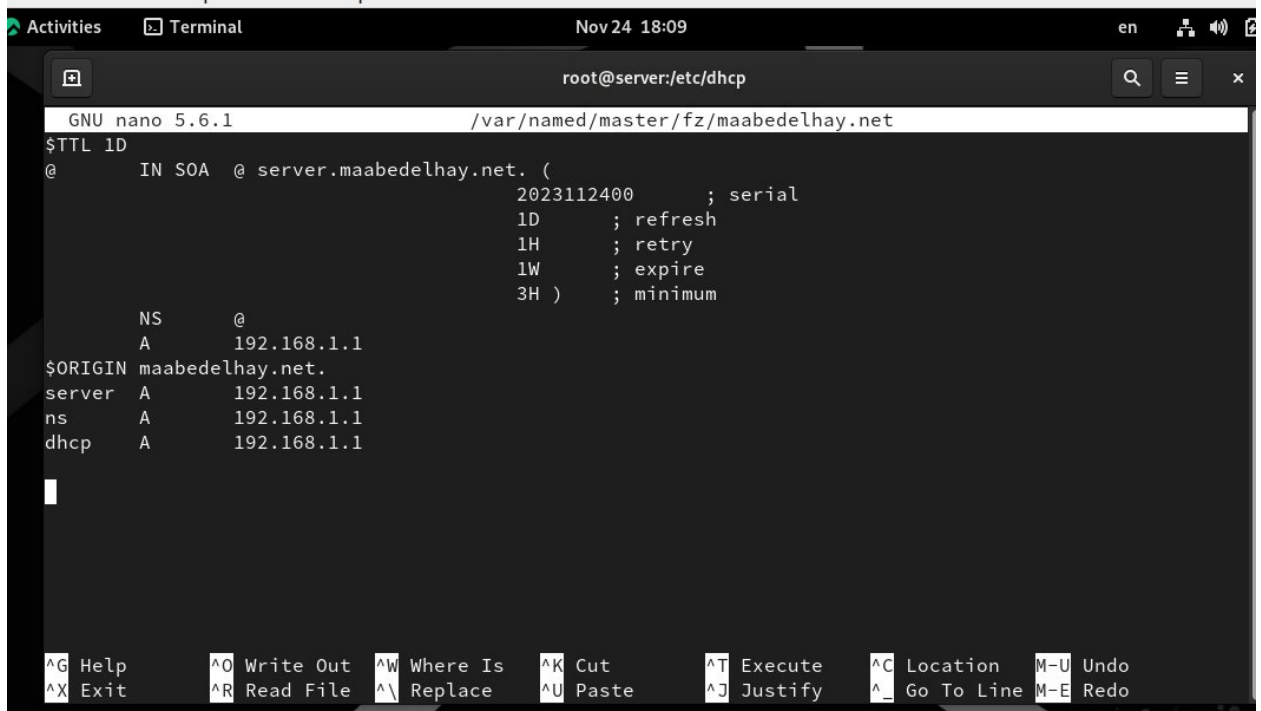
[Service]
Type=notify
EnvironmentFile=-/etc/sysconfig/dhcpd
ExecStart=/usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid eth1
StandardError=null

[Install]
WantedBy=multi-user.target

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location  M-U Undo
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify  ^_ Go To Line M-E Redo
Right Ctrl
```

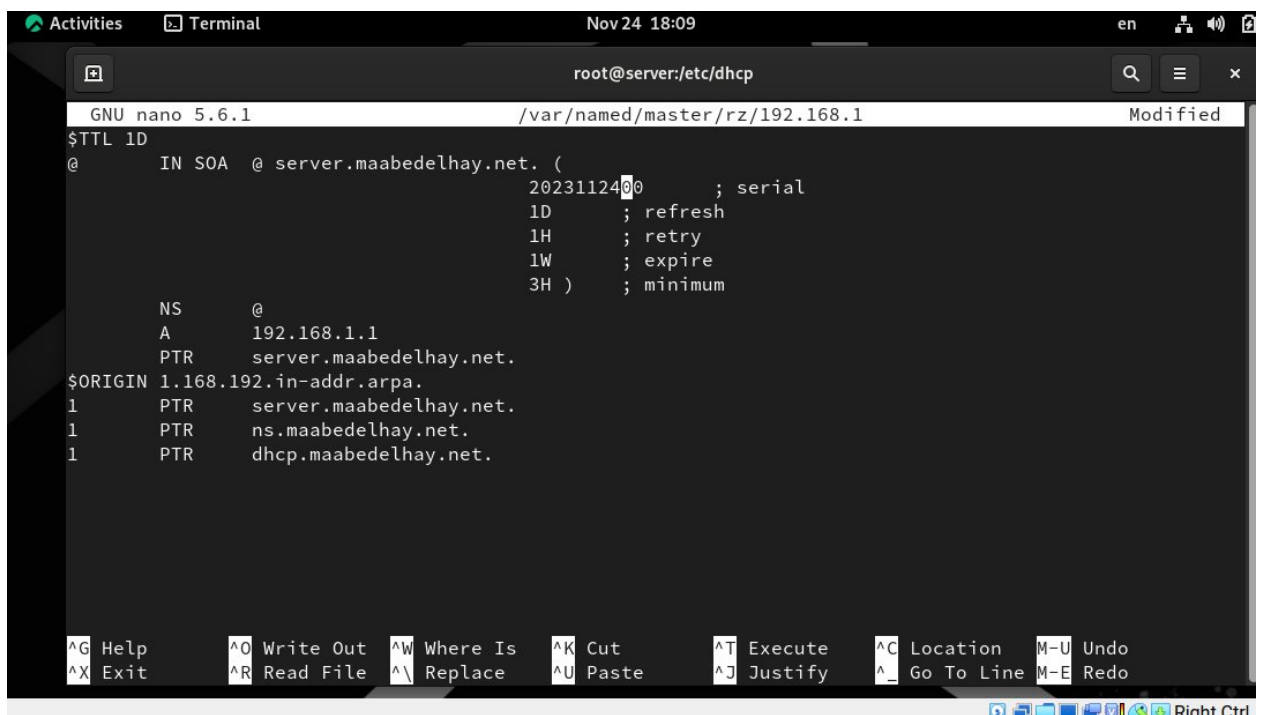
Перезагружаю конфигурацию dhcpd и разрешаю загрузку DHCP-сервера при запуске виртуальной машины server:

4. Добавляю запись для DHCP-сервера в конце файла прямой DNS-зоны /var/named/master/fz/maabedelhay.net: dhcp A 192.168.1.1 и в конце файла обратной зоны /var/named/master/rz/192.168.1: 1 PTR dhcp.maabedelhay.net. В обоих файлах изменяю серийный номер файла зоны, указав текущую дату в нотации ГГГГММДДВВ



```
GNU nano 5.6.1 /var/named/master/fz/maabedelhay.net
$TTL 1D
@      IN SOA  @ server.maabedelhay.net. (
                                2023112400      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )   ; minimum

NS     @
A      192.168.1.1
$ORIGIN maabedelhay.net.
server A      192.168.1.1
ns     A      192.168.1.1
dhcp   A      192.168.1.1
```



```
GNU nano 5.6.1 /var/named/master/rz/192.168.1 Modified
$TTL 1D
@      IN SOA  @ server.maabedelhay.net. (
                                2023112400      ; serial
                                1D      ; refresh
                                1H      ; retry
                                1W      ; expire
                                3H )   ; minimum

NS     @
A      192.168.1.1
PTR     server.maabedelhay.net.
$ORIGIN 1.168.192.in-addr.arpa.
1      PTR     server.maabedelhay.net.
1      PTR     ns.maabedelhay.net.
1      PTR     dhcp.maabedelhay.net.
```

5. Перезапускаю named: systemctl restart named

6. Проверяю, что можно обратиться к DHCP-серверу по имени: ping dhcp.maabeldelhay.net.

```
[root@server.maabeldelhay.net dhcp]# ping dhcp.maabeldelhay.net
PING dhcp.maabeldelhay.net (192.168.1.1) 56(84) bytes of data.
64 bytes from ns.maabeldelhay.net (192.168.1.1): icmp_seq=1 ttl=64 time=0.040 ms
64 bytes from ns.maabeldelhay.net (192.168.1.1): icmp_seq=2 ttl=64 time=0.066 ms
64 bytes from ns.maabeldelhay.net (192.168.1.1): icmp_seq=3 ttl=64 time=0.091 ms
64 bytes from ns.maabeldelhay.net (192.168.1.1): icmp_seq=4 ttl=64 time=0.116 ms
64 bytes from server.maabeldelhay.net (192.168.1.1): icmp_seq=5 ttl=64 time=0.043 ms
^C
```

7. Вношу изменения в настройки межсетевого экрана узла server, разрешив работу с DHCP:
8. Восстанавливаю контекст безопасности в SELinux:

```
[root@server.maabeldelhay.net dhcp]# firewall-cmd --add-service=dhcp
success
[root@server.maabeldelhay.net dhcp]# firewall-cmd --add-service=dhcp --permanent
success
[root@server.maabeldelhay.net dhcp]#
```

9. В дополнительном терминале запускаю мониторинг происходящих в системе процессов в реальном времени
10. Запуск DHCP-сервера прошёл успешно.

Анализ работы DHCP-сервера

1. Перед запуском виртуальной машины client в каталоге с проектом в моей операционной системе в подкаталоге vagrant/provision/client создаю файл 01-routing.sh:

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

2. В Vagrantfile подключаю этот скрипт в разделе конфигурации для клиента

cltt дата;

дата - означает следующее: день_недели год/месяц/день час:минута:секунда

Оператор *binding state* объявляет обязательное состояние соединения. Если DHCP-сервер не настроен на использование протокола восстановления после отказа, *binding state* может быть *active*, *free* или *abandoned*. Протокол отказоустойчивости добавляет некоторые дополнительные переходные состояния, а также состояние резервного копирования.

Next binding state указывает к какому состоянию переносится соединение, когда истекает время текущего состояния. Время истечения текущего состояния указано в операторе *ends*.

binding state state;

next binding state state;

rewind binding state state - является частью оптимизации. Оно помогает серверу возвращать соединение в состояние, которое недавно было передано client.

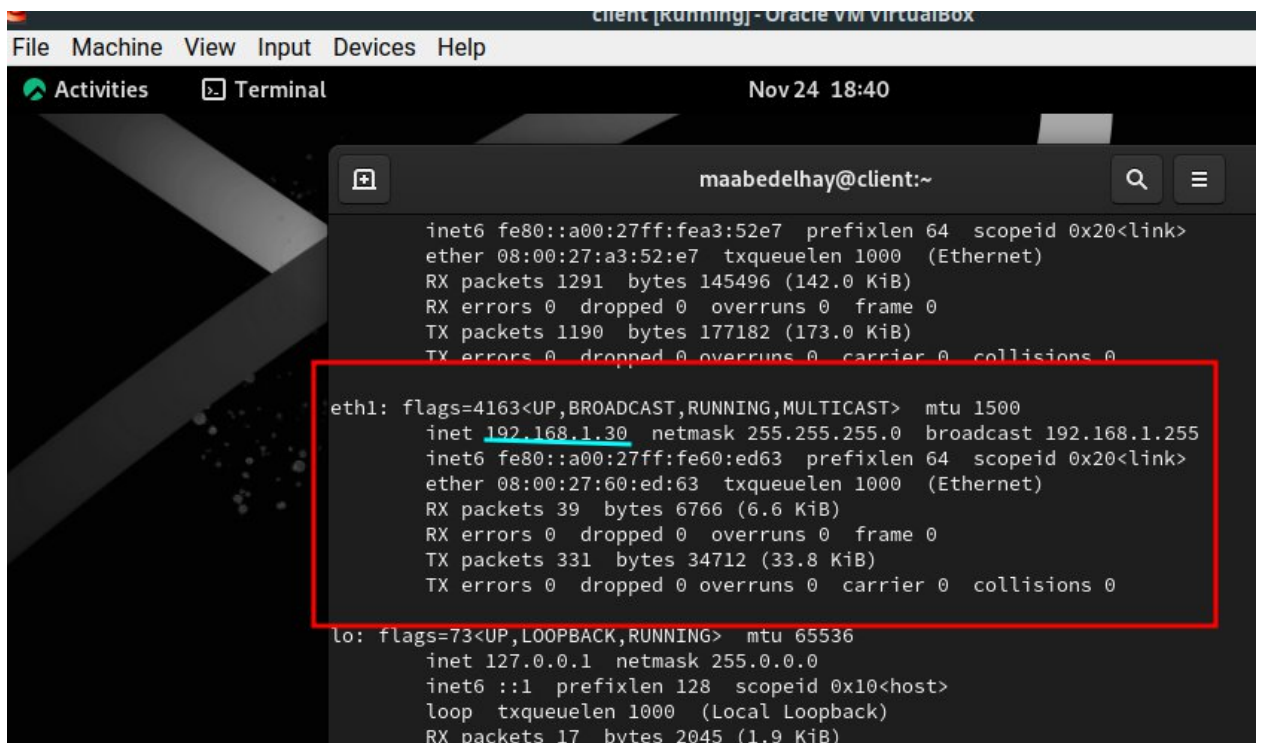
MAC адрес сетевого интерфейса, который был использован при получении IP адреса записывается с помощью инструкции *hardware*:

hardware hardware-type mac-address;

Если клиент посылает серверу собственное имя, то имя хоста записывается с использованием инструкции *client-hostname*.

client-hostname "hostname";

5. Вхожу в систему виртуальной машины client под своим пользователем и открываю терминал. В терминале ввожу: `ifconfig`



```
client [running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities Terminal Nov 24 18:40
maabedelhay@client:~
inet6 fe80::a00:27ff:fea3:52e7 prefixlen 64 scopeid 0x20<link>
ether 08:00:27:a3:52:e7 txqueuelen 1000 (Ethernet)
RX packets 1291 bytes 145496 (142.0 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 1190 bytes 177182 (173.0 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

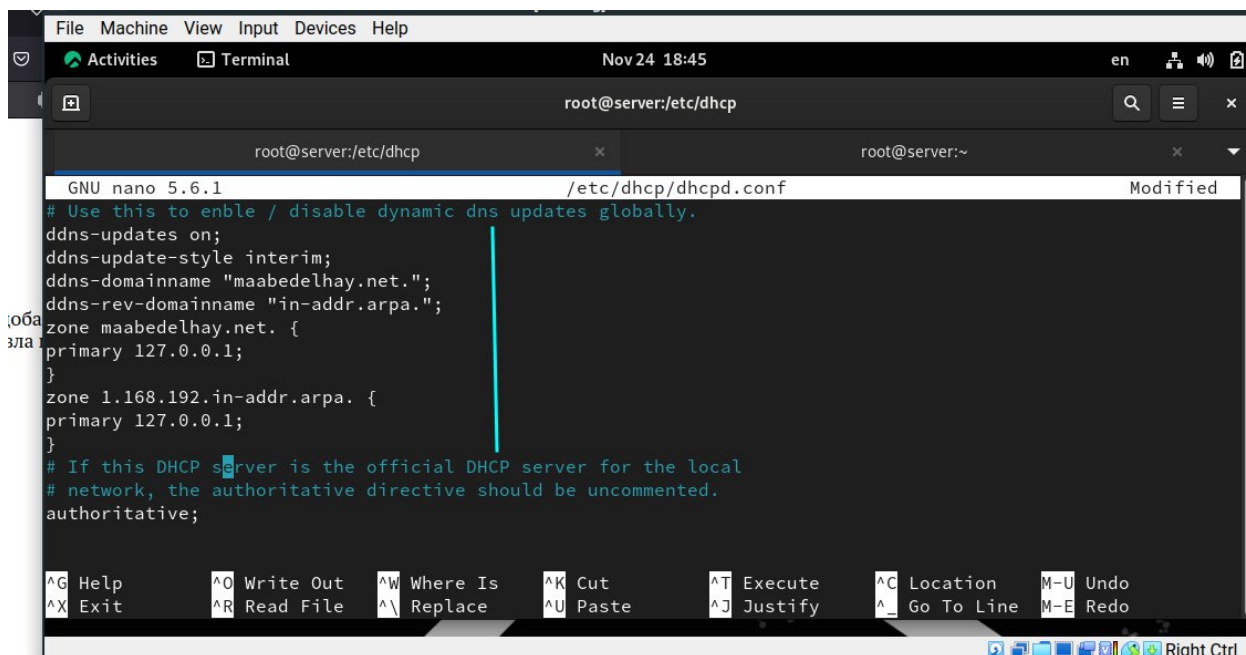
eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
  inet 192.168.1.30 netmask 255.255.255.0 broadcast 192.168.1.255
  inet6 fe80::a00:27ff:fe60:ed63 prefixlen 64 scopeid 0x20<link>
  ether 08:00:27:60:ed:63 txqueuelen 1000 (Ethernet)
  RX packets 39 bytes 6766 (6.6 KiB)
  RX errors 0 dropped 0 overruns 0 frame 0
  TX packets 331 bytes 34712 (33.8 KiB)
  TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
  inet 127.0.0.1 netmask 255.0.0.0
  inet6 ::1 prefixlen 128 scopeid 0x10<host>
  loop txqueuelen 1000 (Local Loopback)
  RX packets 17 bytes 2045 (1.9 KiB)
```

Настройка обновления DNS-зоны

1. На виртуальной машине server под пользователем с правами суперпользователя редактирую файл `/etc/named/maabedelhay.net`, разрешив обновление зоны с локального адреса, т.е. заменив в этом файле в строке `allow-update` слово `none` на `127.0.0.1`:
2. Перезапускаю DNS-сервер: `systemctl restart named`

3. Вношу изменения в конфигурационный файл `/etc/dhcp/dhcpd.conf`, добавив в него разрешение на динамическое обновление DNS-записей с локального узла прямой и обратной зон:



```
File Machine View Input Devices Help
Activities Terminal Nov 24 18:45 en
root@server:/etc/dhcp
root@server:/etc/dhcp
GNU nano 5.6.1 /etc/dhcp/dhcpd.conf Modified
# Use this to enable / disable dynamic dns updates globally.
ddns-updates on;
ddns-update-style interim;
ddns-domainname "maabeldelhay.net.";
ddns-rev-domainname "in-addr.arpa.";
zone maabeldelhay.net. {
primary 127.0.0.1;
}
zone 1.168.192.in-addr.arpa. {
primary 127.0.0.1;
}
# If this DHCP server is the official DHCP server for the local
# network, the authoritative directive should be uncommented.
authoritative;
^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^_ Go To Line M-E Redo
Right Ctrl
```

4. Перезапускаю DHCP-сервер: `systemctl restart dhcpd`

Анализ работы DHCP-сервера после настройки обновления DNS-зоны

1. На виртуальной машине client под своим пользователем открываю терминал и с помощью утилиты `dig` проверяю наличие DNS-записи о клиенте в прямой DNS-зоне:
`dig @192.168.1.1 client.maabeldelhay.net`
В отчёте построчно прокомментируйте выведенную на экран информацию

Сначала выводится информация о версии DIG, глобальные опции, используемые с командой.

Тип посланного сообщения – запрос, выполнен без ошибок, использовались флаги `qr aa rd ra`, запрос отправлен один, ответов получено один.

Записи с серверов, поддерживающих EDNS0, включают OPT RR(специфичный тип RR-записи, которая не несёт DNS-данные, нужна исключительно для стандартизации обмена служебной информацией),

который не имеет текстового формата rdata, поэтому он не печатается, но можно видеть, что он описан в комментариях выше раздела вопросов как «OPT PSEUDOSECTION».

AUTHORITY SECTION содержит имя сервера или серверов доменных имен, которые предоставляют информацию об указанном имени – maabedelhay.net.

ADDITIONAL SECTION содержит IP-адреса серверов доменных имен, перечисленных в предыдущей секции – 192.168.1.1.

QUESTION SECTION (секция запроса): Показывает запрос показать A-запись (команда DIG без параметров) для домена client.maabedelhay.net;

ANSWER SECTION (секция ответа): Показывает ответ, полученный от DNS – A-запись для client.maabedelhay.net.

Последняя секция — это статистика по запросу - время выполнения запроса, имя DNS-сервера, который запрашивался, когда был создан запрос и размер сообщения.

```
[maabedelhay@client.maabedelhay.net ~]$ dig @192.168.1.1 client.maabedelhay.net

; <<>> DiG 9.16.23-RH <<>> @192.168.1.1 client.maabedelhay.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6104
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8978df0d090930c7010000006560f0ca42f7d2c15bf6afcf (good)
;; QUESTION SECTION:
;client.maabedelhay.net.                IN      A

;; ANSWER SECTION:
client.maabedelhay.net. 300      IN      A      192.168.1.30

;; Query time: 7 msec
;; SERVER: 192.168.1.1#53(192.168.1.1)
;; WHEN: Fri Nov 24 18:51:53 UTC 2023
;; MSG SIZE rcvd: 95

[maabedelhay@client.maabedelhay.net ~]$
```

Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перехожу в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создаю в нём каталог dhcp, в который помещаю в соответствующие подкаталоги конфигурационные файлы DHCP:
cd /vagrant/provision/server
mkdir -p /vagrant/provision/server/dhcp/etc/dhcp
mkdir -p /vagrant/provision/server/dhcp/etc/systemd/system

```
cp -R /etc/dhcp/dhcpd.conf /vagrant/provision/server/dhcp/etc/dhcp/  
cp -R /etc/systemd/system/dhcpd.services  
/vagrant/provision/server/dhcp/etc/systemd/system/
```

2. Заменяю конфигурационные файлы DNS-сервера:

```
cd /vagrant/dns/  
cp -R /var/named/* /vagrant/dns/var/named/
```

3. В каталоге /vagrant/provision/server создаю исполняемый файл dhcp.sh:

```
cd /vagrant/provision/server  
touch dhcp.sh  
chmod +x dhcp.sh
```

Этот скрипт по сути повторяет произведённые Вами действия по установке и настройке DHCP-сервера.

4. Для отработки созданного скрипта во время загрузки виртуальной машины server в конфигурационном файле Vagrantfile необходимо добавить в разделе конфигурации для сервера:
server.vm.provision "server dhcp",
type: "shell",
preserve_order: true,
path: "provision/server/dhcp.sh"

5. После этого включаю виртуальные машины client и server.

Вывод:

Я приобрел практические навыки по установке и конфигурированию DHCP-сервера.

Ответы на контрольные вопросы:

1. В каких файлах хранятся настройки сетевых подключений?

```
/etc/network/interfaces  
/etc/hosts  
/etc/networks  
/etc/nsswitch.conf  
/etc/resolv.conf
```

2. За что отвечает протокол DHCP?

Протокол динамической конфигурации узла (Dynamic Host Configuration Protocol, DHCP) — сетевой протокол, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети TCP/IP.

3. Поясните принцип работы протокола DHCP. Какими сообщениями обмениваются клиент и сервер, используя протокол DHCP?
Принцип работы протокола DHCP заключается в автоматическом получении необходимой конфигурации сети для устройства пользователя.

DHCPDISCOVER

Это сообщение обозначает начало DHCP взаимодействия между клиентом и сервером. Данное сообщение отправляется клиентом (компьютером или устройством), подключенным к сети. В этом сообщении используется 255.255.255.255 как IP-адрес доставки, тогда как исходным адресом является 0.0.0.0

DHCPOFFER

Это сообщение отправляется в ответ на DHCPDISCOVER от сервера DHCP для подключенных клиентов. В этом сообщении содержатся необходимые сетевые настройки.

DHCPREQUEST

Данное сообщение является ответом на DHCPOFFER, и обозначает, что клиент принял отправленные настройки.

DHCPACK

Данное сообщение отправляется на сервер протокола DHCP в ответ на DHCPREQUEST от клиента. Сообщение обозначает конец процесса, начатого с сообщения DHCPDISCOVER. Т.е. DHCPACK - это не что иное, как подтверждение от сервера начала авторизации клиента и принятие параметров конфигурации, полученных в самом начале от сервера.

DHCPNAK

Данное сообщение является противоположностью DHCPACK, описанного выше. Оно отправляется на сервер в случае, если невозможно удовлетворить параметры DHCPREQUEST клиента.

DHCPDECLINE

Сообщение отправляется клиентом на сервер в случае, если IP-адрес, присваиваемый в DHCP уже используется.

DHCPINFORM

Сообщение отправляется серверу в том случае, если клиенту DHCP присвоен статический IP-адрес, а по настройкам конфигурации необходим динамический адрес.

DHCPRELEASE

Сообщение отправляется клиентом в том случае, если он завершает процесс

использования сетевого адреса.

Теперь, когда мы познакомились с различными сообщениями в DHCP, можно изучить весь процесс работы, чтобы получить более полное представление. Шаги ниже описываются исходя из того, что все настройки установлены по умолчанию.

Шаг 1.

Когда клиент (компьютер или устройство) загружается или подключается к сети, серверу отправляется сообщение DHCPDISCOVER. Если нет никаких дополнительных данных о конфигурации, то сообщение отправляется с адреса 0.0.0.0 к 255.255.255.255. Если сервер DHCP находится в локальной подсети, то она напрямую получает сообщение, если он находится в другой подсети, то используется агент ретрансляции для передачи запроса к серверу DHCP. Используется протокол передачи UDP через порт 67. Клиент на данном этапе начинает стадию авторизации.

Шаг 2.

В тот момент как сервер получил запрос DHCPDISCOVER, то он отправляет в ответ сообщение DHCPOFFER. Как говорилось ранее, в этом сообщении содержатся все необходимые параметры конфигурации, запрашиваемые клиентом. Например, IP-адрес, необходимый клиенту, а также значение маски подсети и информация о шлюзе. Также сервер сразу заполняет значения MAC-адреса в поле CHADDR. Сообщение отправляется клиенту от адреса 255.255.255.255 напрямую, а если сервер находится в другой подсети, то используются агенты ретрансляции, который отвечает за то, чтобы сообщение было доставлено. В этом случае для передачи применяется протокол UDP через порт 68. На этом этапе клиент начинает подбирать параметры.

Шаг 3.

Клиент формирует сообщение DHCPREQUEST, которое служит ответом на DHCPOFFER от сервера, указав, что он принимает параметры конфигурации, отправленные ему. Если бы было несколько серверов DHCP, то клиент бы получил также несколько сообщений DHCPOFFER, но клиент отвечает только одному серверу, заполняя параметры конфигурации для настройки. Таким образом, он проходит авторизацию с получением IP-адреса от одного конкретного сервера DHCP. Все сообщения от других серверов блокируются. Сообщение DHCPREQUEST по-прежнему будет содержать адрес источника 0.0.0.0, если клиенту все еще нельзя использовать IP-адреса, полученные в сообщении DHCPOFFER. В течение этого этапа клиент получает ответы на свои запросы.

Шаг 4.

Как только сервер получает DHCPREQUEST от клиента, он посылает DHCPACK сообщение о том, что теперь клиент может использовать IP-адрес, назначенный к нему. Клиент окончательно подключается к сети и с настроенными параметрами.

4. В каких файлах обычно находятся настройки DHCP-сервера? За что отвечает каждый из файлов?
DHCP используют файл конфигурации /etc/dhcpd.conf и файл

/var/lib/dhcp/dhcpd.leases в качестве базы данных, хранящей аренды клиентов **Файл конфигурации** может содержать любые дополнительные символы табуляции и пустые строки, облегчающие форматирование. Ключевые слова нечувствительны к регистру, а строки, начинающиеся с символа решетки (#), являются комментариями.

В файле конфигурации существует два типа предложений:

Параметры — определяют, как выполнять задачу, выполнять ли задачу или какие сетевые параметры будут переданы клиенту.

Объявления — описывают топологию сети, клиентов, предоставляют адреса для клиентов, или сопоставляют группу параметров группе объявлений.

Некоторые параметры должны начинаться с ключевого слова option. Ключевое слово option используется для указания необязательных параметров DHCP; тогда как параметры определяют значения, которые являются обязательными или управляют поведением DHCP сервера.

В файле /var/lib/dhcp/dhcpd.leases на DHCP сервере находится база данных аренды адресов DHCP-клиентами. Этот файл не следует изменять вручную. Информация о DHCP аренде для каждого только что выданного IP адреса автоматически заносится в эту базу. Эта информация включает в себя продолжительность аренды адреса арендующим узлом, даты начала и конца аренды, а также MAC адрес сетевой карты, который был использован для получения аренды.

В базе данных аренды указывается не местное время, а время по Гринвичу (GMT).

5. Что такое DDNS? Для чего применяется DDNS?

Динамический DNS — технология, позволяющая информации на DNS-сервере обновляться в реальном времени и по желанию в автоматическом режиме.

Данная служба позволяет сопоставить доменное имя с динамическим IP-адресом сетевого устройства. Системы NAS от QNAP поддерживают работу со службами DDNS, обеспечивающими быстрый доступ к серверу через Интернет с использованием простого в запоминании доменного имени (адреса URL) вместо IP-адреса. При изменении IP-адреса система NAS автоматически обновит информацию в DDNS, благодаря чему к ней всегда можно будет получить удаленный доступ через Интернет по одному и тому же доменному имени.

6. Какую информацию можно получить, используя утилиту ifconfig? Приведите примеры с использованием различных опций.

Ifconfig – команда, предназначенная для настройки, мониторинга и отладки сетевого интерфейса в операционных системах Linux.

Чтобы отобразить краткий список, используется аргумент –s: `ifconfig –s`

Аргумент –a отображает все интерфейсы, которые в настоящее время доступны, даже если выключены: `ifconfig –a`

7. Какую информацию можно получить, используя утилиту ping? Приведите примеры с использованием различных опций.

С помощью ping с опциями можно получить следующую информацию:
Сколько отправлено и получено пакетов, процент потерянных пакетов, а также:
icmp_seq – номер отправленного пакета.
time — общее время работы;
rtt min/avg/max/mdev — минимальное время/среднее время/максимальное время/квадратичное отклонение.
ping -c — количество пакетов, которые нужно отправить;

ping -i — интервал в секундах между отправкой пакетов;

ping -n — не получать домены для ip адресов;

ping -A — адаптивный режим, время между отправками пакета адаптируется к времени передачи и приема пакета, но не меньше чем 200мс;

Вывод