

Лабораторная работа № 3. Настройка DHCP-сервера

3.1. Цель работы

Приобретение практических навыков по установке и конфигурированию DHCP-сервера.

3.2. Предварительные сведения

3.2.1. Кратко о 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.

DHCP:

- работает по модели «клиент-сервер»;
- позволяет избежать ручной настройки компьютеров сети;
- выделяет каждому компьютеру произвольный свободный IP-адрес из определённого администратором диапазона;
- передача данных осуществляется через протокол UDP, при этом сервер принимает сообщения от клиентов на порт 67 и отправляет сообщения клиентам на порт 68.

Некоторые из наиболее часто используемых опций DHCP:

- IP-адрес маршрутизатора по умолчанию;
- маска подсети;
- адреса серверов DNS;
- имя домена DNS.

3.2.2. Регламент выделения IP-адресов

Регламент выделения IP-адресов приведён в табл. 3.1.

Регламент выделения ip-адресов (для сети класса C)

Таблица 3.1

IP-адреса	Назначение
1	Шлюз
2–19	Сетевое оборудование
20–29	Серверы
30–199	Компьютеры, DHCP
200–219	Компьютеры, Static
220–229	Принтеры
230–254	Резерв

3.2.3. Сетевые утилиты диагностики DHCP

3.2.3.1. Команда `ifconfig`

Команда `ifconfig` используется для конфигурирования и диагностики сетевых интерфейсов операционной системы.

Формат команды `ifconfig`:

```
ifconfig [interface]
ifconfig interface [atype] options | address ...
```

Здесь `interface` — имя интерфейса, `address` — IP-адрес, который требуется назначить интерфейсу. Это может быть IP-адрес или имя, которое `ifconfig` будет искать в файле `/etc/hosts`.

Если `ifconfig` используется только с именем интерфейса, он показывает конфигурацию этого интерфейса. Когда `ifconfig` вызывается без параметров, он показывает все интерфейсы, которые сконфигурированы в системе; опция `-a` вынуждает показать бездействующие интерфейсы.

Более подробно об опциях команды `ifconfig` см. в соответствующем руководстве `man`.

3.2.3.2. Утилита `ping`

Утилита `ping` предназначена для проверки соединений в сетях на основе TCP/IP.

Утилита отправляет запросы (ICMP Echo-Request) протокола ICMP указанному узлу сети и фиксирует поступающие ответы (ICMP Echo-Reply). Время между отправкой запроса и получением ответа (RTT, Round Trip Time) позволяет определять двусторонние задержки (RTT) по маршруту и частоту потери пакетов, т.е. косвенно определять загруженность на каналах передачи данных и промежуточных устройствах. Полное отсутствие ICMP-ответов может также означать, что удалённый узел (или какой-либо из промежуточных маршрутизаторов) блокирует ICMP Echo-Reply или игнорирует ICMP Echo-Request.

Более подробно об опциях команды `ping` см. в соответствующем `man` руководстве.

3.3. Задание

1. Установите на виртуальной машине `server` DHCP-сервер (см. раздел 3.4.1).
2. Настройте виртуальную машину `server` в качестве DHCP-сервера для виртуальной внутренней сети (см. раздел 3.4.2).
3. Проверьте корректность работы DHCP-сервера в виртуальной внутренней сети путём запуска виртуальной машины `client` и применения соответствующих утилит диагностики (см. раздел 3.4.3).
4. Настройте обновление DNS-зоны при появлении в виртуальной внутренней сети новых узлов (см. раздел 3.4.4).
5. Проверьте корректность работы DHCP-сервера и обновления DNS-зоны в виртуальной внутренней сети путём запуска виртуальной машины `client` и применения соответствующих утилит диагностики (см. раздел 3.4.5).
6. Напишите скрипт для Vagrant, фиксирующий действия по установке и настройке DHCP-сервера во внутреннем окружении виртуальной машины `server`. Соответствующим образом внести изменения в `Vagrantfile` (см. раздел 3.4.6).

3.4. Последовательность выполнения работы

3.4.1. Установка DHCP-сервера

1. Загрузите вашу операционную систему и перейдите в рабочий каталог с проектом:
`cd /var/tmp/user_name/vagrant`
Здесь `user_name` — идентифицирующее вас имя пользователя, обычно первые буквы инициалов и фамилия.
2. Запустите виртуальную машину `server`:
`make server`
(или, если вы работаете под ОС Windows, то `vagrant up server`).
3. На виртуальной машине `server` войдите под вашим пользователем и откройте терминал. Перейдите в режим суперпользователя:
`sudo -i`
4. Установите `dhcp`:
`dnf -y install dhcp-server`

3.4.2. Конфигурирование DHCP-сервера

1. Скопируйте 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`:
`cd /etc/dhcp`
`cp /usr/share/doc/dhcp*/dhcpd.conf.example /etc/dhcp`
`mv /etc/dhcp/dhcpd.conf.example /etc/dhcp/dhcpd.conf`
(`dhcp*` означает, что каталог в названии содержит текущий номер версии установленного в системе DHCP).
2. Откройте файл `/etc/dhcp/dhcpd.conf` на редактирование. В этом файле:
 - замените строку
`option domain-name "example.org";`
на строку
`option domain-name "user.net";`
(при этом вместо `user` укажите свой логин);
 - замените строку
`option domain-name-servers ns1.example.org, ns2.example.org;`
на строку
`option domain-name-servers ns.user.net;`
(при этом вместо `user` укажите свой логин);
 - раскомментируйте строку `authoritative`;
 - на базе одного из приведённых в файле примеров конфигурирования подсети задайте 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;
}
```
3. Остальные примеры задания конфигураций подсетей удалите.
3. Настройте привязку `dhcpd` к интерфейсу `eth1` виртуальной машины `server`. Для этого скопируйте файл `dhcpd.service` из каталога `/lib/systemd/system` в каталог `/etc/systemd/system`:
`cp /lib/systemd/system/dhcpd.service /etc/systemd/system/`

Откройте файл `/etc/systemd/system/dhcpd.service` на редактирование и замените 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
```

Перезагрузите конфигурацию `dhcpd` и разрешите загрузку DHCP-сервера при запуске виртуальной машины `server`:

```
systemctl --system daemon-reload  
systemctl enable dhcpd
```

4. Добавьте запись для DHCP-сервера в конце файла прямой DNS-зоны `/var/named/master/fz/user.net`:

```
dhcp      A      192.168.1.1
```

и в конце файла обратной зоны `/var/named/master/rz/192.168.1`:

```
1          PTR    dhcp.user.net.
```

(вместо `user` укажите свой логин).

При этом не забудьте в обоих файлах изменить серийный номер файла зоны, указав текущую дату в нотации ГГТТММДДВВ.

5. Перезапустите `named`:

```
systemctl restart named
```

6. Проверьте, что можно обратиться к DHCP-серверу по имени:

```
ping dhcp.user.net
```

(вместо `user` укажите свой логин).

Если в доступе будет отказано, то возможно потребуется исправить ошибки в конфигурационных файлах, скорректировать права доступа:

```
chown -R named:named /var/named
```

и ещё раз перезапустить `named`.

7. Внесите изменения в настройки межсетевого экрана узла `server`, разрешив работу с DHCP:

```
firewall-cmd --list-services  
firewall-cmd --get-services  
firewall-cmd --add-service=dhcp  
firewall-cmd --add-service=dhcp --permanent
```

8. Восстановите контекст безопасности в SELinux:

```
restorecon -vR /etc  
restorecon -vR /var/named  
restorecon -vR /var/lib/dhcpd/
```

9. В дополнительном терминале запустите мониторинг происходящих в системе процессов в реальном времени:

```
tail -f /var/log/messages
```

10. В основном рабочем терминале запустите DHCP-сервер:

```
systemctl start dhcpd
```

11. Если запуск DHCP-сервера прошёл успешно, то, не выключая виртуальной машины `server` и не прерывая на ней мониторинга происходящих в системе процессов, приступите к анализу работы DHCP-сервера на клиенте (раздел 3.4.3).

3.4.3. Анализ работы DHCP-сервера

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

```
cd /var/tmp/user_name/vagrant/provision/client
touch 01-routing.sh
chmod +x 01-routing.sh
```

Открыв его на редактирование, пропишите в нём следующий скрипт:

```
#!/bin/bash
```

```
echo "Provisioning script $0"
```

```
nmcli connection modify "System eth1" ipv4.route-metric 1
systemctl restart NetworkManager
```

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

2. В Vagrantfile подключите этот скрипт в разделе конфигурации для клиента:

```
client.vm.provision "client routing",
  type: "shell",
  preserve_order: true,
  run: "always",
  path: "provision/client/01-routing.sh"
```

3. Зафиксируйте внесённые изменения для внутренних настроек виртуальной машины `client` и запустите её, введя в терминале:

```
make client-provision
```

(для работающих под ОС Windows: `vagrant up client --provision`).

4. После загрузки виртуальной машины `client` вы можете 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`. В отчёте прокомментируйте построчно информацию из этого файла.

5. Войдите в систему виртуальной машины `client` под вашим пользователем и откройте терминал. В терминале введите:

```
ifconfig
```

На экран будет выведена информация об имеющихся интерфейсах. Прокомментируйте её построчно в отчёте.

3.4.4. Настройка обновления DNS-зоны

Требуется настроить обновление DNS-зоны при появлении в виртуальной внутренней сети новых узлов.

1. На виртуальной машине `server` под пользователем с правами суперпользователя отредактируйте файл `/etc/named/user.net` (вместо `user` укажите свой логин), разрешив обновление зоны с локального адреса, т.е. заменив в этом файле в строке `allow-update` слово `none` на `127.0.0.1`:

```
zone "user.net" IN {
  type master;
  file "master/fz/user.net";
  allow-update { 127.0.0.1; };
};
```

```
zone "1.168.192.in-addr.arpa" IN {
    type master;
    file "master/rz/192.168.1";
    allow-update { 127.0.0.1; };
};
```

2. Перезапустите DNS-сервер:
systemctl restart named
3. Внесите изменения в конфигурационный файл /etc/dhcp/dhcpd.conf, добавив в него разрешение на динамическое обновление DNS-записей с локального узла прямой и обратной зон:

```
# Use this to enable / disable dynamic dns updates globally.
ddns-updates on;
ddns-update-style interim;
ddns-domainname "user.net.";
ddns-rev-domainname "in-addr.arpa.";

zone user.net. {
    primary 127.0.0.1;
}

zone 1.168.192.in-addr.arpa. {
    primary 127.0.0.1;
}
```

(вместо user укажите свой логин).

4. Перезапустите DHCP-сервер:
systemctl restart dhcpd
5. Если перезапуск DHCP-сервера прошёл успешно, то в каталоге прямой DNS-зоны /var/named/master/fz должен появиться файл user.net.jnl, в котором в бинарном файле автоматически вносятся изменения записей зоны.

3.4.5. Анализ работы DHCP-сервера после настройки обновления DNS-зоны

На виртуальной машине client под вашим пользователем откройте терминал и с помощью утилиты dig убедитесь в наличии DNS-записи о клиенте в прямой DNS-зоне:

```
dig @192.168.1.1 client.user.net
```

В отчёте построчно прокомментируйте выведенную на экран информацию.

3.4.6. Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине server перейдите в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/, создайте в нём каталог dhcp, в который поместите 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. Замените конфигурационные файлы DNS-сервера:

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

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

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

Открыв его на редактирование, пропишите в нём следующий скрипт:

```
#!/bin/bash
```

```
echo "Provisioning script $0"
```

```
echo "Install needed packages"  
dnf -y install dhcp-server
```

```
echo "Copy configuration files"  
cp -R /vagrant/provision/server/dhcp/etc/* /etc
```

```
chown -R dhcpd:dhcpd /etc/dhcp
```

```
restorecon -vR /etc  
restorecon -vR /var/lib/dhcpd
```

```
echo "Configure firewall"  
firewall-cmd --add-service=dhcp  
firewall-cmd --add-service=dhcp --permanent
```

```
echo "Start dhcpd service"  
systemctl --system daemon-reload  
systemctl enable dhcpd  
systemctl start dhcpd
```

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 виртуальные машины client и server можно выключить.

3.5. 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 работы;
 - подробное описание настроек служб в соответствии с заданием;
 - полные тексты конфигурационных файлов настраиваемых в работе служб;

- результаты проверки корректности настроек служб в соответствии с заданием (подтверждённые скриншотами).
- 4. Выводы, согласованные с заданием работы.
- 5. Ответы на контрольные вопросы.

3.6. Контрольные вопросы

1. В каких файлах хранятся настройки сетевых подключений?
2. За что отвечает протокол DHCP?
3. Поясните принцип работы протокола DHCP. Какими сообщениями обмениваются клиент и сервер, используя протокол DHCP?
4. В каких файлах обычно находятся настройки DHCP-сервера? За что отвечает каждый из файлов?
5. Что такое DDNS? Для чего применяется DDNS?
6. Какую информацию можно получить, используя утилиту `ifconfig`? Приведите примеры с использованием различных опций.
7. Какую информацию можно получить, используя утилиту `ping`? Приведите примеры с использованием различных опций.

При ответах на вопросы рекомендуется ознакомиться с источниками [1–3].

Список литературы

1. *Barr D.* Common DNS Operational and Configuration Errors : RFC / RFC Editor. — 02.1996. — DOI: 10.17487/rfc1912.
2. *Droms R.* Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1–45. — DOI: 10.17487/rfc2131.
3. Dynamic Updates in the Domain Name System (DNS UPDATE), RFC 2136 : RFC / P. Vixie, S. Thomson, Y. Rekhter, J. Bound ; RFC Editor. — 04.1997. — DOI: 10.17487/RFC2136.