

МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И
МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ
ФЕДЕРАЦИИ

«Сибирский государственный университет
телекоммуникаций и информатики»
(СибГУТИ)

ОТЧЕТ
по дисциплине
«*WEB-технологии*»

по теме:
Настройка DNS, DHCP сервера для локальной сети и динамическое
выделение DNS зон
UBUNTU 24.10

Студент:
Группы ИКС-432

А.А. Пастухов

Предподаватель:

А.В. Андреев

Новосибирск 2025

Оглавление

ВВЕДЕНИЕ.....	3
1 Основные настройки DNS+DHCP сервера	4
2 Подготовка для установки DNS сервера	6
Заключение.....	14

ВВЕДЕНИЕ

В рамках данной работы рассматривается процесс настройки сетевого шлюза на базе операционной системы Ubuntu 24.10. Будут подробно разобраны основные этапы конфигурации, включая настройку сетевых интерфейсов, активацию функций маршрутизации, а также применение инструмента iptables для управления сетевым трафиком. Эти шаги необходимы для обеспечения стабильной и безопасной работы сети, а также для эффективного распределения ресурсов между подключенными устройствами.

Особое внимание уделяется роли DNS (Domain Name System) и DHCP (Dynamic Host Configuration Protocol) серверов в современных локальных сетях. DNS-сервер выполняет критически важную функцию, преобразуя доменные имена в IP-адреса, что значительно упрощает доступ к сетевым ресурсам. DHCP-сервер, в свою очередь, автоматически назначает IP-адреса устройствам, что минимизирует необходимость ручной настройки и снижает вероятность ошибок. В рамках работы будет произведена настройка DNS и DHCP серверов, а также реализована интеграция между ними для обеспечения динамического обновления DNS-зон. Это позволит автоматически регистрировать устройства в DNS при получении IP-адресов через DHCP, что повысит удобство управления сетью и обеспечит более гибкую работу с подключенными устройствами.

Такой подход не только упрощает администрирование сети, но и повышает ее отказоустойчивость, что особенно важно в условиях растущего числа подключенных устройств и увеличения нагрузки на сетевую инфраструктуру.

1 ОСНОВНЫЕ НАСТРОЙКИ DNS+DHCP СЕРВЕРА

DNS (Domain Name System) — это система, которая преобразует доменные имена в IP-адреса. DNS-сервер хранит записи о доменных именах и соответствующих им IP-адресах, что позволяет пользователям обращаться к сетевым ресурсам по именам, а не по числовым адресам.

DHCP — это протокол, который автоматически назначает IP-адреса и другие сетевые параметры (например, шлюз по умолчанию, DNS-серверы) устройствам в сети. Это упрощает управление сетью, так как администратору не нужно вручную настраивать IP-адреса для каждого устройства. DHCP-сервер выдает IP-адреса из заданного диапазона (пула) на определенное время (аренда). По истечении срока аренды устройство может запросить новый IP-адрес.

Динамическое обновление DNS-зон — это процесс, при котором DHCP-сервер автоматически обновляет записи в DNS-сервере при назначении IP-адресов устройствам. Это позволяет устройствам в сети быть доступными по доменным именам, которые автоматически регистрируются при получении IP-адреса.

BIND9 — это популярный DNS-сервер, который используется для управления доменными зонами и обработки DNS-запросов.

Основные файлы конфигурации BIND9:

- `named.conf.options`: Содержит общие настройки DNS-сервера, такие как `forwarders` (вышестоящие DNS-серверы) и `listen-on` (IP-адреса, на которых сервер будет принимать запросы).
- `named.conf.local`: Содержит описание локальных зон, которые обслуживают DNS-серверы и `listen-on` (IP-адреса, на которых сервер будет принимать запросы).
- `named.conf.local`: Содержит описание локальных зон, которые обслуживает DNS-сервер.

- forward.db: Файл зоны прямого просмотра, содержащий записи типа A, NS, SOA и т.д.
- reverse.db: Файл зоны обратного просмотра, содержащий записи типа PTR.

ISC DHCP — это популярный DHCP-сервер, который используется для автоматического назначения IP-адресов устройствам в сети.

Основные параметры DHCP-сервера:

- range: Диапазон IP-адресов, которые будут выдаваться устройствам.
- option domain-name-servers: Указывает DNS-серверы, которые будут использоваться клиентами.
- option domain-name: Указывает доменное имя, которое будет присвоено клиентам.
- option routers: Указывает шлюз по умолчанию для клиентов.
- ddns-updates: Включает динамическое обновление DNS-зон.

Для того чтобы DHCP-сервер мог обновлять DNS-записи, необходимо настроить взаимодействие между DHCP и DNS серверами. Это делается с помощью ключа rndc-key, который используется для аутентификации DHCP-сервера при обновлении DNS-зон.

DHCP-сервер автоматически создает DNS-записи для устройств, которые получают IP-адреса. Например, если устройство с именем DESKTOP_NAME01 получает IP-адрес 192.168.1.1

2 Подготовка для установки DNS сервера

Перед началом работы необходимо переименовать имя хоста в рабочей системе для его дальнейшей настройки и использования.

```
root@server:/home/arown# hostnamectl set-hostname sanya
root@server:/home/arown# nano /etc/hosts
root@server:/home/arown# nano /etc/hosts
root@server:/home/arown#
```

Рисунок 1 – изменение имени хоста

Так же необходимым этапом является изменение имени хоста не только через команду `hostnamectl set-hostname SERVER_HOSTNAME`, но и так же требуется внести изменения в файле `/etc/hosts`.

```
GNU nano 8.1 /etc/hosts
127.0.0.1 localhost
127.0.1.1 sanya

# The following lines are desirable for IPv6 capable hosts
::1      ip6-localhost ip6-loopback
fe00::0  ip6-localnet
ff00::0  ip6-mcastprefix
ff02::1  ip6-allnodes
ff02::2  ip6-allrouters
```

Рисунок 2 – изменение имени хоста в файле `/etc/hosts`

Повторяем аналогичные этапы для виртуальной машины Desktop 1.

Выполняя команду `nano /etc/iptables/rules.v4`, мы попадаем в файл с установленными правилами маршрутизации пакетов. Нам необходимо удалить два правила по маршрутизации:

- `-A PREROUTING -i enp0s8 -p tcp -m tcp --dport 53 -j DNAT --to-destination 8.8.8.8:53`

- -A PREROUTING -i enp0s8 -p udp -m udp --dport 53 -j DNAT --to-destination 8.8.8.8:53

```

root@server: /home/arown
GNU nano 8.1 /etc/iptables/rules.v4
# Generated by iptables-save v1.8.10 (nf_tables) on Tue Mar 18 15:55:17 2025
*filter
:INPUT ACCEPT [1967:9632375]
:FORWARD ACCEPT [9:784]
:OUTPUT ACCEPT [1398:117169]
-A FORWARD -p tcp -m tcp --tcp-flags SYN,RST SYN -j TCPMSS --clamp-mss-to-pmtu
-A FORWARD -i enp0s3 -o enp0s3 -j REJECT --reject-with icmp-port-unreachable
COMMIT
# Completed on Tue Mar 18 15:55:17 2025
# Generated by iptables-save v1.8.10 (nf_tables) on Tue Mar 18 15:55:17 2025
*nat
:PREROUTING ACCEPT [460:30097]
:INPUT ACCEPT [371:23679]
:OUTPUT ACCEPT [117:10096]
:POSTROUTING ACCEPT [70:5846]
-A POSTROUTING -o enp0s3 -j MASQUERADE
COMMIT
# Completed on Tue Mar 18 15:55:17 2025
[ Прочитано 18 строк ]
^G Справка      ^O Записать    ^F Поиск      ^K Вырезать   ^T Выполнить  ^С Позиция
^X Выход        ^R ЧитФайл    ^\ Замена    ^U Вставить   ^J Выводить   ^/ К строке

```

Рисунок 3 – удаление двух правил маршрутизации

Как уже упоминалось в теоретической части, Bind - это популярный DNS – сервер, который используется для управления доменными зонами и обработки DNS – запросов. Для его установки потребуется для начало проверить обновления всех пакетов командой `apt-get update`, после чего можно приступить к установке сервера командой `apt install bind9`.

```
root@sanya:/home/arown# sudo apt install bind9 -y
К установке:
  bind9

Зависимости к установке:
  bind9-utils

Предлагаемые пакеты:
  bind-doc ufw

Сводка:
```

Рисунок 4 – установка DNS-сервера bind9

Переходим к настройке bind9. Для этого отредактируем файл `named.conf.options`

```
forwarders {
    8.8.8.8;
};

//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys.  See https://www.isc.org/bind-keys
//=====
dnssec-validation auto;

listen-on {
    127.0.0.1;
    192.168.11.1;
};

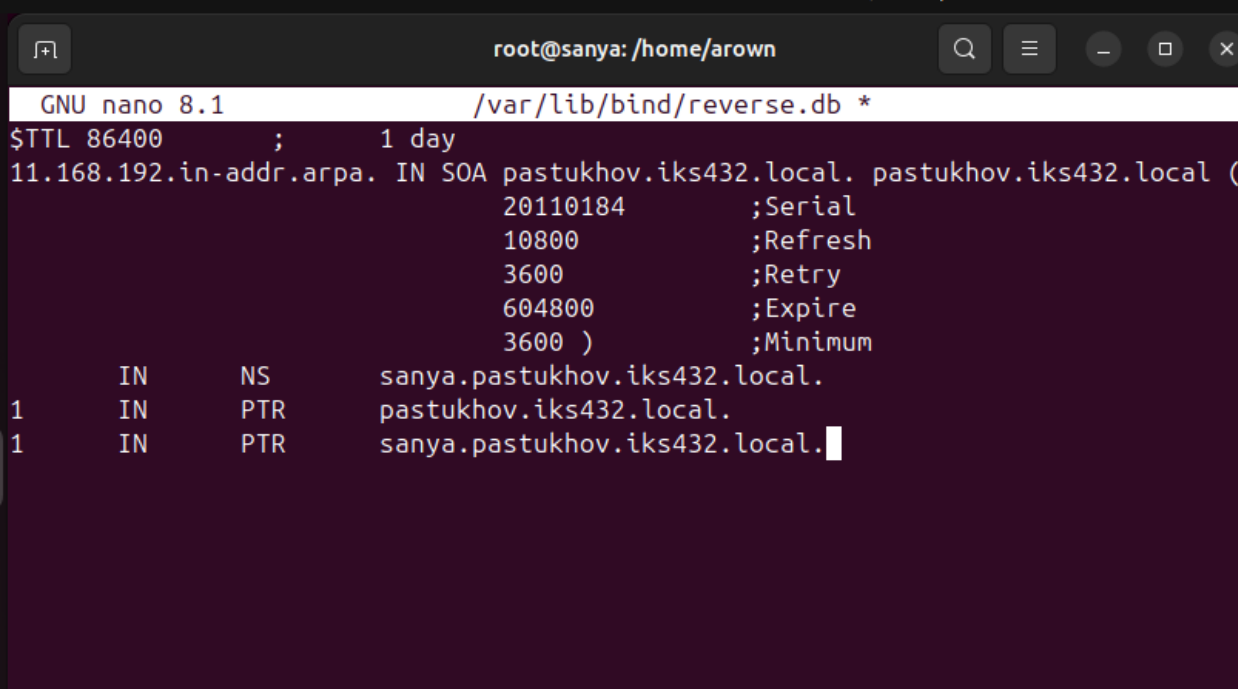
};
```

Рисунок 5 – Настройка DNS-сервера Bind9

Далее переходим к настройке зон, которые DNS-сервер будет обслуживать.

Для этого переходим в содержимое файла `named.conf.local` и вносим информацию о ключе, который позволит настройку автоматического обновления зоны, а так же и саму зону обслуживания.

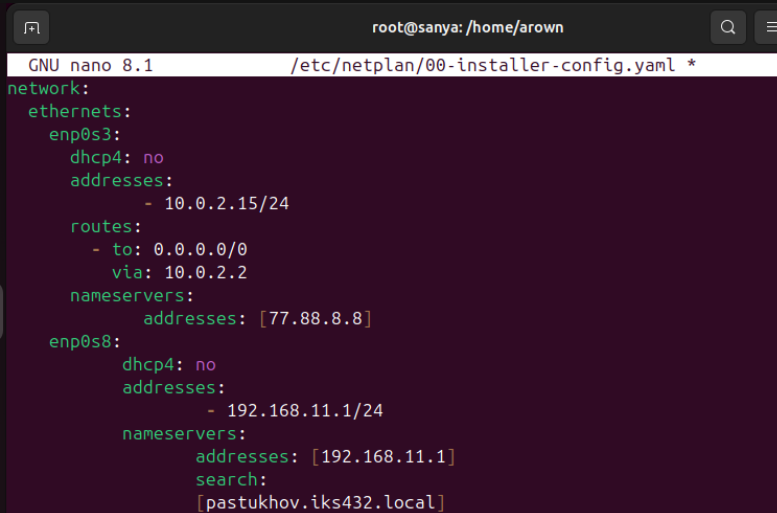
Теперь создадим файл зоны обратного просмотра, чтобы не выдумывать ничего, назовём его reverse.db.



```
root@sanya: /home/arown
GNU nano 8.1 /var/lib/bind/reverse.db *
$TTL 86400 ; 1 day
11.168.192.in-addr.arpa. IN SOA pastukhov.iks432.local. pastukhov.iks432.local (
                                20110184 ;Serial
                                10800 ;Refresh
                                3600 ;Retry
                                604800 ;Expire
                                3600 ) ;Minimum
IN NS sanya.pastukhov.iks432.local.
1 IN PTR pastukhov.iks432.local.
1 IN PTR sanya.pastukhov.iks432.local.
```

Рисунок 8 – создание файла зоны обратного просмотра

Перезапустим bind9 с помощью команды `systemctl restart bind9`. Теперь необходимо проверить работоспособность нашего сервера локально. Необходимо поправить запись `dns – nameserveres` в настройках сети. Для этого переходим в `nano /etc/netplan/00-installer-config.yaml` и вносим следующие изменения.



```
root@sanya: /home/arown
GNU nano 8.1 /etc/netplan/00-installer-config.yaml *
network:
  ethernet:
    enp0s3:
      dhcp4: no
      addresses:
        - 10.0.2.15/24
      routes:
        - to: 0.0.0.0/0
          via: 10.0.2.2
      nameservers:
        addresses: [77.88.8.8]
    enp0s8:
      dhcp4: no
      addresses:
        - 192.168.11.1/24
      nameservers:
        addresses: [192.168.11.1]
        search:
          [pastukhov.iks432.local]
```

Рисунок 9 – изменение настроек сети

После внесения изменений, необходимо перезагрузить сервер.
Проверим самоопределение имени нашего сервера, введя команду
nslookup SERVER_HOSTNAME.

```
root@sanya:/home/arown# nslookup sanya
Server:          127.0.0.53
Address:         127.0.0.53#53

Name:   sanya
Address: 127.0.1.1

root@sanya:/home/arown#
```

Рисунок 10 – результаты команды nslookup SERVER_HOSTNAME

Если имя преобразовано в IP значит зона прямого просмотра работает нормально. Теперь проверим зону обратного просмотра, введя команду
nslookup 192.168.N.1

```
root@sanya:/home/arown# nslookup 192.168.11.1 127.0.0.1
1.11.168.192.in-addr.arpa      name = pastukhov.iks432.local.
1.11.168.192.in-addr.arpa      name = sanya.pastukhov.iks432.local.

root@sanya:/home/arown#
```

Рисунок 11 – результаты вывода команд nslookup

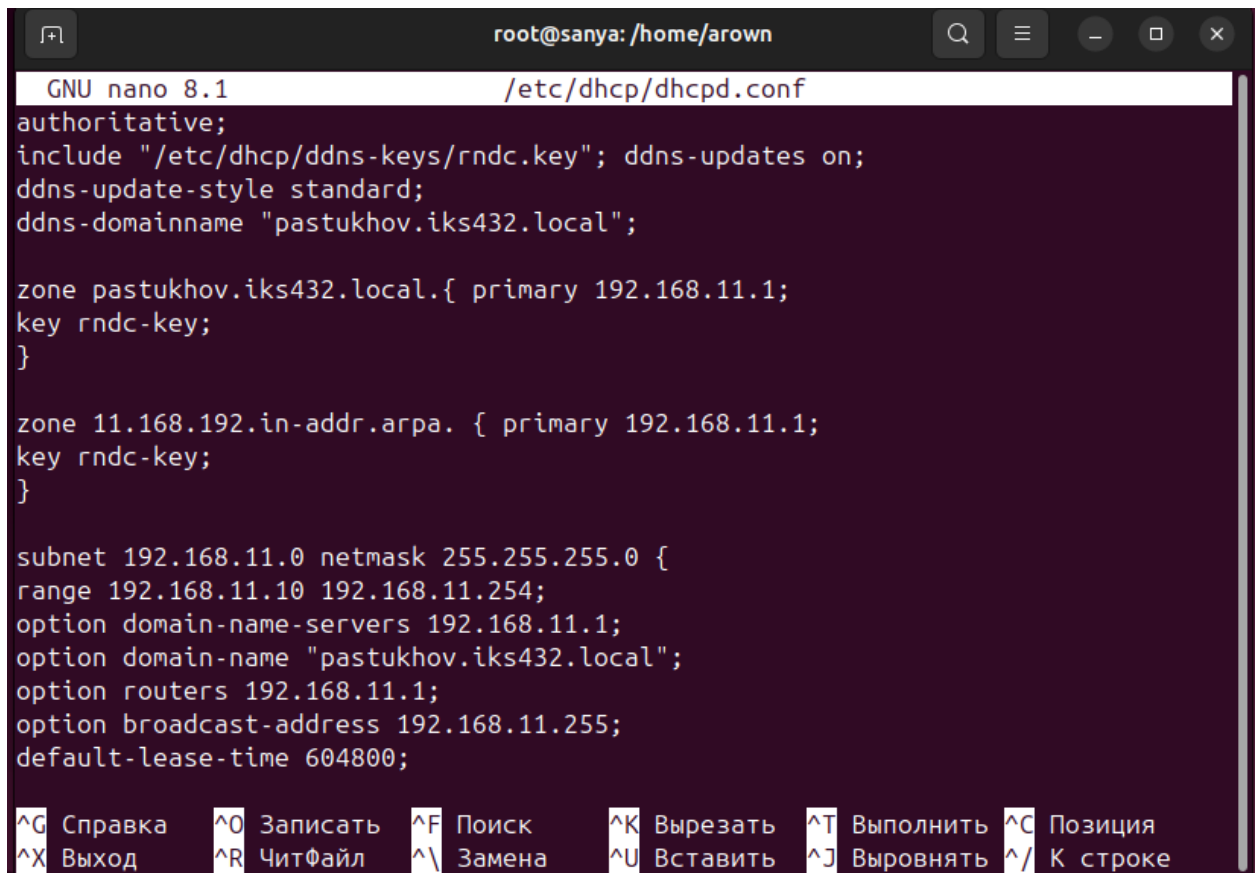
Если ответ получен, значит обратное разрешение имён работает.
Скопируем файл с ключом из Bind, так как у сервиса не хватит прав доступа к каталогу Bind.

Вводим команду:

```
cp -Rr /etc/bind/rndc.key /etc/dhcp/ddns-keys
```

Отредактируем конфигурационный файл DHCP сервера.
Для этого введём команду:

```
nano /etc/dhcp/dhcpd.conf
```



```
GNU nano 8.1 /etc/dhcp/dhcpd.conf
authoritative;
include "/etc/dhcp/ddns-keys/rndc.key"; ddns-updates on;
ddns-update-style standard;
ddns-domainname "pastukhov.iks432.local";

zone pastukhov.iks432.local.{ primary 192.168.11.1;
key rndc-key;
}

zone 11.168.192.in-addr.arpa. { primary 192.168.11.1;
key rndc-key;
}

subnet 192.168.11.0 netmask 255.255.255.0 {
range 192.168.11.10 192.168.11.254;
option domain-name-servers 192.168.11.1;
option domain-name "pastukhov.iks432.local";
option routers 192.168.11.1;
option broadcast-address 192.168.11.255;
default-lease-time 604800;
}
```

Рисунок 12 – редактирование конфигурации DHCP сервера

После внесения изменений в файл, перезапустим DNS – сервер.

Введём команды:

```
systemctl restart bind9
```

```
service isc-dhcp-server restart
```

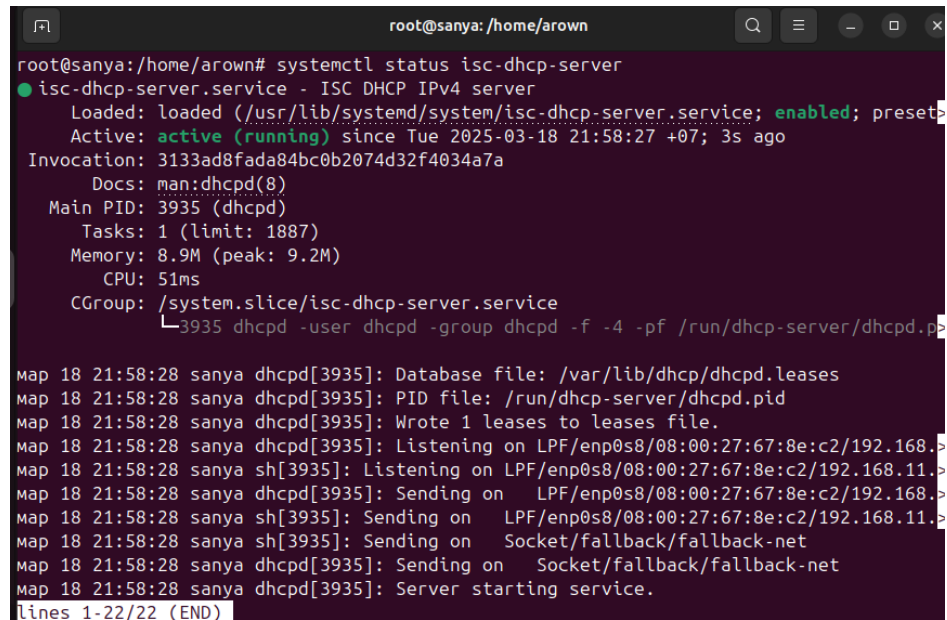
Подключаем наш клиентский хост к локальной сети, предположим, что его имя `DESKTOP_NAME01`, он получит IP от нашего DHCP сервера, а DHCP сервер создаст DNS запись вида `DESKTOP_NAME01.STUDENT.GROUP.local`.

Попробуем выполнить запрос по имени, введя команду:

```
nslookup DESKTOP_NAME01
```

Если же в процессе выполнения команды, не был корректно выполнены вывод, проверяем файлы на наличие синтаксических ошибок или ошибок в настройке сервера.

Итогом работы после перезапуска DHCP – сервера, результатом программы должен быть вывод статуса DHCP – сервера.



```
root@sanya:/home/arown# systemctl status isc-dhcp-server
● isc-dhcp-server.service - ISC DHCP IPv4 server
   Loaded: loaded (/usr/lib/systemd/system/isc-dhcp-server.service; enabled; preset
   Active: active (running) since Tue 2025-03-18 21:58:27 +07; 3s ago
   Invocation: 3133ad8fada84bc0b2074d32f4034a7a
     Docs: man:dhcpcd(8)
    Main PID: 3935 (dhcpcd)
      Tasks: 1 (limit: 1887)
     Memory: 8.9M (peak: 9.2M)
        CPU: 51ms
    CGroup: /system.slice/isc-dhcp-server.service
            └─3935 dhcpcd -user dhcpcd -group dhcpcd -f -4 -pf /run/dhcp-server/dhcpcd.p

map 18 21:58:28 sanya dhcpcd[3935]: Database file: /var/lib/dhcp/dhcpcd.leases
map 18 21:58:28 sanya dhcpcd[3935]: PID file: /run/dhcp-server/dhcpcd.pid
map 18 21:58:28 sanya dhcpcd[3935]: Wrote 1 leases to leases file.
map 18 21:58:28 sanya dhcpcd[3935]: Listening on LPF/enp0s8/08:00:27:67:8e:c2/192.168.
map 18 21:58:28 sanya sh[3935]: Listening on LPF/enp0s8/08:00:27:67:8e:c2/192.168.11.
map 18 21:58:28 sanya dhcpcd[3935]: Sending on LPF/enp0s8/08:00:27:67:8e:c2/192.168.
map 18 21:58:28 sanya sh[3935]: Sending on LPF/enp0s8/08:00:27:67:8e:c2/192.168.11.
map 18 21:58:28 sanya sh[3935]: Sending on Socket/fallback/fallback-net
map 18 21:58:28 sanya dhcpcd[3935]: Sending on Socket/fallback/fallback-net
map 18 21:58:28 sanya dhcpcd[3935]: Server starting service.
lines 1-22/22 (END)
```

Рисунок 13 – проверка статуса DHCP – сервера

Заключение

В данной практической работе была выполнена настройка связки **DNS** и **DHCP** серверов для локальной сети с поддержкой динамического обновления DNS-зон. Основная цель работы заключалась в автоматизации процессов назначения IP-адресов устройствам в сети и их регистрации в DNS, что позволяет упростить управление сетевыми ресурсами и обеспечить удобный доступ к устройствам по доменным именам.