Отчёт по лабораторной работе 2

Настройка DNS-сервера

Суннатилло Махмудов

Содержание

# 1 Цель работы

Приобретение практических навыков по установке и конфигурированию DNS-сервера, а также освоение принципов работы системы доменных имён.

# 2 Теоретические сведения

**DNS (Domain Name System)** — распределённая система, сопоставляющая доменные имена и IP-адреса. Основные элементы:

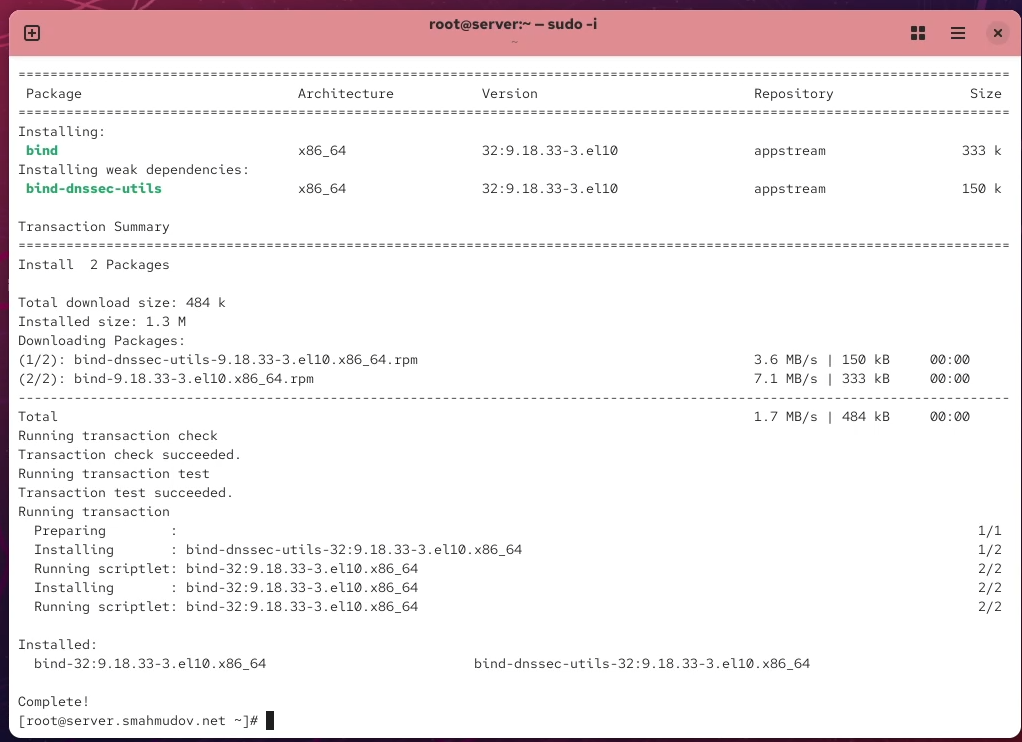
* **DNS-сервер** — программное обеспечение (чаще всего *BIND*), обслуживающее запросы клиентов.
* **DNS-клиент** — библиотека или утилита, формирующая запросы к серверам.
* **Зона** — часть пространства имён доменов.
* **Прямая зона** — сопоставляет имя хоста с IP-адресом.
* **Обратная зона** — сопоставляет IP-адрес с именем хоста.
* **Типы записей**:
  + **SOA** — начало зоны, параметры обновления;
  + **NS** — список DNS-серверов;
  + **A** — соответствие имени хоста IP;
  + **PTR** — обратное соответствие IP имени;
  + **CNAME** — псевдоним;
  + **MX** — почтовый сервер.

Для диагностики используются утилиты **dig** и **host**. Первая позволяет гибко формировать DNS-запросы, вторая упрощает получение записей зоны.

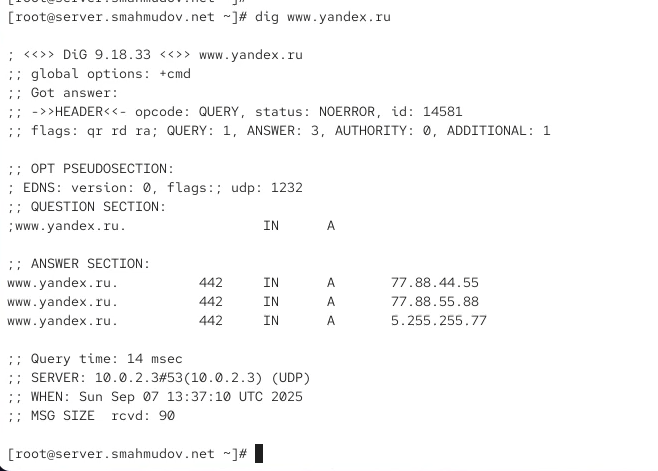
# 3 Выполнение лабораторной работы

## 3.1 Установка DNS-сервера

1. Была запущена виртуальная машина **server** и подготовлено окружение для дальнейшей установки сервисов.
2. Выполнена установка пакетов **bind** и **bind-utils**, обеспечивающих работу DNS-сервера и предоставляющих вспомогательные инструменты.

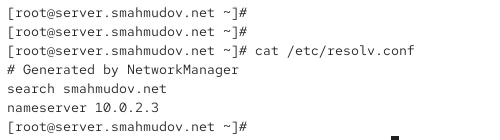
* 
* Рис. 1: Установка bind и bind-utils

1. Проведена проверка работы сервиса с использованием утилиты **dig**. Запрос к внешнему ресурсу показал, что сервер корректно обрабатывает DNS-запросы.

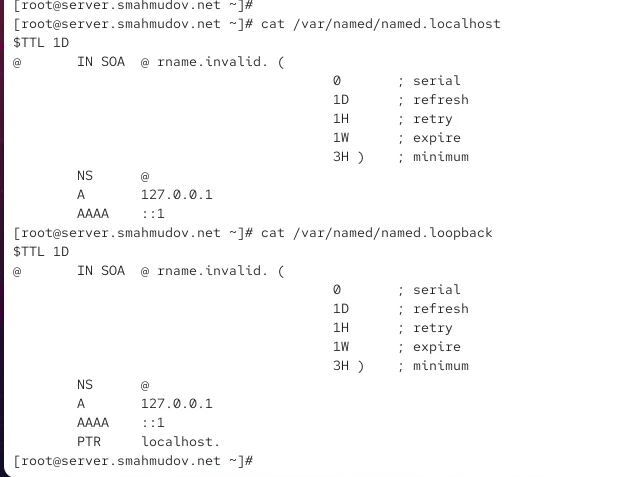
* 
* Рис. 2: Результат запроса dig к www.yandex.ru

## 3.2 Конфигурирование кэширующего DNS-сервера

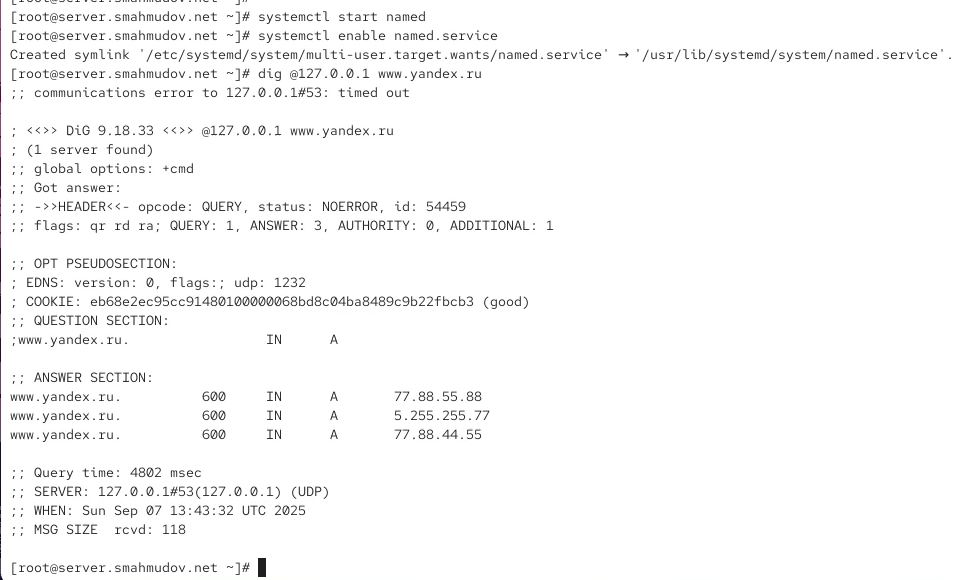
1. Изучено содержимое файла /etc/resolv.conf, где задаются адреса DNS-серверов по умолчанию.

* 
* Рис. 3: Файл resolv.conf с настройками

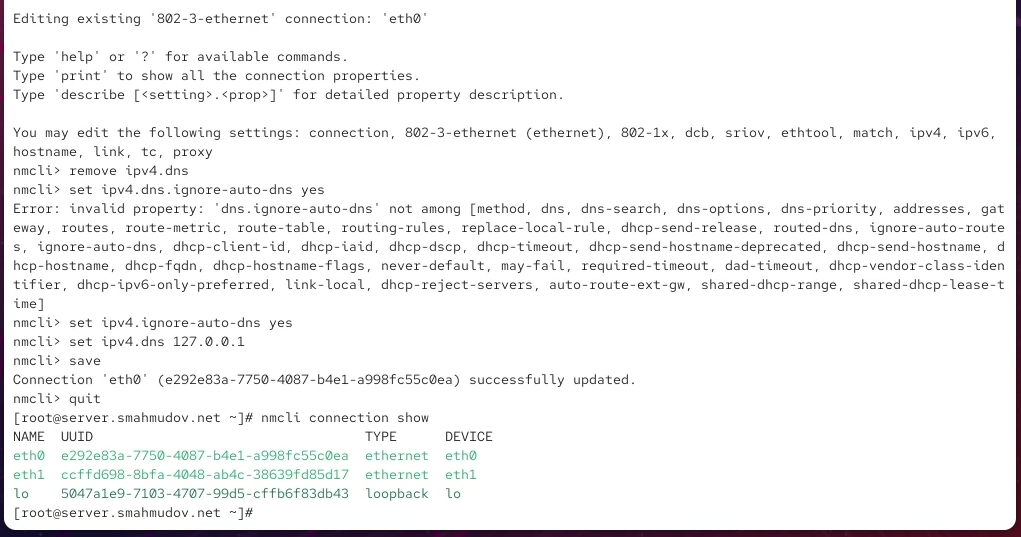
1. Ознакомление с базовыми зонами named.localhost и named.loopback, которые применяются для проверки локальной работы сервера.

* 
* Рис. 4: Содержимое файлов named.localhost и named.loopback

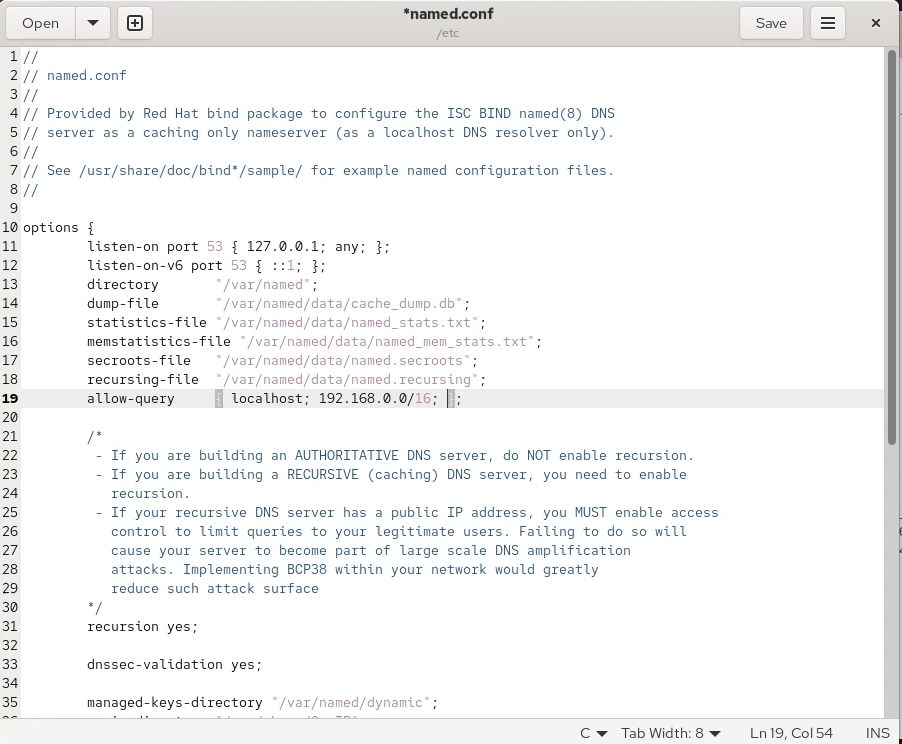
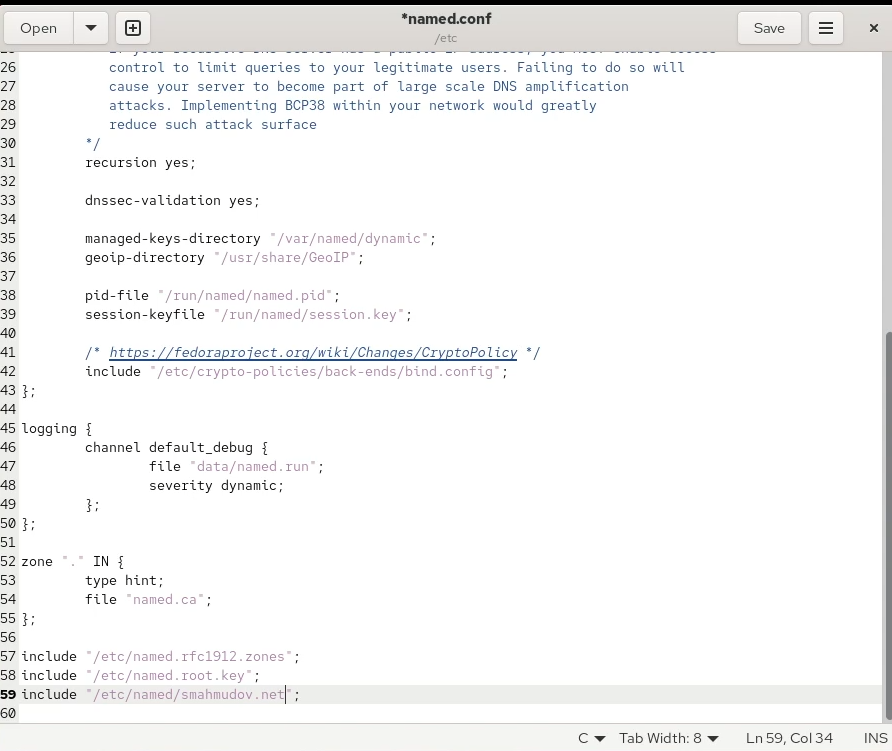
1. Сервис **named** был запущен и добавлен в автозагрузку, что гарантирует его постоянную работу после перезапуска системы.
2. Проведено сравнение запросов через внешний сервер и через локальный. В результате было установлено, что локальный сервер способен самостоятельно выполнять резолвинг.

* 
* Рис. 5: Сравнение запросов через внешний и локальный сервер

1. С помощью утилиты **nmcli** была изменена конфигурация сетевого подключения: заданы параметры для использования локального сервера как основного DNS.

* 
* Рис. 6: Настройка DNS через nmcli

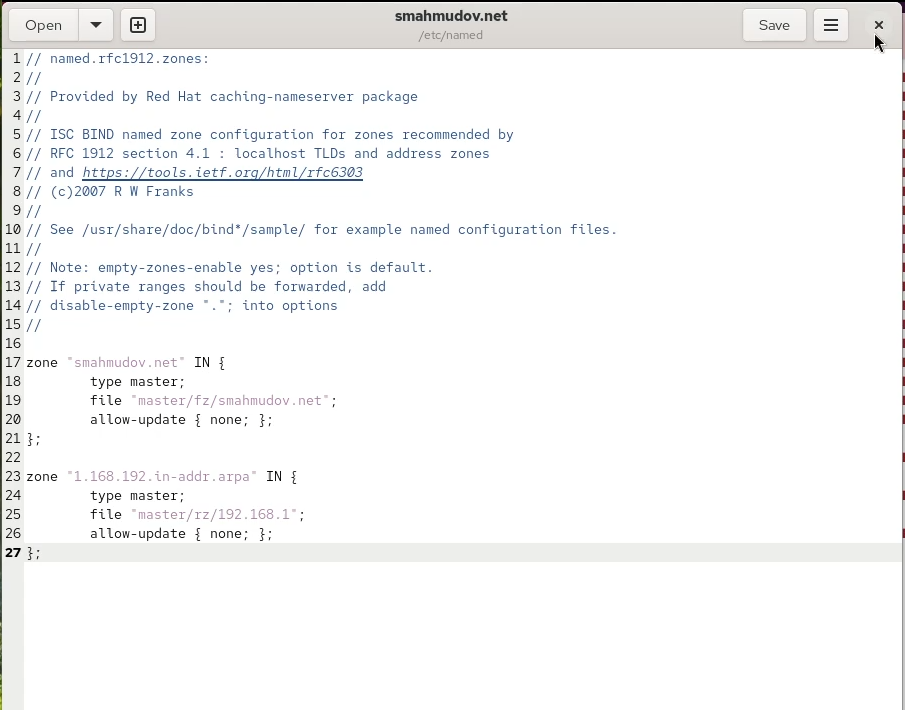
1. Внесены изменения в основной конфигурационный файл named.conf. Был расширен список клиентов, которым разрешены запросы, и разрешено использование сети 192.168.0.0/16.

* 
* Рис. 7: Изменения в named.conf (часть 1)
* 
* Рис. 8: Изменения в named.conf (часть 2)

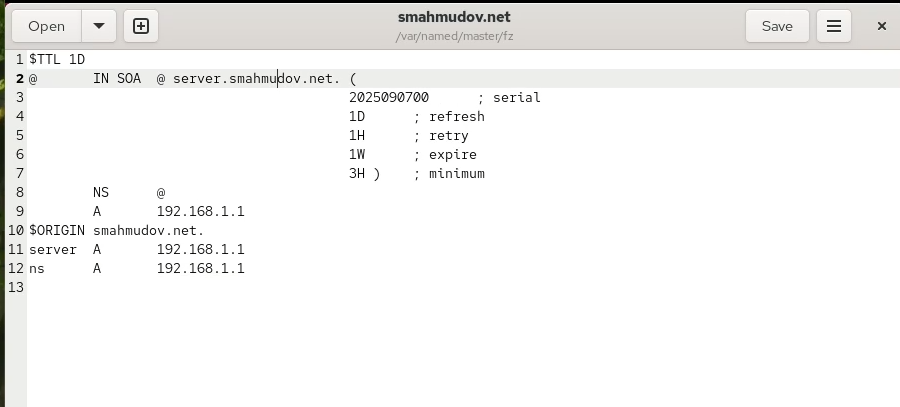
1. Настроены правила файрвола, что обеспечило доступность сервиса DNS из внутренней сети.

## 3.3 Конфигурирование первичного DNS-сервера

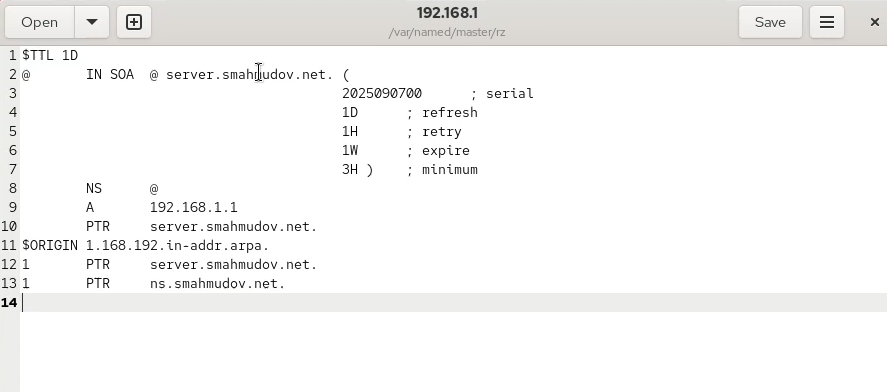
1. Создан новый файл зоны smahmudov.net, куда были добавлены записи для прямого и обратного разрешения. Это позволило связать доменные имена с IP-адресами.

* 
* Рис. 9: Файл конфигурации зоны smahmudov.net

1. Настроен файл прямой зоны, где указаны адреса серверов и NS-записи.

* 
* Рис. 10: Прямая зона smahmudov.net

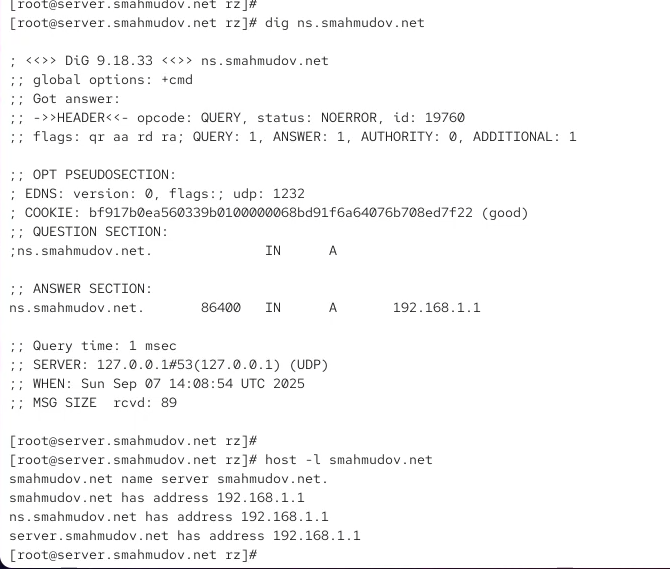
1. Настроен файл обратной зоны, в котором определены записи PTR для IP-адресов.

* 
* Рис. 11: Обратная зона для сети 192.168.1

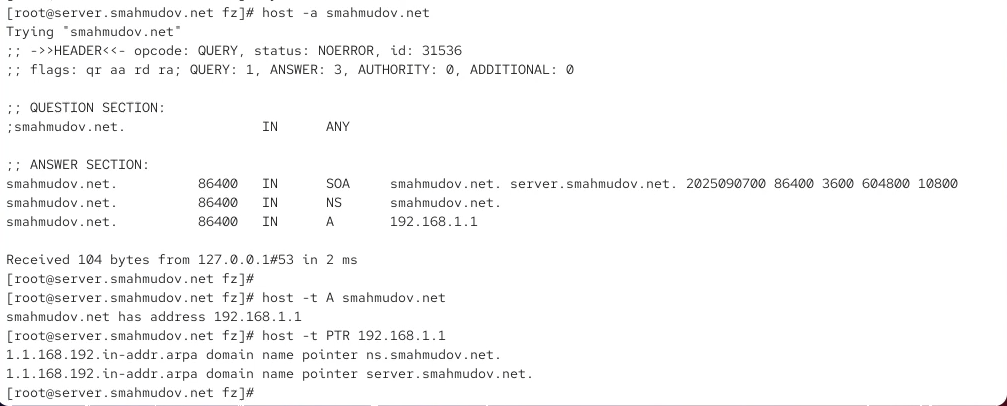
1. После корректировки конфигурации был перезапущен сервис **named**. Это позволило применить все внесённые изменения.

## 3.4 Анализ работы DNS-сервера

1. С помощью утилиты **dig** была проверена работоспособность зоны: запрос к имени ns.smahmudov.net показал корректный IP-адрес.

* 
* Рис. 12: Проверка зоны с помощью dig

1. Проверка через утилиту **host** подтвердила, что записи зоны доступны и корректно разрешаются. Получены результаты как по прямым, так и по обратным запросам.

* 
* Рис. 13: Проверка зоны с помощью host

## 3.5 Настройка Vagrant

Был создан скрипт автоматизации dns.sh, который выполняет установку пакетов, копирование подготовленных конфигурационных файлов, настройку прав доступа и SELinux, а также включает службу **named** и настраивает firewall. Этот скрипт позволяет воспроизводить выполненные действия автоматически при развёртывании виртуальной машины.

В Vagrantfile добавлен вызов этого скрипта, что обеспечивает автоматическую настройку DNS-сервера в процессе provision.

# 4 Вывод

В ходе работы установлен и настроен DNS-сервер на основе BIND. Реализована прямая и обратная зоны, проверена их корректность с помощью утилит dig и host. Настроен кэширующий и первичный сервер. Автоматизация обеспечена через скрипт Vagrant, что позволяет ускорить процесс развёртывания и исключить ошибки ручной конфигурации.

# 5 Контрольные вопросы

1. **Что такое DNS?** DNS (Domain Name System) — это распределённая иерархическая система, которая связывает доменные имена с IP-адресами и наоборот. Она облегчает работу пользователей, позволяя использовать понятные имена вместо числовых адресов.
2. **Каково назначение кэширующего DNS-сервера?** Кэширующий DNS-сервер хранит результаты предыдущих запросов, чтобы при повторных обращениях не обращаться к внешним серверам. Это ускоряет резолвинг имён и снижает нагрузку на сеть.
3. **Чем отличается прямая DNS-зона от обратной?** Прямая зона отображает имя хоста в IP-адрес, а обратная зона наоборот — IP-адрес в доменное имя. Оба типа зон используются для полного функционирования DNS.
4. **В каких каталогах и файлах располагаются настройки DNS-сервера? Кратко охарактеризуйте, за что они отвечают.** Основные файлы: /etc/named.conf (главный конфигурационный файл), /etc/named/ (вспомогательные зоны и включения), /var/named/ (файлы зон). В них задаются параметры сервера, зоны и ресурсные записи.
5. **Что указывается в файле resolv.conf?** В /etc/resolv.conf перечисляются адреса DNS-серверов, к которым будет обращаться клиент по умолчанию, а также поисковые домены.
6. **Какие типы записи описания ресурсов есть в DNS и для чего они используются?**

* **SOA** — старт зоны, хранит параметры синхронизации;
* **NS** — список серверов зоны;
* **A** — имя → IPv4;
* **AAAA** — имя → IPv6;
* **PTR** — обратное разрешение IP;
* **CNAME** — каноническое имя (псевдоним);
* **MX** — почтовый сервер;
* **TXT** — произвольный текст (например, SPF-записи).

1. **Для чего используется домен in-addr.arpa?** Этот домен предназначен для обратного разрешения имён: сопоставления IP-адресов с доменными именами.
2. **Для чего нужен демон named?** named — это основной процесс BIND, реализующий функции DNS-сервера: обработка запросов, кэширование и работа с зонами.
3. **В чём заключаются основные функции slave-сервера и master-сервера?** Master хранит оригинальные файлы зоны, а slave периодически синхронизируется с master, обеспечивая отказоустойчивость и балансировку нагрузки.
4. **Какие параметры отвечают за время обновления зоны?** В SOA-записи:

* **serial** — версия зоны;
* **refresh** — интервал обновления;
* **retry** — интервал повторной попытки;
* **expire** — время жизни зоны без обновления;
* **minimum** — время кэширования отрицательных ответов.

1. **Как обеспечить защиту зоны от скачивания и просмотра?** Использовать ограничение allow-query, ACL, а также ключи TSIG для аутентификации серверов.
2. **Какая запись RR применяется при создании почтовых серверов?** Используется запись **MX**, которая указывает почтовый сервер и его приоритет.
3. **Как протестировать работу сервера доменных имён?** С помощью утилит dig, host, nslookup, а также проверкой логов через journalctl.
4. **Как запустить, перезапустить или остановить какую-либо службу в системе?** Использовать systemd: systemctl start|stop|restart <service>.
5. **Как посмотреть отладочную информацию при запуске какого-либо сервиса или службы?** Через journalctl -xe, включение уровня debug в конфигурации или добавление параметров запуска.
6. **Где храниться отладочная информация по работе системы и служб? Как её посмотреть?** В системных журналах /var/log/messages, /var/log/secure, доступных через journalctl.
7. **Как посмотреть, какие файлы использует в своей работе тот или иной процесс? Приведите несколько примеров.** С помощью lsof -p PID или ls /proc/<PID>/fd. Пример: lsof -i :53 покажет файлы/сокеты, связанные с DNS.
8. **Приведите несколько примеров по изменению сетевого соединения при помощи командного интерфейса nmcli.**

* nmcli connection show — список соединений;
* nmcli connection edit eth0 — изменение параметров;
* nmcli connection up eth0 — активация соединения.

1. **Что такое SELinux?** Security-Enhanced Linux — механизм мандатного контроля доступа, повышающий безопасность системы.
2. **Что такое контекст (метка) SELinux?** Это набор атрибутов безопасности, который присваивается каждому объекту (файлу, процессу). Контекст определяет права доступа.
3. **Как восстановить контекст SELinux после внесения изменений в конфигурационные файлы?** С помощью команды restorecon -vR <path>.
4. **Как создать разрешающие правила политики SELinux из файлов журналов, содержащих сообщения о запрете операций?** Использовать утилиту audit2allow, которая на основе логов генерирует модули правил.
5. **Что такое булевый переключатель в SELinux?** Это параметр, позволяющий динамически менять политику (например, разрешить сервису доступ к сети).
6. **Как посмотреть список переключателей SELinux и их состояние?** Командой getsebool -a.
7. **Как изменить значение переключателя SELinux?** Командой setsebool -P <switch> on|off для постоянного изменения или без -P для временного.

# 6 Список литературы

1. Barr D. Common DNS Operational and Configuration Errors: RFC 1912. — DOI: 10.17487/rfc1912.
2. Security-Enhanced Linux: руководство пользователя. — URL: <https://docs-old.fedoraproject.org/ru-RU/Fedora/13/html/Security-Enhanced_Linux/index.html>
3. Systemd. — URL: <https://wiki.archlinux.org/index.php/Systemd>
4. Костромин В. А. Утилита lsof. — URL: <http://rus-linux.net/kos.php?name=/papers/lsof/lsof.html>
5. Поттеринг Л. Systemd для администраторов. — URL: <http://wiki.opennet.ru/Systemd>
6. NetworkManager project. — URL: <https://wiki.gnome.org/Projects/NetworkManager>
7. nmcli project. — URL: <https://developer.gnome.org/NetworkManager/stable/nmcli.html>