**Министерство науки и высшего образования Российской Федерации**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
**НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИТМО**

**Факультет цифровых трансформаций**

**Дисциплина:**

«**Телекоммуникационные системы и технологии**»

**ПРАКТИЧЕСКАЯ РАБОТА №7**

«DNS»

**Выполнили:**

Гаджиев С. И., Васильков Д. A., Лавренов Д. А. M3304

*\_\_\_\_\_\_\_\_\_\_Pulpy\_\_\_\_\_\_\_\_*

(подпись)

**Проверила:**

Дяченко Екатерина Олеговна

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(отметка о выполнении)

*\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_*

(подпись)

***Цель работы:***

Закрепить понимание принципов работы DNS, получить практические навыки использования утилит работы с серверами системы DNS и конфигурирования DNS сервера на платформе Linux;

***Требования:***

Установленная на компьютере среда виртуализации ORACLE Virtual Box с виртуальной машиной Linux Cent OS 7 (выполнять работу можно в любой ОС Linux, но все описания будут даваться для CentOS 7).

***Инструментальные средства:***

*Утилиты: firewall-cmd systemctl ip ping journalctlss netstat lsof dig*

*Файлы: /etc/named.conf, /etc/named*

*Утилиты работы с текстом: echo, grep, sed*

*Редакторы: vi, nano*

***Порядок выполнения работы:***

***Часть 1. Подготовка и проверка конфигурации.***

В VirtualBox:

1. Сделайте связанный клон виртуальной машины. Одну машину назовите c7-1, другой с7-2

2. Для виртуальной машины c7-1 добавьте второй сетевой интерфейс.

3. Подключите сетевой интерфейс c7-2 и новый сетевой интерфейс с7-1 к внутренней сети intnet.

4. Подключите исходный сетевой интерфейс с7-1 к NAT. В Linux:

5. Для внутренней сети задайте для машин с7-1 и c7-2 адреса 10.0.0.1 и 10.0.0.2 с маской 255.255.255.0.

6. Для исходного интерфейса c7-1 оставьте получение адреса автоматически от dhcp сервара VirtualBox

7. Для обоих хостов отключите использование ipv6.

8. Задайте имена хостов, советующие именам виртуальных машин.

9. Проверьте доступность хостов по внутренней сети и доступность внешней сети на хосте c7 -1.

10. Убедитесь, что на c7-2 в качестве шлюза по умолчанию и DNS задан адрес c7-1.

11. Установите на машине c7-1 пакеты bind и bind-utils

***Часть 2. Получение информации из DNS с помощью утилиты dig***

1. На хосте c7-1 с выполните команду dig www.itmo.ru. В консольном выводе изучите состав секций HEADER, QUESTION SECTION, ANSWER SECTION, AUTHORITY SECTION, SERVER: 192.168.0.1, WHEN и MSG SIZE. Соотнесите значения полей секции HEADER со значениями остальных полей. (!)

2. На хосте c7-1 с помощью утилиты dig решите следующие задачи (!):

a. Выведите только результат разрешения имени www.itmo.ru (только IP адрес)

b. Выведите на экран подробную информацию о разрешении имени, с выводом всех промежуточных серверов, определите какой именно DNS сервер вернул IP адрес хоста.

c. Выведите конфигурационную запись (SOA) домена itmo.ru, определите, значения каждого из числовых параметров записи, что они означают?

d. Определите, какие сервера обрабатывают почту домена itmo.ru.

e. Определите какие DNS сервера обслуживают зону itmo.ru и какие у них ip адреса.

f. Значение записи в зоне обратного просмотра для 87.250.250.242.

g. Определите количество серверов, поддерживающих корневую зону.

***Часть 3. Настройка кэширующего DNS сервера***

Цель этой части – настроить хост c7-1 как кэширующий DNS сервер для хоста c7-2.

1. С помощью утилиты firewall-cmd разрешите службе dns получать доступ к сети.

2. С помощью systemctl включите и запустите службу bind (она называется named)

3. Отредактируйте /etc/named.conf так, чтобы:

a. Сервер отвечал на IPv4 адресе из вашей локальной сети

b. Не работал поверх IPv6

c. Позволял обычные и рекурсивные запросы только с ip адресов вашей локальной сети (между c7-1 и с7-2) и с самого хоста c7-1.

d. Делал рекурсивные запросы.

e. Вместо версии сервера выводил при запросе «My Own DNS Server»

4. Проверьте разрешение имен на хосте c7-2.

***Часть 4. Создание собственной доменной зоны***

1. Отредактируйте /etc/named.conf так, чтобы добавить зону на сервер зону домена <fio>.local, где <fio> - ваши инициалы, причем ваш сервер должен быть для этого домена основным, не допускать трансфер зоны, разрешать все обновления и хранить зону в файле /var/named/<fio>.loсal.db

2. Для проверки файла конфигурации используйте утилиту named-checkconf

3. Создайте файл <fio>.local.db, содержащий следующие параметры для домена <fio>.local:

a. Имя основного DNS сервера ns1

b. E-mail администратора [hostmaster@<fio>.local](mailto:hostmaster@%3cfio%3e.local)

c. Серийный номер зоны по шаблону YYYYMMDDhh

d. Время обновления реплики 43200

e. Время до повторной попытки 3600

f. Время работы реплики без обновления 3600000

g. Минимальный TTL 300

h. Ip адрес ns1 равный внутреннему IP хоста c7-1

i. Имя gate с IP равным внутреннему IP хоста c7-1

j. Псевдоним www, направляющий клиента на хост gate.<fio>.local.

4. Для проверки файла зоны используйте утилиту named-checkzone

5. На хосте c7-2 проверьте, что все записи в вашем домене работают

***Вопросы и задания:***

1. Опишите, как в выводе команды dig соотносятся секции HEADER, QUESTION SECTION, ANSWER SECTION, AUTHORITY SECTION, SERVER, WHEN и MSG SIZE с полями секции HEADER. Опишите назначение каждой секции.

*Ответ*: Команда dig (Domain Information Groper) используется для запроса DNS-записей. В её выводе представлены различные секции, каждая из которых имеет своё назначение.

**1.1 HEADER**

Секция **HEADER** содержит метаданные запроса и ответа. Она включает такие поля, как:

* **id**: Уникальный идентификатор запроса, используемый для соответствия между запросом и ответом.
* **qr**: Флаг, указывающий, является ли сообщение ответом (1) или запросом (0).
* **opcode**: Тип запроса (обычно QUERY).
* **aa**: Флаг, указывающий, является ли ответ авторитетным (1) или нет (0).
* **tc**: Флаг, указывающий, что ответ обрезан.
* **rd**: Флаг рекурсивного запроса.
* **ra**: Флаг, указывающий, что сервер поддерживает рекурсивные запросы.
* **z**: Зарезервировано для будущего использования.
* **rcode**: Код ответа (например, NOERROR, NXDOMAIN и т.д.).
* **qdcount**: Количество вопросов в секции QUESTION.
* **ancount**: Количество ответов в секции ANSWER.
* **nscount**: Количество записей в секции AUTHORITY.
* **arcount**: Количество записей в секции ADDITIONAL.

**1.2 QUESTION SECTION**

Секция **QUESTION SECTION** содержит запрашиваемую информацию. Она включает в себя:

* **NAME**: Имя запрашиваемого домена.
* **TYPE**: Тип записи (A, AAAA, MX, и т.д.).
* **CLASS**: Класс записи (обычно IN для Internet).

**1.3 ANSWER SECTION**

Секция **ANSWER SECTION** содержит ответ на запрос. Каждая запись включает:

* **NAME**: Имя запрашиваемого домена.
* **TTL**: Время жизни записи, указывающее, как долго она может кэшироваться.
* **CLASS**: Класс записи (обычно IN).
* **TYPE**: Тип записи (например, A, AAAA).
* **DATA**: Данные, связанные с записью (например, IP-адрес для записи A).

**1.4 AUTHORITY SECTION**

Секция **AUTHORITY SECTION** содержит информацию об авторитетных DNS-серверах для запрашиваемого домена. Она включает записи о серверах имен (NS) и их IP-адресах, которые могут дать дополнительные сведения о домене.

**1.5 ADDITIONAL SECTION**

Секция **ADDITIONAL** (если присутствует) содержит дополнительные записи, которые могут быть полезны. Например, IP-адреса авторитетных DNS-серверов из секции AUTHORITY.

**1.6 SERVER**

Поле **SERVER** указывает на DNS-сервер, к которому был сделан запрос. Здесь отображается IP-адрес или имя сервера, использованного для разрешения запроса.

**1.7 WHEN**

Поле **WHEN** показывает дату и время выполнения запроса. Это полезно для аудита и отладки.

**1.8 MSG SIZE**

Поле **MSG SIZE** указывает размер ответа в байтах. Это может быть полезно для оценки объема данных, возвращаемых в ответе.

2. Как по ответу утилиты dig в Части 3 можно понять, что ответ получен именно от вашего кэширующего DNS сервера?

*Ответ*: чтобы понять, что ответ получен от вашего кэширующего DNS сервера, нужно обратить внимание на следующие аспекты в выводе dig:

1. Секция HEADER: если поле qr равно 1, это означает, что ответ получен от DNS-сервера.
2. ID: Идентификатор в секции HEADER должен совпадать с ID, который был отправлен в запросе. Это подтверждает, что ответ соответствует вашему запросу.
3. SERVER: IP-адрес в поле SERVER должен совпадать с IP-адресом вашего кэширующего DNS сервера.
4. Секция ANSWER: если вы видите ожидаемые записи (например, A или CNAME) в секции ANSWER, это подтверждает, что кэширующий сервер обработал запрос и вернул данные.
5. Метаданные (например, TTL): если значение TTL (в секции ANSWER) невелико, это может указывать на то, что данные были кэшированы на вашем DNS-сервере, а не получены из первоисточника.

Если все эти условия соблюдаются, вы можете быть уверены, что ответ пришёл от вашего кэширующего DNS сервера.