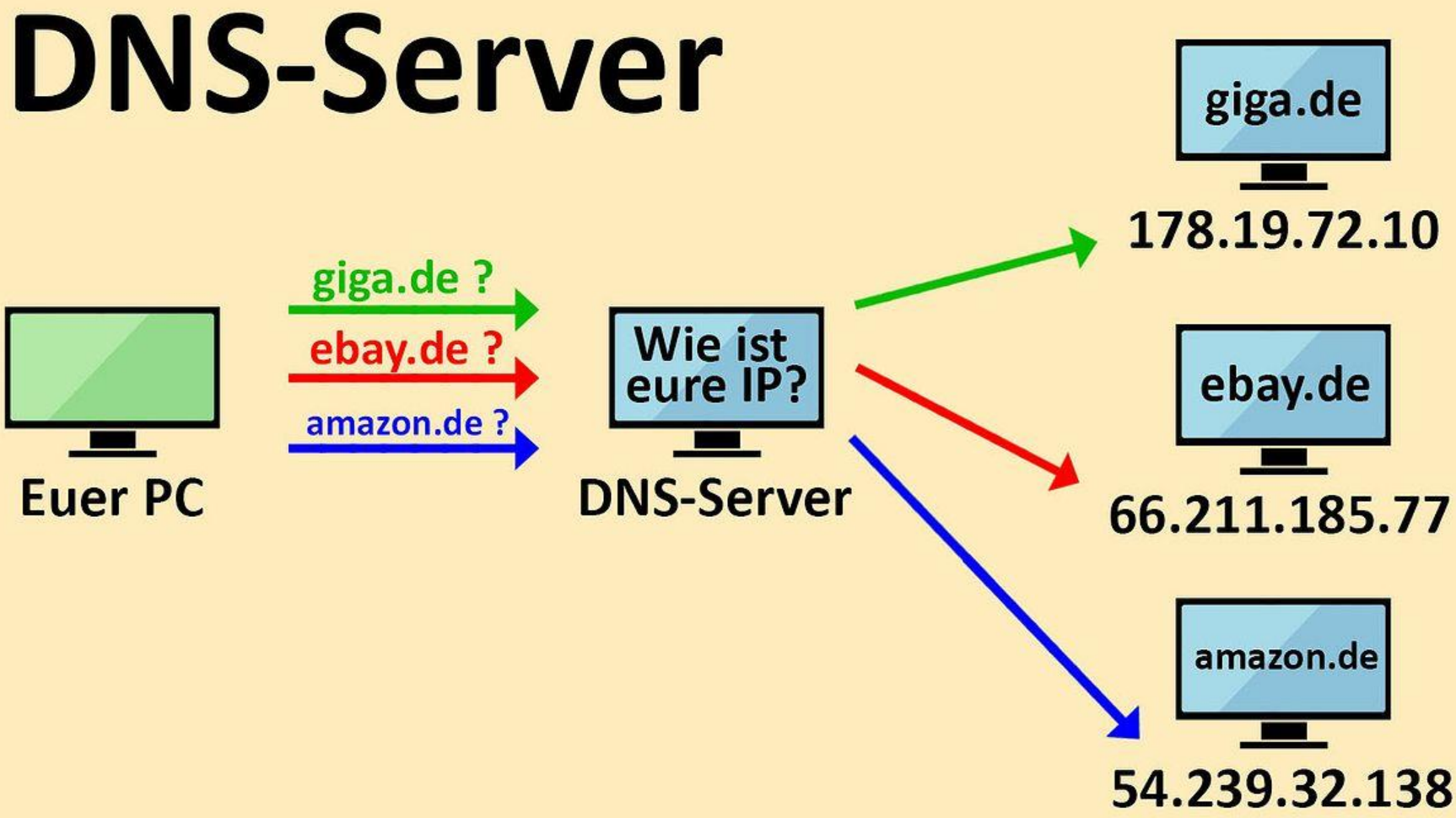
Тема:
Основные сервисы на Linux .
DNS-сервер.



План занятия:

1. Определение и роль DNS
2. Архитектура DNS
3. Принципы работы DNS
4. Иерархия доменных имен в DNS
5. Записи DNS
6. Настройка и управление DNS-сервером

1. Определение и роль DNS.

DNS (Domain Name System — система доменных имен) — это иерархическая распределённая система для преобразования доменных имен в IP-адреса и наоборот.

Система доменных имен представляет собой глобальную систему перевода доменных имен, которые легко запоминаются и понимаются людьми, в числовые идентификаторы (IP-адреса), используемые для адресации компьютеров и устройств в сети.

DNS функционирует как своего рода телефонный справочник интернета, позволяя пользователям вводить легко запоминающиеся адреса веб-сайтов вместо сложных числовых IP-адресов.

Роль DNS:

1.Разрешение доменных имен: DNS обеспечивает преобразование доменных имен, таких как example.com, в соответствующие им IP-адреса, которые используются компьютерами и сетевыми устройствами для идентификации и нахождения ресурсов в сети. Без DNS пользователи должны были бы запоминать и использовать числовые IP-адреса для доступа к веб-сайтам и другим ресурсам.

2.Распределение нагрузки: DNS позволяет распределять нагрузку между несколькими серверами с одним и тем же доменным именем. Например, крупные веб-сайты могут иметь несколько серверов, обслуживающих один домен, и DNS может использоваться для балансировки нагрузки между этими серверами, чтобы обеспечить более эффективное и надежное обслуживание.

3.Почтовые сервисы: DNS играет важную роль в маршрутизации электронной почты. Он используется для определения серверов, ответственных за обработку почтовых запросов для определенного домена. Поэтому, когда вы отправляете электронное письмо на адрес example.com, DNS помогает определить, на какой сервер должно быть отправлено это письмо.

4.Другие службы: DNS также может использоваться для настройки других служб, таких как передача файлов (FTP), виртуальные частные сети (VPN), голосовые услуги по протоколу IP (VoIP) и др. DNS позволяет пользователям использовать удобные доменные имена для доступа к этим службам, скрывая сложные сетевые адреса.

2. Архитектура DNS

Архитектура системы доменных имен (DNS) — это иерархическая и распределённая структура, состоящая из нескольких уровней доменов, начиная от корневых серверов и заканчивая авторитетными серверами для конкретных доменов. Эта структура обеспечивает масштабируемость, стабильность и гибкость управления в глобальной сети Интернет.

Корневые серверы DNS (Root Servers)

Корневые серверы являются центральной частью системы DNS, содержат информацию о топ-уровне доменных зон (TLD, например, .com, .org, .net, географические и национальные домены типа .uk, .ru и т.д.).

Корневые серверы направляют запросы к серверам, ответственным за топ-уровневые доменные зоны (TLD servers), которые, в свою очередь, направляют запросы к серверам следующего уровня.

Серверы топ-уровневых доменов (TLD Servers)

Серверы топ-уровневых доменов управляют доменами верхнего уровня, такими как .com, .net, .edu и национальные доменные зоны (.ru, .uk и др.).

Они хранят информацию о серверах имен, которые авторитетны для доменов второго уровня внутри соответствующих TLD.

Авторитетные серверы имен (Authoritative Name Servers)

Авторитетные серверы имен являются источником авторитетной информации о доменах (например, о домене example.com), включая IP-адреса соответствующих серверов (A и AAAA записи), почтовые серверы (MX записи), серверы имен (NS записи) и т.д.

Они обрабатывают запросы к конкретным доменам, предоставляя необходимую информацию для резолвинга доменных имен.

Рекурсивные серверы (Resolving Name Servers)

Рекурсивные серверы, также известные как DNS **резолверы**, выполняют запросы от клиентов (например, от веб-браузера пользователя) для преобразования доменных имен в IP-адреса.

Если рекурсивный сервер не имеет запрашиваемой информации в своём кэше, он выполняет серию запросов к другим серверам DNS, начиная от корневых и двигаясь вниз по иерархии, чтобы найти нужные данные.

Промежуточный кэш

Рекурсивные серверы кэшируют полученные данные, что позволяет сократить время обработки повторных запросов к тем же доменам.

Кэширование уменьшает нагрузку на DNS инфраструктуру и ускоряет процесс резолвинга доменных имен для конечных пользователей.

3. Принципы работы DNS

1.Разрешение доменного имени: Когда пользователь вводит доменное имя в веб-браузере или другом приложении, происходит запрос на разрешение этого имени в соответствующий IP-адрес. DNS выполняет функцию преобразования доменного имени в IP-адрес, который используется для установления соединения с желаемым ресурсом (например, веб-сайтом).

2.Клиентский запрос: Клиентское приложение, такое как веб-браузер, отправляет запрос DNS на разрешение доменного имени к локальному DNS-серверу, который обычно предоставляется интернет-провайдером или настраивается в сети.

3.Кэширование: Локальный DNS-сервер проверяет свой кэш для поиска ранее разрешенной информации об IP-адресе для запрашиваемого доменного имени. Если запись есть и не устарела, сервер возвращает IP-адрес непосредственно клиентскому приложению без дальнейшего запроса.

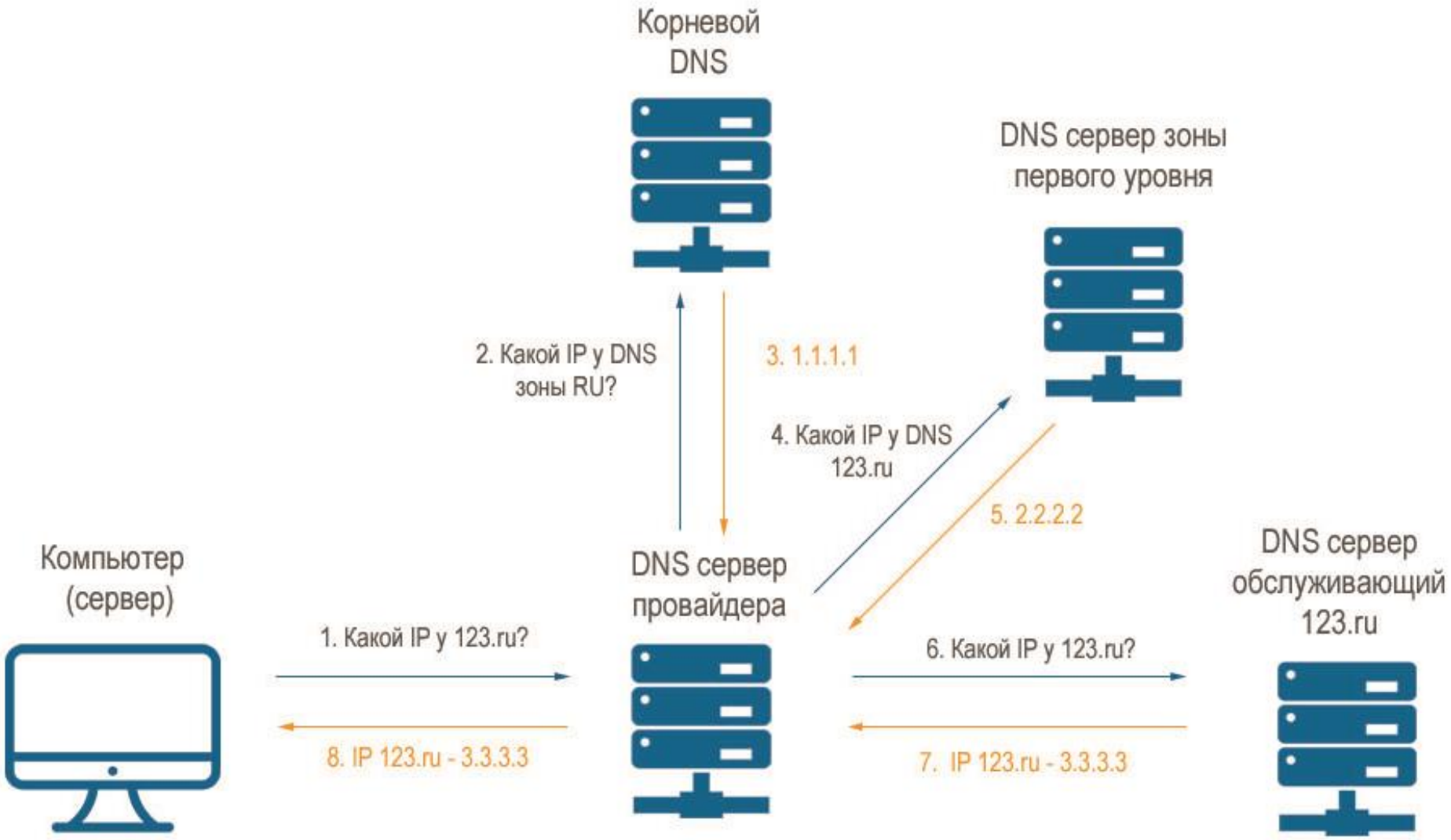
4.Иерархический поиск: Если локальный DNS-сервер не имеет кэшированной записи для запрашиваемого доменного имени, он начинает иерархический поиск. Он отправляет запрос на разрешение доменного имени к другим DNS-серверам, начиная с корневых DNS-серверов.

4. Расширение запроса: Корневые DNS-серверы не содержат прямой информации о конкретных доменах, но они могут указать локальному DNS-серверу, какой сервер доменной зоны (например, .com, .org) обслуживает интересующий домен. Локальный DNS-сервер перенаправляет запрос на соответствующий сервер доменной зоны.

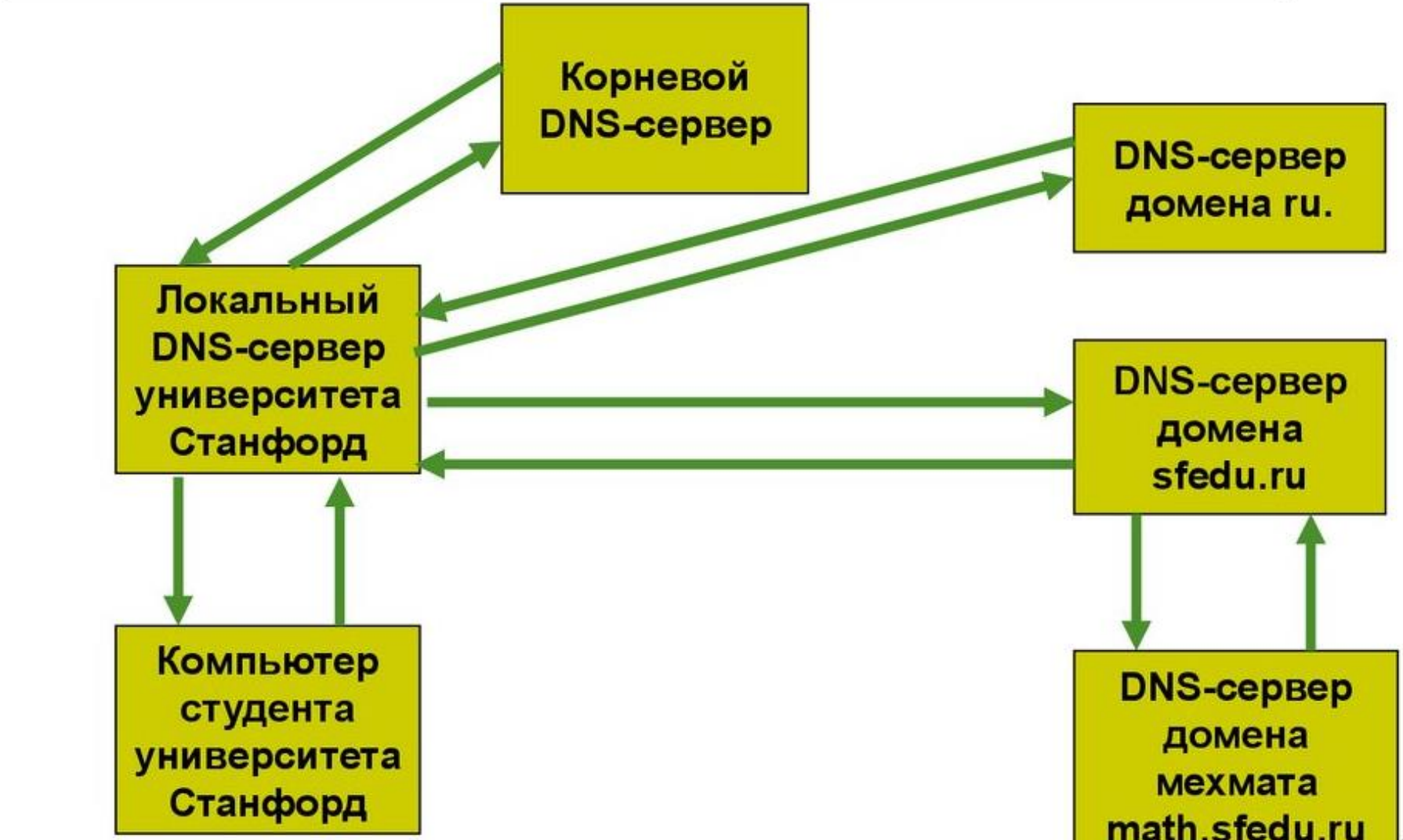
5. Авторитетный поиск: Сервер доменной зоны, ответственный за обслуживание интересующего домена (например, .com), проверяет свою базу данных на наличие записи для запрашиваемого домена (например, example.com). Если запись найдена, сервер возвращает IP-адрес клиентскому приложению и информацию о других записях, связанных с доменом (например, записи MX для обработки почты).

6. Кэширование и обновление: Локальный DNS-сервер кэширует полученную информацию, чтобы в следующий раз быстро отвечать на запросы для того же домена. Записи в кэше имеют временной срок действия, после которого они считаются устаревшими и должны быть обновлены.

7. Ответ DNS: Локальный DNS-сервер отправляет IP-адрес клиентскому приложению, которое инициировало запрос DNS. Клиентское приложение использует полученный IP-адрес для установления соединения с запрашиваемым ресурсом.


Корневой DNS
DNS сервер зоны первого уровня
2. Какой IP у DNS зоны RU?
3. 1.1.1.1
4. Какой IP у DNS 123.ru
5. 2.2.2.2
Компьютер (сервер)
DNS сервер провайдера
DNS сервер обслуживающий 123.ru
1. Какой IP у 123.ru?
6. Какой IP у 123.ru?
8. IP 123.ru - 3.3.3.3
7. IP 123.ru - 3.3.3.3

Принципы работы DNS



sunschool.math.sfedu.ru - ??

Процесс разрешения доменного имени можно посмотреть с помощью утилиты dig (входит в пакет bind-utils):

```
user@user:~$ dig www.vk.com +trace

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> www.vk.com +trace
;; global options: +cmd
.                       85523   IN      NS      i.root-servers.net.
.                       85523   IN      NS      f.root-servers.net.
.                       85523   IN      NS      l.root-servers.net.
.                       85523   IN      NS      e.root-servers.net.
.                       85523   IN      NS      g.root-servers.net.
.                       85523   IN      NS      a.root-servers.net.
.                       85523   IN      NS      h.root-servers.net.
.                       85523   IN      NS      k.root-servers.net.
.                       85523   IN      NS      m.root-servers.net.
.                       85523   IN      NS      d.root-servers.net.
.                       85523   IN      NS      j.root-servers.net.
.                       85523   IN      NS      c.root-servers.net.
.                       85523   IN      NS      b.root-servers.net.
;; Received 239 bytes from 127.0.0.53#53(127.0.0.53) in 8 ms
```

4. Иерархия доменных имен в DNS

0.Корневая зона (Root Zone): Корневая зона обозначается символом "." (точка) и является верхним уровнем иерархии доменных имен. В корневой зоне находятся корневые DNS-серверы, которые отвечают на запросы, связанные с верхними уровнями доменных зон (например, .com, .org, .net) и указывают на серверы доменных зон верхнего уровня.

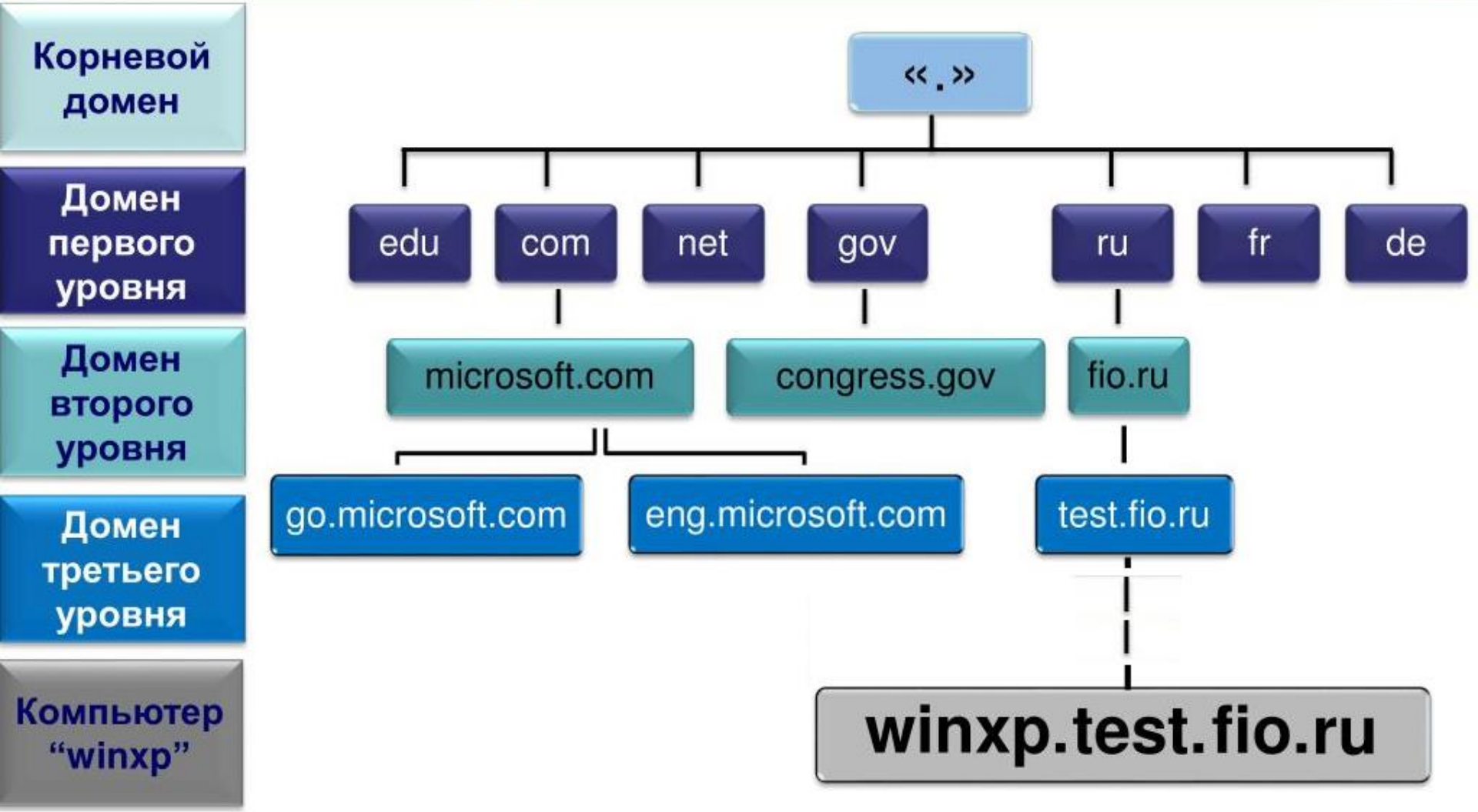
1.Верхние уровни доменных зон (Top-Level Domains - TLDs): На следующем уровне иерархии находятся верхние уровни доменных зон. Это доменные зоны, которые обозначаются после точки в доменном имени, например, .com, .org, .net, .edu, .gov и т.д. Каждая верхняя уровня доменная зона имеет свои серверы, которые содержат информацию о доменах внутри этой зоны или указывают на серверы следующего уровня.

2.Второй уровень доменных зон (Second-Level Domains - SLDs): Второй уровень доменных зон находится непосредственно под верхними уровнями доменных зон. Он представляет собой домены второго уровня, которые обычно представляют организации или конкретные страны. Например, в доменном имени "example.com" домен второго уровня - "example". Домены второго уровня могут быть зарегистрированы пользователями с соответствующими правами.

3.Поддомены: Поддомены представляют собой дополнительные уровни в иерархии доменных имен и располагаются ниже доменов второго уровня. Они добавляются перед основным доменным именем и разделяются точками. Например, в доменном имени "www.example.com" "www" является поддоменом домена "example.com". Домены третьего уровня обычно относятся к подразделениям внутри компаний.

4.Конкретные доменные имена: На самом нижнем уровне иерархии находятся конкретные доменные имена, которые уже не делятся на поддомены. Они представляют собой полные доменные имена соответствующие конкретным ресурсам или узлам в сети, таким как веб-сайты, почтовые серверы и другие.
Домены ниже третьего уровня, как правило, встречаются редко.

Иерархическая структура доменных имён



Доменное имя

5. Записи DNS

Существует несколько типов записей DNS, каждый из которых выполняет определённую функцию. Вот некоторые из наиболее распространённых типов записей:

1.A (Address Record): Запись A указывает на прямой IP-адрес домена в версии IPv4.

2.AAAA (IPv6 Address Record): Подобно записи A, но указывает на адрес IPv6 домена.

3.CNAME (Canonical Name Record): Запись CNAME используется для указания, что домен является псевдонимом для другого домена, который называется "каноническим именем".

4.MX (Mail Exchange Record): Указывает на серверы, которые принимают электронную почту для вашего домена. Записи MX имеют приоритет, что позволяет настроить резервирование и балансировку нагрузки для электронной почты.

5.SRV (Service Record): Запись SRV предоставляет информацию о доступных сервисах и их расположении в домене. Эти записи используются для описания местонахождения серверов для определённых услуг.

6.NS (Name Server Record): Запись NS указывает на серверы имен (DNS-серверы), которые имеют авторитет для данного домена. Это позволяет делегировать управление доменом от одного DNS-сервера к другому.

7.PTR (Pointer Record): Обратная запись DNS, используемая для выполнения обратного DNS-поиска, т.е. перевода IP-адресов в доменные имена. Это противоположность записям типа A и AAAA.

Хост	Тип	Значение записи
www	A	95.213.184.148

Добавить DNS-запись

DNS-записи

Хост	Тип	Значение записи	Приоритет		
@	A	95.213.184.148		настроить	удалить
mail	CNAME	domain.mail.yandex.net.		настроить	удалить
_xmpp-client._tcp.conference	SRV	0 5222 domain-xmpp.yandex.net.	20	настроить	удалить
_xmpp-client._tcp	SRV	0 5222 domain-xmpp.yandex.net.	20	настроить	удалить
_xmpp-server._tcp.conference	SRV	0 5269 domain-xmpp.yandex.net.	20	настроить	удалить
_xmpp-server._tcp	SRV	0 5269 domain-xmpp.yandex.net.	20	настроить	удалить
@	TXT	v=spf1 redirect=_spf.yandex.net		настроить	удалить
@	NS	dns1.yandex.net.		настроить	удалить
@	NS	dns2.yandex.net.		настроить	удалить
@	MX	mx.yandex.net.	10	настроить	удалить

5. Реализации DNS

Существует несколько различных реализаций DNS-серверов, которые обеспечивают функциональность DNS и выполняют разрешение доменных имен. Вот некоторые из наиболее распространенных реализаций DNS:

BIND (Berkeley Internet Name Domain) является одной из самых широко используемых реализаций DNS-сервера. Разработанный в Университете Беркли, BIND предоставляет полнофункциональный DNS-сервер с поддержкой различных типов записей и расширений. Он доступен для различных операционных систем и широко применяется в большинстве серверных окружений.

Microsoft DNS является DNS-сервером, включенным в операционные системы Microsoft Windows Server. Он предоставляет функциональность DNS-сервера для среды Windows и может использоваться для обслуживания внутренних сетей и доменных имен Windows Active Directory.

Unbound является другой популярной реализацией DNS-сервера. Он изначально разработан как резолвер, который обеспечивает быстрое и безопасное разрешение доменных имен. Unbound легковесный и может быть использован как автономный DNS-сервер или резолвер для клиентских устройств.

PowerDNS представляет собой распределенную и расширяемую систему DNS, которая предлагает различные режимы работы, включая авторитетные и резолверные функции. PowerDNS также поддерживает различные базы данных для хранения DNS-записей и может быть интегрирован с другими системами и инструментами.

Knot DNS является другим гибким и производительным DNS-сервером с открытым исходным кодом. Он разработан с упором на производительность и безопасность, а также поддерживает функции авторитетного и резолверного DNS.

И др.

6. Настройка и управление DNS-сервером

Основные этапы настройки DNS-сервера:

Выбор и установка DNS-сервера. Выберите подходящий DNS-сервер для вашей среды и требований. Установите DNS-сервер, используя менеджер пакетов вашей операционной системы или скачав и установив его с официального сайта.

Конфигурация основных параметров. Настройте основные параметры сервера, такие как адрес и порт, которые будут прослушиваться, логирование и т. д. Включите или отключите опции по вашему усмотрению в зависимости от требований к безопасности и функциональности.

Настройка зон. Определите зоны, которые будет управлять ваш DNS-сервер. Создайте файлы зон, содержащие записи для каждой зоны. Эти файлы обычно находятся в каталоге /etc/bind или аналогичном месте. Добавьте информацию о зонах в конфигурационные файлы DNS-сервера.

Добавление записей. Добавьте необходимые DNS-записи для каждой зоны, такие как записи A, CNAME, MX, NS и т. д. Обеспечьте точность и согласованность записей, чтобы предотвратить ошибки и неполадки.

Настройка обратных зон. Настройте обратные зоны (Reverse DNS) для соответствия IP-адресов и доменных имен. Это обычно включает добавление записей PTR, которые отображают IP-адреса в доменные имена.

Обеспечение безопасности. Примените меры безопасности, такие как ограничение доступа к DNS-серверу, использование аутентификации и шифрования данных, настройка файрвола и т. д. Регулярно обновляйте DNS-сервер и мониторьте его работу для выявления аномалий или атак.

Тестирование и отладка. Проведите тестирование настроек DNS-сервера, чтобы убедиться, что он работает должным образом. Используйте инструменты для проверки правильности настройки и разрешения DNS-запросов.

Документация и резервное копирование. Создайте документацию, описывающую настройки и конфигурацию DNS-сервера. Регулярно создавайте резервные копии конфигурационных файлов и данных DNS-сервера для предотвращения потери информации при сбоях или авариях.

2. Настройка конфигурационных файлов:

Основные файлы конфигурации BIND находятся в каталоге /etc/bind. Основные файлы включают named.conf, named.conf.options, named.conf.local и т. д. Настройте эти файлы в соответствии с вашими требованиями.

3. Настройка зон:

Создание файлов зон:

Создайте файлы зон для доменов, которые вы хотите управлять с помощью BIND. Эти файлы могут включать записи A, CNAME, MX и т. д. Обычно они находятся в каталоге /etc/bind или /var/cache/bind.

2. Настройка конфигурационных файлов:

Основные файлы конфигурации BIND находятся в каталоге /etc/bind. Основные файлы включают named.conf, named.conf.options, named.conf.local и т. д. Настройте эти файлы в соответствии с вашими требованиями.

3. Настройка зон:

Создание файлов зон:

Создайте файлы зон для доменов, которые вы хотите управлять с помощью BIND. Эти файлы могут включать записи A, CNAME, MX и т. д. Обычно они находятся в каталоге /etc/bind или /var/cache/bind.

Домашнее задание:

1. Изучить дополнительные материалы.