нетология

Сеть и сетевые протоколы: **DNS**

Андрей
Кондрашов

Андрей Кондрашов

Системный администратор

Восток-лизинг

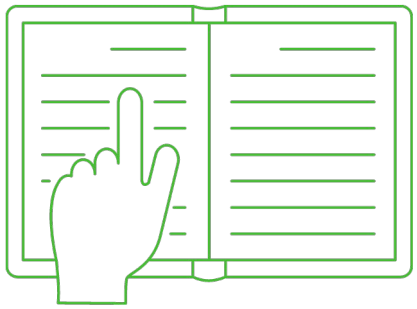
Андрей Кондрашов

Предисловие

На этом занятии мы поговорим о том:

- что такое DNS, для чего он нужен;
- возможностях службы DNS;
- содержимом пакетов DNS;
- настройках сервера / клиента DNS.

По итогу занятия вы получите представление протоколе DNS и научитесь настраивать DNS сервер в Linux.

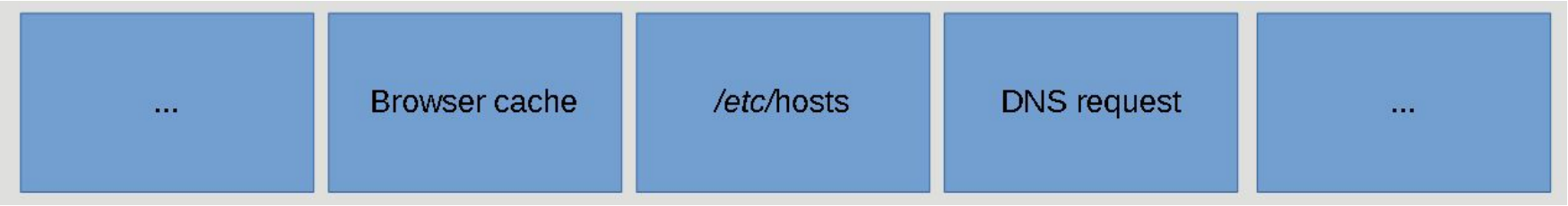


План занятия

1. Предисловие
2. Основные понятия
3. DNS сервер
4. Настройка DNS сервера
5. Утилиты для диагностики
6. Безопасность DNS
7. DNS для IPv6
8. Итоги
9. Домашнее задание

Основные понятия

Что случается, когда вы печатаете в адресной строке google.com и нажимаете Enter?



Перевод на Habr

Ссылка из перевода на оргинал

Что такое DNS?

DNS (Domain Name System, система доменных имён) – это распределённая иерархическая система доменных имён, которая связывает буквенные названия (имена) доменов с IP-адресами компьютеров, соответствующих этим доменам.

Идея и первые реализации появились в 1980-е годы.

Описание протокола можно найти в RFC 1034 – RFC 1035.

Источник изображения

Телефонная книга

Основная задача DNS похожа на работу телефонной книги: по понятному для человека имени найти числовой идентификатор (телефонный номер, IP адрес).

До первой реализации пользователи сети ARPA скачивали файл hosts или же получив информацию другим способом вносили DNS-записи вручную в файл hosts.txt.

Файл hosts

Файл hosts выполняет то же функцию что и DNS-сервер, но делает это локально. По умолчанию это первый источник, где Linux будет пытаться разрешить имя в IP адрес.

Если в вашей сети нет DNS сервера или он неисправен – временным решением может служить внесение записей в файл /etc/hosts.

Посмотреть как выглядели hosts файлы в 1980-е можно, например, здесь.

FQDN

FQDN (Fully Qualifed Domain Name, полностью определённое имя домена) – это имя домена, однозначно определяющее доменное имя и включающее в себя имена всех родительских доменов иерархии DNS, в том числе и корневого.

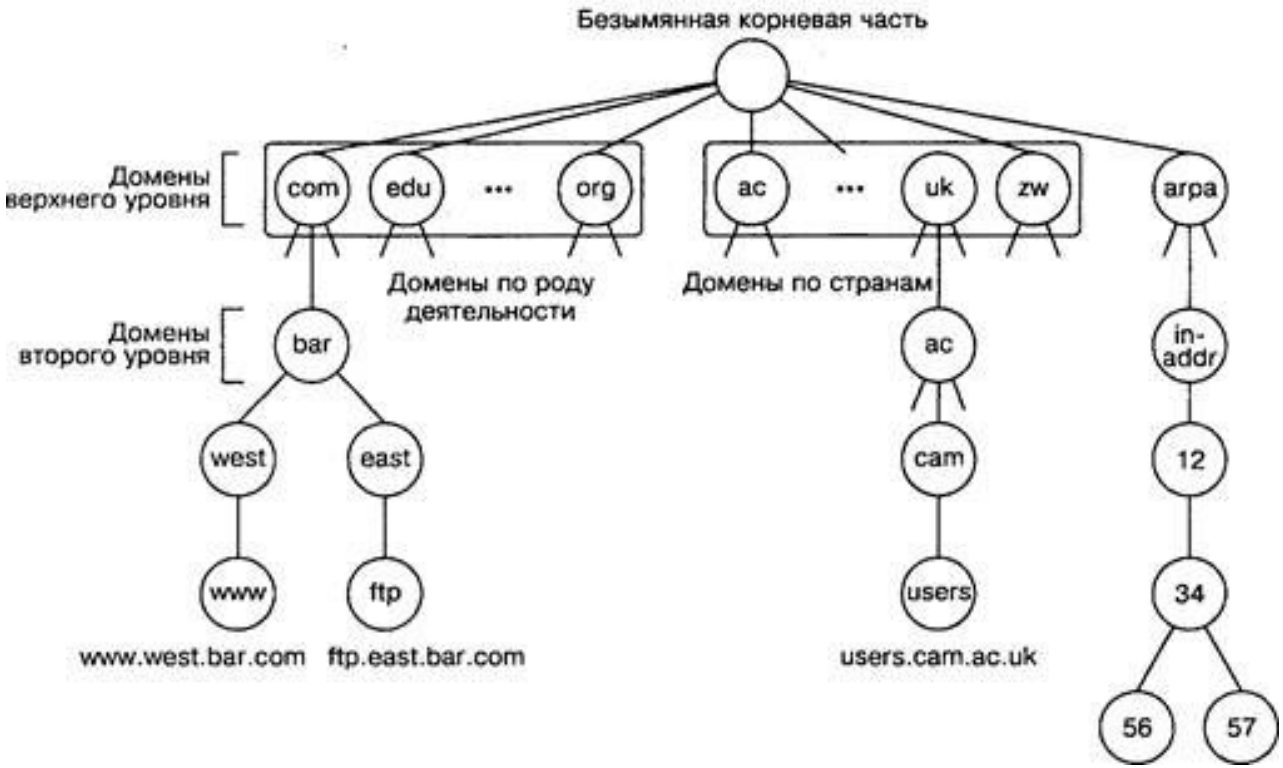
Ближайший аналог абсолютный путь в файловой системе.

```
mail.k-max.name.
 |     |  |  | |
 |     |  |  | +-корневой домен
 |     |  |  +---домен первого уровня
 |     |  +------точка, разделяющая домены/части FQDN
 |     +---------домен второго уровня
 +---------------поддомен/домен третьего уровня, возможно - имя хоста
```

Источник изображения

Архитектура DNS

Архитектурно система DNS строится на иерархической распределенной модели.



Источник изображения

Регистрация имен

До конца 1990-х за управление DNS именами отвечали правительственные организации США. Позже эти вопросы были переданы ICANN (Internet Corporation for Assigned Names and Numbers).

Организации, уполномоченные создавать (регистрировать) новые доменные имена называются регистраторами.

В РФ существует Координационный центр национального домена сети Интернет, который регулирует работу регистраторов.

Покупка продажа доменов

Доменные имена регистрируются на время и чаще всего регистратор берет за свои услуги деньги.

➡ Список аккредитованых регистраторов для зоны .РФ и .RU представлен здесь.

Личный кабинет регистраторов позволяет после регистрации имени указать авторитативный сервер для зоны.

Большинство регистраторов также предоставляет сопутствующие услуги: DNS сервера, хостинг, VPS.

Источник изображения

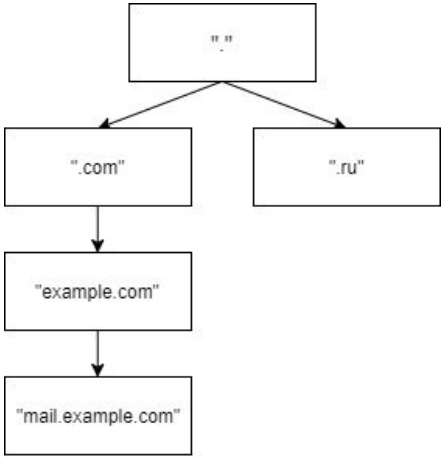
DNS-сервер

Корневые сервера

В верхней части иерархической системы доменных имен находится 13 корневых серверов. До 30% обращений приводит к обращению к корневому серверу. У корневых серверов множество реплик.

Имена корневых серверов выглядят {a-m}.root-servers.net.

В РФ также есть несколько реплик корневых DNS серверов.



Источник изображения

Типы DNS-серверов

- **корневой** – это DNS-сервер, который хранит в себе адреса всех TLD-серверов (TLD – top-level domain, домен верхнего уровня);
- **TLD-серверы** – эти серверы связаны с доменами верхнего уровня (TLD), обычно они идут после корневых DNS-серверов;
- **авторитативный DNS-сервер** – это серверы, которые ответственны за зону. Они хранят фактические записи типа A, NS, CNAME, TXT, и т. п. Авторитативные DNS-серверы по возможности возвращают IP-адреса хостов. Если сервер этого сделать не может — он выдаёт ошибку, и на этом поиск IP-адреса по серверам заканчивается.

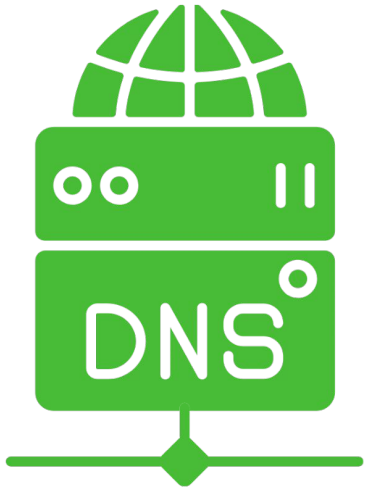
Авторитативные DNS-сервера

- **первичный** (primary master) – вносить изменения в описание зоны может только администратор данного сервера. Все остальные серверы только копируют информацию с master-сервера.
- **вторичный** (secondary master) – также является ответственным (authoritative) за зону. Его основное назначение заключается в том, чтобы подстраховать работу основного сервера доменных имен (master server), ответственного за зону, на случай его выхода из строя, а также для того, чтобы разгрузить основной сервер, приняв часть запросов на себя.

Кэширующий DNS-сервер

Кэширующий DNS-сервер занимается обработкой DNS запросов, которые выполняет ваша система, затем сохраняет результаты в памяти или кэширует их.

В следующий раз, когда система посылает DNS запрос для того же адреса, то локальный сервер выдает результат быстрее чем если бы запрос был отправлен на DNS-сервер провайдера.



Делегирование домена

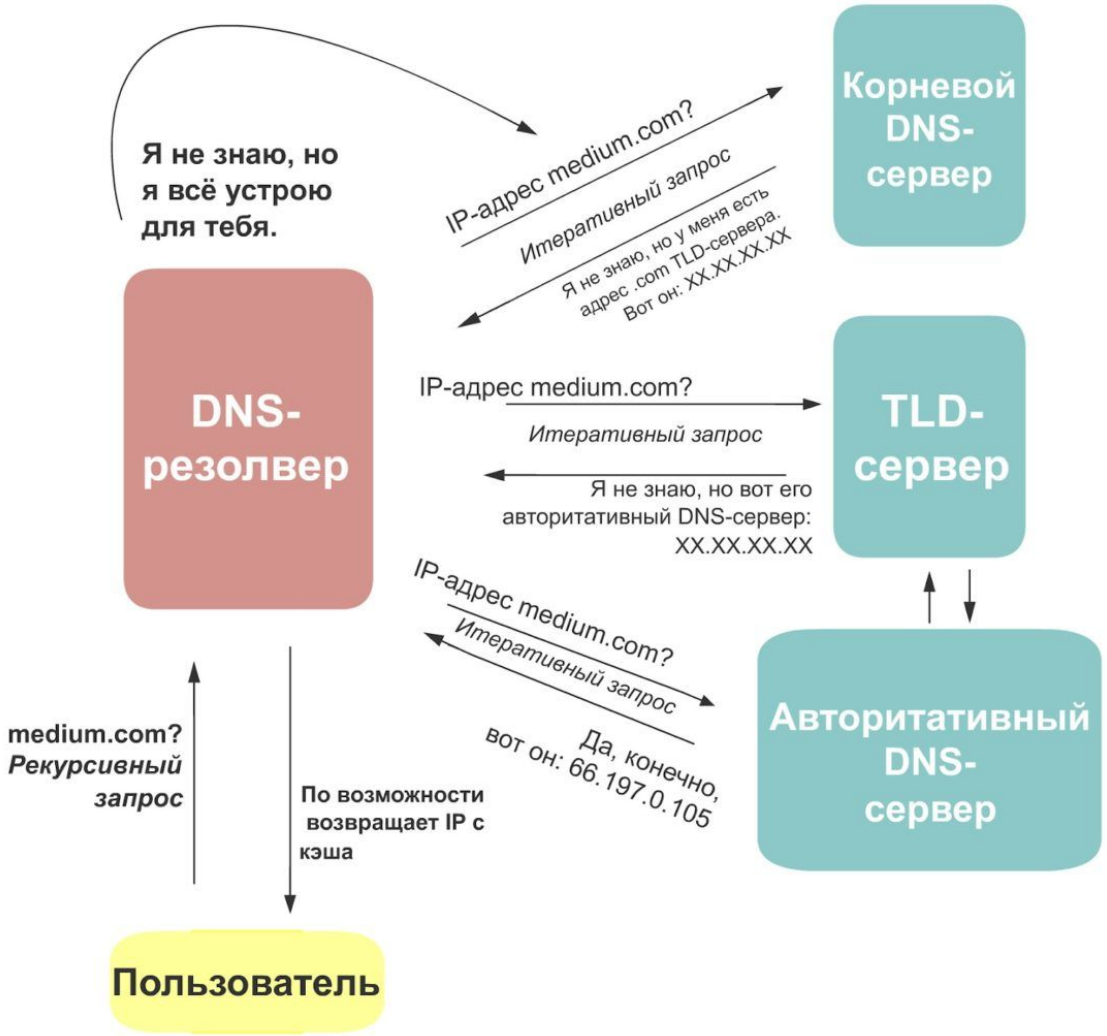
Делегирование домена — это передача контроля над частью доменной зоны другой ответственной стороне.

Делегирование осуществляется с помощью записи NS, в которой указывается адрес DNS-сервера , отвечающего за поддержание зоны и определяющего её содержимое.

Виды запросов

- **рекурсивный** – это первый запрос, который выполняется в процессе DNS-поиска и выполняется от пользователя к резолверу;
- **нерекурсивные** – резолвер сразу возвращает ответ без каких-либо дополнительных запросов на другие сервера имён; это случается, если в DNS-сервере был закэширован необходимый IP-адрес либо если запрос поступает напрямую на авторитативные сервер;
- **итеративный** – итеративный запрос выполняется, когда резолвер не может вернуть ответ, потому что он не закэширован и он выполняет запрос на корневой DNS-сервер.

Виды запросов



Источник изображения

Типы ресурсных записей

A	Address record (запись адреса) указывает на соответствие между доменным именем и IP-адресом (IPv4).
AAAA	Аналогична записи A, но указывает соответствие доменного имени для IPv6.
CNAME	Canonical name – запись, которая позволяет присваивать домену каноническое имя для псевдонима (одноуровневая переадресация).
DKIM	DomainKeys Identified Mail – технология e-mail-аутентификации, которая позволяет подтвердить подлинность отправителя. DKIM добавляет в сообщение цифровую подпись, удостоверяющую, что письмо действительно поступило с ящика на указанном домене. Наличие DKIM повышает доверие серверов-получателей к письму и тем самым снижает его шансы оказаться в папке «Спам» или вовсе быть отклоненным принимающим сервером.
MX	Запись, указывающая на адрес почтового шлюза для домена. Состоит из двух частей: приоритета (чем число больше, тем ниже приоритет) и адреса узла.

Типы ресурсных записей

NS	Указывает на DNS-сервер, обслуживающий данный домен, т.е. указывает серверы, на которые домен делегирован. Данный тип записи критически важен для функционирования самой системы доменных имён.
PTR	Pointer – запись, которая указывает на соответствие адреса имени — обратное соответствие для A и AAAA.
SRV	Server selection – этот тип записи указывает на серверы, обеспечивающие работу тех или иных служб в данном домене (например, Jabber, Active Directory).
SOA	Start of Authority (начальная запись зоны) – запись описывает основные/начальные настройки зоны, определяет зону ответственности данного сервера. Для каждой зоны должна существовать только одна запись SOA.
TXT	Запись содержит вспомогательную информацию о домене (запись произвольных данных). Записи TXT используются для различных целей: подтверждения права собственности на домен, обеспечения безопасности электронной почты, а также подтверждения SSL-сертификата. Можно прописывать неограниченное количество TXT-записей

Установка и настройка DNS сервера

Реализации DNS-сервера

- **BIND** (Berkeley Internet Name Domain) – наиболее распространенная реализация DNS-сервера (10 из 13 корневых серверов работают на BIND);
- **NSD** (NLnet Labs Name Server Daemon) – быстрый DNS сервер, выступающий только в роли мастера (не реализует рекурсивные запросы и кэширование);
- **PowerDNS** – open source продукт, поставляется в 3 версиях, позиционируется как быстрый;
- **Microsoft DNS Server** – роль на Microsoft Server, прекрасно интегрируется в экосистему добавляя много функционала.

Решения «все-в-одном»

- **389 server** – LDAP-сервер с дополнительными функциями, в том числе BIND с хранением информации в LDAP;
- **FreeIPA** (Red Hat Directory Server) – основанное на 389 server решение, с дополнительными возможностями по безопасности и управлению;
- **Microsoft Server** – если строить инфраструктуру на базе Microsoft, то это хорошее решение для DNS, LDAP, DHCP.

BIND

BIND (Berkeley Internet Name Domain) – разработанная в 1980-х годах в Университете Berkley реализация DNS-сервера.

Является самым популярной в интернете и входит в поставку почти всех дистрибутивов LInux.

BIND обладает огромным количеством настроек и интеграций.

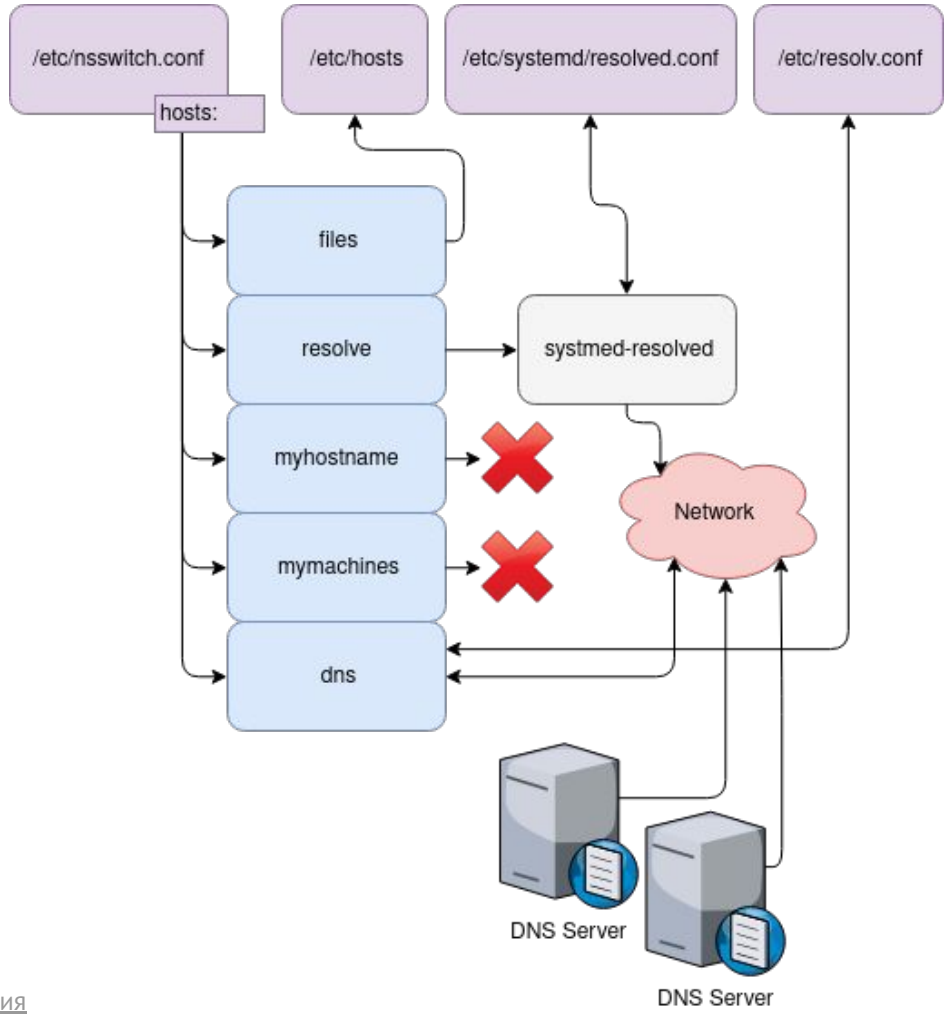
Установка DNS сервера

- yum install bind bind-utils -y
- sudo vim /etc/named.conf
- systemctl enable-now named
- firewall-cmd --permanent --add-port=53/udp
- firewall-cmd --reload

Настройка DNS клиента

- vim /etc/hosts
- vim /etc/resolv.conf
- vim /etc/nsswitch.conf
- Автоматическая через опции DHCP
- resolvconf
- systemctl status systemd-resolved
- systemd-resolve --flush-caches
- systemctl status dnsmasq

Механизм работы DNS клиента



Источник изображения

Утилиты для диагностики

Утилиты для диагностики

- **nslookup** – утилита для отправки запросов DNS серверам;
- **dig** (Domain information groper) – утилита для отправки запросов DNS серверам; входит в пакет bind-utils.

  Примеры:

  - dig any google.com
  - dig google.com +trace
  - dig google.com @208.67.222.222

Утилиты для диагностики

- **whois** – утилита, выводящая информацию о домене:
  - ns сервера;
  - регистратора;
  - дату регистрации;
  - дату истечения срока регистрации;
  - информацию о владельце.
- **systemd-resolve** – демон для настроки / диагностики настроек DNS на стороне клиента.
- **dnstop** – программа позволяет отслеживать трафик от/к DNS серверу.

Безопасность DNS

Атаки на DNS

- DNS-флуд – на DNS-сервер отправляется множество запросов, которые потребляют ресурсы сервера / сети, тем самым не давая возможности легитимным клиентам получить ответы на их запросы;
- Атака посредством отраженных DNS-запросов – на DNS сервер отправляется множество запросов, при этом адрес отправителя меняется на адрес сервера-жертвы. Т.к. ответ больше запроса, то канал до сервера жертвы забивается паразитным трафиком, ем самым не давая возможности легитимным клиентам получить ответы на их запросы.
- ...

Атаки на DNS

- ...
- Атака при помощи рекурсивных DNS-запросов – отправляется множество рекурсивных запросов к DNS серверу. Т.к. такие запросы потребляют много ресурсов - производительность сервера падает;
- Garbage DNS – суть данной атаки в переполнении канала до сервера путем отправки пакетов большого размера(1500 байт и больше) на сервер-жертву;
- Подмена DNS сервера - перехватив пакеты или иным способом заставить поверить клиента что атакующая машина и есть легитимный DNS сервер;

DNS поверх HTTPS

Существует реализация DNS поверх HTTPS (RFC8484).

DoH повышает конфиденциальность и безопасность пользователей путём предотвращения перехвата и манипулирования данными DNS.

Однако DoH нарушает концепцию децентрализации DNS, т.к. DoH предоставляется как сервис от коммерческих компаний, среди которых:

- Cloudflare;
- OpenDNS;
- Adguard.

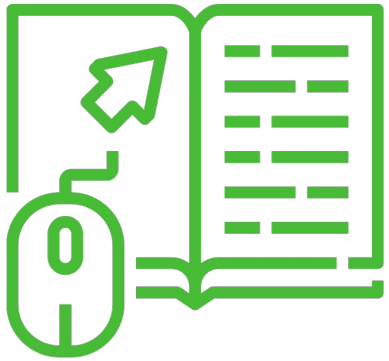
Итоги

Итоги

Сегодня мы рассмотрели:

- протокол DNS;
- виды и настройки DNS серверов;
- возможные атаки на DNS.

.



Домашнее задание

Домашнее задание

Давайте посмотрим ваше домашнее задание.

- Вопросы по домашней работе задавайте **в чате** мессенджера Slack.
- Задачи можно сдавать **по частям**.
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**.

нетология

Задавайте вопросы и пишите отзыв о лекции!

Андрей Кондрашов

Андрей Кондрашов