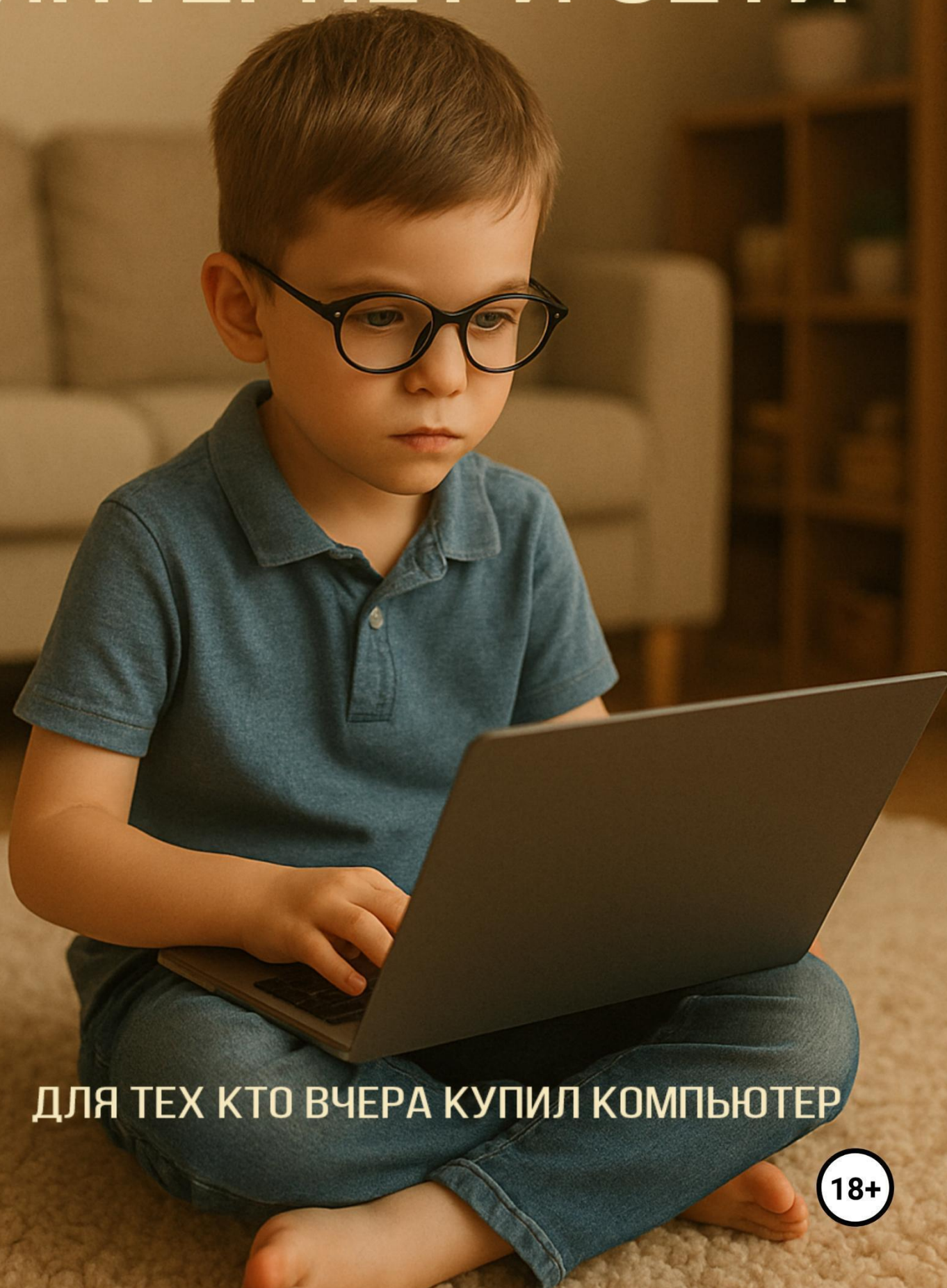


АЛЕКСАНДР СИВИЧЕВ

САМОУЧИТЕЛЬ ИНТЕРНЕТ И СЕТИ



ДЛЯ ТЕХ КТО ВЧЕРА КУПИЛ КОМПЬЮТЕР

18+

Для тех, кто вчера купил компьютер

Александр Сивичев

**Самоучитель: Интернет
и сети. Для тех, кто
вчера купил компьютер**

«Автор»

2025

Сивичев А.

Самоучитель: Интернет и сети. Для тех, кто вчера купил компьютер
/ А. Сивичев — «Автор», 2025 — (Для тех, кто вчера купил
компьютер)

Интернет кажется простым: открыл браузер — и вот он, весь мир. Но за каждой загрузкой страницы скрываются десятки технологий, решений и ограничений. Эта книга — для тех, кто хочет понять, как устроена сеть: что такое IP и DNS, почему сайты блокируются, как работает VPN, откуда соцсети знают о вас всё, и что происходит, когда вы нажимаете «Отправить». Простым языком, без лишней теории, с примерами из жизни — о безопасности, шифровании, мобильных сетях, региональных ограничениях, спутниках и протоколах. После прочтения книги вы перестанете быть просто «пользователем на кнопках» и начнёте видеть, как именно работает цифровой мир вокруг вас.

© Сивичев А., 2025

© Автор, 2025

Александр Сивичев

Самоучитель: Интернет и сети. Для тех, кто вчера купил компьютер

1.1 От ARPANET до сегодняшнего интернета

Большинство того, что мы сегодня называем «айти» – от смартфонов до мемов с котиками – родилось не ради развлечений. Корни современной цифровой эпохи – в военных нуждах.

Ещё в XIX веке Бэббидж разрабатывал вычислительные машины для навигационных таблиц британского флота. В XX веке шифровальная «Энигма» и криптоаналитики Тьюринга положили начало вычислительной гонке: чтобы взламывать коды, потребовались электронные машины – Colossus в Англии, ENIAC в США. Это были не «компьютеры общего пользования», а оружие для доминирования в информационной войне.

После войны наступила эра холодного противостояния. Проект SAGE стал первым опытом создания сети реального времени: радары по всей Америке передавали данные в гигантские вычислительные центры, где принимали решения о перехвате. Для этого понадобились новые интерфейсы, дисплеи, полупроводники – всё, что потом переключалось в гражданский сектор. Подобные системы как NORAD закладывали архитектуру глобального наблюдения и мгновенной передачи команд.

Когда в 1960-х создавался ARPANET, целью было не общение студентов, а сеть, способная пережить ядерную войну. Пакетная передача данных, децентрализация, динамическая маршрутизация – всё это родилось из военной задачи: сохранить управляемость даже после разрушения половины узлов связи. Протоколы TCP/IP, на которых до сих пор работает интернет, появились как технология выживания.

Так интернет вырос не из желания людей делиться знаниями, а из военной логики command & control – систем управления войсками и оружием в условиях катастрофы. То, что сегодня стало пространством мемов и стримов, начиналось как инфраструктура для ведения войны и удержания власти.

Кто платит за магистрали

Большинство думает об интернете как о чём-то «воздушном» и бесплатном. На деле он строится на очень конкретных инфраструктурах, которые стоят колоссальных денег. Магистральные каналы связи – это тысячи километров оптоволокна через страны и океаны, которые принадлежат не государствам, а крупным корпорациям и альянсам операторов. Платят за это телекомы, крупные контент-компании вроде Google, Meta и Amazon, которые уже сами строят сети между своими дата-центрами, а также специализированные консорциумы.

За пропуск трафика на международном уровне взимается плата (transit fees). Есть крупные узлы (Tier-1), через которые идёт весь мировой трафик, и местные провайдеры платят им за доступ. Так интернет вовсе не «равный для всех»: кто платит больше, тот получает более быстрые и надёжные каналы.

Как выглядят подводные кабели и дата-центры

Интернет физически существует в виде толстых кабелей, которые лежат на дне океанов и соединяют континенты. Эти кабели – диаметром с садовый шланг – защищены стальной оплёткой и специальной броней от якорей и подводных течений. На некоторых участках их регулярно проверяют и ремонтируют специальные суда.

А в узлах сети стоят дата-центры – гигантские здания с рядами серверных стоек, системой охлаждения, резервным питанием и многоуровневой охраной. Внутри – просто километры

кабелей и стойки с мигающими лампочками. Это сердца интернета, где хранятся данные, к которым ты подключаешься.

Так магистрали и дата-центры – это вовсе не «виртуальное пространство», а вполне материальные бетон, сталь и километры стекла, за которые платят миллиарды. Без этих объектов интернета бы просто не существовало.

Как передаются данные

Что такое пакеты

Когда ты открываешь сайт или отправляешь сообщение, твои данные разбиваются на маленькие куски – пакеты. Каждый пакет несёт часть полезной информации плюс «служебные поля»: откуда пришёл, куда идёт, как собрать обратно. Это позволяет сети быстро доставлять данные даже через разные маршруты и обходить повреждённые участки.

TCP и UDP – два способа передавать данные

Когда твои данные разбились на пакеты, их ещё надо как-то передать. Для этого существуют протоколы передачи, и самые популярные из них – это TCP и UDP.

Они работают по-разному, и выбор зависит от того, что важнее – надёжность или скорость.

TCP (Transmission Control Protocol)

Представь, что ты отправляешь важное письмо с отчётом.

Ты:

вкладываешь его в конверт,

указываешь адрес,

ждёшь подтверждения, что письмо доставлено и получено,

если потерялось – отправляешь снова.

Вот это и есть TCP – протокол, который:

гарантирует доставку пакетов;

собирает их в правильном порядке;

повторно отправляет, если что-то потерялось;

следит, чтобы всё дошло до адресата корректно.

Примеры, где используется TCP:

сайты (HTTP/HTTPS),

почта (SMTP, IMAP),

передача файлов (FTP),

мессенджеры.

UDP (User Datagram Protocol)

А теперь представь, что ты ведёшь живую трансляцию. Тут главное – передать как можно быстрее, пусть даже что-то потеряется.

Ты просто говоришь – и не пересказываешь фразу заново, если кто-то не расслышал.

Вот это UDP:

не проверяет доставку,

не гарантирует порядок пакетов,

почти не тратит время на «формальности».

Но зато работает быстро и без задержек.

Примеры, где используется UDP:

видеозвонки и голосовая связь (Zoom, Skype),

онлайн-игры,

стриминг в реальном времени,

DNS-запросы.

Кратко:

Характеристика TCP UDP

Надёжность Да Нет

Скорость Ниже Выше

Очерёдность Гарантирована Не гарантирована

Примеры Сайты, почта, мессенджеры Игры, видео, звонки, DNS

Важная часть – у каждого пакета есть IP-адрес назначения и номер порта.

IP – это как адрес дома, а порт – номер квартиры. Сервер может обслуживать сразу сотни сервисов: сайт на порту 80, почту на 25, DNS на 53 и так далее. Когда пакет приходит на IP, маршрутизатор смотрит на порт и решает, кому именно его передать.

Когда пакет приходит на IP, маршрутизатор смотрит на порт и решает, кому именно его передать.

Если хотите увидеть, какой IP у вас сейчас, через какой шлюз вы подключены, какие DNS-серверы используются – на Windows достаточно открыть командную строку и ввести:

```
ipconfig /all
```

Эта команда показывает:

- ваш текущий IP-адрес в сети;
- шлюз (обычно это адрес роутера);
- DNS-серверы;
- MAC-адрес адаптера;
- тип подключения (Ethernet, Wi-Fi) и его статус.

Это первый шаг к пониманию того, куда идут ваши пакеты и как устроена ваша локальная сеть. Полезно как при диагностике неполадок, так и просто ради любопытства.

Почему «интернет» не где-то там, а здесь – в каждом кабеле

Интернет – это не «облако». Это тысячи километров медных и оптических кабелей под твоими ногами, на дне океанов и в стенах зданий. Каждый твой запрос идёт по очень конкретным маршрутам: от модема в твоей квартире – через коммутаторы твоего провайдера – в магистральную сеть – через дата-центры – и обратно.

И если где-то в цепочке оборвётся кабель или кто-то на маршрутизаторе закроет нужный порт – твой «облачный интернет» исчезнет в тот же миг.

Кто управляет интернетом

ICANN, RIPE, операторы

У интернета нет одного хозяина. Но есть организации, которые держат в руках его скелет – систему адресации и распределения ресурсов.

ICANN – американская корпорация, которая управляет глобальными доменными зонами (.com, .org и т.д.) и корневыми серверами DNS.

RIPE NCC – европейский регистратор IP-адресов. Он выдаёт блоки адресов национальным и крупным операторам.

Дальше идут провайдеры и магистральные операторы, которые строят физическую сеть: прокладывают кабели, ставят маршрутизаторы, держат точки обмена трафиком (IX). Они уже управляют доступом к инфраструктуре на уровне стран и регионов.

Почему «никто и все сразу»

Всё это вместе даёт уникальную модель управления: интернетом формально не владеет никто, но реально его поддерживают тысячи организаций.

ICANN и RIPE задают правила адресов, провайдеры строят сеть, а ты как пользователь своими деньгами и трафиком подтверждаешь, что эта конструкция нужна.

Так и получается, что интернет – это «ничей и всех сразу»: нет единого центра, который мог бы выключить его целиком. Но при этом на каждом уровне есть свои узлы управления и точки, где можно перекрыть доступ.

2.1 IP-адреса: домашний и публичный

Каждое устройство, подключённое к интернету – будь то компьютер, смартфон или даже чайник с Wi-Fi – должно иметь свой «адрес», по которому его можно найти. Этот адрес называется IP-адресом (от англ. Internet Protocol address).

Внутренний адрес (192.168...) и внешний

Когда вы дома подключаетесь к интернету, то ваше устройство не выходит сразу в «большой» интернет. Сначала оно подключается к домашнему роутеру. А уже роутер общается с внешним миром.

Роутер раздаёт вашим устройствам внутренние IP-адреса, которые не видны за пределами вашей сети. Обычно они начинаются с 192.168.x.x, например:

- ноутбук получает адрес 192.168.0.12
- телефон – 192.168.0.15
- телевизор – 192.168.0.20

Все эти устройства «живут» внутри вашей сети, и только роутер имеет внешний IP-адрес – тот, который виден в интернете.

Когда вы открываете сайт, например google.com, запрос уходит от вашего устройства к роутеру, а уже роутер отправляет его дальше – от своего внешнего IP.

Можно сказать: внутренний IP – для общения внутри дома, внешний – для выхода наружу.

Динамический и статический IP

Внешний IP-адрес может быть:

Динамическим – меняется каждый раз, когда вы перезапускаете роутер. Так работает у большинства домашних пользователей.

Статическим – закреплён за вами навсегда (или пока вы не откажетесь). Часто используется бизнесом или теми, кто запускает дома сервер (например, для видеонаблюдения или сайтов).

Динамический IP дешевле и проще. Статический удобнее, если нужно, чтобы ваш компьютер или камера были постоянно доступны по одному адресу.

Проверить ваш текущий внешний IP можно на любом сайте вроде 2ip.ru или whatismyip.com.

2.2 DNS – телефонная книга интернета

Когда вы вбиваете в браузер что-то вроде google.com, компьютер не понимает это сразу. Для него всё – это цифры, то есть IP-адреса. А google.com – это всего лишь удобное для человека имя. Задача системы DNS – перевести имя в адрес.

Как DNS превращает google.com в IP

DNS (Domain Name System) – это как телефонная книга интернета. Вы знаете имя (например, «Маша»), а DNS находит вам номер телефона (IP-адрес), по которому нужно звонить.

Когда вы открываете сайт:

1. Компьютер проверяет, знает ли он уже IP-адрес google.com. Может, он запомнил его с прошлого раза.
2. Если нет – он спрашивает DNS-сервер: «Слушай, а какой IP у google.com?»
3. DNS-сервер отвечает, например: 142.250.74.206.
4. После этого начинается обычное соединение – теперь компьютер знает, куда обращаться.

DNS-серверы – это специальные компьютеры в интернете, которые хранят таблицы: «что как называется и где находится». Обычно ваш интернет-провайдер предоставляет свой DNS-сервер автоматически.

Популярные альтернативы:

Google DNS – 8.8.8.8 и 8.8.4.4

Cloudflare DNS – 1.1.1.1 и 1.0.0.1

Yandex DNS – 77.88.8.8 и 77.88.8.1 (есть несколько режимов: базовый, безопасный и семейный, можно включить фильтрацию вредоносных сайтов)

AdGuard DNS – 94.140.14.14 и 94.140.15.15 (есть режим с блокировкой рекламы, трекеров и вредоносных сайтов)

OpenDNS – 208.67.222.222 и 208.67.220.220 (поддержка фильтрации контента и защита от фишинга)

Эти адреса можно прописать вручную в настройках устройства или роутера, если стандартный DNS-сервер провайдера работает нестабильно или не фильтрует угрозы.

Иногда проблема остаётся даже после смены DNS-сервера. Это может быть связано с локальным кэшем – ваш компьютер запомнил старый или некорректный IP-адрес и продолжает его использовать. В этом случае помогает команда `flushdns`, которая очищает DNS-кэш.

Как это сделать:

Windows: откройте командную строку (Пуск → CMD) и введите `ipconfig /flushdns`

После этого появится сообщение, что кэш успешно очищен.

macOS: откройте Терминал и введите

`sudo dscacheutil -flushcache; sudo killall -HUP mDNSResponder`

Система не покажет подтверждения, но команда сработает.

Linux: в зависимости от дистрибутива, команды могут отличаться. Пример для systemd: `sudo systemd-resolve --flush-caches`

После очистки кэша ваш компьютер снова запросит IP-адрес сайта у DNS-сервера, и если раньше были ошибки – теперь всё должно заработать.

Это простое, но мощное действие – особенно полезно, когда сайт уже переехал на новый сервер, а вы всё ещё «видите» старый.

Почему иногда «не работает сайт» – а это всего лишь DNS

Бывает, вы открываете сайт – и видите ошибку: «Не удаётся найти сервер» или «Проверьте подключение». При этом интернет работает, другие сайты грузятся. Что случилось?

Возможно, просто не работает DNS-сервер. Он «заболел», не отвечает или выдаёт неправильные адреса. А ваш компьютер без него не может найти нужный сайт, как без телефонной книги.

Что можно сделать:

Перезагрузить роутер (он может «зависнуть» вместе с DNS-кэшем).

Указать вручную другой DNS-сервер – например, 8.8.8.8 или 1.1.1.1.

Проверить сайт с телефона через мобильный интернет – если откроется, значит дело точно не в сайте.

Важно: DNS – это не сам интернет, а лишь способ найти нужное. Он как указатель, который может сбиться. Но когда вы это понимаете, даже странные ошибки уже не пугают.

Легко проверить, действительно ли проблема именно в DNS. Откройте сайт <http://test.vsi.ru/> Он же открывается при прямом запросе по IP `http://80.82.32.2`. Если по запросу по IP этот сайт открывается, а при запросе по домену – нет, это значит, что DNS-запрос не резолвится, то есть не удаётся «перевести имя в адрес».

В таком случае:

Проблема не в сайте – он работает.

Не в интернете – соединение есть.

А именно в DNS-сервере или его кэше на вашем устройстве.

В этом случае особенно полезно:

Попробовать другой DNS (например, 1.1.1.1).

Очистить кэш DNS через `flushdns`.

Проверить через мобильный интернет – если сайт откроется там, значит ваш домашний DNS-сервер или роутер «залип».

Понимание таких тонкостей позволяет не паниковать и быстро выявить источник проблемы – особенно когда «вроде бы всё работает, но сайт не грузится».

2.3 Шлюзы и NAT – зачем нужен роутер

Допустим, у вас дома – ноутбук, телефон, телевизор и пара умных лампочек. Но интернет-провайдер дал вам только один IP-адрес. Как же тогда все устройства работают одновременно?

Ответ: потому что между ними и интернетом стоит роутер – особое устройство, которое выступает как шлюз и посредник. Он использует технологию под названием NAT.

Почему весь дом сидит за одним IP

Представьте себе многоквартирный дом с одним почтовым адресом. Почтальон приносит письмо на этот адрес, а дальше консьерж решает, в какую квартиру его передать. Примерно так же работает роутер.

Снаружи – один IP-адрес, например 94.25.16.112. Это адрес вашего роутера. Все запросы в интернет (на сайты, видео, игры) идут именно от него. А внутри он уже распределяет трафик между устройствами.

Внутри домашней сети у всех устройств – внутренние IP-адреса вроде 192.168.0.12, 192.168.0.15 и т.д. С интернетом напрямую они не общаются.

Это и называется NAT – Network Address Translation, или «преобразование сетевых адресов». Благодаря NAT:

все домашние устройства могут использовать один внешний IP;

снаружи никто не видит, что у вас внутри – это повышает безопасность;

провайдеру не нужно выдавать каждому чайнику по отдельному IP.

Как роутер понимает, кому что отправить

Допустим, вы на ноутбуке открыли YouTube. Роутер получает ответ с сервера Google, но у него вопрос: «А кому это видео? Ведь у меня в доме 8 устройств!»

Ответ прост: когда вы отправляете запрос, роутер запоминает, кто именно его отправил, и какой порт использовался (небольшой номер, вроде ярлыка). Потом, когда приходит ответ, роутер смотрит в таблицу: этот ответ – для 192.168.0.12, порт 54831. И направляет пакет туда.

Это называется таблица NAT – роутер ведёт список всех текущих соединений и точно знает, кому что вернуть. Работает это быстро и незаметно.

Кстати, по этой же причине:

иногда «падает интернет» из-за перегруженной NAT-таблицы – особенно на дешёвых роутерах;

определённые игры или программы требуют «проброс портов» – чтобы входящие запросы снаружи доходили до нужного устройства внутри.

Но в целом: NAT – это магия, которая позволяет всем пользоваться интернетом одновременно, даже если снаружи у вас всего один IP.

3.1 Провайдеры и их маршруты

Почему сайты могут не открываться даже при рабочем интернете

Многие пользователи думают, что интернет – это «единое облако», и если у вас работает Wi-Fi, то должно работать всё. Но на деле интернет устроен как сеть разных провайдеров, соединённых между собой. И от того, по какому маршруту идёт ваш запрос, зависит многое.

Кто такие провайдеры

Интернет-провайдер (ISP, Internet Service Provider) – это компания, которая подключает вас к интернету. Они бывают:

Домашние/частные – те, кто обслуживает квартиры: Ростелеком, МТС, Билайн, Дом.ру и т.д.

Региональные – небольшие провайдеры в городах и посёлках.

Магистральные – большие компании, у которых есть доступ к мировым сетям и подводным кабелям. Они обслуживают более мелких провайдеров.

Провайдер не просто «включает вам интернет», он строит каналы связи, арендует или владеет маршрутизаторами, и определяет, по какому пути пойдут ваши данные.

Почему у одних сайты грузятся, а у других – нет

Бывает, вы не можете зайти на сайт, а ваш друг с другого провайдера – может. Почему так?

Потому что интернет – это сеть сетей. Между провайдерами заключены соглашения, маршруты могут идти по разным путям. И если где-то сломался канал, перегружен маршрут, или блокируется часть трафика – сайт может «не открываться» только у одного провайдера.

Примеры:

У провайдера в регионе сбоит канал связи с Москвой – сайты на московских серверах «висят».

Провайдер «А» не договорился напрямую с CDN-сетью YouTube и идёт в обход – видео тормозит.

У провайдера плохой пинг до зарубежных серверов – иностранные сайты медленные.

Или наоборот: у провайдера локальный фильтр или ограничение на определённые ресурсы.

Иногда проблемы решаются сами – маршруты перенастраиваются автоматически. Но бывают ситуации, когда помогает только смена провайдера или использование VPN.

Важно: если сайт не открывается, это не всегда «сломался сайт». Чаще всего – что-то не так на пути между вами и сервером, и в этом участвует ваш провайдер.

Преимущества оптоволоконного интернета

Оптоволокно (или «оптика») – это технология передачи данных с помощью света через специальные стеклянные или пластиковые волокна. В отличие от старых медных кабелей (ADSL, витая пара), оптоволокно обеспечивает значительно более высокую скорость, стабильность и надёжность.

Скорость – главное преимущество. По оптике можно передавать сотни мегабит и даже гигабиты в секунду без ощутимых задержек. Это особенно заметно при видеозвонках, стриминге и загрузке больших файлов.

Вторая важная особенность – стабильность сигнала. В отличие от меди, оптоволокно не подвержено помехам от бытовой техники, гроз, электропроводки и других источников наводок. Интернет по оптике почти не «прыгает» и не зависает без видимых причин.

Ещё один плюс – расстояние. Сигнал по оптоволокну может передаваться на километры без потерь. Это важно при подключении удалённых районов и прокладке «магистралей» между городами.

Кроме того, оптика меньше изнашивается, устойчива к влаге и не требует усилителей на небольших расстояниях, что снижает вероятность поломок и аварий.

На практике это означает, что при наличии выбора между ADSL, 4G или оптикой – всегда лучше выбрать оптику. Это не просто «маркетинг», а действительно самая технологичная и перспективная основа интернета.

3.2 Что такое пинг и трассировка маршрута

Как узнать, где тормозит интернет

Когда сайт долго грузится или вообще не открывается, хочется понять: где именно проблема? На вашей стороне? У провайдера? У самого сайта?

Для этого существуют простые сетевые инструменты – пинг и трассировка маршрута. Ими можно пользоваться даже без особых знаний.

Пингуем google.com и смотрим ответ

Пинг (ping) – это команда, которая отправляет крошечный запрос (пакет) на сервер и измеряет, за сколько миллисекунд пришёл ответ. Это как сказать «привет» и засечь, через сколько секунд тебе ответят «привет» в ответ.

В Windows:

ping google.com

В Linux/macOS – то же самое. Результат будет выглядеть примерно так:

Ответ от 142.250.74.206: число байт=32 время=24мс TTL=115

Что это значит:

время=24мс – это задержка. Меньше = быстрее.

TTL – время жизни пакета (об этом в следующем разделе).

Если появляется сообщение вроде «Превышен интервал ожидания» – значит, нет ответа (сервер не отвечает или пакет потерялся).

Пинг помогает понять: сайт живой? Есть связь? Или всё встало?

Трассировка маршрута (tracert/traceroute)

Но что делать, если пинг не приходит вообще, или сайт работает нестабильно? Тогда используем трассировку маршрута – она показывает, по каким промежуточным узлам проходит ваш запрос.

В Windows:

tracert google.com

В Linux/macOS:

traceroute google.com

Вы увидите список «прыжков» (hops) – через какие сервера проходит ваш запрос на пути к цели. Например:

1 192.168.0.1 <1 ms

2 10.10.0.1 5 ms

3 94.25.16.1 12 ms

4 ...и т.д...

9 142.250.74.206 25 ms

Если на каком-то этапе появляются * * * или задержка резко растёт (вдруг стало 300+ мс) – значит, проблема именно там.

Например:

задержка между вашим роутером и первым хопом → проблема в домашней сети;

замедление на 2–3-м узле → у провайдера перегрузка;

замедление ближе к концу → проблемы у сервиса или на международном маршруте.

Почему где-то «зависает»

Причин может быть много:

Физическая перегрузка – роутер или узел обрабатывает слишком много трафика.

Поломка или обрыв – один из маршрутов недоступен, идёт обход.

Ограничения провайдера – часть маршрутов фильтруется или приоритет ниже.

Сервер не принимает пинг – некоторые сайты отключают ответы на ping по соображениям безопасности. Это не всегда значит, что сайт «упал».

Таким образом, пинг и трассировка – это как фонарик в темноте. Вы видите, куда идёт запрос, и где именно он спотыкается.

3.3 Время жизни пакета (TTL)

Почему у интернет-пакета есть «срок годности»

Когда вы отправляете запрос в интернет – например, открываете сайт – ваш компьютер разбивает этот запрос на маленькие кусочки данных, которые называются пакеты. Эти пакеты бегут по сети от узла к узлу, пока не доберутся до цели.

Но что будет, если в маршруте ошибка? Или петля? Или пакет не может дойти до места назначения? Чтобы такие пакеты не бродили по сети бесконечно, у них есть встроенный счётчик – TTL.

Что такое TTL

TTL расшифровывается как Time To Live – «время жизни». Но на самом деле это не «время» в секундах, а количество шагов (прыжков, hops), которое пакет может пройти.

Пример:

Пакет стартует с TTL = 64.

Каждый раз, когда он проходит через очередной маршрутизатор, TTL уменьшается на 1.

Когда TTL достигает 0 – пакет уничтожается.

Это защищает интернет от заиклившись пакетов, которые иначе могли бы перегружать сети и бесконечно путешествовать туда-сюда.

Как это выглядит на практике

Когда вы запускаете команду tracert (или traceroute), система искусственно отправляет пакеты с TTL = 1, 2, 3, и так далее. На каждом шаге, когда TTL обнуляется, промежуточный узел говорит: «Привет, это я, вот где пакет остановился». Так строится цепочка маршрута до конечной точки.

TTL также можно увидеть в ответе на пинг:

Ответ от 142.250.74.206: число байт=32 время=24мс TTL=115

Чем меньше TTL – тем ближе пакет к своей цели. Если TTL = 1, а вы ещё не добрались – значит, что-то не так в маршруте или петля.

Почему это важно

TTL может помочь:

понять длину маршрута до сайта;

обнаружить петли и ошибки в сети;

защитить сеть от бесконечного движения "потерянных" пакетов.

Иногда TTL используется и в безопасности – например, чтобы определить, с какого расстояния идёт запрос, или отличить настоящие запросы от вредоносных ботов.

Итак, TTL – это простой, но очень важный механизм, без которого интернет быстро превратился бы в кашу из заблудившихся данных.

Что такое URL и протокол

Когда вы открываете сайт, вы набираете в адресной строке не просто имя, а URL – это сокращение от Uniform Resource Locator, то есть «унифицированный указатель ресурса». Он подсказывает браузеру, где искать нужный ресурс и как именно с ним работать.

Каждый URL начинается с протокола – способа, по которому происходит обмен данными между вашим устройством и сервером. Примеры:

http:// – протокол передачи гипертекста без шифрования, аббревиатура от HyperText Transfer Protocol, «протокол передачи гипертекста».

https:// – защищённый вариант HTTP, использующий шифрование, HyperText Transfer Protocol Secure, то же самое, но «зашифрованный».

Сегодня во многих браузерах используется автоматическая переадресация с HTTP на HTTPS. Это значит, что даже если вы вручную вбили в адресную строку http://, браузер автоматически попытается открыть защищённую версию – https://.

Это стало стандартом: поисковики вроде Google понижают сайты без HTTPS в выдаче, а браузеры могут даже блокировать или пометать их как небезопасные. В результате большинство хостингов и веб-серверов по умолчанию перенаправляют весь трафик на HTTPS.

Однако в некоторых случаях это вызывает проблемы:

Если у сайта нет действующего SSL-сертификата, HTTPS-версия не откроется, и браузер покажет ошибку.

Если сайт работает только по HTTP, но браузер всё равно пытается «насильно» перейти на HTTPS – вы получите сообщение об ошибке или пустую страницу.

Некоторые старые или локальные сайты (например, админки «умных» устройств) могут не поддерживать HTTPS вообще – и тогда к ним бывает сложно подключиться с современных браузеров.

Конец ознакомительного фрагмента.

Текст предоставлен ООО «Литрес».

Прочитайте эту книгу целиком, [купив полную легальную версию](#) на Литрес.

Безопасно оплатить книгу можно банковской картой Visa, MasterCard, Maestro, со счета мобильного телефона, с платежного терминала, в салоне МТС или Связной, через PayPal, WebMoney, Яндекс.Деньги, QIWI Кошелек, бонусными картами или другим удобным Вам способом.