

Мир на связи:

Как устроены вычислительные
сети и передаются данные



ии

Максим Рубин

Максим Рубин

Мир на связи: Как устроены вычислительные сети и передаются данные

*<https://litres.ru/74618008>
SelfPub; 2026*

Аннотация

Почему фотография зависает при отправке, сайт не открывается, а значок WiFi обещает связь, которой будто нет? Между нажатием кнопки и результатом скрывается целый мир: данные превращаются в сигналы, проходят через сети и устройства — и могут задержаться на любом участке пути.

«Мир на связи» шаг за шагом объясняет, как устроено это путешествие. Вы разберётесь, как работают пакеты, адреса и маршрутизаторы, зачем нужны DNS, TCP и TLS, чем различаются WiFi и мобильная связь и как провайдеры, дата-центры, облака и CDN доставляют данные до пользователя. Книга познакомит с основами сетевой безопасности и научит искать причину неполадок: от проверки соединения и маршрута до анализа журналов и работы приложения. Вы увидите не набор разрозненных технологий, а единую цепочку — от устройства до сервиса и обратно.

Книга подойдёт тем, кто только начинает изучать сети, и всем, кто хочет увереннее понимать и диагностировать цифровые сервисы.

Содержание

Зачем нужны сети: устройства, узлы, каналы связи и путь от сообщения к пакету	6
Как передаются данные: сигналы, кодирование, кабели, оптоволокно, радиоканалы и компромиссы скорости и задержки	20
Локальная доставка данных: Ethernet, Wi-Fi, кадры, MAC-адреса, коммутаторы и виртуальные сети	33
Адресация внутри сети: IPv4 и IPv6, маски, подсети, DHCP и разрешение адресов	46
Конец ознакомительного фрагмента.	54

Максим Рубин

Мир на связи: Как

**устроены вычислительные
сети и передаются данные**

**Мир на связи: Как устроены вычислительные сети
и передаются данные**

Максим Рубин

Зачем нужны сети: устройства, узлы, каналы связи и путь от сообщения к пакету

Вечером Лена стоит на перроне и фотографирует первый снег: белые хлопья кружатся в свете фонаря, а на заднем плане уже темнеет город. Она открывает мессенджер, выбирает папу и нажимает «Отправить». На экране появляется фотография с маленьким вращающимся кружком. Лена убирает телефон в карман, достаёт его снова через минуту — кружок всё ещё на месте. Потом появляется короткое сообщение: «Не удалось отправить».

Папа ждёт фотографию дома. У него включён телефон, интернет работает, приложение открыто. И всё же снимок пока не у него. Между нажатием кнопки и появлением картинки лежит путь, которого не видно на экране: от приложения на телефоне Лены через беспроводное соединение и сети операторов к компьютерам мессенджера, а затем — к устройству папы.

Этот путь не похож на волшебную трубу, по которой сообщение беспрепятственно течёт из одного телефона в другой. Скорее, это цепочка дорог, перекрёстков и почтовых сортировочных центров. У каждого участка свои устройства, свои правила и свои возможные задержки. Чтобы понять, что слу-

чилось с фотографией, начнём с участников этой истории.

Кто участвует в передаче

Первый участник — **отправитель**, точнее, устройство отправителя. Телефон Лены не просто «показывает интернет». Он запускает приложения, хранит фотографию, обрабатывает её и передаёт данные другим устройствам.

Второй участник — **получатель**: телефон папы и приложение, в котором он должен увидеть снимок. Но в обычном мессенджере это не обязательно означает, что телефон Лены напрямую связывается с телефоном папы. Часто фотография сначала отправляется на сервер сервиса. Сервер сохраняет её и сообщает приложению папы, что появилось новое сообщение. Телефон папы может получить снимок сразу или позже — например, когда снова подключится к интернету.

Сервер в этой истории — не загадочная «облачная» пустота, а компьютер или группа компьютеров в центре обработки данных. Они принимают запросы, обрабатывают их и помогают приложениям обмениваться сообщениями. Пользователь может не знать, где физически находится такой центр. Для работы сети достаточно, чтобы устройства могли найти нужную службу и передать ей данные.

Телефоны, серверы, ноутбуки, маршрутизаторы, коммутаторы, сетевые принтеры и многие другие устройства, участвующие в обмене, называют **узлами**. Термин широкий: узел может создавать данные, принимать их, хранить или пересылать дальше. Телефон Лены и сервер мессенджера —

узлы. Маршрутизатор, который направляет трафик в другую сеть, — тоже узел, хотя пользователь с ним обычно не разговаривает.

Узлы соединяются посредством **каналов связи**. Каналом может быть медный провод, оптоволокно, радиосвязь Wi-Fi или мобильная сеть. Канал — это участок, по которому могут перемещаться сигналы. Сам по себе он не решает, кому именно адресованы данные и что с ними делать: для этого нужны устройства и правила.

А совокупность соединённых узлов и каналов, которые могут обмениваться данными, — это **сеть**. Домашняя сеть объединяет, например, телефоны, ноутбуки и маршрутизатор. Интернет соединяет множество отдельных сетей по всему миру. Поэтому интернет точнее представлять не одной гигантской сетью с единым хозяином, а «сетью сетей».

От телефона — к ближайшей сети

Предположим, телефон Лены подключён к домашнему или вокзальному Wi-Fi. Он передаёт данные по радиоканалу ближайшей точке доступа. Часто точка доступа встроена в маршрутизатор, хотя это не обязательное устройство одно и то же.

Точка доступа связывает беспроводные устройства с локальной сетью. Маршрутизатор, в свою очередь, помогает передавать данные между разными сетями: например, из домашней или вокзальной сети — в сеть интернет-провайдера. Если Лена пользуется мобильным интернетом, роль ближай-

шей точки связи играет базовая станция оператора. Далее данные всё равно попадут в сеть оператора и пойдут к другим сетям.

Эти различия полезны при поиске неполадки. Если телефон не может подключиться к Wi-Fi, проблема может быть в радиосоединении или настройках точки доступа. Если Wi-Fi подключён, но сайты не открываются, беспроводной участок может работать исправно, а сбой находится дальше — например, в маршрутизаторе или соединении провайдера. Значок Wi-Fi показывает наличие одного соединения, а не обещает, что весь путь до нужного сервера доступен.

Путь редко бывает прямым. Данные могут пройти через несколько маршрутизаторов и сетей, прежде чем достигнут сервиса. Каждый маршрутизатор рассматривает адрес назначения и выбирает, куда передать пакет дальше. Он не обязан знать весь маршрут целиком: обычно ему достаточно решить, как отправить данные на следующий участок.

Правила, без которых узлы не договорятся

Представьте, что Лена отправляет посылку, но на ней нет адреса, а служба доставки не договорилась, какой размер коробок принимать и что делать с повреждённой упаковкой. Даже отличная дорога тут не поможет. В сети похожую роль играют **протоколы** — согласованные правила обмена данными.

Протокол определяет, например, как представить адрес, как оформить сообщение, когда считать его полученным и

что предпринять при ошибке. Правил много, потому что задачи разные. Одни протоколы помогают устройствам передавать данные по локальному каналу, другие — направлять их между сетями, третьи — организуют надёжный обмен, а протоколы прикладного уровня определяют, как приложения понимают содержимое сообщений.

Важно, что два устройства могут быть произведены разными компаниями и работать на разных операционных системах. Если они придерживаются совместимых протоколов, они всё равно смогут обмениваться данными. Это похоже на общий язык и общий формат письма: отправитель и получатель не обязаны быть знакомы лично, но должны понимать, как читать адрес и где искать текст.

Приложение Лены обычно обращается к службе мессенджера по понятному имени — например, имени сайта или сервиса. Система доменных имён **DNS** помогает найти соответствующий сетевой адрес. Затем сетевой протокол IP использует адрес назначения, чтобы направлять данные между сетями. На устройстве обмен связывается также с нужным приложением при помощи номера порта: условно говоря, адрес указывает на нужное здание, а порт — на нужную дверь в нём.

На локальном участке действуют и свои адреса. Например, Wi-Fi и Ethernet используют адреса, необходимые для доставки данных в пределах текущего канала или локальной сети. Поэтому «адрес устройства» — не всегда один универ-

сальный номер, который сопровождает сообщение от начала до конца. Разные уровни сети используют разные адреса для разных задач.

Как фотография становится данными для сети

Для Лены фотография — картинка на экране. Для телефона это последовательность байтов: чисел, записанных в определённом порядке. Фотография уже может быть сжата в формате вроде JPEG или HEIF, чтобы занимать меньше места. Приложение может дополнить её служебной информацией: например, указать, в каком сообщении она отправляется.

Но целая фотография может быть слишком велика, чтобы передать её за один раз. Поэтому данные делят на части. Важно не представлять, будто существует универсальный способ разрезать каждое сообщение на одинаковые «кусочки фотографии»: приложение, транспортный протокол и сетевой уровень решают связанные, но не одинаковые задачи. Приложение может загружать файл блоками, транспортный уровень передаёт поток или отдельные датаграммы, а сетевой уровень оформляет данные в IP-пакеты. В повседневном объяснении словом **пакет** часто называют порцию данных с адресной и служебной информацией.

У пакета есть полезная нагрузка — часть передаваемых данных, — и заголовок с информацией, которая помогает его доставлять и обрабатывать. Заголовок может указывать адреса, тип протокола и другие параметры. На каждом кон-

кретном участке передачи данные дополнительно оформляются так, как требует используемый канал. Например, в Wi-Fi по радиоканалу передаются кадры. Упрощённо говоря, пакет путешествует внутри кадра, предназначенного для ближайшего участка, а затем на другом участке может быть помещён в кадр другого типа.

Здесь возникает важный принцип: большое сообщение обменивается не обязательно как одна неделимая посылка. Оно может быть передано многими порциями. Если одна из них задержалась или потерялась, это не всегда означает, что придётся отправлять заново всё сообщение. Механизм восстановления зависит от используемых протоколов и приложения.

Часто транспортный протокол, например TCP, помогает обнаруживать потери и повторно передавать недостающие данные, а также собирать поток в правильном порядке. Другие способы передачи, например UDP, сами по себе не обещают доставку и порядок; при необходимости такие функции реализуются выше. Протокол QUIC, который применяется многими современными сервисами, использует UDP как основу, но добавляет собственные механизмы надёжной передачи. Выбор зависит от задач приложения.

Сетевой протокол IP сам по себе не обещает, что каждый пакет непременно дойдёт, что он придёт вовремя или что все части придут в нужном порядке. Его часто описывают как систему передачи «по возможности»: сети стараются

ся переслать пакет дальше, но перегрузка, обрыв связи или неисправность могут помешать. Надёжность, если она нужна, обеспечивают другие уровни и само приложение.

Почему пакеты могут задерживаться и менять путь

Пакет не едет по сети в отдельной герметичной полосе. Каналы связи делят между множеством пользователей: одновременно могут загружаться страницы, отправляться видео и обновляться приложения. Когда данных много, маршрутизаторы ставят их в очередь. Как на загруженном перекрёстке, ожидание бывает коротким или заметным.

Кроме перегрузки, встречаются помехи в радиоканале, временное отключение маршрутизатора, потеря связи с оператором или недоступность сервера. Если конкретный канал перестал работать, сеть может направить следующие пакеты другим путём. Поэтому не следует считать, что все части сообщения всегда идут одной дорогой. Они могут пройти через разные промежуточные узлы, а затем снова собраться у получателя. Для протоколов более высокого уровня это обычно скрыто от приложения.

Сеть тоже не может в одиночку гарантировать, что папа увидит фотографию. Его телефон может быть выключен, приложение — не иметь доступа к сети, а сервер — временно не отвечать. Приложение мессенджера может сохранить отправку в очереди, повторить попытку позже и показать Лене статус. Но значение отметок вроде «отправлено» или «доставлено» зависит от конкретного сервиса: одна может озна-

чать, что сообщение принял сервер, другая — что его получил телефон адресата. Подробности определяет приложение.

Возвращаясь к фотографии со снегом, возможны разные причины задержки. Телефон Лены мог потерять соединение с Wi-Fi. Вокзальная сеть могла иметь выход в интернет, но перегружаться. Сервер мессенджера мог быть временно недоступен. Наконец, передача на сторону папы могла ждать, пока его телефон снова подключится. Один и тот же кружок на экране не раскрывает точный участок неисправности: он лишь сообщает, что приложение пока не завершило свою задачу.

Отправка фотографии по шагам

Чтобы увидеть всю дорогу, проследим за снимком от кнопки «Отправить» до экрана папы. Для наглядности предположим, что мессенджер использует сервер-посредник.

Этап

Зона

Назначение

1. Подготовка

Приложение Лены

Приложение связывает фотографию с сообщением, подготавливает данные и определяет нужную службу.

2. Обмен внутри телефона

Устройство отправителя

Операционная система передаёт запрос от приложения сетевым компонентам телефона.

3. Поиск службы

Локальная сеть и DNS

Устройство получает сетевой адрес сервиса по его имени, если этот адрес ещё не известен или требуется обновление.

4. Выход в интернет

Wi-Fi или мобильная сеть

Телефон передаёт данные ближайшей точке доступа или базовой станции, а затем — сети оператора или провайдера.

5. Путь через сети

Промежуточные маршрутизаторы

Пакеты пересылаются от сети к сети. По пути возможны очереди, задержки и смена маршрута.

6. Приём сервером

Сеть и сервер мессенджера

Сервер получает данные, обрабатывает их и может сохранить фотографию для адресата.

7. Доставка адресату

Сеть папы

Когда телефон папы доступен, сервис передаёт ему уведомление и нужные данные.

8. Показ сообщения

Приложение папы

Приложение собирает полученные данные, проверяет сообщение и отображает фотографию.

В современных приложениях данные нередко защищены шифрованием. Соединение может быть зашифровано между телефоном и сервером; в некоторых мессенджерах используется сквозное шифрование, при котором прочитать содержание должны только устройства участников. Но это не отменяет адресации и маршрутизации: сети всё ещё нужно доставить данные нужному сервису и устройству, даже если промежуточные узлы не могут понять содержимое.

Как самостоятельно разобраться с похожей проблемой

Когда сообщение не отправляется, полезно идти по пути от ближайшего участка к дальнему, а не сразу винить «интернет вообще».

1. Проверьте соединение устройства. Работает ли Wi-Fi или мобильная сеть? Не включён ли режим полёта? Получает ли телефон сигнал?

2. Проверьте выход за пределы локальной сети. От-

кroyте страницу или попробуйте другое приложение. Если Wi-Fi подключён, но ничего не загружается, проблема может быть уже за точкой доступа.

3. Сравните способы подключения. Если допустимо, переключитесь с Wi-Fi на мобильную сеть или наоборот. Так станет яснее, связан ли сбой с конкретным каналом или провайдером.

4. Проверьте приложение и получателя. Обновлено ли приложение? Может ли получатель принимать сообщения? Есть ли у сервиса сообщение о перебоях?

5. Дайте приложению повторить отправку. При временном обрыве повторная попытка может сработать без дополнительных действий.

Это не способ точно диагностировать каждый сбой: одна и та же внешняя ошибка может иметь разные причины. Но такой порядок помогает не смешивать радиосоединение, доступ к интернету, работу сервера и доступность телефона получателя.

Можно провести маленький опыт и без специальных приборов. Отправьте себе или близкому короткий текст и фотографию сначала по Wi-Fi, а затем через мобильную сеть. Сравните, что меняется: скорость, время ожидания, появление ошибок. Подумайте, какие узлы и каналы задействованы в каждом случае и где могла бы возникнуть задержка. Вы не увидите весь маршрут, но начнёте замечать, что связь — это не одна кнопка, а последовательность взаимодействий.

Сообщение нашло дорогу

Фотография Лены в итоге отправляется: после выхода с перрона телефон снова подключается к устойчивой сети, приложение повторяет попытку, а сервер принимает снимок. Через некоторое время папа открывает мессенджер и видит снег под фонарём. Между двумя экранами не возникло прямой магической связи. Сработала цепочка узлов, соединённых каналами, и правила, которые позволили каждому участнику понять, что передавать дальше.

Главная мысль проста: сеть соединяет устройства не абстрактно, а через конкретные участки связи и промежуточные узлы. Приложение превращает действие пользователя в данные, протоколы помогают эти данные оформить и адресовать, а разделение на пакеты делает передачу гибкой. Путь может быть длинным, общим для множества пользователей и не всегда безошибочным. Именно поэтому приложения и сетевые протоколы умеют обнаруживать проблемы, ждать, повторять попытки и собирать полученные части.

Когда в следующий раз на экране появится вращающийся кружок, за ним можно будет представить не пустоту, а целую эстафету: приложение передало данные устройству, устройство — ближайшей сети, промежуточные узлы — следующему участку, а служба должна доставить результат приложению адресата. Чтобы эта эстафета вообще состоялась, данные должны превратиться в сигналы, которые можно передать по проводу или радиоканалу. С этого и начнётся следу-

ющий шаг.

Как передаются данные: сигналы, кодирование, кабели, оптоволокно, радиоканалы и компромиссы скорости и задержки

Вечером вы отправляете коллеге презентацию: файл большой, срок — через десять минут. Полоса загрузки сначала уверенно ползёт вправо, потом замирает. Видеозвонок, который идёт рядом, распадается на отдельные слова. Вы переключаете ноутбук с Wi-Fi на кабель — и передача снова ускоряется. Файл остался тем же. Изменился путь, по которому он добирается до адресата.

Но что именно движется по этому пути? Нули и единицы не катятся по проводу, как бусины по нитке, и не летят через комнату миниатюрными записками. Биты — это способ описать данные. Чтобы они пересекли расстояние, их приходится превратить в физический сигнал: изменение напряжения в кабеле, свет в оптоволокне или электромагнитную волну в воздухе.

Проследим за одним и тем же потоком данных по трём дорогам и выясним, почему каждая из них где-то оказывается быстрой, а где-то — неудобной.

От файла к физическому сигналу

Начало путешествия — не кабель и не антенна, а приложение. Оно представляет данные в виде последовательности байтов, а байты — в виде битов. Но отправить длинную череду нулей и единиц недостаточно: получатель должен понять, где один бит заканчивается и начинается следующий, распознать сигнал среди помех и восстановить исходные данные.

Поэтому передатчик выполняет несколько действий. Он превращает поток битов в удобные для передачи группы, добавляет служебную информацию, кодирует последовательность, а затем управляет передающим устройством — например, заставляет электрический сигнал менять уровень или включает лазер. На другой стороне приёмник измеряет пришедший сигнал, распознаёт символы, проверяет данные и восстанавливает биты.

Этап

Что происходит

Зачем это нужно

Подготовка

Данные приложения делятся на порции и получают служебные сведения

Чтобы получатель понимал, что и откуда пришло

Кодирование

Биты представляются комбинациями сигналов

Чтобы их можно было надёжно передать и распознать

Передача

Передатчик создаёт электрический, оптический или радиосигнал

Чтобы данные преодолели физическое расстояние

Приём

Приёмник измеряет сигнал и восстанавливает последовательность

Чтобы на другом конце снова появились нужные биты

Здесь важно различать бит и символ. Бит — это единица информации, ноль или единица. Символ — одно из различимых состояний передаваемого сигнала. Иногда одному символу соответствует один бит, иногда — несколько. Так, радиосистема может кодировать данные комбинациями амплитуды и фазы волны. Чем больше состояний используется, тем больше данных можно уместить в заданном времени, но тем труднее приёмнику отличить близкие состояния друг от друга при помехах.

Кодирование — не декоративная упаковка. Оно помогает передатчику и приёмнику не потерять ритм, обнаруживать ошибки и иногда исправлять их. Для этого в передаваемый поток могут добавляться избыточные сведения: как контрольные цифры в банковской операции, которые помо-

гают заметить, что при переписывании что-то пошло не так. У этой надёжности есть цена: часть ресурсов канала расходуется не на полезные данные.

Первая дорога: медный кабель

Представьте, что передатчик — музыкант, а приёмник — слушатель за тонкой стеной. Музыкант меняет напряжение в проводе по заранее согласованному правилу. Приёмник наблюдает за изменениями и определяет, какие символы были отправлены.

В сетевых кабелях обычно используют не один прямой провод, а пары проводников, скрученные вместе. Такая конструкция помогает уменьшить влияние внешних помех. В распространённых кабелях Ethernet приёмник анализирует разницу между сигналами в паре: помеха, одинаково наведённая на оба проводника, в значительной мере подавляется. Но это не делает медь неуязвимой. Сигнал ослабевает по мере прохождения, соседние пары могут влиять друг на друга, а сильные электромагнитные помехи способны ухудшить связь.

Медный кабель удобен: он относительно недорог, хорошо подходит для подключения компьютеров, камер, телевизоров и оборудования внутри здания. Обычный Ethernet по витой паре для многих задач рассчитан на участки до примерно ста метров; конкретный предел зависит от стандарта и оборудования. Если расстояние больше, можно использовать промежуточное оборудование или выбрать другой тип

линии.

Электрический сигнал распространяется по кабелю не мгновенно. Скорость распространения зависит от конструкции кабеля и обычно составляет заметную долю скорости света. На коротком участке задержка распространения настолько мала, что чаще важнее ожидание обработки устройства или очередь данных. А вот на длинных трассах время в пути становится ощутимее.

Важная подробность: по проводу не обязательно проносятся те самые электроны, которые «вышли» из ноутбука и прибыли в компьютер коллеги. Электрические заряды в проводнике создают меняющееся электромагнитное поле, а возмущение этого поля распространяется вдоль кабеля. Для передачи информации существенно именно распространение сигнала, а не путешествие отдельных электронов от одного конца провода до другого.

Вторая дорога: оптоволокно

Теперь представьте не музыканта за стеной, а маленький маяк внутри прозрачной нити. Передатчик включает и изменяет световой сигнал, а волокно направляет его к приёмнику. В реальных системах картина сложнее простых вспышек: данные могут кодироваться тонкими изменениями светового сигнала. Но образ маяка помогает представить главное — вместо электрического сигнала здесь используется свет.

Волокно состоит из тонкой сердцевины и окружающей её оболочки. Их оптические свойства подобраны так, что-

бы свет распространялся вдоль волокна, отражаясь внутри него или оставаясь направленным по заданным модам. Оптический сигнал постепенно ослабевает, а при очень больших расстояниях на него влияют дисперсия и другие особенности передачи. Поэтому и оптоволокну нужны подходящие передатчики, приёмники, а иногда усилители или регенерирующее оборудование.

Оптоволокну особенно полезно там, где нужно передавать много данных на большие расстояния и где нежелательны электрические помехи. На него не действует электромагнитная наводка от электродвигателя так, как на медный провод. Волокно может соединять здания, районы и континенты. Внутри него сигнал тоже не бесконечно быстрый: свет в волокне идёт медленнее, чем в вакууме, примерно со скоростью около двух третей скорости света.

Одномодовое волокно обычно применяют для дальних линий и больших расстояний; многомодовое часто используют на сравнительно коротких участках, например внутри зданий и центров обработки данных. Это не простая шкала «хорошее — плохое»: важны расстояние, оборудование, требования к пропускной способности и стоимость всей системы.

Оптоволокну легко вообразить как идеальную трубу для данных. В действительности у него есть свои ограничения: волокно нужно аккуратно проложить, соединить подходящими разъёмами и обслуживать; его нельзя перегибать как

попало, а оптические модули и монтаж требуют затрат. Зато на длинном маршруте оно часто выигрывает у меди по возможностям и устойчивости к электромагнитным помехам.

Третья дорога: радиоканал

С радиосвязью исчезает необходимость протянуть физический кабель до каждого устройства. Передающая антенна создаёт электромагнитную волну, а принимающая улавливает её и превращает изменения волны обратно в данные. Так работают Wi-Fi, Bluetooth, мобильная связь и множество специализированных радиосистем.

Волна не несёт внутри крошечные буквы «ноль» и «единица». Информация закодирована в её параметрах: например, в изменениях амплитуды, частоты или фазы. Эти изменения приёмник должен распознать на фоне шума и сигналов от других устройств.

Радио даёт свободу движения и позволяет связать устройства, между которыми нельзя или невыгодно прокладывать кабель. Но среда здесь общая и непредсказуемая. Сигнал отражается от стен и мебели, ослабевает за препятствиями, может накладываться на другие передачи. Даже человек, вставший между ноутбуком и точкой доступа, способен изменить условия приёма. Разные сети делят ограниченный радиочастотный ресурс, а устройства должны договариваться, когда именно передавать.

Поэтому «Wi-Fi показывает полный уровень сигнала» ещё не означает, что соединение будет быстрым и ровным:

дело может быть в загруженном эфире или перегрузке точки доступа. И наоборот, более слабый сигнал не всегда означает полную потерю связи — современные системы умеют адаптироваться, снижая скорость передачи или меняя способ кодирования, чтобы сохранить надёжность.

Радиоканал не обязательно медленнее кабеля во всех ситуациях, а кабель не автоматически обеспечивает меньшую задержку на любом маршруте. Но проводное подключение обычно меньше зависит от помех в эфире, а качество радиосвязи сильнее меняется с расстоянием, препятствиями и загруженностью канала.

Один поток — три дороги

Мысленно отправим один и тот же большой файл через медный кабель, оптоволокно и радиоканал. Содержимое файла не меняется; меняется физическая среда, а вместе с ней — доступные скорости, устойчивость и условия работы.

Медь может оказаться отличным выбором для короткого соединения внутри дома или офиса: подключили кабель — и устройство получает предсказуемый канал. Оптоволокно особенно привлекательно для длинных линий и крупных потоков данных. Радио выигрывает там, где нужна мобильность или кабель невозможно провести. Но даже по самой вместительной дороге файл не полетит быстрее, чем позволяют ограничения всех участков маршрута: домашний роутер, провайдерская сеть, удалённый сервер и их загруженность.

Чтобы разобраться, почему передача то ускоряется, то замедляется, нужно различать три характеристики.

Пропускная способность — сколько данных канал способен передавать за единицу времени при заданных условиях. Её часто указывают в битах в секунду. В повседневной речи словом «скорость» нередко называют именно этот предел.

Фактическая скорость передачи, или полезная скорость, — сколько данных приложение действительно получает за определённое время. Она зависит не только от канала, но и от протоколов, помех, потерь, работы оборудования и конкурирующего трафика. Линия на сто мегабит в секунду не гарантирует, что пользователь увидит ровно сто мегабит полезных данных.

Задержка — время, которое требуется данным, чтобы добраться от отправителя до получателя. Она включает не только физическое распространение сигнала, но и сериализацию, обработку и ожидание в очередях. Например, передачу пакета размером около 1500 байт по каналу со скоростью 10 мегабит в секунду нельзя завершить быстрее чем примерно за 1,2 миллисекунды: это время, необходимое, чтобы «вытолкнуть» его биты в канал. А задержка распространения добавляется отдельно.

Для ориентира: свет проходит один километр в оптоволокне примерно за пять микросекунд. Значит, тысячекilометровый участок даёт уже несколько миллисекунд задерж-

ки только на распространение в одну сторону — и это без учёта изгибов маршрута, оборудования и очередей. Радиоволна в воздухе распространяется быстрее, но если ей приходится проходить через загруженную сеть с несколькими промежуточными узлами, выигрыш в скорости самой волны может потеряться в обработке и ожидании.

Вот почему можно иметь быстрый канал, но неприятный видеозвонок: данные прибывают с большими колебаниями задержки, то есть джиттером, или отдельные пакеты теряются и приходится ждать их повторной передачи. Для скачивания фильма важнее пропускная способность и стабильный поток. Для разговора важны низкая и ровная задержка: лишнее ожидание превращает естественную беседу в обмен репликами с паузами.

Где важнее что

Датчик на производстве. Он может передавать короткие сообщения, но должен делать это предсказуемо. Если кабель рядом проходит с мощным двигателем, стоит уделить внимание помехозащите и способу прокладки; в некоторых случаях удобнее оптоволокно, которое не восприимчиво к электромагнитным наводкам. Радиосвязь пригодится для мобильного датчика или там, где кабель трудно проложить, но нужно проверить покрытие, помехи и поведение при сбое связи. Решение зависит не от размера одного сообщения, а от того, насколько критична своевременная доставка.

Видеозвонок. Здесь важны стабильная задержка и достаточная фактическая скорость. Ноутбук рядом с хорошей точкой доступа может прекрасно работать по Wi-Fi. Если эфир перегружен или сигнал проходит через несколько стен, кабель способен сделать соединение ровнее. Для видеозвонка не обязательно покупать самый быстрый тариф: иногда полезнее переместить роутер, убрать помехи или перестать загружать канал резервным копированием во время разговора.

Связь между центрами обработки данных. Когда большие объёмы данных нужно перемещать между удалёнными площадками, часто используют оптоволокно. Оно подходит для дальних и высокоскоростных линий и не боится электромагнитных помех. Но расстояние всё равно важно: даже очень быстрый канал не отменяет времени, которое сигнал тратит на путь. Если приложения чувствительны к задержке, приходится учитывать географию и маршрут, а не только цифру пропускной способности.

Среда

Сильная сторона

Что учитывать

Где часто подходит

Медный кабель

Удобен и предсказуем на коротких участках

Ограничения по расстоянию, затухание и электромагнитные помехи

Подключение устройств внутри дома, офиса или здания

Оптоволокно

Большие объёмы данных и длинные линии; устойчивость к электромагнитным помехам

Стоимость оборудования и монтажа, требования к аккуратной прокладке

Магистральные линии, связь между зданиями и дата-центрами

Радиоканал

Мобильность и отсутствие кабеля до устройства

Помехи, препятствия, загруженность эфира и колебания качества

Wi-Fi, мобильные устройства, датчики в труднодоступных местах

Небольшой эксперимент

Проверить разницу можно без лаборатории. Запустите тест скорости и измерение задержки сначала рядом с домашним роутером, затем в соседней комнате. Если есть возможность, повторите измерения по Ethernet-кабелю. Сравните не только пиковую скорость, но и то, насколько сильно меняются результаты. Затем запустите видеозвонок или пото-

ковое видео и повторите наблюдения.

Не делайте вывод по одному числу: скорость доступа в интернет зависит от сервера тестирования и загруженности сети. Но если проводное подключение даёт заметно более ровный результат, чем Wi-Fi, причина может быть не в провайдере, а в условиях радиоканала. Попробуйте изменить положение роутера: поднять его выше, убрать за металлическую мебель или поставить ближе к месту, где часто работаете. Небольшое перемещение устройства иногда полезнее, чем покупка оборудования с громким обещанием максимальной скорости.

Главный урок прост: данные не летят по сети абстрактным облаком. На каждом участке они становятся физическим сигналом — электрическим, оптическим или радиоволной. Кодирование помогает этому сигналу не потеряться, но ни один способ не избавляет от ограничений среды. Выбирая канал, нужно спрашивать не только «где быстрее?», но и «на каком расстоянии?», «насколько важна задержка?», «что может мешать?» и «должно ли устройство двигаться?».

Когда сигнал добрался до ближайшего сетевого узла, путешествие не заканчивается. Следующий вопрос — как сеть доставляет данные именно нужному устройству в пределах локального сегмента и как отличает его от соседей.

Локальная доставка данных: Ethernet, Wi-Fi, кадры, MAC-адреса, коммутаторы и виртуальные сети

В 9:07 принтер в маленьком офисе ожил: индикатор сетевого порта замигал, хотя никто не отправлял ему документ. На соседнем столе сотрудница копировала большой файл с ноутбука на рабочую станцию. Ещё через минуту новый ноутбук подключили к свободной розетке, но до принтера он так и не достучался.

«Принтер получает чужие данные, а новый компьютер не видит нужный сегмент», — сказал администратор. Для расследования хватило не отвёртки, а блокнота. Нужно было понять, какие устройства связаны друг с другом, как коммутатор принимает решения и почему кабель, который подходит к розетке, ещё не гарантирует попадание в нужную часть сети.

Представим офис как работающий механизм: компьютеры подключены кабелями к коммутатору, принтер — к другому его порту, а ноутбуки выходят в сеть через точку доступа Wi-Fi. Все эти устройства могут обмениваться данными, но делают это не бесформенным потоком битов. Для ло-

канальной доставки данные упаковываются в **кадры** — словно письма в конверты с адресом ближайшего получателя.

Сначала выясним, кому предназначен кадр

Вспомним важное различие. IP-пакет отвечает на вопрос: «К какому узлу или сети направлены данные?» Кадр канального уровня отвечает на более непосредственный вопрос: «Кому передать эти данные на этом участке сети?»

У Ethernet-кадра есть MAC-адрес отправителя и MAC-адрес получателя. В нём также указывается, какой протокол находится внутри, например IPv4 или IPv6; могут присутствовать дополнительные поля и контрольная сумма для обнаружения повреждений. Если коротко, IP-пакет — это содержимое, а кадр — оболочка, позволяющая доставить его по локальному каналу. При переходе к следующему участку сети оболочка может измениться, даже если IP-пакет продолжает путь.

MAC-адрес обычно записывают как шесть пар шестнадцатеричных цифр, например 02:1A:2B:3C:4D:5E. Это адрес канального уровня, а не адрес, по которому выбирают маршрут через множество сетей. Коммутатор использует его, чтобы переслать кадр на нужный порт; маршрутизатор решает, куда отправить IP-пакет дальше.

Адреса MAC часто назначаются сетевым интерфейсам производителем и рассчитаны на уникальность в пределах системы их выдачи. Но не стоит считать их вечными паспортами устройств: адрес можно изменить программно, вирту-

альные интерфейсы получают собственные адреса, а современные ноутбуки могут использовать для Wi-Fi временный, приватный MAC-адрес. Поэтому MAC удобен для локальной доставки, но сам по себе не доказывает личность устройства.

Когда компьютер отправляет данные, ему зачастую сначала нужно узнать MAC-адрес следующего получателя. Если нужный узел находится в той же IP-подсети, это может быть MAC самого узла. Если узел удалённый — например, сервер в интернете, — кадр предназначается MAC-адресу локального маршрутизатора. IP-адрес назначения при этом остаётся адресом сервера. Подробно разбирать, как компьютер узнаёт нужный MAC, будем в следующей главе; сейчас важно другое: кадр доставляет данные только до ближайшего узла локального участка.

Коммутатор учится на проходящих кадрах

Нарисуем движение данных на бумаге. Пусть компьютер А хочет отправить кадр компьютеру Б, а оба подключены к одному коммутатору. Чтобы увидеть работу коммутатора, следуйте за кадром шаг за шагом:

1. Компьютер А отправляет кадр. В поле источника стоит MAC-адрес А, в поле получателя — MAC-адрес Б.

2. Коммутатор принимает кадр на одном из портов. По адресу источника он запоминает: «MAC-адрес А находится за портом 3».

3. Коммутатор ищет адрес Б в своей таблице. Табли-

ца связывает MAC-адреса с портами, через которые эти адреса недавно были замечены.

4. Если адрес Б известен, кадр уходит только в нужный порт. Остальным компьютерам его передавать не требуется.

5. Компьютер Б принимает кадр. Его сетевой интерфейс проверяет адрес назначения и, если кадр предназначен ему, передаёт содержимое выше — например, сетевому протоколу.

Упрощённо запись в таблице коммутатора выглядит так:

VLAN

MAC-адрес

Порт

20

MAC компьютера А

3

20

MAC принтера

8

20

MAC компьютера Б

11

Коммутатор обычно **обучается по адресу источника**: он запоминает не только адрес, но и порт, с которого пришёл кадр. Записи динамические: если устройство исчезло или переместилось, старая запись со временем устареет и будет заменена новой. Благодаря этому сеть не нужно вручную настраивать так, чтобы коммутатор знал заранее расположение каждого компьютера.

Но в нашем офисе компьютеры копируют файл, а принтер мигает. Как такое возможно, если он не получатель?

Если коммутатор пока не знает, где находится МАС-адрес Б, он не может выбрать один порт. Тогда он разошлёт **неизвестный одноадресный кадр** через остальные порты той же виртуальной сети, кроме того, с которого кадр пришёл. Так коммутатор как бы спрашивает: «Кто здесь знает адрес Б?» Похожим образом он распространяет широковещательные кадры — те, которые предназначены всем участникам локального сегмента.

Сетевой интерфейс принтера может увидеть такой кадр, но это не значит, что принтер примет его как задание на печать. Если МАС-адрес назначения не совпадает с его адресом и кадр не широковещательный, интерфейс обычно отбрасывает его, не передавая приложению печати. Иными словами, «порт увидел кадр» и «принтер получил документ» — совершенно разные утверждения.

Широковещательные кадры нужны для некоторых слу-

жебных действий и обнаружения устройств. Их получают многие участники одного сегмента, поэтому объём таких рассылок важно контролировать. Коммутатор не разносит их повсюду без разбора: рассылка ограничена соответствующей виртуальной локальной сетью.

Вид кадра

Как выбирается получатель

Что делает коммутатор

Известный одноадресный

Один MAC-адрес

Пересылает на порт, указанный в таблице

Неизвестный одноадресный

Один MAC-адрес, ещё не найденный в таблице

Рассылает в пределах соответствующей VLAN, кроме входного порта

Широковещательный

Все участники локального сегмента

Рассылает в пределах соответствующей VLAN, кроме входного порта

В первые мгновения после перезапуска коммутатора таблица может быть почти пустой. Поэтому часть кадров прихо-

дится разослать по нескольким портам. Как только устройства ответят, коммутатор выучит их адреса и сможет действовать точнее. Так что мигающий индикатор принтера при чужой передаче может быть нормальным следствием работы сети, а не признаком того, что принтер «читает» соседние документы.

Ethernet и Wi-Fi: разные пути к одной локальной сети

У рабочего компьютера путь в локальную сеть обычно проходит по кабелю Ethernet. В кабеле данные передаются электрическими или оптическими сигналами — в зависимости от типа среды. В современном офисе Ethernet-соединение с коммутатором, как правило, работает в полнодуплексном режиме: устройство и коммутатор могут передавать данные одновременно, а отдельные пары проводников служат направлениям передачи. Это не та ситуация, когда весь офис делит один общий провод и устройства по очереди «кричат» в него.

Ноутбук может попасть в ту же локальную сеть по Wi-Fi. Точка доступа связывает беспроводных клиентов с проводной сетью, часто работая для них как мост. Устройство передаёт кадры по радиоканалу, а точка доступа пересылает их дальше, например в коммутатор. В итоге ноутбук и проводной компьютер могут оказаться участниками одной логической сети, хотя один подключён радиоволнами, а другой — кабелем.

Wi-Fi и Ethernet при этом не становятся одним и тем же. Ethernet использует собственный формат кадров и способ передачи по кабелю; Wi-Fi определён стандартами семейства 802.11 и имеет другой формат радиок кадров. В беспроводной сети устройства делят доступ к радиоэфир: перед передачей они оценивают, занят ли канал, а получатель может подтвердить приём кадра. Помехи и удалённые друг от друга передатчики усложняют этот обмен. Точка доступа принимает и перенаправляет данные, но радиоэфир не становится от этого проводом.

Главное для нашей задачи: **Wi-Fi — другой способ подключиться к локальной сети, а не другая форма IP-пакета.** Внутри кадра по-прежнему могут находиться IP-пакеты. Но подробности канального обмена и адресных полей отличаются от Ethernet.

Зачем офису виртуальные сегменты

Вернёмся к новому ноутбуку. Он подключён кабелем, индикатор розетки горит, но принтер остаётся недоступным. Проверка показывает: розетка настроена не для рабочей сети, а для гостевой. Ноутбук попал не туда, куда его владелец рассчитывал попасть.

Здесь помогают **VLAN — виртуальные локальные сети.** Они позволяют разделить одну физическую инфраструктуру на несколько логических сетей. Один коммутатор может обслуживать рабочие компьютеры, принтеры и гостевые устройства так, будто для них созданы отдельные локальные

сегменты.

Например, офисный коммутатор настроен так:

VLAN

Назначение

Пример подключения

20

Рабочие устройства

Порты сотрудников и офисный Wi-Fi

30

Принтеры

Сетевые принтеры

40

Гостевые устройства

Гостевой Wi-Fi и гостевые розетки

Если ноутбук подключён к порту VLAN 40, он не станет участником VLAN 20 лишь потому, что стоит рядом с рабочим компьютером или подключён к тому же коммутатору. Коммутатор обрабатывает кадры каждой VLAN отдельно: широковещательная рассылка из VLAN 40 не уходит в VLAN 20, а таблица MAC-адресов учитывает, к какой VLAN относится адрес.

Обычный порт для конечного устройства часто настраивают как **порт доступа**: он относится к одной VLAN, а компьютер отправляет и принимает кадры без специальной метки VLAN. Для связи коммутаторов между собой используют **транковые порты**, которые могут переносить трафик нескольких VLAN. К кадрам на таком соединении добавляется метка, указывающая, к какой VLAN они относятся. Точку доступа также можно настроить так, чтобы рабочая и гостевая Wi-Fi-сети попадали в разные VLAN.

Следствие для нашего ноутбука простое: загоревшийся индикатор подтверждает наличие физического соединения, но не правильность настройки порта. Нужно проверить, в какую VLAN назначена розетка, а если ноутбук подключается по Wi-Fi — какая VLAN связана с выбранным именем беспроводной сети.

VLAN — не шифрование и не автоматический брандмауэр. Она разделяет локальный обмен кадрами, но обмен между VLAN возможен, если его разрешает маршрутизатор или коммутатор третьего уровня. Именно на этом переходе можно применять правила доступа: например, разрешить сотрудникам печатать, а гостям — только выходить в интернет.

Не следует также считать VLAN и IP-подсеть одним и тем же понятием. На практике их часто проектируют парами: одна VLAN — одна IP-подсеть. Так проще управлять сетью. Но VLAN описывает разделение на канальном уровне, а IP-

подсеть — группировку адресов на сетевом. Это связанные, но не тождественные вещи.

Проведём диагностику

Чтобы понять, кто в офисе находится в одном логическом сегменте, недостаточно посмотреть, кто подключён к одному коммутатору или кто находится в одной комнате. Нужно выяснить настройки VLAN. Рассмотрим конфигурацию:

Устройство

Подключение

VLAN

Рабочий компьютер А

Порт коммутатора 3

20

Принтер

Порт коммутатора 8

20

Ноутбук сотрудника

Wi-Fi «Office»

20

Гостевой телефон

Wi-Fi «Guest»

Новый ноутбук

Порт коммутатора 12

40

Предположим, между коммутатором и точкой доступа настроен транк, по которому проходят VLAN 20 и 40, и для клиентов не включена изоляция друг от друга. Тогда компьютер А, принтер и ноутбук в сети «Office» находятся в одном логическом L2-сегменте — **VLAN 20**. Гостевой телефон и новый ноутбук находятся в **VLAN 40**. Физически они могут быть подключены к тому же оборудованию, но широковещательный трафик рабочей сети до них не дойдёт.

Теперь попробуйте решить похожую задачу самостоятельно:

1. Два компьютера подключены к разным коммутаторам. Между коммутаторами есть транк, который пропускает VLAN 20.
2. Оба компьютера назначены в VLAN 20.
3. Принтер подключён к Wi-Fi-точке доступа, чей SSID настроен на VLAN 30.
4. Новый ноутбук подключён к порту доступа VLAN 20.

Какие устройства находятся в одном сегменте? Проверьте ответ не по расстоянию и не по типу подключения, а по членству в VLAN. Два компьютера и новый ноутбук нахо-

дятся в VLAN 20, если между коммутаторами действительно передаётся эта VLAN. Принтер — в VLAN 30. Наличие Wi-Fi или кабеля само по себе группу не определяет.

Если устройство оказалось не там, где ожидалось, проверяйте последовательно: работает ли физическое соединение; к какой VLAN привязан порт или Wi-Fi-сеть; разрешена ли нужная VLAN на соединениях между коммутаторами; включены ли ограничения на обмен между беспроводными клиентами. Только после этого имеет смысл переходить к вопросам IP-настроек и маршрутизации.

Коммутатор — не всевидящий диспетчер, а быстрый ученик: он запоминает, с какого порта пришёл каждый MAC-адрес, и направляет известные ему кадры точно. Ethernet и Wi-Fi доставляют данные разными способами, но оба могут включать устройство в локальный сегмент. А VLAN определяет, кто именно входит в этот сегмент и чьи широковещательные кадры может получить.

Запомните простой порядок: сначала выясните, в какой локальной сети находится устройство; затем — по какому адресу оно доставит кадр ближайшему получателю. Это поможет не путать MAC-адреса с IP-адресами и физическое подключение — с принадлежностью к нужной сети.

Адресация внутри сети: IPv4 и IPv6, маски, подсети, DHCP и разрешение адресов

Новый ноутбук подключился к офисному Wi-Fi, получил значок с полными полосками сигнала — и тут же отказался находить сетевой принтер. Принтер включён, ноутбук в сети, оба стоят в соседних комнатах. Кажется, будто они должны просто «увидеть» друг друга. Но Wi-Fi отвечает лишь на один вопрос: получилось ли установить связь по радио. Чтобы отправить данные нужному устройству, сети нужно знать, где оно находится, и понять, как до него добраться.

В этой главе мы пройдем путь от настройки нового устройства до первого обмена данными с соседом: выясним, чем IP-адрес отличается от MAC-адреса, как маска делит адреса на местные и удалённые, что именно выдаёт DHCP и зачем протоколу IP нужен помощник для доставки по локальному каналу.

Адрес — не имя и не вечное место жительства

В предыдущей главе мы познакомились с локальной доставкой кадров по MAC-адресам. Коммутатор смотрит на MAC-адрес назначения и передаёт кадр в нужную сторону внутри сегмента сети. Но MAC-адрес не заменяет IP-адрес, как номер подъезда не заменяет почтовый адрес: каждый от-

вечает на свой вопрос.

MAC-адрес нужен для доставки по локальному каналу. IP-адрес помогает определить сетевое положение устройства и доставить данные между сетями.

Представьте офисный комплекс. Сначала письмо нужно отправить по адресу здания, а затем — найти внутри него нужное помещение. IP-адрес похож на адрес здания в сетевой системе доставки, а MAC-адрес помогает передать кадр конкретному интерфейсу в пределах локального сегмента. Это лишь аналогия: IP-адрес не является постоянным именем устройства и не обязательно принадлежит всему устройству целиком. Обычно он назначается сетевому интерфейсу — например, Wi-Fi-адаптеру ноутбука.

Устройство может получить другой IP-адрес после переподключения или переезда в другую сеть. Даже MAC-адрес не всегда неизменен: некоторые устройства используют случайный MAC-адрес для Wi-Fi или позволяют менять его программно. Имя компьютера, например office-laptop, — тоже отдельная вещь: оно может разрешаться в IP-адрес через DNS, но не заменяет ни IP-, ни MAC-адрес.

Вернёмся к ноутбуку. Чтобы решить задачу с принтером, ему прежде всего нужно получить собственные сетевые настройки.

Шаг первый. Получаем карточку сетевой настройки

В домашней или небольшой офисной сети эту работу

обычно выполняет ДНСР — протокол автоматической настройки узлов. Чаще всего ДНСР-сервером выступает роутер. Когда новое устройство подключается, последовательность выглядит так:

1. Поиск. Устройство сообщает, что ему нужны настройки сети.

2. Предложение. ДНСР-сервер предлагает свободный IP-адрес и параметры подключения.

3. Запрос. Устройство подтверждает, что хочет использовать предложенный адрес.

4. Подтверждение. Сервер закрепляет аренду на определённое время и передаёт настройки.

В первые мгновения устройство ещё может не знать своего IP-адреса, поэтому начальные сообщения ДНСР рассылаются так, чтобы их мог услышать сервер в локальной сети. Детали такого обмена нам сейчас не понадобятся. Важнее то, что ДНСР не просто «называет адрес», а выдаёт целую карточку сетевой настройки.

Параметр

Пример

Для чего нужен

IP-адрес

192.168.1.34

Определяет сетевое положение интерфейса

Маска или префикс

255.255.255.0 или /24

Показывает, какая часть адреса относится к подсети

Шлюз по умолчанию

192.168.1.1

Помогает отправлять данные за пределы локальной подсети

DNS-сервер

192.168.1.1 или другой адрес

Помогает находить IP-адреса по доменным именам

Срок аренды

Например, 24 часа

Показывает, как долго устройство может использовать выданный адрес

Адреса из диапазона 192.168.x.x часто встречаются в частных домашних сетях. К частным также относятся диапазоны 10.x.x.x и 172.16.x.x–172.31.x.x. Такие IPv4-адреса подходят для внутренних сетей, но сами по себе не являются адресами, по которым домашнее устройство доступно из любой точки интернета.

DHCP выдаёт адрес в аренду, а не навечно. Обычно

устройство продлевает аренду автоматически, пока остаётся в сети. При этом администратор может настроить постоянное назначение адреса конкретному устройству — например, чтобы принтер каждый раз получал один и тот же IP. Такая настройка часто называется DHCP-резервированием.

Если устройство вместо ожидаемого адреса получило адрес вида 169.254.x.x, это может означать, что DHCP-сервер не ответил. Такой адрес позволяет в некоторых случаях общаться с соседями в локальном сегменте, но обычно не даёт полноценного доступа к сети через роутер. Это повод проверить подключение к Wi-Fi или кабелю, работу DHCP-сервера и настройки VLAN.

Шаг второй. Читаем маску и находим границу подсети

У ноутбука в нашей истории такая карточка:

- IP-адрес: 192.168.1.34
- Маска: 255.255.255.0
- Шлюз: 192.168.1.1
- Принтер: 192.168.1.80

Маска отвечает на важный вопрос: **какие части IP-адреса обозначают подсеть, а какие — конкретный адрес внутри неё?** Запись 255.255.255.0 можно сокращённо записать как /24. Это означает, что первые 24 бита адреса относятся к сети. Для начального разбора достаточно запомнить: при маске /24 первые три числа в адресе должны совпадать, чтобы адреса оказались в одной подсети.

Посмотрим на ноутбук шаг за шагом:

1. Его адрес — 192.168.1.34.

2. Маска /24 оставляет часть подсети 192.168.1, а последнюю часть считает адресом устройства внутри неё.

3. Получается адрес подсети 192.168.1.0.

4. У принтера адрес 192.168.1.80. Первые три числа совпадают: 192.168.1.

5. Значит, по настройкам IP принтер находится в той же подсети, что и ноутбук.

Типичная подсеть 192.168.1.0/24 включает адреса устройств от 192.168.1.1 до 192.168.1.254. Адрес 192.168.1.0 обозначает саму подсеть, а 192.168.1.255 обычно используется как широковещательный адрес для обращения ко всем узлам этой IPv4-подсети. Поэтому эти два адреса, как правило, не назначают обычным устройствам.

Теперь представим, что ноутбук хочет связаться с устройством 192.168.2.20. При той же маске /24 его адрес подсети будет 192.168.2.0, а не 192.168.1.0. Подсети различаются. Ноутбук понимает: доставить данные напрямую внутри своей локальной подсети он не может, нужен шлюз — в нашем примере 192.168.1.1.

Маска — не декоративная настройка и не просто способ записать диапазон. Она влияет на решение самого устройства: **отправлять ли пакет адресату напрямую или передать его маршрутизатору**. Если маска настроена неверно, компьютер может ошибочно считать соседа удалённым

или, наоборот, пытаться обращаться к удалённому узлу как к местному.

Небольшое упражнение

Ноутбук имеет адрес 192.168.1.70/26. Принтер — 192.168.1.100. Они в одной подсети или нет?

Подсказка: /26 делит последний октет на блоки по 64 адреса. В данном случае первый блок, начинающийся с 0, заканчивается на 63, второй идёт от 64 до 127.

Ответ: адреса .70 и .100 попадают в один блок 64–127, значит, находятся в одной подсети. А устройство с адресом 192.168.1.130 попало бы уже в следующий блок — 128–191.

Шаг третий. Связываем IP-адрес с MAC-адресом

Но ноутбук всё ещё должен как-то передать данные принтеру. IP-адрес говорит: «Нужен узел 192.168.1.80». А локальный кадр, как мы помним, доставляется по MAC-адресу. Как ноутбуку узнать MAC-адрес принтера?

В IPv4 для этого используется **ARP** — протокол разрешения адресов. Если нужного соответствия ещё нет в памяти устройства, ноутбук рассылает по локальному сегменту запрос примерно такого смысла: «Кто использует IP-адрес 192.168.1.80? Сообщите свой MAC-адрес». Устройство с этим IP отвечает, после чего ноутбук может отправить ему локальный кадр.

Узнанные соответствия обычно ненадолго сохраняются в таблице соседей — иначе при каждой передаче пришлось бы заново задавать тот же вопрос. ARP не отправляет данные

между сетями и не ищет адреса во всём интернете. Его задача гораздо уже: сопоставить IPv4-адрес с адресом канального уровня **в локальном сегменте**

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.