

Адресация в Интернете: как устройства находят друг друга

Браузер ищет адрес сайта через домены, DNS и порты, а пакеты идут по маршрутам.





Почему адресация стала основой глобальной сети

Интернет вырос из ARPANET, где адресов хватало. Но с миллиардами устройств понадобились более точные адреса и масштабирование: IPv4 оказался ограничен, поэтому развились NAT и IPv6 — чтобы каждый пакет дошёл до нужной службы.

Что такое IP-адрес и какие бывают его виды

1

IP-адрес — это числовой идентификатор интерфейса в сети, работающей по протоколу IP, чтобы отправитель мог направить пакет конкретному узлу или службе.

2

IPv4 использует 32 бита и записывается как четыре числа 0–255 через точки, а IPv6 — 128 бит и шестнадцатеричные группы через двоеточия.

3

Адреса бывают статическими и динамическими, а также публичными и частными: публичные доступны извне, частные применяются внутри локальных сетей.

IPv4 и IPv6: сравнение основных характеристик

Критерий	IPv4	IPv6
Длина адреса	32 бита	128 бит
Ограничение адресного пространства	Около 4,3 млрд адресов	Практически неограниченно
Запись	Десятичные числа с точками	Шестнадцатеричные с двоеточиями
Статус в сетях	Широкое распространение	Развивает и дополняет IPv4

Сопоставление структуры адресов, возможностей и практических последствий для масштабирования Интернета.

IPv4 исторически удобен, но ограничен по объёму, поэтому IPv6 обеспечивает устойчивый запас для роста сети и устройств.

Базовые положения протоколов IPv4/IPv6 и документы IETF.

Структура IPv4-адреса и маска подсети



1

Сеть и узел в одном адресе

IPv4-адрес делится на часть сети и часть узла. Маска подсети показывает, какие биты относятся к сети. Это определяет, с кем можно обмениваться напрямую внутри подсети.

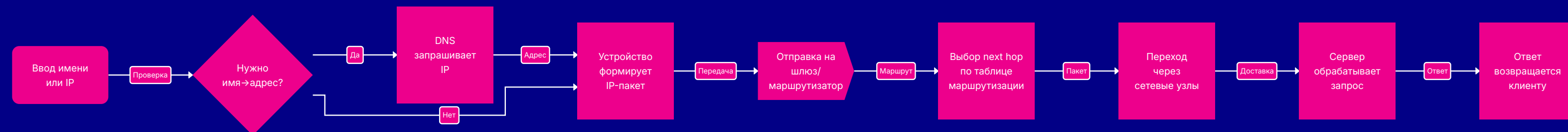
2

Маска подсети и префикс /24

Например, 255.255.255.0 соответствует префиксу /24: 24 бита — для адреса сети. Устройства с одинаковой сетевой частью образуют одну подсеть, а к остальным сетям обращаются через маршрутизатор.

Как пакет находит адресата в сети

Обобщённый путь данных от ввода адреса до получения ответа; в локальной сети часто используется домашний роутер как шлюз по умолчанию.



DNS: система, которая связывает имена и IP-адреса

1

DNS (Domain Name System) нужен, потому что людям удобны имена, а маршрутизаторам и приложениям — IP-адреса. Он выполняет преобразование доменного имени в сетевой адрес.

2

В цепочке обычно участвуют рекурсивный резолвер и серверы разных уровней: корневые, серверы доменных зон и авторитетные серверы конкретного домена.

3

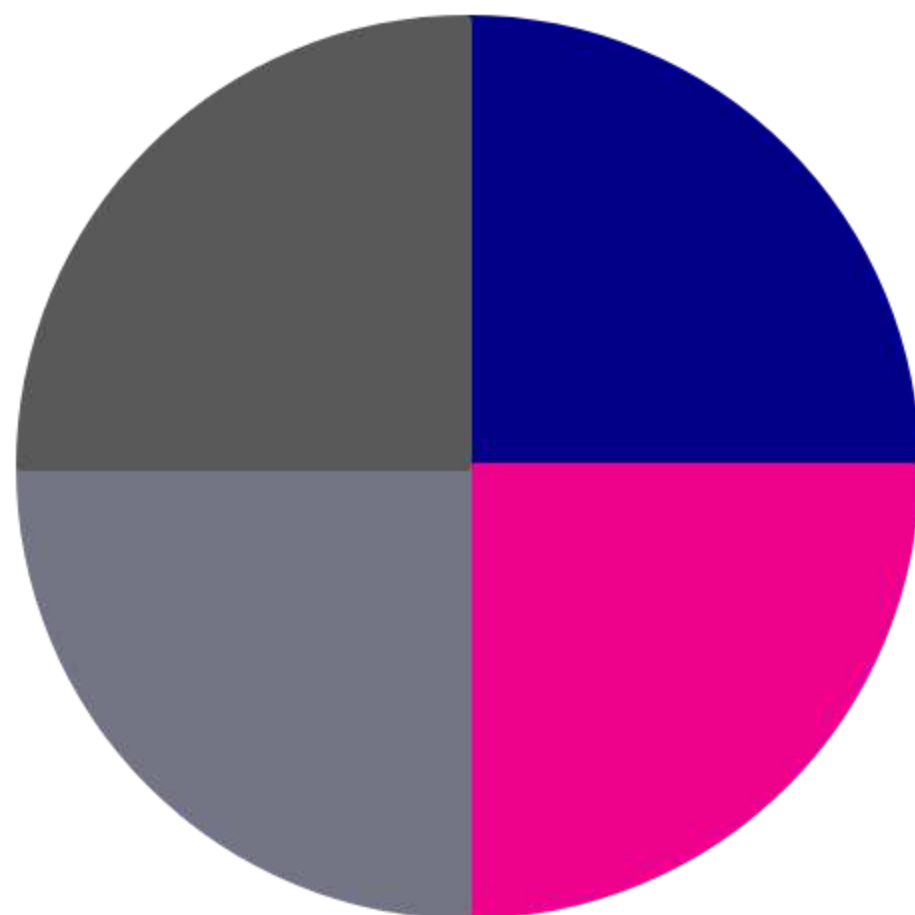
Тип записи определяет, что именно возвращается: A — IPv4, AAAA — IPv6, CNAME — псевдоним, который ведёт к другому имени. Так упрощают поддержку доменов.

4

Благодаря DNS веб-адрес вроде `www.example.ru` работает привычно, а браузер получает конкретный IP-адрес для установления соединения.

Иерархия доменного имени

■ Домен верхнего уровня: .ru ■ Домен второго уровня: example
■ Поддомен/раздел: www ■ Имя хоста (зависит от настройки)



Иерархия всегда читается от более общего уровня к более частному: сначала зона, затем уточняющие части имени.

Разделение на уровни помогает масштабировать управление доменами: каждому уровню соответствует отдельная зона ответственности.

Примеры структуры имён домена; общая практика DNS-делегирования.

Публичные и частные адреса в локальной сети

1

Частные IPv4-адреса не маршрутизируются в Интернете и используются внутри локальных сетей. Они помогают обойти дефицит адресов и удобно объединять домашние устройства.

2

К частным диапазонам относятся 10.0.0.0/8, 172.16.0.0/12 и 192.168.0.0/16. Их выбирают организации и пользователи для внутренней адресации без выхода в глобальную маршрутизацию.

3

Публичный адрес выдаётся провайдером и виден во внешней сети. Обычно в домашней сети у роутера один публичный адрес, а компьютеры, смартфоны и другие устройства — частные.

Основные типы адресов и их назначение

Тип	Назначение	Пример
Публичный	Доступ из Интернета	—
Частный	Внутри локальной сети	—
Статический	Не меняется	—
Динамический	Выдаётся автоматически	—
Loopback	Обращение к самому компьютеру	127.0.0.1
Link-local	Временный адрес при отсутствии DHCP	169.254.0.0/16

Классификация IP-адресов и связанных адресов по назначению: внешний доступ, внутренняя связь, автоконфигурация и проверки.

Разные типы адресов решают разные задачи: от внешнего доступа до временной работоспособности и диагностики служб.

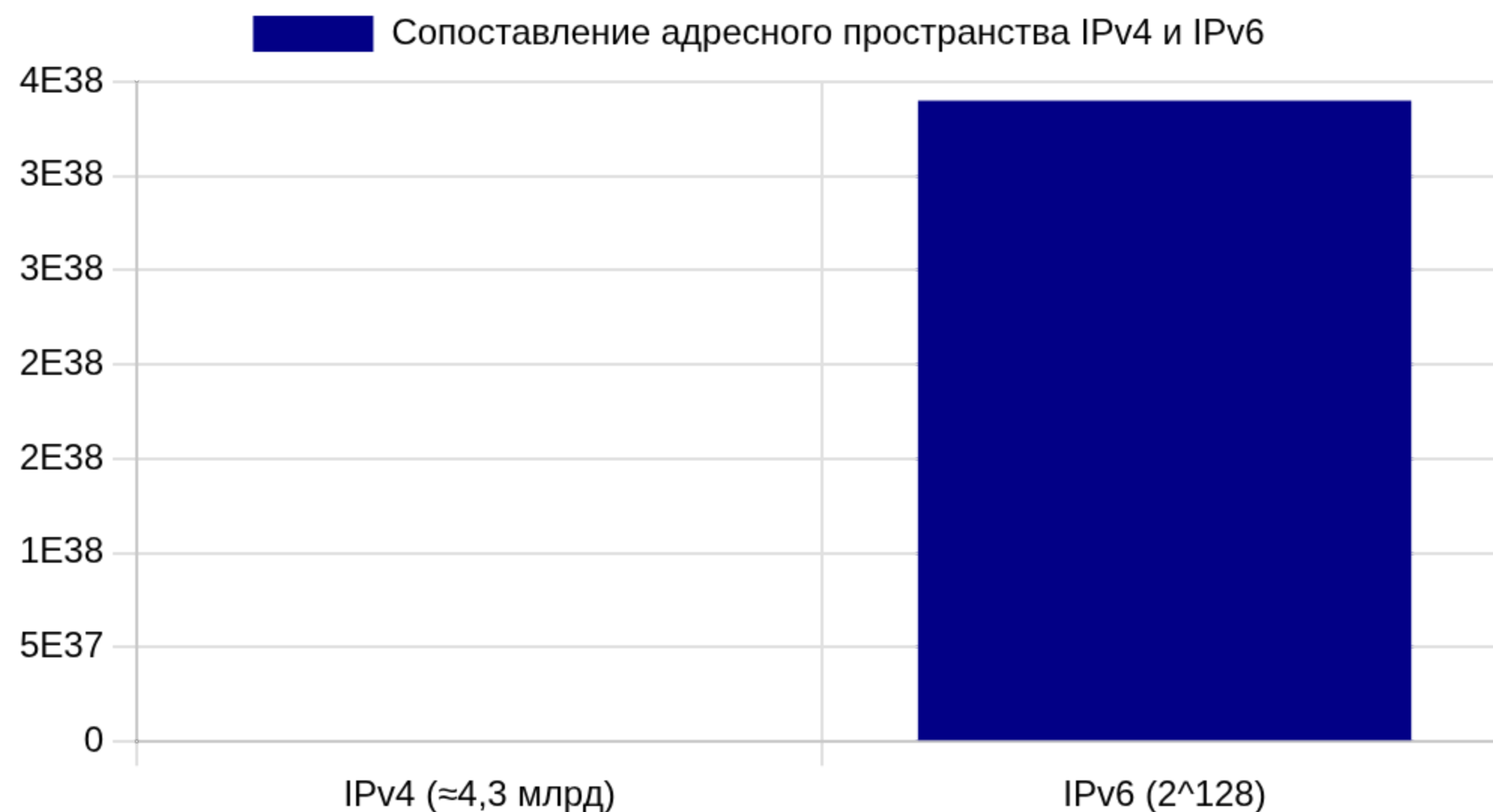
Практика TCP/IP и базовые сетевые стандарты.

NAT: почему один внешний адрес обслуживает много устройств



- NAT (Network Address Translation) преобразует частные адреса устройств во внутренней сети в один или несколько публичных адресов на границе с Интернетом. Поэтому роутер может «сводить» трафик десятков клиентов к внешнему IP без их прямой видимости.
- С практической точки зрения NAT стал ответом на дефицит IPv4-адресов и закрепился в домашних и офисных сетях. На схеме это выглядит как пересылка пакетов от внутренних хостов через роутер к адресу провайдера.

Почему IPv4-адресов стало не хватать



Рост спроса подпитывали смартфоны, облачные сервисы и интернет вещей: адрес нужен не только людям, но и сервисам, обновлениям и соединениям «в фоне».

Разница масштабов показывает системный дефицит: IPv4 исчерпывается быстрее, чем растёт инфраструктура, тогда как IPv6 создаёт долгосрочный запас и гибкость.

Подсчёты адресного пространства: IETF-описания форматов IPv4/IPv6 (IPv4: 32 бита, IPv6: 128 бит); оценка «≈4,3 млрд» широко приводится в учебных материалах по IPv4.

Порты: адресация не только устройства, но и службы

HTTP (80)



Порт 80 используется для веб-трафика по HTTP. На одном и том же IP-адресе он направляет входящие запросы браузера к нужному веб-приложению, отделяя его от других сервисов.

HTTPS (443)



Порт 443 применяют для HTTPS, когда данные передаются по зашифрованному каналу. Благодаря этому один сервер может обслуживать защищённые страницы, не смешивая их с другими типами трафика.

DNS (53)



Порт 53 предназначен для DNS-запросов. Через него клиент обращается к резолверу за IP-адресом доменного имени, а сервер отвечает, позволяя браузеру найти «где находится сайт».

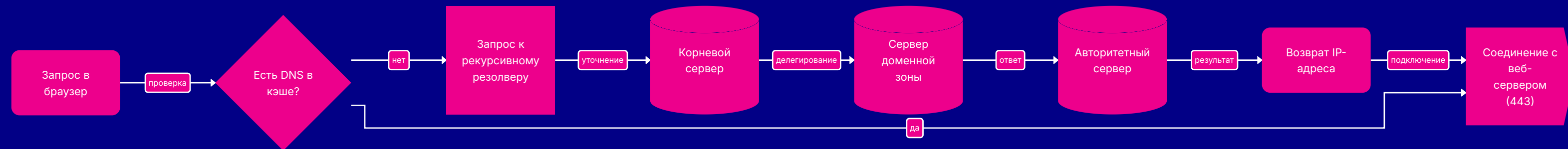
SMTP (25)



Порт 25 часто связывают с SMTP — протоколом отправки почты. Так почтовый обмен не конфликтует с вебом и DNS, потому что маршрутизация трафика учитывает и адрес, и порт.

Что происходит при открытии сайта в браузере

Логика поиска адреса домена и установление соединения на основе DNS и IP. Порт часто бывает 443 для HTTPS.



Кто управляет адресным пространством Интернета

1

IANA координирует глобальное распределение IP-адресов и доменных зон, чтобы в Интернете существовали уникальные идентификаторы. Без такой координации маршрутизация и поиск ресурсов быстро превращались бы в конфликтные ситуации.

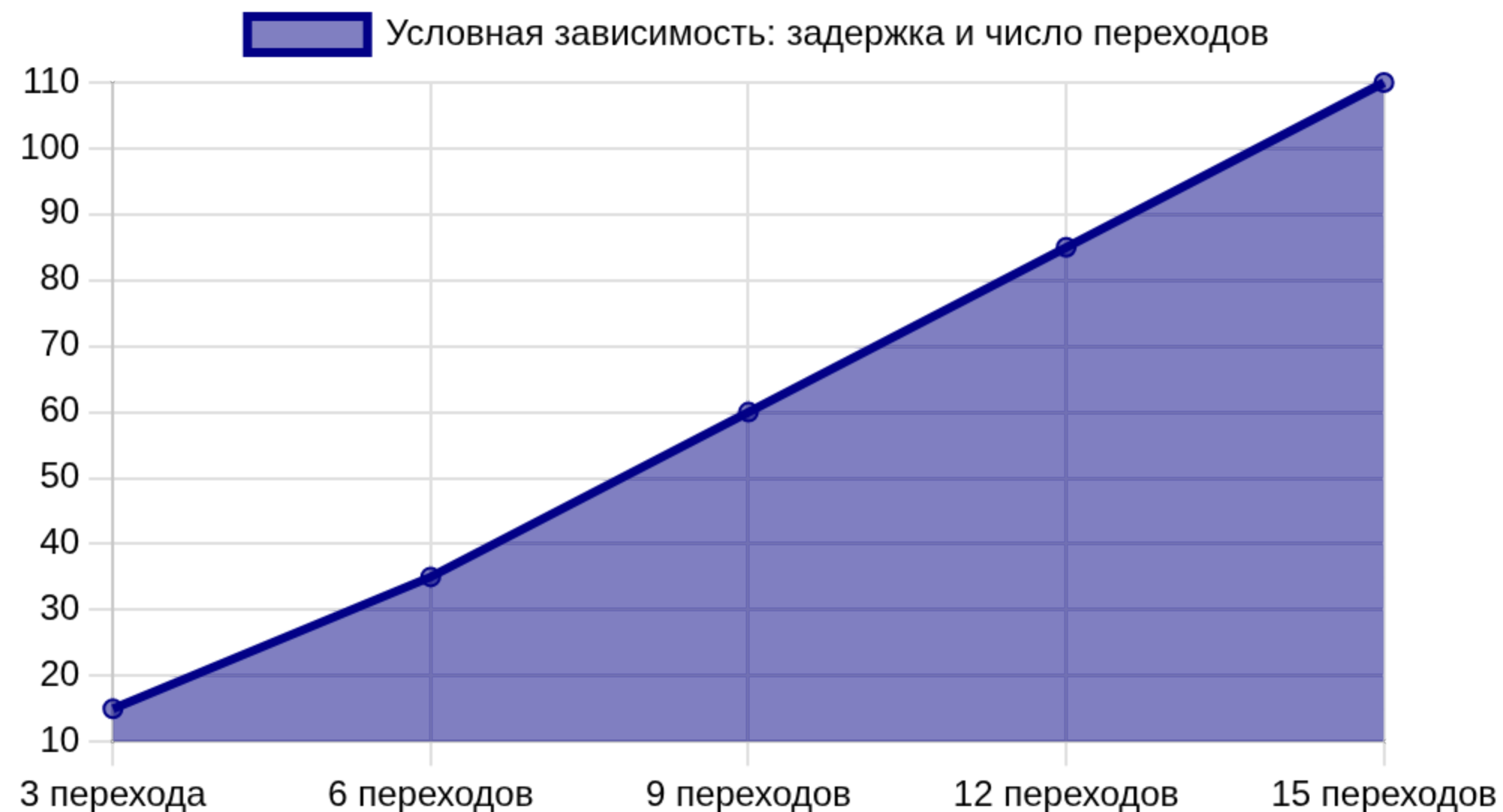
2

Региональные интернет-регистраторы, включая RIPE NCC, распределяют выделенные ресурсы среди провайдеров и организаций в своей зоне ответственности. Они также поддерживают процессы регистрации и помогают вести учёт назначений.

3

Регистраторы доменов оформляют делегирование имён, связывая доменные записи с инфраструктурой, которая обеспечивает их работу. В результате адреса и домены остаются согласованными во всём мире.

Маршрутизация: как пакет выбирает путь через сеть



Чем больше «следующих шагов» между отправителем и получателем, тем чаще растут суммарная задержка и число задействованных узлов. На практике это измеряется трассировкой маршрута.

Так как пакет ориентируется на next hop, путь формируется последовательно. Таблицы маршрутизации и протоколы внутри и между сетями определяют, куда передавать трафик дальше.

Принципиальные сведения о маршрутизации и next hop: общие практики маршрутизаторов, описания OSPF и BGP в документах IETF (точные эмпирические значения в диаграмме не привязаны к конкретному измерению).

Безопасность адресации и типичные сетевые риски

1

Подмена DNS-запросов может направить пользователя на поддельный ресурс. Тогда браузер получает «не тот» IP-адрес, и соединение устанавливается с мошенническим сервером вместо настоящего сайта.

2

Ошибки в настройке NAT или правил доступа иногда приводят к утечкам публичного IP и появлению лишних точек входа. В результате домашняя сеть становится уязвимее, даже если изначально задумывалась как закрытая.

3

В IPv6 сохраняются риски атак на механизмы автоматической конфигурации, включая фальшивые Router Advertisement. Дополнительно опасны ошибки маршрутизации и неправильная фильтрация трафика на границе сети.

4

Защита адресации — это не только про доступность. Она напрямую связана с конфиденциальностью пользователей и целостностью соединений: корректные настройки и контроль трафика снижают вероятность компрометации.

Примеры адресов в повседневных сценариях

Строка	Пример	Назначение
1	192.168.1.10	Локальный хост
2	8.8.8.8	Публичный DNS
3	127.0.0.1	Loopback
4	2001:db8::1	Учебный IPv6
5	www.example.ru	Доменное имя

Несколько часто встречающихся адресов помогают различать локальную работу, обращение к собственному компьютеру, внешние сервисы и доменные имена.

В одном сценарии могут сосуществовать разные «уровни» адресации: IP для доставки пакетов, доменные имена для удобства и специальные адреса для тестирования и локальной работы.

Общепринятые сетевые примеры и справочные материалы по адресации; диапазон 2001:db8::/32 используется для документации.

Что должен уметь пользователь для базовой диагностики сети



Различать IP, домен и порт

Учащийся должен уверенно отличать числовой адрес от имени и понимать роль порта как «точки входа» для конкретного приложения. Это упрощает поиск причины: что именно не работает — имя, узел или служба.



Понимать работу DNS и NAT

Важно знать, что DNS отвечает за перевод имени в адрес, а NAT связывает внутренние устройства с внешним миром. Тогда при сбоях проще сформулировать гипотезу: проблема в резолвинге или в выходе в Интернет.



Знать частные диапазоны IPv4 и распознавать IPv6

Частные диапазоны IPv4 помогают понять, что устройство не видно извне напрямую, а IPv6 имеет иной формат записей. Это снижает ошибки при диагностике и чтении настроек роутера и интерфейсов.



Использовать ping для проверки связности

Команда ping помогает быстро оценить, отвечает ли хост на сетевом уровне. Если имя уже известно, но соединение не устанавливается, ping позволяет отделить проблемы маршрута от проблем приложения или порта.



Применять nslookup и tracer для локализации

nslookup уточняет, как DNS возвращает адрес, а tracer показывает маршрут и где появляются задержки или обрывы. Вместе они помогают определить: сбой возникает на этапе имени, перехода между узлами или доставки пакетов.

Итоги: адресация как язык Интернета

Адресация объединяет устройства, сайты и службы через IP, доменные имена, DNS, порты и маршруты передачи данных. IPv4 остаётся базой, а IPv6 обеспечивает рост. Понимание этих принципов помогает безопасно настраивать сеть и находить неполадки.