

Сети

Модель OSI

Уровень	Назначение	Подробности и примеры
7. Прикладной	Взаимодействие с приложением	Это интерфейс между пользователем и сетью. Он предоставляет доступ к интернет-приложениям (браузеры, почта, FTP-клиенты). Протоколы: HTTP, SMTP, FTP, DNS.
6. Представления	Преобразование данных	Отвечает за кодирование, сжатие, шифрование данных. Например, преобразование текста в ASCII, использование SSL/TLS для шифрования.
5. Сеансовый	Управление сеансами	Устанавливает, управляет и завершает сеансы между двумя приложениями. Может управлять повторным подключением и синхронизацией. Протоколы: NetBIOS, RPC.
4. Транспортный	Обеспечение доставки данных	Разбивает данные на сегменты, управляет порядком доставки, повторной передачей при ошибках. TCP — надёжный, UDP — быстрый, без подтверждений.
3. Сетевой	Маршрутизация и логическая адресация	Определяет маршруты от источника к получателю через разные сети. Использует IP-адреса . Протоколы: IPv4, IPv6, ICMP (ping), BGP.
2. Канальный	Работа в пределах одной сети	Обеспечивает передачу кадров между устройствами в одной физической сети. Использует MAC-адреса и управляет доступом к среде. Протоколы: Ethernet, ARP, STP, VLAN.
1. Физический	Передача битов	Отвечает за физическую передачу данных: электрические сигналы, волны, кабели, коннекторы. Уровень «0 и 1».

Топ понятий


- **IP** — логический адрес устройства в сети.
имеет маску в IPv4 32 битная

- **MAC** — физический адрес сетевой карты. Уникален для каждого устройства.
Используется на канальном уровне
48 битная маска. Включает 6 октетов по 2 символа **шестнадцатеричной** системе счисления. Работает поверх UDP на порту 53
- **DNS** — переводит домены в IP (например, `google.com` → 8.8.8.8).
DNS имеет иерархию вида.
Root (.)
TLD (.com, .org, .ru)
Домен (example.com)
Субдомен (www.example.com)
то есть Root ничего не знает о example.com, он знает только о .com, .org, .ru
- **ARP** — протокол, с помощью которого компьютер узнаёт MAC-адрес устройства, зная его IP-адрес. Работает внутри локальной сети. Например, перед отправкой пакета по IP, нужен MAC-адрес получателя.
- **TCP** — надёжный протокол транспортного уровня. Обеспечивает установку соединения, доставку данных в правильном порядке без потерь, повторную отправку при ошибке. Используется для сайтов (HTTPS), email, FTP и др.
- **UDP** — «лёгкий» протокол транспортного уровня. Не устанавливает соединение, не гарантирует доставку. Применяется там, где важна скорость: видеозвонки, стриминг, DNS.
- **NAT/PAT** — механизм подмены внутренних (частных) IP-адресов на один внешний. Используется, чтобы несколько устройств в локальной сети могли выходить в Интернет с одного IP
Static NAT — 1:1.
Dynamic NAT — из пула.
PAT (Port Address Translation) — много внутренних IP → один внешний с разными портами (NAT Overload).
- **DHCP** — технология логического разделения одной физической сети на несколько виртуальных.
- **VLAN** — логическое разделение сети на уровне коммутатора.
- **STP** — протокол, предотвращающий петли в сетях с коммутаторами. Он блокирует избыточные соединения, создавая логическое дерево. Без него возможны «шторма» в сети.
- **OSPF** — протокол динамической маршрутизации внутри автономной системы.
- **BGP** — основной протокол маршрутизации между автономными системами в Интернете. Работает по политике, а не только по кратчайшему пути. Если BGP ошибается — может «упасть» пол-Интернета.
- **CDN** — сеть серверов, расположенных по всему миру, хранящих копии контента. Уменьшает задержку и ускоряет загрузку, отдавая данные с ближайшего сервера.

- **VPN** — шифрует трафик, делает туннель через интернет.
- **Firewall** — фильтрует входящий и исходящий трафик по заданным правилам. Может блокировать нежелательные подключения, управлять доступом, анализировать трафик.
- **Proxy** — промежуточное звено между клиентом и сервером. Может кэшировать запросы, скрывать реальный IP пользователя, ограничивать доступ.
- **SDN** — концепция управления сетью через централизованный контроллер. Устройства просто пересылают пакеты, вся логика маршрутизации и политики — в ПО.
- **ACL** — список правил на маршрутизаторе или коммутаторе, определяющий, какой трафик (по IP, порту, протоколу) разрешён или запрещён
- **Trunk** — специальный порт коммутатора, по которому одновременно «едут» теги нескольких VLAN, чтобы связать два коммутатора или коммутатор с маршрутизатором.
- **Interface** — сетевой интерфейс на устройстве (физический порт или виртуальный), через который проходит трафик.

Идём глубже

2. Чем отличается частный IP от публичного

- **Частные IP:**
 - 10.0.0.0/8
 - 172.16.0.0/12
 - 192.168.0.0/16 Не маршрутизируются в Интернете.
- **Публичные IP:** Всё остальное. Доступны извне.

3. Что такое шлюз по умолчанию

- Это IP-адрес маршрутизатора, через который идёт весь трафик **за пределы локальной сети**.
 - Если неправильно указан — Интернет не работает.
-

4. Как работает NAT и где ломается

- NAT меняет внутренний IP на внешний.
 - Ломает **входящие соединения**: без port forwarding — сервер внутри не виден извне.
 - Решения: **PAT**, **UPnP**, **STUN/TURN** для VoIP/игр.
-

5. Что такое MTU и фрагментация

- MTU = максимальный размер кадра (обычно 1500 байт).
 - Если пакет больше — **фрагментируется** (разбивается).
 - Некоторые протоколы могут отказываться от фрагментации (Don't Fragment flag) → **black hole** проблемки.
-

6. Типы маршрутизации

- **Статическая** — вручную прописанные маршруты.
 - **Динамическая** — с помощью протоколов (OSPF, RIP, BGP).
 - **По умолчанию (default route)** — маршрут 0.0.0.0/0, куда идёт весь неизвестный трафик.
-

8. Что делает DNSSEC и почему его почти никто не использует

- Подписывает DNS-записи — защищает от подделки.
- Но требует поддержки на всех уровнях цепочки.
- Поддерживается плохо, внедряется медленно.

9. Что происходит, когда ты вводишь адрес в браузере

1. Проверка DNS-кэша.
2. DNS-запрос (UDP/53).
3. Получение IP.
4. TCP-соединение с сервером (3-way handshake).
5. HTTPS: TLS-рукопожатие.
6. HTTP-запрос → ответ.
7. Отображение страницы.

10. Как работают CDN

- Это геораспределённые кэши контента.
- Тот же `youtube.com` в Москве и в Хабаровске — может быть разным по IP и отдаётся с ближайшего сервера.

11. QoS (Quality of Service)

- Механизмы приоритизации трафика: классификация, маркировка, очереди.
- **DSCP/ToS** — поля в IP-заголовке, задающие приоритет.
- **Traffic shaping / policing** — ограничение полосы.

12. SLA (Service Level Agreement)

договор между провайдером и клиентом, где прописаны параметры QoS.

Ещё определения

1. Цифровая модуляция

- Преобразование цифровых данных в сигнал для передачи по физическому каналу.
- Основные виды:
 - **ASK (амплитудная модуляция)** — изменяется амплитуда.
 - **FSK (частотная)** — частота.
 - **PSK (фазовая)** — фаза.
 - **QAM (комбинация амплитуды и фазы)** — используется в Wi-Fi и LTE.
- Применяется для повышения **скорости передачи** и устойчивости к шумам

2. Carrier Sense Multiple Access (CSMA)

- Метод управления доступом к среде (Ethernet, Wi-Fi).
- **"Carrier Sense"** — слушаем канал: если свободен, передаём.
- **"Multiple Access"** — много участников.
- Разновидности:
 - **CSMA/CD (с обнаружением коллизий)** — Ethernet.
 - **CSMA/CA (с избеганием коллизий)** — Wi-Fi.
- Если коллизия: в Ethernet — остановка передачи, в Wi-Fi — отложенная попытка.

3. Локальные, кампусные сети, городские сети, сети ISP


- **LAN (Local Area Network)** — внутри одного офиса/дома. Ethernet, Wi-Fi.
- **Кампусные сети** — объединяют несколько зданий. Например, университет или больничный комплекс.
- **MAN (Metropolitan Area Network)** — городская сеть. Часто соединяет кампусы или филиалы.
- **ISP-сети** — это сети операторов (Rostelecom, Beeline и т.п.). Поддерживают подключение абонентов, BGP, QoS, NAT и т.д.

 Иерархия:

LAN → Кампус → MAN → ISP → Tier-1 → Интернет.

4. Пиринговая интернет-экосистема как совокупность интернет-регионов

- Интернет — это **сеть из сетей** (Autonomous Systems).
- **Пиринговая экосистема** — когда провайдеры напрямую обмениваются трафиком **без посредников** (в т.ч. без оплаты).
- Делится на:
 - **Региональные интернет-регионы** — по географии.
 - **IXP (Internet Exchange Points)** — точки обмена трафиком между операторами.
- Экономически: дешевле передавать трафик напрямую, чем через «транзит».

 Пример: два российских провайдера обмениваются трафиком через MSK-IX, а не через Европу.

5. Regional Internet Registry (RIR), Автономные системы (AS)

RIR — региональные интернет-регистраторы:

- Выдают IP-адреса и **AS-номера**.
- В мире 5 RIR:

- **RIPE NCC** — Европа, Россия.
- **ARIN** — Северная Америка.
- **APNIC** — Азия и Тихий океан.
- **LACNIC** — Латинская Америка.
- **AFRINIC** — Африка.

Автономная система (AS):

- Группа IP-сетей под единым администрированием.
- У каждой есть **ASN (Autonomous System Number)**.
- Общаются с другими через **BGP**.

 Пример: Ростелеком — это AS, Мегафон — другая AS. У каждой свой ASN.

Основные сетевые протоколы — что делают, где работают

1. TCP (Transmission Control Protocol)

- **Уровень:** Транспортный (4)
- **Тип:** соединение-ориентированный
- **Особенности:** надёжная доставка, контроль порядка, подтверждение приёма, управление перегрузками.
- **Используется в:** HTTPS, FTP, SSH, почта.

2. UDP (User Datagram Protocol)

- **Уровень:** Транспортный (4)
- **Тип:** без установления соединения
- **Особенности:** минимальная задержка, без подтверждений, может терять пакеты.
- **Используется в:** DNS, VoIP, видеостриминг, онлайн-игры.

3. IP (Internet Protocol)

- **Уровень:** Сетевой (3)
- **Тип:** маршрутизация
- **Особенности:** доставка пакетов между сетями, без гарантии доставки.
- **Версии:** IPv4 (32-бит), IPv6 (128-бит).

4. ICMP (Internet Control Message Protocol)

- **Уровень:** Сетевой (3)
- **Тип:** вспомогательный

- **Особенности:** используется для ошибок, диагностики (ping, traceroute).
- **Пример:** «пакет не доставлен», «время превышено».

5. ARP (Address Resolution Protocol)

- **Уровень:** Канальный (2)
- **Тип:** разрешение адресов
- **Особенности:** определяет MAC-адрес по известному IP в пределах локальной сети.

6. HTTP (Hypertext Transfer Protocol)

- **Уровень:** Прикладной (7)
- **Особенности:** протокол обмена веб-страницами. Работает поверх TCP. Безопасная версия — HTTPS.

7. HTTPS (HTTP Secure)

- **Уровень:** Прикладной (7)
- **Особенности:** HTTP + шифрование TLS. Обеспечивает защиту данных между клиентом и сайтом.

8. DNS (Domain Name System)

- **Уровень:** Прикладной (7), работает поверх UDP/TCP
- **Особенности:** преобразует домены в IP-адреса. Один из ключевых протоколов Интернета.

9. DHCP (Dynamic Host Configuration Protocol)

- **Уровень:** Прикладной (7), поверх UDP
- **Особенности:** автоматически раздаёт IP-адреса и настройки (шлюз, DNS, маска).

10. FTP (File Transfer Protocol)

- **Уровень:** Прикладной (7)
- **Особенности:** передача файлов. Использует TCP и отдельные порты для команд и данных (21 и 20).

11. BGP (Border Gateway Protocol)

- **Уровень:** Сетевой (3)
- **Особенности:** маршрутизация между автономными системами. Позволяет Интернету существовать как системе сетей.

12. OSPF (Open Shortest Path First)

- **Уровень:** Сетевой (3)
- **Особенности:** внутренний протокол маршрутизации. Использует карту сети и алгоритм Дейкстры.

13. STP (Spanning Tree Protocol)

- **Уровень:** Канальный (2)
- **Особенности:** предотвращает петли в Ethernet-сетях. Создаёт логическое древовидное подключение.

14. TLS (Transport Layer Security)

- **Уровень:** Представления (6)
- **Особенности:** обеспечивает шифрование и аутентификацию. Основа HTTPS, SMTPS, FTPS.

Основные порты по умолчанию

Протокол	Порт	Тип	Назначение
SSH	22	TCP	Защищённый удалённый доступ к серверу (терминал)
Telnet	23	TCP	Удалённый доступ без шифрования (нежелательно использовать)
FTP	21	TCP	Передача файлов, управление сессией
FTPS / FTP-DATA	20	TCP	Поток данных FTP
SFTP	(через 22)	TCP	FTP по SSH (без отдельного порта)
TFTP	69	UDP	Простой, незащищённый FTP без авторизации
HTTP	80	TCP	Протокол передачи веб-страниц без шифрования
HTTPS	443	TCP	Защищённый HTTP (TLS/SSL)
DNS	53	TCP/UDP	Разрешение имён в IP (UDP — быстрый, TCP — для больших ответов/запросов)
DHCP (сервер)	67	UDP	Выдаёт IP-адреса клиентам
DHCP	68	UDP	Получает IP от сервера

Протокол	Порт	Тип	Назначение
(клиент)			