Абсолютная база:

IP (Internet Protocol) — маршрутизируемый протокол сетевого уровня стека TCP/IP. Это основной протокол интернета, по которому «общаются» и передают информацию разные устройства в сети.

TCP/IP — сетевая модель передачи данных, представленных в цифровом виде. Модель описывает способ передачи данных от источника информации к получателю. Включает в себя 4 уровня: прикладной (application), транспортный (transport), межсетевой (internet) и канальный (link). Протоколы этих уровней полностью реализуют функциональные возможности модели OSI.

MAC-адрес (Media Access Control) - уникальный идентификатор, который присваивается каждому устройству, подключённому к сети. В отличие от IP-адреса, который меняется в зависимости от сетевых настроек, MAC-адрес устройства всегда один и тот же, его задаёт производитель.

LAN (Local Area Network) — локальная сеть, объединяющая устройства в пределах одного здания или небольшой территории для общего доступа к ресурсам (файлам, принтерам, интернету).

OSI (Open Systems Interconnection) — модель из семи уровней, помогающая понимать, как данные проходят от пользователя к сети и обратно (физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной).

Модель					
Уровень (layer)		Тип данных (PDU)	Функции	Примеры	Оборудование
Host layers	7. Прикладной (application)	Данные	Доступ к сетевым службам	HTTP, FTP, POP3, SMTP, WebSocket	Хосты (клиенты сети), Межсетевой экран
	6. Представления (presentation)		Представление и шифрование данных	ASCII, EBCDIC, SSL, gzip	
	5. Сеансовый (session)		Управление сеансом связи	RPC, PAP, L2TP, gRPC	
	4. Транспортный (transport)	Сегменты (segment) / Датаграммы (datagram)	Прямая связь между конечными пунктами и надёжность	TCP, UDP, SCTP, Порты	
Media layers	3. Сетевой (network)	Пакеты (packet)	Определение маршрута и логическая адресация	IPv4, IPv6, IPsec, AppleTalk, ICMP	Маршрутизатор, Сетевой шлюз, Межсетевой экран
	2. Канальный (data link)	Биты (bit)/ Кадры (frame)	Физическая адресация	PPP, IEEE 802.22, Ethernet, DSL, ARP, сетевая карта.	Сетевой мост, Коммутатор, точка доступа
	1. Физический (physical)	Биты (bit)	Работа со средой передачи, сигналами и двоичными данными	USB, RJ («витая пара», коаксиальный, оптоволоконный), радиоканал	Концентратор, Повторитель (сетевое оборудование)

Subnetting (субсетирование) — разбивка большой сети на более мелкие подсети, чтобы проще управлять адресами и повысить безопасность.

DHCP (Dynamic Host Configuration Protocol) — протокол автоматической выдачи IP-адресов и других сетевых настроек (маска, шлюз, DNS) по запросу устройства.

DNS (Domain Name System) — «телефонная книга» интернета: переводит понятные человеку доменные имена (например, `example.com`) в IP-адреса серверов.

HTTP (HyperText Transfer Protocol) — протокол передачи веб-страниц: браузер запрашивает страницу у сервера, а сервер возвращает её в виде HTML, CSS, JavaScript и медиафайлов.

FTP (File Transfer Protocol) — протокол для загрузки и выгрузки файлов между клиентом и сервером; бывает в открытом (FTP) и защищённом (SFTP/FTPS) вариантах.

NAT (PAT) (Network Address Translation / Port Address Translation) — технология, когда один публичный IP-адрес «маскирует» множество приватных, подставляя порты, чтобы устройства внутри сети могли выходить в интернет под одним адресом. NAT сопоставляет одному внутреннему IP один внешний, а PAT позволяет выходить под одним IP, но в разных портах.

Сетевая практика и вводная маршрутизация

Статическая маршрутизация — когда администратор вручную прописывает в маршрутизаторе, куда отправлять пакеты для тех или иных сетей (не меняется автоматически).

VLAN (Virtual LAN) — виртуальная локальная сеть внутри одного физического коммутатора, позволяющая разделять трафик разных групп устройств без разных кабелей.

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.

SSH (Secure Shell) — защищённое шифрованное соединение для удалённого управления сетевыми устройствами и серверами.

ACL (Access Control List) — список правил на маршрутизаторе или коммутаторе, определяющий, какой трафик (по IP, порту, протоколу) разрешён или запрещён.

STP (Spanning Tree Protocol) — протокол предотвращения петель в Ethernet-сетях: автоматически отключает «лишние» каналы, чтобы трафик не зацикливался.

ISP (Internet Service Provider) — компания-провайдер, предоставляющая доступ в интернет, каналы связи и другие сетевые услуги пользователям и организациям.

Динамическая маршрутизация и VPN

OSPF (Open Shortest Path First) — протокол динамической маршрутизации, который автоматически обменивается информацией о доступных сетях между роутерами и

выбирает самый короткий путь.

VPN (Virtual Private Network) — технология создания «туннеля» поверх интернета для безопасного обмена данными между удалёнными сетями или пользователем и корпоративной сетью.

Теория по IPsec:
IPsec (Internet Protocol Security) работает на сетевом уровне (уровень 3) модели OSI (вау).

- **Основные компоненты**
  - **Security Association (SA)** — согласованный набор параметров (шифр, метод хэширования, ключи), по которым два узла защищённо общаются.
  - **IKE (Internet Key Exchange)** — протокол обмена и согласования ключей; обычно использует IKEv2, разбитый на две фазы:
    - Фаза 1: аутентификация сторон и создание защищённого канала (IKE SA).
    - Фаза 2: по защищённому каналу договариваются об SA для защищаемых туннелей (IPsec SA).
- **Протоколы защиты**
  - **AH (Authentication Header)** — обеспечивает целостность (Integrity) и аутентификацию пакетов, но не шифрует их.
  - **ESP (Encapsulating Security Payload)** — обеспечивает шифрование (Confidentiality), а также, опционально, аутентификацию и контроль целостности.
- **Режимы работы**
  - **Transport Mode** — шифруются и/или аутентифицируются только данные в IP-пакете; сам заголовок IP остаётся открытым. Используется для защиты «хост-к-хосту».
  - **Tunnel Mode** — весь исходный IP-пакет инкапсулируется внутрь нового пакета с новым IP-заголовком; идеально для «сеть-к-сети» VPN.
- **Как это работает на практике**
  - Гибкая настройка: можно выбрать разные алгоритмы шифрования (AES, 3DES) и хэширования (SHA-2, SHA-1).
  - Часто применяется в корпоративных VPN для безопасного соединения филиалов или внешних сотрудников.

Docker, виртуализация, балансировка

Основы Docker:

- **Контейнер vs Образ (Image)**
  - **Image** — готовый «слепок» файловой системы с приложением и всеми его зависимостями; похоже на шаблон.
  - **Container** — запущенный экземпляр образа, изолированный от хоста по пространствам имён (namespaces) и контрольным группам (cgroups).
- **Dockerfile и Registry**
  - **Dockerfile** — текстовый рецепт для сборки образа: указывается базовый образ, набор команд (`RUN`, `COPY`, `CMD` и др.) и метаданные.
  - **Docker Registry** — центральный репозиторий образов (Docker Hub или частный), откуда их можно «тянуть» (`docker pull`) и «толкать» (`docker push`).
- **Изоляция и ресурсы**
  - Контейнеры делят ядро хоста, но имеют свои сети, процессы и файловые системы (read-only слои плюс слой изменений).
  - Лёгкие (обычно сотни мегабайт) и быстрые в старте, по сравнению с полноценными виртуальными машинами.
- **Сетевые режимы и данные**
  - Поддерживаются разные драйверы сети (bridge, host, overlay) для связки контейнеров и хоста.
  - Для постоянного хранения данных используют **volumes** или **bind mounts**, чтобы изменения не терялись при пересоздании контейнера.

NAT vs Bridge — два режима сетевого подключения контейнеров:

- **NAT** — контейнер получает приватный IP и выходит в сеть под IP хоста через трансляцию;
- **Bridge** — контейнеры находятся в своей виртуальной сети с мостовым подключением к интерфейсу хоста.

VM vs Container — виртуальная машина эмулирует целый гостевой ОС с ядром, а контейнер разделяет ядро хоста и легче по ресурсам, но менее изолирован.

HAProxy — высокопроизводительный программный балансировщик нагрузки, распределяющий запросы между серверами по разным алгоритмам (round robin, least connections и т. д.).

- **Общая роль**
  - Высокопроизводительный прокси и балансировщик нагрузки уровня 4 (TCP) и уровня 7 (HTTP).
  - Используется для распределения входящих запросов между рабочими серверами, повышения отказоустойчивости и масштабирования.
- **Ключевые возможности**
  - **Алгоритмы балансировки**: round-robin, leastconn (наименее загруженные), source-hash (фиксация клиента на одном сервере) и другие.
  - **Проверки «здоровья» (health checks)**: регулярно опрашивает backend-сервера и автоматически исключает упавшие из пула.
- **Дополнительные фичи**
  - **SSL/TLS-терминация**: HAProxy может распаковывать HTTPS-трафик, разгружая этим веб-узлы.
  - **URL-routing**, переписывание заголовков и сессий («sticky sessions»).
  - **Масштабируемая архитектура**: легко интегрируется с облачными и контейнерными средами, поддерживает динамическую конфигурацию через API.
- **Пример использования**
  - На фронтенд ставят HAProxy, он принимает все запросы и распределяет их на несколько веб-серверов (например, Nginx), при этом следит за их состоянием и умеет плавно выводить и возвращать машины в пул без остановки сервисов.

HACluster (High-Availability Cluster) — группа серверов, настроенных так, чтобы при падении одного автоматически брал на себя его функции другой, обеспечивая непрерывную работу сервисов.