Модель OSI:

Физический уровень

Смысл: передача физических сигналов от источника получателю. Работаем с кабелями, каналами, кодированием 1 и 0, модуляцией сигнала и т.д.
Технологии: Ethernet (описывает, как сигналы кодируются и передаются), Bluetooth, WIFI, ИК-порт.
Устройства: хаб (концентратор) и репитер

Канальный уровень

Смысл: нам нужно раскодировать сигнал, убрать помехи и ошибки передачи. Фрейм (кадр) - хранит помимо основной информации адрес отправителя и получателя. Тут же появляются MAC-адреса - состоят из 48 бит, выглядят так: FF:FF:FF:FF:FF:FF, он идентифицирует адрес внутри сети.
Технологии: CDP, PPP, MPLS, ARP и др.
Устройства: коммутаторы и мосты

Сетевой уровень

Смысл: вводятся понятия маршрутизации и IP-адресов. Здесь уже информация передается не в фреймах, а в пакетах. Внутри пакета хранится еще один пакет с реальными IP-адресами. Переход между уровнями называется инкапсуляцией (вниз) и декапсуляцией (вверх).
Технологии: BGP, OSPF, RIP, EIGRP
Устройства: маршрутизатор

Транспортный уровень

Смысл: отвечает за передачу данных по сети. Если трафик чувствителен к потерям - TCP. Немного потеряем и не страшно - UDP.
Технологии: TCP и UDP (ВСЕ!)

Сеансовый уровень

Смысл: управляет соединениями (сессиями), он их разрывает. Это кодеки. RPC и gRPC

Уровень представления

Смысл: преобразование форматов сообщений. Это кодирование и сжатие (jpeg, gif). То есть нули и единицы преобразуются в картинку, например.

Уровень приложения

Смысл: службы, необходимые для работы с интернетом. Они нужны, чтобы приложения имели доступ к сетевым службам: файлам, пересылкам по почте и бд.

Технологии: telnet, LPD, TFTP, NFS, DNS, DHCP??????, SNMP, X window, HTTP/HTTPS, FPT, SMTP

BGP - Border Gateway Protocol

Это протокол граничного шлюза, предназначенный для обмена информацией о маршрутизации и доступности между автономными системами в интернете.
Есть внутренний - iBGP (internal, внутри системы) и внешний - eBGP (external. между АС).

EGP (Exterior Gateway Protocol) - протокол внешнего шлюза, простейший протокол с древовидной структурой, очень медленный (нужно проходить к корню и обратно).

Автономная система (AS) - это сеть, набор подсетей с общей политикой. У них свой протокол маршрутизации (OSPF или EIGRP). АС управляется провайдерами, вузами, корпорации. Каждая система имеет свой уникальный номер ASN (number) и диапазон ip адресов.

BGP обеспечивает обмен информацией между AS.

Как работает:

- BGP маршрутизатор устанавливает TCP сессию с соседом на 179 порт
- Сообщают свой номер АС, RouterID, hold timer (время сессии) и начинают общение
- Дальше отрабатывают как кластер, посылают сообщения keepalive
- Сообщения update: откуда и куда передать, какие адреса нужно добавить в сеть
- Анализирует всех соседей на нагрузку, сколько прыжков понадобится и оптимально отправляет сообщение следующему соседу

HTTP/HTTPS (hypertext transfer protocol)

Как мы переходим по URL: устанавливается TCP соединение по порту 80.

URL (Uniform Resouce Locator)

HTTP под капотом:

- Стартовая строка - URL и метод запроса (GET, POST, PUT, DELETE и др.), сервер - код (200)
- Заголовок - браузер, язык, логин/пароль
- Тело сообщения - данные

HTTPS - шифрует данные через SSL и TLS
SSL (Secure Socker Layer): Просит сертификат сайта, получает и проверяет его
TLS (Transport Layer Security): круче. Работает аналогично, но безопаснее

OSPF

Таблица маршрутизации описывает маршруты, необходимые для доставки пакет куда нужно.

Есть статическая и динамическая маршрутизация. При статической все происходит вручную, т.е. явно указываются интерфейсы, куда нужно отправить.

OSPF (open shortest path first) - протокол динамической маршрутизации, использующий для нахождения кратчайшего пути алгоритм Дейкстры. Он является протоколом внутридоменной маршрутизации (IGP). Другие протоколы IGP: RIP, EIGRP, IS-IS.

OSPF роутер начинает слать hello сообщения всем интерфейсам и ждет ответное приветствие, иначе признает его мертвым.

LSA (link-state advertisement) - сообщения с информацией о соседском роутере, состояние каждого подключенного канала и стоимость.

Полученные данные роутер хранит в LSDB (link-state db) и строит полную топологию, а затем выполняет алгоритм Дейкстры.

Чтобы такие LSA запросов не было так много, среди всех роутеров выделяются Выделенный маршрутизатор (designated router, dr) и запасной выделенный маршрутизатор (backup dr). Собственно, через них и происходит пересылка всем остальным. Они выбираются администратором.

DHCP (Dynamic Host Configuration Protocol)

На DHCP сервере задается доступный набор адресов (пул адресов). Также он выдает клиентам маску подсети, шлюз по умолчанию и может сообщить dns серверы.

Как работает:

- Комп отправляет запрос DHCPdiscover, адрес отправителя: 0.0.0.0, а получателя: 255.255.255.255 - широковещательный
- Роутер находит свободный ip и отправляет DHCPoffer. Но как он узнает, кому отправить? Он использует не IP, а MAC-адрес, которого достаточно по 2 уровню коммуникации модели OSI.
- Комп шлет DHCPrequest - забираю ip, и шлет его всем DHCP серверам
- Сервер в ответ шлет DHCPack - ок этот адрес твой, сопоставляет IP и MAC адрес

Для устройств, у которых не должен меняться IP, есть механизм статической резервации. IP-адрес закрепляется за устройством на постоянной основе

DNS (Domain Name System)

Как работает:

- Смотрит кэш. Если ты уже заходил на сайт, скорее всего он будет там. Это нужно, чтобы лишний раз не нагружать сеть.
- Если его нет, мы шлем запрос resolver (распознающий) DNS server. Обычно он у провайдера, но мы можем выбрать 8.8.8.8 (гугла) или 1.1.1.1
- Если находит - отправляет, иначе начинаем искать. Шлет запрос корневому dns серверу.

- Он скажет, к какому серверу нужно обратиться.
- Мы идем к серверу верхнего уровня (Top level domain, TLD) (.com, .ru, .org и т.д.)
- Далее спускаемся в сервер авторитарных имен. Если там ничего нет, значит такого домена не существует. Если есть, то он запишет ip-адрес и маршрут.

Типы запросов:

- recursive - ip-адрес сайта
- iterative - ip-адрес сайта или авторитативный DNS сервер
- inverse - какой домен у такого-то ip-адреса

TCP и UDP

Эти протоколы нужны для передачи данных между устройствами по сети.

TCP установка соединения:

- первое устройство отправляет sin-запрос - можно ли начать общение
- второе отправляет sin ack - давай начнем
- первый отправляет ack - ок погнали

В TCP соединении в ответ шлется подтверждение, что данные дошли успешно, давай дальше. Если не пришли - переспрашивает. Поэтому он довольно медленный.

В UDP не нужно устанавливать соединение. Лови файлы! Некоторые фрагменты данных могут потеряться, а упорядоченность данных не соблюдается. Зато скорость передачи данных более высокая.

IP-адрес

IPv4 имеет вид 192.168.0.0 - 32 бита
IPv6 имеет вид 2001:0db8:0000:0000:0000:ff00:0042:8329 - 128 бит

IP-адресов мало, но в интернет выходить нужно всем.
NAT (Network Address Translation, PAT - Port Address Translation) - много устройств могут выходить под одним и тем же адресом. Есть внутренний адрес (серый) и внешний адрес (белый) под которым устройства выйдут в интернет. К адресу добавляется порт, по которому и отличают адреса.

MAC-адрес

MAC (Media Access Control) - представляет собой уникальный адрес из 48 бит FF:FF:FF:FF:FF:FF, который присваивается еще на производстве.
Первые 6 цифр - производитель сетевой карты (OUI organization unique identifier)
Последние 6 цифр - NIC (network interface controller) уникальные

Если IP определяет местоположение (куда), то MAC идентифицирует само устройство (кому).

Docker

Мы запихиваем в контейнер все необходимые вещи: ос, библиотеки, зависимости и т.д.
В этом случае нам не нужен гипервизор и гостевые ОС (мы используем конфиг и зависимости), что сильно облегчает запуск такого контейнера на любом устройстве. Мы используем ядро только нашей системы с помощью Docker Engine.

Docker имеет 3 основных компонента:

- Докер файл - из него собирается образ. Набор инструкций, как создать образ и что там должно быть
- Образ - из него запускается контейнер. Готовое приложение: библиотеки и зависимости
- Контейнер - запущенный экземпляр образа

Docker Compose упрощает развертывание сервиса с несколькими контейнерами с помощью YAML файла, в котором прописываются сервисы, которые нужно запустить, и их настройки.

Kubernetes нужен для мониторинга контейнеров и работой с ними. Он проверяет, что все отрабатывает корректно.

Разница между IP и MAC-адресами

MAC-адреса используются преимущественно в свитчах (то есть на L2 уровне). Они анализируют порты и мак адреса, и создают таблицу коммутации. Он используется только в рамках одной локальной сети

IP это уже не физический, а логический адрес. Используется уже не для коммутации, а для маршрутизации, то есть па L3 уровне.

ARP - Address Resolution Protocol - связывает IP и MAC адреса

Маска подсети

Показывает, какая часть IP-адреса относится к сети, а какая к устройству (хосту).

Private IPs	Mask	Gateway	Hosts	Broadcast	Class
10.0.0.0	255.0.0.0	10.0.0.1	16,777,214	10.255.255.255	A
172.16.0.0	255.240.0.0	172.168.0.1	524,286	172.31.255.255	B
192.168.0.0	255.255.0.0	192.168.0.1	65,534	192.168.255.255	C

Notation	Mask	Addresses	Hosts		
Slash 12	255.240.0.0	1,048,576	1,048,574		
Slash 13	255.248.0.0	524,288	524,286		
Slash 14	255.252.0.0	262,144	262,142		
Slash 15	255.254.0.0	131,072	131,070		
Slash 16	255.255.0.0	65,536	65,534		
Slash 17	255.255.128.0	32,768	32,766		
Slash 18	255.255.192.0	16,384	16,382		
Slash 19	255.255.224.0	8,192	8,190		
Slash 20	255.255.240.0	4,096	4,094		
Slash 21	255.255.248.0	2,048	2,046		
Slash 22	255.255.252.0	1,024	1,022		
Slash 23	255.255.254.0	512	510		
Slash 24	255.255.255.0	256	254		
Slash 25	255.255.255.128	128	126		
Slash 26	255.255.255.192	64	62		
Slash 27	255.255.255.224	32	30		
Slash 28	255.255.255.240	16	14		
Slash 29	255.255.255.248	8	6		
Slash 30	255.255.255.252	4	2		
Slash 31	255.255.255.254	2	0		

Как устроена маска: в двоичном виде если стоит 1 - значит принадлежит сети, если 0 - принадлежит хосту
Использовать мы можем на 2 меньше: 0 (первый) - адрес самой сети, а 255 (последний) - широковещательный.

Если сети совпадают - отправляет напрямую, иначе - отправляет маршрутизатору.

Пакет данных

Структура пакета

Инкапсуляция пакетов