# Типы адресов стека TCP/IP. Локальные адреса. Сетевые IP-адреса. Доменные имена.

# Компьютерная сеть

Компьютерная сеть — это множество вычислительных устройств, взаимодействующих между собой и совместно использующих ресурсы. Понятие сеть близко по смыслу к понятию графа. Сеть также состоит из множества узлов (nodes) и множества звеньев (links). Узлы — это вычислительные устройства, а звенья представляют связи этих устройств

# Локальные и глобальные компьютерные сети

В зависимости от охвата территории компьютерные сети бывают:

- Персональные — Personal Area Network (PAN).
- Локальные — Local Area Network (LAN).
- Городские — Metropolitan Area Network (MAN).
- Глобальные — Wide Area Network (WAN).

# Локальные и глобальные компьютерные сети

Различные датчики, подключённые к смартфону, образуют сеть PAN. Компьютерная сеть из устройств, подключённых к вашему домашнему роутеру, является LAN-сетью, сеть из абонентов провайдера в городе — это MAN-сеть, а весь интернет, который вам предоставляет провайдер — WAN-сеть.

# Базовые понятия из модели TCP/IP:

- хост (host);
- сообщение;
- IP-датаграмма;
- пакет;
- фрейм;
- IP-адрес;
- MAC-адрес;
- TCP-сегмент;
- UDP-датаграмма;
- MTU.

# Как работает сеть

IP-сеть представляет собой множество связанных между собой хостов. Хосты связаны непосредственно или косвенно при помощи ретранслирующих устройств (маршрутизаторов и коммутаторов).

# Как работает сеть

Для приёма сообщений из сети и отправку их в сеть хост использует интерфейсы. Физический интерфейс отправляет и принимает фреймы, а логический интерфейс отправляет и принимает IP-пакеты. Физический интерфейс идентифицируется MAC-адресом, логический интерфейс — IP-адресом.

# Как работает сеть

Передаваемое сообщение представляет собой UDP-датаграмму или TCP-сегмент. Сообщение содержит заголовок и полезные данные. Чтобы передать сообщение внутри IP-сети оно помещается в IP-датаграмму. Конкретный физический интерфейс позволяет передавать данные порциями, которые имеют определённый максимально допустимый размер (MTU). Если размер IP-датаграммы превышает MTU, выполняется её фрагментация и создаётся несколько IP-пакетов, иначе создаётся только один IP-пакет для всей IP-датаграммы.

# Как работает сеть

Передаваемое сообщение представляет собой UDP-датаграмму или TCP-сегмент. Сообщение содержит заголовок и полезные данные. Чтобы передать сообщение внутри IP-сети оно помещается в IP-датаграмму. Конкретный физический интерфейс позволяет передавать данные порциями, которые имеют определённый максимально допустимый размер (MTU). Если размер IP-датаграммы превышает MTU, выполняется её фрагментация и создаётся несколько IP-пакетов, иначе создаётся только один IP-пакет для всей IP-датаграммы.

# 1. Сообщение: UDP-датаграмма или TCP-сегмент

- UDP-датаграмма — это блок данных протокола UDP (ненадёжный, без установки соединения).
- TCP-сегмент — блок данных протокола TCP (надёжный, с установкой соединения).

Оба содержат:

- Заголовок (информация для доставки: порты, контрольные суммы, флаги).
- Полезные данные (например, часть файла )

# 2. Инкапсуляция в IP-датаграмму

**Чтобы передать UDP/TCP-сообщение по сети, оно помещается в IP-датаграмму.**

# 3. Ограничение MTU и фрагментация

MTU (Maximum Transmission Unit) — максимальный размер кадра, который может передать физический интерфейс. Например, Ethernet обычно имеет MTU = 1500 байт.

# 3. Ограничение MTU и фрагментация

Если размер IP-датаграммы > MTU, она разбивается на несколько IP-пакетов.

Каждый фрагмент получает:

Свой IP-заголовок (с пометкой, что это часть большой датаграммы).

Смещение (Fragment Offset) — позиция в исходных данных.

Флаг MF (More Fragments), указывающий, есть ли ещё фрагменты.

# 3. Ограничение MTU и фрагментация

Пример для MTU = 1500 байт:

Исходная IP-датаграмма: 4000 байт (заголовок 20 + данные 3980).

Фрагментация:

- Пакет 1: 20 (IP) + 1480 (данные), offset = 0, MF = 1.
- Пакет 2: 20 (IP) + 1480 (данные), offset = 1480, MF = 1.
- Пакет 3: 20 (IP) + 1020 (данные), offset = 2960, MF = 0.

# 4. Сборка фрагментов

Получатель собирает фрагменты в исходную датаграмму по:

- Идентификатору (ID) в IP-заголовке.
- Смещению (Offset) и флагу MF.

Если какой-то фрагмент потерян, вся датаграмма считается недействительной (в TCP будет повторная передача, в UDP данные потеряются).

# Как работает сеть

IP-пакет в соответствии с таблицей маршрутизации хоста передаётся на выбранный логический интерфейс.

# 1. Таблица маршрутизации хоста

Это структура данных в операционной системе, которая хранит правила пересылки пакетов. Она отвечает на вопрос:

"Куда отправить пакет с определённым IP-адресом назначения?"

Просмотр таблицы маршрутизации с помощью route

# 2. Как работает выбор интерфейса?

**Алгоритм принятия решения:**

**1. Сравнение адреса назначения в IP-пакете с записями в таблице маршрутизации.**

- **Например, для Destination IP = 8.8.8.8 система ищет наиболее специфичный маршрут.**

# 2. Как работает выбор интерфейса?

2. Выбор маршрута:

- Если получатель в локальной сети (например, 192.168.1.5), пакет отправляется напрямую через указанный интерфейс
- Если получатель в другой сети (например, 8.8.8.8), пакет отправляется на шлюз

# 2. Как работает выбор интерфейса?

3. Передача на интерфейс:

- Пакет передаётся драйверу сетевого интерфейса (например, Ethernet-карты или Wi-Fi-адаптера).
- Далее он преобразуется в кадр канального уровня (например, Ethernet-фрейм с MAC-адресами).

# Как работает сеть

Логический интерфейс сам непосредственно не может передать IP-пакет, он использует физический интерфейс. Физический интерфейс передаёт данные фреймами. Фрейм имеет заголовок и полезные данные (payload). В заголовке фрейма указывается MAC-адрес получателя, MAC-адрес отправителя и какому протоколу принадлежат данные в payload (Ethertype). Адрес отправителя известен, это MAC-адрес интерфейса отправляющего хоста. Для протокола IPv4 Ethertype=0x0800.

# 1. Физический интерфейс

Физический интерфейс (например, Ethernet-порт, Wi-Fi чип) — это "железо", которое:

- Преобразует данные в электрические/радиосигналы.
- Передаёт информацию фреймами (кадрами) по проводам или воздуху.

# 2. Что такое фрейм?

Фрейм — это "конверт" для передачи данных на канальном уровне (L2). Его структура:

| MAC-адрес получателя | MAC-адрес отправителя | EtherType | Полезные данные | CRC |

# 3. Ключевые поля фрейма

## 3.1. MAC-адреса

MAC отправителя — известен (адрес вашей сетевой карты, например, 00:1A:2B:3C:4D:5E).

MAC получателя:

- Если получатель в локальной сети — его реальный MAC.
- Если получатель в другой сети — MAC шлюза (роутера).

Как узнать MAC получателя?

Через ARP-протокол (для IPv4) или NDP (для IPv6).

# 3. Ключевые поля фрейма

## 3.2. EtherType

Это число, указывающее, какой протокол лежит в payload. Примеры:

- 0x0800 — IPv4.
- 0x86DD — IPv6.
- 0x0806 — ARP.

# Как работает сеть

Передаваемое сообщение представляет собой UDP-датаграмму или TCP-сегмент. Сообщение содержит заголовок и полезные данные. Чтобы передать сообщение внутри IP-сети оно помещается в IP-датаграмму. Конкретный физический интерфейс позволяет передавать данные порциями, которые имеют определённый максимально допустимый размер (MTU). Если размер IP-датаграммы превышает MTU, выполняется её фрагментация и создаётся несколько IP-пакетов, иначе создаётся только один IP-пакет для всей IP-датаграммы.

# Как работает сеть

IP-пакет в соответствии с таблицей маршрутизации хоста передаётся на выбранный логический интерфейс.

# Как работает сеть

Логический интерфейс сам непосредственно не может передать IP-пакет, он использует физический интерфейс. Физический интерфейс передаёт данные фреймами. Фрейм имеет заголовок и полезные данные (payload). В заголовке фрейма указывается MAC-адрес получателя, MAC-адрес отправителя и какому протоколу принадлежат данные в payload (Ethertype). Адрес отправителя известен, это MAC-адрес интерфейса отправляющего хоста. Для протокола IPv4 Ethertype=0x0800.

# Локальные адреса (MAC-адреса)

Локальные адреса (MAC-адреса) — уникальные идентификаторы сетевых интерфейсов на канальном уровне (L2) модели OSI.

# Локальные адреса (MAC-адреса)

Формат MAC-адреса

Состоит из 6 байт (48 бит), записывается в шестнадцатеричном формате:

```
00:1A:2B:3C:4D:5E
```

- Первые 3 байта — идентификатор производителя.
- Последние 3 байта — уникальный номер устройства.

# Сетевые IP-адреса

IP-адреса (IPv4/IPv6) — числовые идентификаторы устройств на сетевом уровне (L3), используемые для маршрутизации в интернете.

# Сетевые IP-адреса

Типы IP-адресов

3.2.1. IPv4

32 бита, записывается в виде 4 октетов:

```
192.168.1.1
```

IPv6

128 бит, записывается в hex:

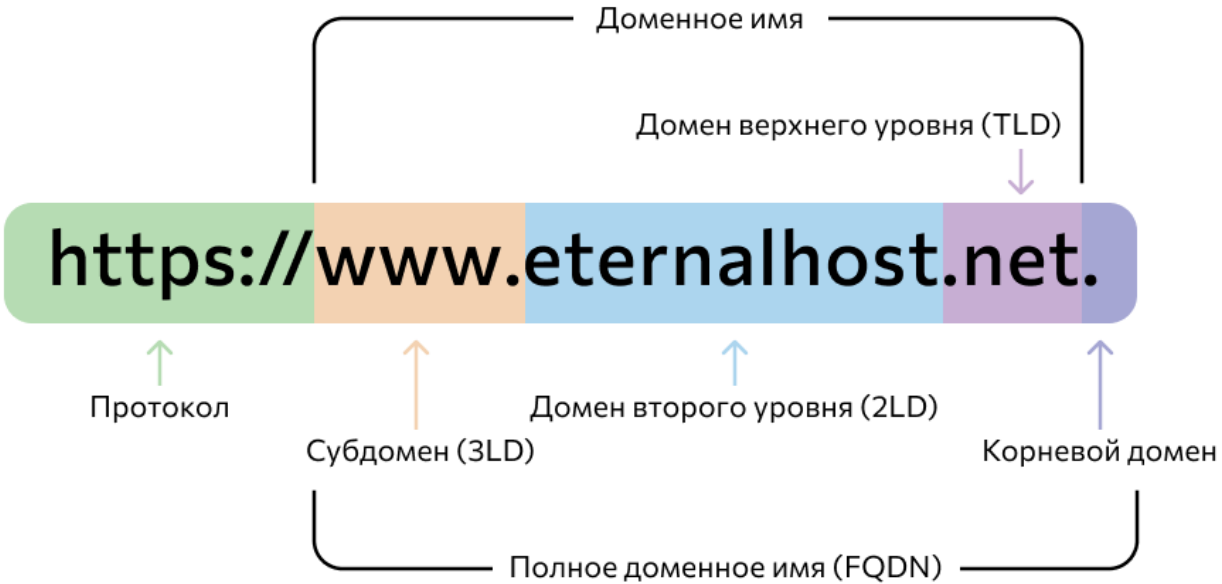
```
2001:0db8:85a3:0000:0000:8a2e:0370:7334
```

# Доменные имена (DNS)

Доменное имя — символьный адрес (например, google.com), преобразуемый в IP через DNS (Domain Name System).

# Доменные имена (DNS)

## Структура доменного имени



# Доменные имена (DNS)

1) Браузер запрашивает у локального DNS-сервера IP для example.com.
2) Если сервер не знает, он обращается к корневым серверам → TLD-серверам (.com) → авторитативным серверам домена.
3) IP-адрес возвращается клиенту.

# Доменные имена (DNS)

Важность DNS

- Упрощает запоминание адресов.
- Позволяет менять IP без смены домена.