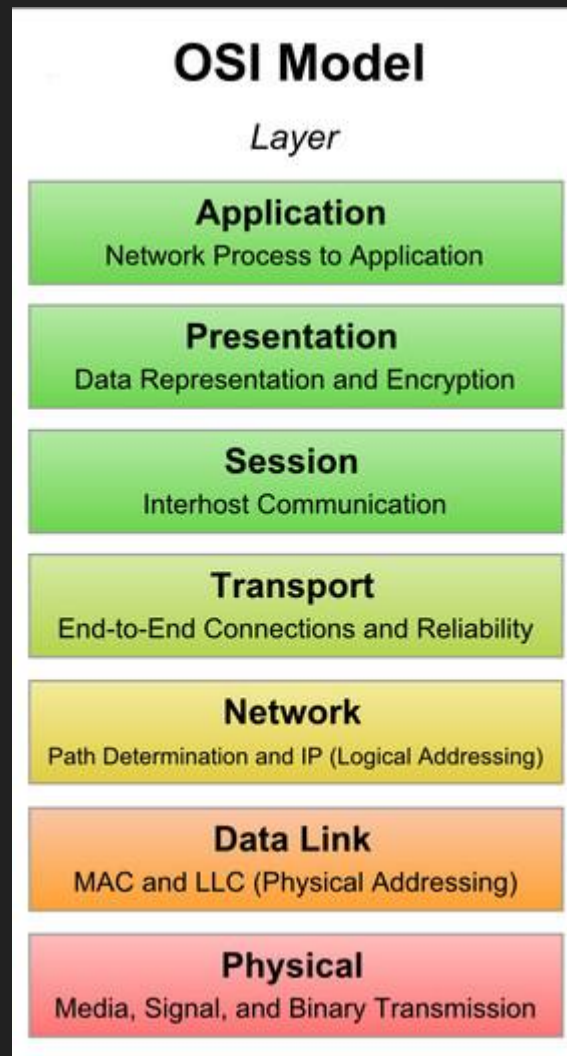


TCP UDP TSL HTTP WEBSOCKET WHATNOT

SUPER-DIMA & MEGA-NIKISH
PREDSTAVLYAYUT

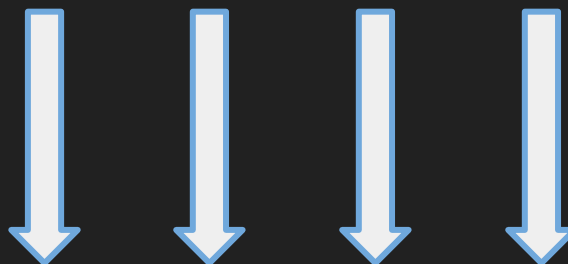
Что такое UDP и TCP?

Протоколы транспортного уровня:
предназначены для доставки
данных, не важно куда и как.



UDP - это просто

- Порт источника
- Порт получателя
- Длина пакета
- Контрольная сумма



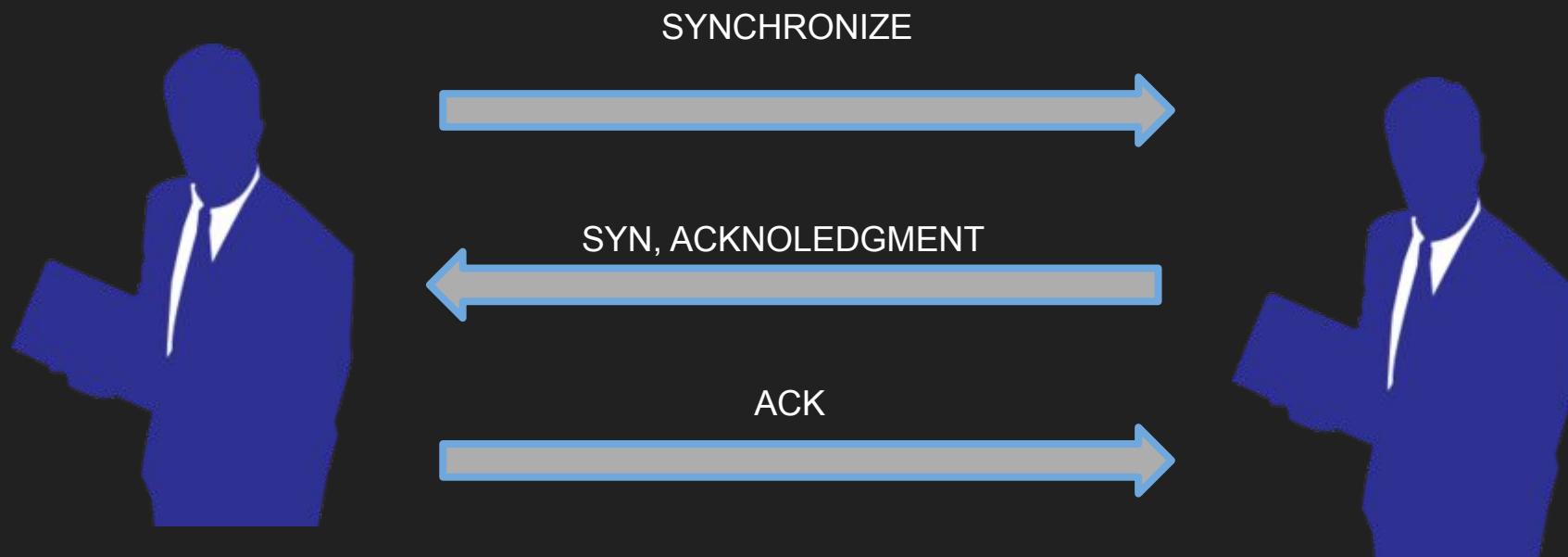
```
UDP HEADER: 8e 0b fc e2 00 16 84 37 .....7
DATA:      48 49 54 4c 45 52 20 57 HITLER W
           41 53 20 41 20 47 4f 4f AS A G00
           44 20 47 55 59 D GUY
```

ТСР: заголовок

- Порт источника, порт получателя
- Sequence number
- Acknowledgement number
- Дина заголовка, резерв, флаги
- Размер буфера
- Контрольная сумма
- Смещение конца важных данных
- Опции

Итого: более чем 16 байт

ТСР: установка соединения



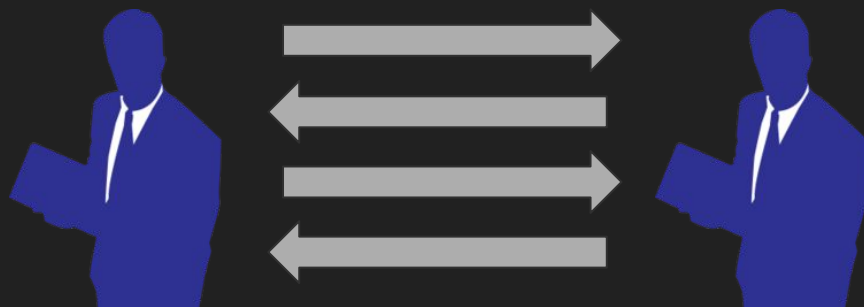
TCP: передача данных

На каждую переданную порцию данных приходит пакет подтверждения доставки.

Sequence number хранит номер байта начала передаваемых данных.

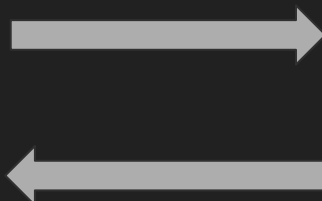
Acknowledgement number хранит номер байта конца принимаемых данных.

Аск-флаг всегда выставлен.



HTTP: что же это?

Протокол передачи гипертекста.



HTTP: запрос

Стартовая строка - метод, адрес, версия протокола

Заголовки - самые разные параметры

Данные (отделены пустой строкой)

```
GET /path/to/file.html HTTP/2.0  
User-Agent: Opera/12.17-Presto  
Location: Good_Old_Times  
|
```


HTTP: методы

GET - получить данные

HEAD - получить заголовок

POST - отправить информацию

PUT, PATCH, DELETE, TRACE, CONNECT...

HTTP: ответ

Стартовая строка: версия протокола, код состояния

Заголовки

Тело (отделено пустой строкой)

```
HTTP/2.0 200 OK
Server: Apache
Content-Language: ru

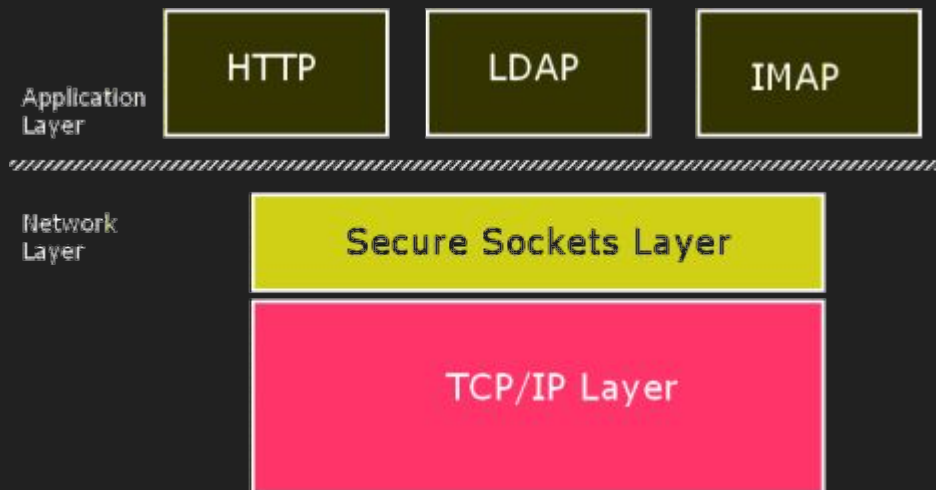
i am a sample file
```

Что такое SSL?

SSL (*Secure Sockets Layer*) – криптографический протокол, который нужен для установления безопасного (т.е. зашифрованного) соединения между клиентом и сервером.

SSL использует как асимметричную, так и симметричную криптографию.

Работает как прозрачный для пользователя wrapper вокруг соединения.



Установка соединения



Установление соединения на примере SMTP

S: <waits for connection on TCP port 25>
C: <opens connection>
S: 220 mail.example.org ESMTP service ready
C: EHLO client.example.org
S: 250-mail.example.org offers a warm hug of welcome
S: 250 STARTTLS
C: STARTTLS
S: 220 Go ahead
C: <starts TLS negotiation>
C & S: <negotiate a TLS session>
C & S: <check result of negotiation>
C: EHLO client.example.org
...

- GeoTrust Global CA
- Google Internet Authority G2
- google.com**



google.com

Выдан: Google Internet Authority G2
Истекает: четверг, 30 июня 2016 г., 14:20:00 Новосибирск, стандартное время

Сертификат действителен

▼ Подробнее

Тема	
Страна	US
Страна/Территория	California
Где	Mountain View
Организация	Google Inc
Общее имя	google.com
Кем выдан	
Страна	US
Организация	Google Inc
Общее имя	Google Internet Authority G2

OK

- Valid Certificate
The connection to this site is using a valid, trusted server certificate.
[View certificate](#)
- Secure TLS connection
The connection to this site is using a strong protocol version and cipher suite.

Что такое WebSocket?

WebSocket — протокол полнодуплексной связи поверх TCP-соединения, предназначенный для обмена сообщениями между браузером и веб-сервером в режиме реального времени.

Как происходит соединение?

Все начинается так же как в обычном HTTP-запросе. Браузер подключается по протоколу TCP на 80 порт сервера и дает немного необычный GET-запрос:

GET /demo HTTP/1.1

Upgrade: WebSocket

Connection: Upgrade

Host: site.com

Origin: http://site.com

Как происходит соединение?

Если сервер поддерживает ВебСокеты, то он отвечает таким образом:

HTTP/1.1 101 Web Socket Protocol Handshake

Upgrade: WebSocket

Connection: Upgrade

WebSocket-Origin: http://site.com

WebSocket-Location: ws://site.com/demo

Как происходит соединение?

Если браузер это устраивает, то он просто оставляет *TCP-соединение открытым*. Все — «рукопожатие» совершено, канал обмена данными готов.

Как только одна сторона хочет передать другой какую-то информацию, она отправляет дата-фрейм следующего вида:

0x00, <строка в кодировке UTF-8>, 0xFF

Как происходит соединение?

