Все сайты фактически находятся на отдельном устройстве. Эти устройства имеют отдельный номер IP (уникальный числовой идентификатор устройства в компьютерной сети). Благодаря этому номер можно найти источник ресурса (сервер/компьютер). Получается IP это телефонный номер, а DNS это телефонная книга где мы можем найти IP. Но техническое определение у DNS такое - система доменных имен, которая обеспечивает связь между именем сайта и его цифровым номером.

А если точнее, то когда человек вводит адрес сайта, то DNS конвертирует его в IP-адрес и передаёт на компьютер который поддерживает сайт. Он обрабатывает информацию и передаёт ей обратно для открытия сайта.

**HTTP** — это протокол передачи данных, изначально предназначенный для передачи гипертекстовых документов (то есть документов, которые могут содержать ссылки, позволяющие организовать переход к другим документам). Аббревиатура HTTP расшифровывается как HyperText Transfer Protocol, «протокол передачи гипертекста». Задача, которая традиционно решается с помощью протокола HTTP — обмен данными между пользовательским приложением, осуществляющим доступ к веб-ресурсам (обычно это веб-браузер) и веб-сервером.

У HTTP есть основных протокола 1.1 и 2.0. HTTP 1.1 это протокол который обеспечивает обмен информацией между клиентским компьютером и локальным или удаленным веб-сервером. В этом процессе клиент отправляет текстовый запрос на сервер, вызывая метод (GET или POST). В ответ сервер отправляет клиенту ресурс, например, HTML-страницу. HTTP 2.0 появился как протокол SPDY, разработанный в основном в Google с целью снижения задержки загрузки веб-страниц такими методами, как сжатие, мультиплексирование **(уплотнение канала связи, то есть передача нескольких потоков данных с меньшей скоростью по одному каналу связи)** и приоритизация **(распределение данных по очередям)**. То есть основная цель это уменьшить задержки при загрузке веб-страниц, а также обеспечить дополнительную безопасность. В отличие от HTTP/1.1, в котором все запросы и ответы хранятся в простом текстовом формате, HTTP/2 использует двоичный уровень кадрирования для объединения всех сообщений в двоичном формате, при этом сохраняя основу HTTP.

Но чтобы решить проблему безопасности передачи данных был изобретён **HTTP Secure (HTTPS)**, позволяющий клиенту и серверу устанавливать зашифрованный канал связи, а затем передавать сообщения чистым текстом по этому каналу, эффективно защищая их от прослушивания. Существует несколько типов сертификатов HTTPS. Их можно классифицировать по следующим критериям:

- Подтверждённый домен (DV) - подтверждает, что домен соответствует определённому публичному ключу;

- Расширенное подтверждение (EV) - подтверждает юридическое лицо, которому принадлежит веб-сайт.

- Подтверждённая организация (OV) - подтверждает юридическое лицо, которому принадлежит веб-сайт. Но в отличие от EV, сертификаты OV HTTPS не отображают название подтверждённого юридического лица в пользовательском интерфейсе.