DNS это система, которая сопоставляет текстовые адреса сайтов с IP адресами серверов, на которых эти сайты находятся физически.

Система доменных имен действует посредством DNS-сервера, который нужен для выполнения двух основных функций:

* хранения данных о соответствии имени домена конкретному IP-адресу,
* кэширования ресурсных записей прочих DNS-серверов.

Буквы HTTP в начале адресной строки означают, что клиент и сервер обмениваются данными по прикладному протоколу – hypertext transfer protocol. Это стандартный протокол для обмена любыми данными в Интернете. Внешне аббревиатура HTTP ничем не выделяется – она такого же черного цвета, что и остальная часть адресной строки.

Если в адресной строке вместо черной надписи HTTPS появилась зеленая HTTPS, значит, данные передаются по тому же HTTP протоколу, но с дополнительной надстройкой, обеспечивающей криптографическую защиту (отсюда и буква «s», означающая «security», т.е. безопасность). Передаваемые данные шифруются с помощью протокола SSL, который невозможно расшифровать без ключа. Узнать защищенное соединение просто – помимо зеленого цвета букв, в адресной строке появляется изображение закрытого замка и надпись: «Надежный».

Стандартный протокол HTTP передаёт данные в открытом виде. Злоумышленники могут “вклиниться” в передачу — изменить или перехватить данные. В HTTPS для передачи данных создаётся защищённый канал. Вот как это происходит:

Вася хочет перейти на сайт некийсайтSSL, защищённый SSL-сертификатом:

→ Васин браузер посылает запрос к сайту

→ сайт отправляет в ответ копию сертификата

→ браузер проверяет подлинность сертификата – узнаёт у центра сертификации, который его выдал

→ если сертификат не поддельный, сайт и браузер договариваются о секретном ключе. С помощью этого ключа Васин браузер и сайт устанавливают защищённое HTTPS-соединение.

SSL расшифровывается как «уровень защищённых сокетов» или secure sockets layer. Это список определённых правил, которые позволяют более безопасно использовать связь. Для этого с помощью особых алгоритмов применяют шифровальное преобразование.

Существует несколько версий протоколов HTTP. Самая ранняя версия протокола -это HTTP-0.9.Впервые была опубликована в 1992 году. Спецификация протокола привела к упорядочению правил взаимодействия между клиентами и серверами HTTP, а также разделению функций между этими двумя компонентами.

Следующая версия была выпущена в 1996 году -это HTTP-1.Более современная его версия — HTTP/1.1 — появилась в 1999 году.

Этот протокол научился поддерживать режим постоянного соединения, то есть оставлять соединение открытым после того, как получен ответ на запрос. Это позволило за одно соединение посылать сразу несколько запросов, а не открывать сессию каждый раз.

В 2015 году вышла новая версия – протокол HTTP-2. В отличии от предыдущего протокола он бинарный, то есть использует двоичный уровень кадрирования. Двоичный уровень кадрирования организует сообщения в параллельные потоки данных, что позволяет существенно ускорить загрузку сайта.

Основные его особенности:

1. Расстановка и управление приоритетами запросов/потоков — клиент самостоятельно задает для сервера приоритетность ресурсов и данных;
2. Сжатие HTTP заголовков;
3. Параллельная загрузка по TCP-соединению нескольких элементов сайта, то есть через одно соединение отправляется несколько запросов.
4. Наличие и поддержка со стороны сервера проактивных push-уведомлений — сервер самостоятельно может отправлять данные для клиента, которые тот еще не запросил.