Networks

application

На прикладном уровне (Application layer) работает большинство сетевых приложений. Эти программы имеют свои собственные протоколы обмена информацией, например, HTTP для WWW, FTP (передача файлов), SMTP (электронная почта), SSH (безопасное соединение с удалённой машиной), DNS (преобразование символьных имён в IP-адреса) и многие другие.

http

Протокол передачи данных для передачи гипертекстовых документов. Актуальная версия протокола, HTTP 1.1, описана в спецификации RFC 2616.
Протокол HTTP предполагает использование клиент-серверной структуры передачи данных. Клиентское приложение формирует запрос и отправляет его на сервер, после чего серверное программное обеспечение обрабатывает данный запрос, формирует ответ и передаёт его обратно клиенту.
Задача, которая традиционно решается с помощью протокола HTTP — обмен данными между пользовательским приложением и веб-сервером.
Также HTTP часто используется как протокол передачи информации для других протоколов прикладного уровня.
API многих программных продуктов также подразумевает использование HTTP для передачи данных — сами данные при этом могут иметь любой формат.

https

Расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов TLS или устаревшего в 2015 году SSL. В отличие от HTTP с TCP-портом 80, для HTTPS по умолчанию используется TCP-порт 443

SSL 3.0 — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. Протокол широко использовался для обмена мгновенными сообщениями и передачи голоса через IP . В 2014 году правительство США сообщило об уязвимости в текущей версии протокола. SSL должен быть исключён из работы в пользу TLS

TSL 1.3 — Протокол защиты транспортного уровня, криптографический протокол, обеспечивающий защищённую передачу данных между узлами в сети Интерне. Использует асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентичности сообщений для сохранения целостности сообщений. Широко используется в приложениях, работающих с сетью Интернет, таких как веб-браузеры, работа с электронной почтой, обмен мгновенными сообщениями и IP-телефония

dns

Распределённая система для получения информации о доменах. Чаще всего используется для получения IP-адреса по имени хоста (компьютера или устройства), получения информации о маршрутизации почты и/или обслуживающих узлах для протоколов в домене

ssh

Сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений, шифрует весь трафик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH позволяет безопасно передавать в незащищённой среде практически любой другой сетевой протокол. Таким образом, можно не только удалённо работать на компьютере через командную оболочку, но и передавать по шифрованному каналу звуковой поток или видео.

ftp

Протокол передачи файлов по сети, появившийся в 1971 году задолго до HTTP и даже до TCP/IP, является одним из старейших прикладных протоколов. На сегодняшний день широко используется для распространения ПО и доступа к удалённым хостам. Протокол построен на архитектуре «клиент-сервер» и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером.

smtp

Это широко используемый сетевой протокол, предназначенный для передачи электронной почты в сетях TCP/IP. Протокол SMTP предназначен для передачи исходящей почты с использованием порта TCP 25.
Для получения сообщений клиентские приложения обычно используют либо POP, либо IMAP.