Относится к прикладному уровню и отвечает за передачу данных между двумя системами. Как и протокол HTTP, он работает поверх протокола TCP. При передаче файлов FTP использует одновременно два TCP-канала: один из них отвечает за управление передачей данных, а второй - передает их.

Передача файлов FTP-протоколом между клиентом и сервером

FTP-соединение создается между клиентом и сервером, после чего они общаются друг с другом при помощи сети. Для этого пользователь может получить разрешение, предоставив учетные данные FTP-серверу, или использовать анонимный FTp.
При установлении FTP-соединения создаются два типа каналов связи, которые называются канал команд и канал данных
Командный канал требуется для:

- Передачи сообщений о тех или иных действиях
- Ответов между клиентом и сервером (и наоборот)
  Протокол FTP применяет тот же подход, что TELNET и SMTP, для связи посредством управляющего соединения. Для этого используется набор символов NVT ASCII. Общение осуществляется через порт 21.

Канал данных используется непосредственно для передачи информации и работает через порт 20.
FTP-клиент, применяя URL в качестве адреса, посылает команду FTP и адрес клиента. После установки соединения пользователь выполняет авторизацию, вводя логин и пароль.
В зависимости от настроек сервера пользователь может получить к нему доступ без логина и пароля. Данная форма авторизации называется "Анонимный FTP". В таком случае а сервере заранее создана специальная учетная запись, которая разрешает авторизацию при любых данных, внесенных в поле пароля. После этого со стороны сервера выполняется проверка введенных данных и выдается разрешение/запрет на действия с данными. Клиент/Сервер обмениваются нужными файлами, после чего происходит выходи из соединения.

FTPS

Тот же самый FTP с использованием SSL. Работает по модели клиент-сервер, используя канал управления и передачи данных для обмена командами FTP и данными во время клиентского сеанса FTPS.
Сессия FTPS аутентифицируется при помощи логина, пароля и сертификата открытого ключа (аналогично тому, как работает HTTPS). Инструменты, такие как OpenSSL, позволяют запрашивать и создавать сертификат ключа. При соединении с сервером FTPS клиент сначала проверяет надежность сертификата сервера, после чего осуществляет подключение. Когда доверенный центр сертификации (CA) подписывает эти сертификаты, он гарантирует, что клиент подключен к надежному и безопасному серверу. Это помогает защититься от ряда атак, в том числе от атак посредника. Сертификаты, не подписанные CA, которые известны как самозаверяющие сертификаты, могут побудить клиента FTPS создать уведомление о том, что сертификат не является подлинным. После этого пользователь может либо подтвердить действие и осуществить подключение или отклонить его.

SFTP

Протокол прикладного уровня модели OSI. Является часть SSH и не относится к протоколу FTP напрямую. При его работе происходит шифрование данных при помощи SSH, установка соединения осуществляется через порт 22. Это отличает его от FTPS, который осуществляет открытие порта каждый раз при взаимодействии с файлом. Аутентификация может происходить как при помощи логина и пароля, так и при помощи SSH-ключа