* HTTP
  + Application layer communication protocol
  + W3C & IETF
  + HTTP/2 builds on the success of SPDY, which was used as a starting point for the new protocol.
    - it’s a **tunnel for the protocol** and modifies the way existing HTTP requests and responses are sent.
  + usually takes place over TCP/IP connections
  + default port is TCP 80
  + Network socket – combination of port & IP
  + TLS &SSL – TLS and his predecessor SSL (Secure Sockets Layer) is the standard security technology for establishing secure communications between a web server and a browser
  + port 443 is the standard TCP port that is used for website which use SSL
* HTTP – client server architecture
  + Server
    - Hosting web resources
    - Waiting for clients
    - Origin server - server on which a given resource resides or is to be created.
    - Proxy server - intermediary program which acts as both a server and a client

for the purpose of making requests on behalf of other clients.

* + - Gateway - server which acts as an intermediary for some other server.
    - Tunnel - server which acts as an intermediary for some other server.
  + Client(User Agent)
    - Make request
    - Any application that contacts a web server
    - Ex. Web browser
    - Web crawlers/spider - is an Internet bot which systematically browses the World Wide Web, typically for the purpose of Web indexing
  + Major Characteristic
    - Request – response protocol
      * Pull protocol - clients always initiates the request from the server
      * “Polling” - process where the computer or controlling device waits for an external device to check for its readiness or state, often with low-level hardware
      * HTTP 2 – server can now send information to the client
    - Stateless protocol – serve and forget protocol
      * Server does not keep any information about clients in between request
    - Cache Control
      * Locality of reference Principle - phenomenon in which the same values, or related storage locations, are frequently accessed, depending on the memory access pattern.
      * MIME – Multipurpose Internet Mail Extension
* <http://info.cern.ch/> - home of the first website
* <http://archive.org/web/> - version of websites
* Features and functionality
  + Cache Control - allows a client or server to transmit a variety of directives in either requests or responses
  + Content media type specification
    - HTTP uses Internet Media Types [17] in the Content-Type (section 14.17) and Accept (section 14.1) header fields in order to provide open and extensible data typing and type negotiation.
  + Language and character set specification
    - "character set" - a method used with one or more tables to convert a sequence of octets into a sequence of characters.
  + Content / transfer coding
    - Content coding values indicate an encoding transformation that has been or can be applied to an entity. Primarily used to allow a document to be compressed or otherwise usefully transformed without losing the identity of its underlying media type and without loss of information.
    - Transfer-coding values are used to indicate an encoding transformation that has been, can be, or may need to be applied to an entity-body in order to ensure "safe transport" through the network.
  + Content negotiation - process of selecting the best representation for a given response when there are multiple representations available
  + Client-server protocol/negotiation
    - An HTTP/1.1 server MAY assume that a HTTP/1.1 client intends to maintain a persistent connection unless a Connection header including the connection-token "close" was sent in the request.
    - An HTTP/1.1 client MAY expect a connection to remain open, but would decide to keep it open based on whether the response from a server contains a Connection header with the connection-token close
    - Either the client or the server sends the close token in the Connection header, that request becomes the last one for the connection.
    - Clients and servers SHOULD NOT assume that a persistent connection is maintained for HTTP versions less than 1.1 unless it is explicitly signaled.
    - In order to remain persistent, all messages on the connection MUST have a self-defined message length
  + Persistent connection
    - Persistent connections provide a mechanism by which a client and a server can signal the close of a TCP connection. This signaling takes place using the Connection header field (section 14.10). Once a close has been signaled, the client MUST NOT send any more requests on that connection.
  + Request pipelining
    - Pipelining allows a client to make multiple requests without waiting for each response, allowing a single TCP connection to be used much more efficiently, with much lower elapsed time.
  + Authentication/authorization
    - Authorization field value consists of credentials containing the authentication information of the user agent for the realm of the resource being requested.