Http1.1 vs Http2

HTTP (Hypertext Transfer Protocol) is a set of rules that runs on top of the TCP/IP suite of protocols and defines how files are to be transferred between clients and servers on the world wide web.

**HTTP 1.1**

HTTP/1.1, the first standardized version of HTTP, was introduced in 1997. It presented significant performance optimizations (over HTTP/0.9 and HTTP/1.0) and transformed the way requests and responses were exchanged between clients and servers.

**Features of HTTP1.1**

* It was no longer required for each connection to be terminated immediately after every request was served with a response; instead, with the keep-alive header, it was possible to have persistent connections. It allowed multiple requests/responses per TCP connection.
* The Upgrade header was used to indicate a preference from the client that made it possible to switch to a more preferred protocol if found appropriate by the server.
* HTTP/1.1 provided support for chunk transfers that allowed streaming of content dynamically as chunks and for additional headers to be sent after the message body. This enhancement was particularly useful in cases where values of a field remained unknown until the content had been produced. For example, when the content had to be digitally signed, it was not possible to do so before the entire content gets generated.
* Other features that reinforced its stability were introduced such as:
  + pipelining (the second request is sent before the response to the first is adequately served)
  + content negotiation (an exchange between client and server to determine the media type, it also provides the provision to serve different versions of a resource at the same URI)
  + cache control (used to specify caching policies in both requests and responses)

**HTTP 2**

HTTP/2 was released at Google as the significant improvement of its predecessor. It was initially modelled after the SPDY protocol and went through significant changes to include features like multiplexing, header compression, and stream prioritization to minimize page load latency. After its release, Google announced that it would not provide support for SPDY in favor of HTTP/2.

The major feature that differentiates HTTP/2 from HTTP/1.1 is the binary framing layer. Unlike HTTP/1.1, HTTP/2 uses a binary framing layer. This layer encapsulates messages – converted to its binary equivalent – while making sure that its HTTP semantics (method details, header information, etc.) remain untamed. This feature of HTTP/2 enables gRPC to use lesser resources.

**Difference between HTTP1 and HTTP2**

**Multiplexing:** HTTP/1.1 loads resources one after the other, so if one resource cannot be loaded, it blocks all the other resources behind it. In contrast, HTTP/2 is able to use a single TCP connection to send multiple streams of data at once so that no one resource blocks any other resource. HTTP/2 does this by splitting data into binary-code messages and numbering these messages so that the client knows which stream each binary message belongs to.

**Server push:** Typically, a server only serves content to a client device if the client asks for it. However, this approach is not always practical for modern webpages, which often involve several dozen separate resources that the client must request. HTTP/2 solves this problem by allowing a server to "push" content to a client before the client asks for it. The server also sends a message letting the client know what pushed content to expect – like if Bob had sent Alice a Table of Contents of his novel before sending the whole thing.

**Header compression:** Small files load more quickly than large ones. To speed up web performance, both HTTP/1.1 and HTTP/2 compress HTTP messages to make them smaller. However, HTTP/2 uses a more advanced compression method called HPACK that eliminates redundant information in HTTP header packets. This eliminates a few bytes from every HTTP packet. Given the volume of HTTP packets involved in loading even a single webpage, those bytes add up quickly, resulting in faster loading.

**Advantages and Disadvantages of HTTP/2**

Naturally, as the updated technology, HTTP/2 brings its fair share of benefits and drawbacks to the cyber world. Below is the list of the advantages and disadvantages of HTTP/2:

**Advantages:**

* HTTP/2 supports full multiplexing for requests as well as responses over a single TCP connection. Due to these capabilities, lower page load times are achieved by removing needless latency and improving the overall capacity of network alongside its availability.
* Resource usage has increased dramatically for machines processing requests to deliver media-rich content and complex web designs. Developers worked hard around optimization hacks, and as a result, the robust solution of HTTP/2 was obtained. Features, such as server push, stream dependency and prioritizing, header compression, and binary format layer, have improved network utilization as the core advantage.
* The HTTP/2’s ability to transmit more data per client-server communication cycle greatly improves web performance. As a result, increased user satisfaction, better SEO, greater productivity, growing userbase, and improved sales figures can be achieved.
* All modern browsers support HTTP/2 over HTTPS with the SSL certificate installation. To open HTTPS capable invisible proxy ports on every relevant port, OWASP ZAP or its alternatives could be used.
* The use of the HPACK algorithm enables HTTP/2 to overcome the common API security threats. This protocol has commands in binary format and compresses the HTTP header metadata to protect sensitive data shared between both machines.

**Disadvantages:**

* While HTTP/2 mitigated the effects of HOL blocking in its predecessor, TCP-level block still causes problems.
* For client machines operating on a slow network, data packets drop bit by bit, and the network quality gets degraded to a single HTTP/2 connection. Due to this, the entire process slows down, thereby blocking a lot of data transfer.
* The cookie security failure is still not addressed in HTTP/2 like its precursor. Cookies are .txt files containing client data obtained by the server and website. However, these cookies may get stolen or tampered with by hackers, who can access personal user data, even without passwords.