HTTP1

KEY FEATURES

For every TCP connection there is only one request and one response.

STATUS CODE

Can define 16 status codes; the error prompt is not specific enough.

AUTHENTICATION MECHANISM

Uses basic authentication scheme which is unsafe since username and passwords are transmitted in clear text or base64 encoded.

CACHING

Provides support for caching via the If-Modified-Since header.

WEB TRAFFIC

HTTP/1.1 provides faster delivery of web pages and reduces web traffic as compared to HTTP/1.0. However, TCP starts slowly and with domain shading (resources can be downloaded simultaneously by using multiple domains), connection reuse and pipelining, there is an increased risk of network congestion.

HTTP2

KEY FEATURES

Uses multiplexing, where over a single TCP connection resources to be delivered are interleaved and arrive at the client almost at the same time. It is done using streams which can be prioritized, can have dependencies and individual flow control. It also provides a feature called server push that allows the server to send data that the client will need but has not yet requested.

STATUS CODE

Underlying semantics of HTTP such as headers, status codes remains the same.

AUTHENTICATION MECHANISM

Security concerns from previous versions will continue to be seen in HTTP/2. However, it is better equipped to deal with them due to new TLS features like connection error of type Inadequate Security.

CACHING

HTTP/2 does not change much in terms of caching. With the server push feature if the client finds the resources are already present in the cache, it can cancel the pushed stream.

WEB TRAFFIC

HTTP/2 utilizes multiplexing and server push to effectively reduce the page load time by a greater margin along with being less sensitive to network delays.