影响一个HTTP网络请求速度的有两个原因：带宽和延迟。

延迟包括浏览器的阻塞、DNS查询、建立连接（三次握手）

HTTP/1.0与HTTP/1.1的区别：

1. 最大的区别在与Connection：keep-alive，长连接
2. 节省带宽。新加了一个状态码100（Continue）。它支持客户端发送请求体只求先发送请求头，如果返回100，则继续发送；返回401，则不用再发送body了。GET和POST
3. HOST字段的加入。关于虚拟站点的建立，也就是说web server上的多个虚拟站点共享一个IP和端口。
4. Content-Length和Transform-Encoding:chunked。

现在的基础设施建设使得带宽得到极大的提升，大部分时候都是延迟在影响响应速度。HTTP/1.0被抱怨最多的就是两个地方：连接无法复用和head of line blocking（队头堵塞）。

因为客户端都是依据域名来发起请求建立连接的，一般PC端的浏览器针对单个域名有可能会同时建立6~8个连接，连接数并不是越多越好，资源开销和整体延迟都会随之增大。

连接无法复用会导致每次请求都会经历三次握手和慢启动。三次握手在高延迟的场景下影响较为明显，慢启动对文件类大请求影响较大。

Head of line of blocking 会导致带宽无法被充分利用（HTTP1.1）存在这个问题。

HTTP/2.0和HTTP/1.x的主要区别：

1. 多路复用。即允许单一的HTTP/2.0连接可以发起多个请求--相应消息。  
   因为在HTTP/1.1中，浏览器的客户端在同一时间内对同一域名的请求有一定的数量限制，超过一定的数量限制请求会堵塞，且还容易造成Head of line blocking。  
   HTTP/2.0使用多路复用的技术，能做到一个连接并发处理多个请求。而且并发请求的数量比HTTP/1.1大了好几个数量级。  
   当然，HTTP/1.1也可以多建几个TCP连接，来支持处理更多的请求，但是创建TCP连接本身就是要有开销的。
2. Header支持压缩，这样数据体积小了之后，在网络上传输就会更快。
3. 服务器推送。  
   在HTTP/2.0中，服务器可以对客户端的一个请求发送多个响应。服务器会顺带把一些客户端需要资源一起推送到客户端，省的客户端再次创建连接发送请求。这种方法非常适用于静态资源加载。
4. 二进制分帧

HTTPS：

在HTTP层和TCP层中间加入了TLS。  
为什么需要数字证书？

因为中间人攻击时可能会替换你的公钥，问题出在了公钥的分发上，实际上就是证明这个公钥的的确确是你的。到CA去做一个数字证书。  
数字证书包括两部分，一是基本信息，二是数字签名。

基本信息包括：公钥，个人的一些信息，以及加密所使用的Hash算法。

将这些基本信息经过HASH加密之后会成为一段消息摘要，消息摘要再使用CA的私钥加密，就成为数字签名。

浏览器和操作系统都会维护一个权威的第三方机构列表，包括他们的公钥。

每一个证书中都会包含这个证书的颁发机构和域名信息，浏览器在接收到这个证书后，会首先从自己的可信证书列表中判断该证书是否可信，如不在，立刻报警。如果可信，他会用浏览器保存的CA的公钥解密数字签名，得到信息摘要，然后再从数字证书中查看所使用的HASH算法，加密基本信息，得到消息摘要，两个消息摘要对比，如果相同，则通过，如果不相同，则说明证书有问题。

HTTPS连接：

1. 客户端发起HTTPS连接请求
2. 服务器端发过来自己的数字证书
3. 客户端验证数字证书。如果不通过，报警；如果通过，随机生成一个用于对称加密的密钥，然后用服务器的公钥加密
4. 发送对称密钥
5. 服务器收到消息，用自己的私钥解密，得到对称密钥
6. 双方都得到了对称密钥，用该对称密钥通信。

网景公司设计了SSL安全链路层协议。默认443端口，HTTP默认80端口。

HTTP握手3个包，加上SSL的9个包，HTTPS一共12个包。